UNIVERSITÉ PARIS XI
U.E.R. MATHÉMATIQUE
91-ORSAY (FRANCE)

Nº 2

2ème Année de Maîtrise des Sciences Mathématiques -

(Cours de M. CARTAN en 1969-70,

édition corrigée en 1971).

-=-=-=-=-=-

-=-=-=-

-=-

Nº 2

2ème Année de Maîtrise

des Sciences Mathématiques -

(Cours de M. CARTAN en 1969-70,

édition corrigée en 1971).

- Table des matières -

Première partie. I

Chap. I- L'anneau Z des entiers naturels et l'anneau des entiers de Gauss. 2

L'anneau Z des entiers naturels. Divisibilité

Généralités sur les anneaux intègres ; anneaux factoriels 1

Exemples d'anneaux factoriels 2

L'anneau des entiers de Gauss 2

Digression sur les restes quadratiques mod p (p premier) 3

Sommes de deux carrés et sommes de quatre carrés 42

(avec digression sur les quaternions)

Chap.II - Corps quadratiques 51

Entiers d'un corps quadratique 53

Unités d'un corps quadratique (= él. inversibles de l'anneau des entiers) 56

Divisibilité dans l'anneau des entiers d'un corps quadratique 62

Chap.III- Corps commutatifs, corps finis. 71

Caractéristique 72

Degré d'une extension 75

Sous-corps engendré par un élément (alg., resp. transcendant) 77

Corps de décomposition d'un polynôme 85

Racines n-ièmes de l'unité ; polynômes cyclotomiques 89

Corps finis 95

Application : loi de réciprocité quadratique 103

Chap.IV - Répartition des nombres premiers dans Z. 107

Notions sur la croissance de la suite des nombres premiers 107

Répartition des nombres premiers dans les congruences mod.3 et mod.4 109

Digression sur les fonctions analytiques d'une variable complexe 111

La fonction $\zeta(s)$ 127

Enoncé précis du théorème de Dirichlet 136

Le groupe $G(m)$ 137

Caractères des groupes abéliens finis 139

Les fonctions $L(s,\chi)$ 146

Chap. V - Théorie de Galois. 159

Prolongement d'homomorphismes, ext. séparables 159

Théorème de l'élément primitif 163

Extensions normales 164
Théorie de Galois 166

Chap. VI- Problèmes de géométrie plane résolubles par la règle et le compas 172

Démonstration du théorème d'Eisenstein 183
Construction des polygones réguliers 187

Deuxième Partie.

Chap. I - Groupes classiques. 197

$GL(n, \mathbb{R})$ et $GL(n, \mathbb{C})$ 197
Produits scalaires, matrices symétriques, matrices hermitiennes 201
Groupe orthogonal, groupe unitaire 205
Groupes linéaires quaternioniens 211
Application exponentielle 218
Exponentielle des matrices hermitiennes 231
Décomposition canonique de $GL(n, \mathbb{C})$ 235

Chap.II - Le groupe homographique à une variable. 241

La droite projective $P_1(\mathbb{C})$ et le groupe homographique complexe 241
Automorphismes holomorphes de $P_1(\mathbb{C})$ 251
Le groupe homographique réel et le demi-plan de Poincaré 255
Invariant différentiel dans le demi-plan de Poincaré, et géométrie non-euclidienne. 261

Chap.III- Une axiomatique de la géométrie plane. 276

Chap. IV- Notions de géométrie affine et de géométrie projective. 293

Géométrie affine 293
Géométrie euclidienne 298
Géométrie projective réelle 303
Le groupe linéaire-projectif 310
Caractérisation des transformations projectives 317
Géométrie elliptique 326
Géométrie elliptique en dimension 2 330

Chap. V - Eléments de géométrie algébrique. 334

1 - L'espace affine 334
2 - Polynômes 335
3 - Variétés algébriques

4 – Idéal associé à une variété 3
5 – Structure des idéaux de $k[X_1, \ldots, X_n]$ 3
6 – Variété associée à un idéal 3
7 – Variétés irréductibles 3
8 – Agrandissement du corps Ω 3
9 – Rapetissement du corps k 3
10 – Cas où Ω est algébriquement clos 3
11 – Démonstration du théorème 5 3
12 – Dimension ; degré de transcendance 3
13 – Démonstration du lemme de normalisation 3
14 – Le théorème des zéros de Hilbert 3
15 – Variétés algébriques dans l'espace projectif 3
16 – Relation entre variétés algébriques affines et variétés algébriques projectives. 3

MAITRISE DES SCIENCES MATHEMATIQUES

Cours de M. CARTAN

Année 1969/70

-:-:-:-:-:-

- BIBLIOGRAPHIE -

pour la Première Partie

- Algèbre de S. LANG
- HARDY and WRIGHT : "The theory of numbers" (Oxford , Clarendon Press, Ch. 1, 2, 5, 6, 7, 12, 15, 20.
- P. SAMUEL : Théorie algébrique des nombres (collection "Methodes" Hermann).

L'ANNEAU $\mathbb{Z}$ DES ENTIERS NATURELS $\geqslant 0$ et < 0 .

Rappels : $\mathbb{N}$ désigne l'ensemble des entiers naturels $\geqslant 0$.

Démonstration par récurrence :

$[P(0)$ et $(P(n) \Rightarrow P(n+1))] \Rightarrow \forall n \geqslant 0$ on a $P(n)$ pour $n \in \mathbb{N}$.

L'addition et la multiplication sont définies par récurrence :

$$n + (n'+1) = (n+n') + 1 \ , \quad n + 0 = n$$

$$n(n'+1) = nn' + n \ , \quad n \cdot 0 = 0 \ .$$

Elles se prolongent à $\mathbb{Z}$.

Ces deux opérations jouissent des propriétés bien connues vis-à-vis de la relation d'ordre (total) de $\mathbb{Z}$. Rappelons que tout sous-ensemble non vide et majoré de $\mathbb{Z}$ possède un plus grand élément.

Relation de divisibilité dans $\mathbb{Z}$:

Définition :

$$a|b \iff \exists c / ac = b \ .$$

c est unique si $a \neq 0$, car $\begin{matrix} ac = b \\ ac' = b \end{matrix} \Rightarrow a(c-c') = 0$

et puisque $a \neq 0$, on a $c - c' = 0$, car $\mathbb{Z}$ est intègre.

Définition :

A est un anneau intègre si A est un anneau commutatif avec élément unité 1 tel que $1 \neq 0$, et tel que $ab = 0 \Rightarrow a = 0$ ou $b = 0$.

Théorème : $\mathbb{Z}$ est un anneau intègre.

Définition :

I est un idéal d'un anneau A si I est un sous-groupe du groupe additif de A , et si $i \in I$ et $g \in A \Rightarrow i.g \in I$.

Notation :

(a) = ensemble des multiples de a

(a) est un idéal - en effet :

$ax - ax' = a(x-x')$, $(ax)y = a(xy)$.

idéal principal : un idéal est principal s'il se compose des multiples d'un certain élément.

$(a|b) \Leftrightarrow b \in (a) \Leftrightarrow (b) \subset (a)$

$$(a) = (b) \Leftrightarrow \left.\begin{array}{l} \exists u / b = ua \\ \exists v / a = vb \end{array}\right| \Rightarrow \quad a = vua \ ; \text{ si } a \neq 0 \text{ on en déduit}$$

$1 = vu$.

Donc si $(a) = (b) \neq 0$, c'est-à-dire si $a \neq 0$ et $b \neq 0$ engendrent le même idéal principal, alors b est de la forme $b = ua$, avec u inversible. Et réciproquement.

Les éléments inversibles forment un groupe pour la multiplication.

Tout ce qui précède vaut pour tout anneau commutatif à élément unité, intègre. Dans le cas de $\mathbb{Z}$:

Théorème : + 1 et - 1 sont les seuls éléments inversibles de $\mathbb{Z}$.

Autrement dit : $(a) = (b) \Leftrightarrow a = \pm b$.

En particulier $\mathbb{Z}$ n'est pas un corps.

Par ailleurs, tout sous-groupe du groupe additif de $\mathbb{Z}$ est automatiquement un idéal.

Remarques :

- dans tout anneau A, la relation $(b) \subset (a)$ est une relation d'ordre entre idéaux principaux (car la relation d'inclusion est une relation d'ordre).

- la relation $a|b$ n'est pas une relation d'ordre sur $\mathbb{Z}$; mais c'est une relation d'ordre sur l'ensemble $\mathbb{N}$ (entiers $\geqslant 0$).

Définition :

Un anneau principal est un anneau intègre dans lequel tout idéal est principal.

Théorème : l'anneau $\mathbb{Z}$ est principal.

La démonstration est basée sur la division euclidienne.

> Soit $n > 0$.
>
> $\forall x \in \mathbb{Z}$, $\exists q \in \mathbb{Z}$ et $r \in \mathbb{Z}$ tels que $x = nq + r$, $0 \leqslant r < n$.
>
> Le couple (q,r) est unique, car q est le plus grand des entiers $\geqslant 0$ tels que $nq \leqslant x$; ces entiers forment un ensemble non vide et majoré.

Soit $I \subset \mathbb{Z}$ un idéal (sous-groupe).

. si $I = \{0\}$, on a $I = (0)$, et le théorème est vrai dans ce cas

. si $I \neq \{0\}$: considérons l'ensemble des entiers > 0 de I ; cet ensemble est non vide (car si $n < 0$ appartient à I, $-n$ appartient à I), il possède un plus petit élément n (car dans $\mathbb{Z}$ tout ensemble non vide et minoré a un plus petit élément).

Soit $x \in I$; alors $\left.\begin{array}{l} x = nq + r \\ 0 \leqslant r < n \end{array}\right| \Rightarrow \begin{cases} x - nq = r \in I \\ 0 \leqslant r < n \end{cases}$

Ceci n'est possible que si $r = 0$. Donc $x \in (n)$, et par suite $I = (n)$.

C.Q.F.D.

Théorie du plus grand commun diviseur :

Soit $E(a,b)$ = ensemble des diviseurs communs à a et à b .

$d \in E(a,b) \Rightarrow d \mid xa + yb$, $\forall x$ et $\forall y$.

Or $\{xa + yb\}$ est un idéal (engendré par a et b) et cet idéal est principal, donc de la forme (n) , et on peut supposer $n \geqslant 0$. On a $n \in E(a,b)$ puisque $a \in (n)$ et $b \in (n)$. De plus tout $d \in E(a,b)$ divise n . Ainsi

Théorème : $E(a,b)$ se compose de tous les diviseurs d'un de ses éléments $n \geqslant 0$; n s'appelle le plus grand commun diviseur de a et b et se note (a,b) .

Il existe des entiers x et y tels que $(a,b) = xa + yb$, puisque (a,b) est dans l'idéal engendré par a et b .

Pratiquement : algorithme avec lequel on est sûr d'aboutir, après un nombre fini d'opérations, au calcul du plus grand commun diviseur.

Si l'un des nombres a et b est nul (b par exemple), alors $(a,b) = |a|$.

On peut donc supposer $a \neq 0$, $b \neq 0$, et même $a > 0$, $b > 0$.

Soit $a > b$.

On effectue la division :

- $a = bq + r_1$ $\quad 0 \leqslant r_1 < b$ et on a

  $(a,b) = (b, r_1)$

  . si $r_1 = 0$ alors $(a,b) = b$

  . si $r_1 \neq 0$ on recommence

- $b = r_1 q_1 + r_2$ $\quad 0 \leqslant r_2 < r_1$

  . si $r_2 = 0$ alors $(a,b) = r_1$

  . si $r_2 \neq 0$ on recommence.

Comme la suite des restes successifs est strictement décroissante, à un moment donné on obtiendra un r_i nul .

Le dernier reste non nul est le plus grand commun diviseur cherché.

Proposition importante :

(1) $\quad (ac, bc) = (a,b) \cdot |c|$

Il suffit de le prouver lorsque a, b, c sont $\neq 0$.

(ac, bc) est le générateur > 0 de l'idéal engendré par ac et bc ; or $xac + ybc = (xa + yb)c$; donc l'application $z \mapsto zc$ est une bijection de l'idéal engendré par a et b sur l'idéal engendré par ac et bc . Elle transforme le générateur > 0 du premier idéal dans un générateur du second idéal D'où la relation (1) .

Définition :

a et b sont premiers entre eux si $(a,b) = 1$

$(a,b) = 1 \iff \exists x\ \exists y / xa + yb = 1$; ceci est la relation de Bezout.

Lemme d'Euclide (Gauss).

Si $c|ab$ et si c est premier avec a, alors $c|b$

Démonstration :

$(a,c) = 1$

$(ab, cb) = \pm b$

$c|ab$ et $c|cb$, donc c divise le plus grand commun diviseur, c'est-à-dire $c|b$.

Nombres premiers :

Définition :

p premier $\iff$ $p > 1$ et les seuls diviseurs de p sont ± 1 et $\pm p$. Autrement dit, p est > 0, non - inversible, et n'est pas le produit de deux éléments non-inversibles.

Remarque : 1 n'est pas un nombre premier.

On remarque qu'il y a effectivement des nombres premiers, ex. 2, 3, 5, 7, (remarque : tout nombre pair $\neq 2$ n'est pas premier : après 2, tous les nombres premiers sont impairs).

On a un moyen mécanique pour trouver les nombres premiers.

Crible d'Erasthostène :

|2| |3| 4 5 6 7 8 9 ~~10~~ 11 ~~12~~ 13 ~~14~~

On garde 2 puis on raye tous les multiples suivants de 2 ;

on garde 3 puis on raye tous les multiples suivants de 3 (certains ont déjà été rayés comme multiples de 2) ;

on garde 5 puis on raye .....

Le premier nombre non rayé est chaque fois un nombre premier.

Remarque : un entier n qui n'a pas de diviseur > 1 et $< \sqrt{n}$ est premier.

Proposition :

Soit p premier : $\forall a$, $p|a$ ou $(p,a) = 1$.

Démonstration :

$(a,p)|p \Longrightarrow (a,p) = p$ ou $(a,p) = 1$.

Corollaire :

si p est premier et si p divise ab , alors $p|a$ ou $p|b$.

Théorème :

Soit n un entier divisible par 2 nombres premiers distincts p_1 et p_2 ; alors $p_1p_2|n$.

Puisque $p_1|n$, on a $n = ap_1$

Puisque $p_2|n$, p_2 divise ap_1 , or p_2 est premier à p_1 , donc p_2 divise a : $a = bp_2$, et par suite $n = bp_1p_2$.

Théorème :

Tout $n \geqslant 2$ possède au moins un diviseur premier.

Cela va résulter du :

Théorème :

Tout $n \geqslant 2$ s'écrit comme produit d'une famille finie (non vide) de nombres premiers (distincts ou non).

Démonstration :

Montrons ceci par récurrence sur n. C'est vrai si n est premier, donc, c'est vrai pour $n = 2$.

Supposons le théorème vrai pour tous les entiers $< n$.

Si n est premier, le théorème est vrai. Sinon, $n = n_1 n_2$, $n_1 < n$, $n_2 < n$; par l'hypothèse de récurrence, n_1 et n_2 sont produits de facteurs premiers, donc n aussi.

Remarque : on convient que 1 est produit d'une famille vide de nombres premiers.

Théorème :

L'ensemble P des nombres premiers est infini.

Soient $p_1, \ldots, p_n$ des nombres premiers donnés, distincts. Les diviseurs premiers de $1 + p_1 p_2 \ldots p_n$ sont $\neq$ de $p_1, p_2, \ldots, p_n$. Donc, $\forall n$, il existe au moins $n + 1$ nombres premiers distincts.

C.Q.F.D.

Convention d'écriture :

Soit P l'ensemble (infini) de tous les nombres premiers. Soit $n \neq 0$; puisque tout entier > 0 est produit d'une famille finie de nombres premiers, on peut écrire :

$$n = \pm \prod_{p \in P} p^{k(p)} ,$$

où $k(p)$ est un entier $\geqslant 0$, presque toujours nul ($\equiv$ nul sauf pour un nombre fini de valeurs de p).

Théorème :

Pour un $n \neq 0$ donné, il existe un seul système d'exposants entiers $k(p)$, presque tous nuls, tels que la relation $n = \pm \prod_{p \in P} p^{k(p)}$ ait lieu.

Démonstration :

Elle repose sur le lemme d'Euclide. Supposons :

$$\pm \prod_{p} p^{k(p)} = \pm \prod_{p} p^{k'(p)} ;$$

un nombre > 0 ne pouvant être égal à un nombre < 0, cette égalité se ramène à la suivante :

$$\prod_{p} p^{k(p)} = \prod_{p} p^{k'(p)} \qquad (1)$$

raisonnons par l'absurde, et supposons $\exists p_o / k(p_o) > k'(p_o)$

(1) devient alors :

$$p_o^{k(p_o)-k'(p_o)} \cdot \left(\prod_{p \neq p_o} p^{k(p)} \right) = \prod_{p \neq p_o} p^{k'(p)}$$

or $p_o^{k(p_o) - k'(p_o)}$ divise le premier membre donc il divise le second membre donc il doit diviser l'un des facteurs $p \neq p_o$, ce qui est absurde. L'unicité est donc prouvée.

Exercice : Soit $p_1 < p_2 < \ldots < p_n < \ldots$ la suite des nombres premiers numérotés dans l'ordre croissant $(p_1 = 2,\ p_2 = 3,\ \ldots)$

Alors

$$\sum_{n \geqslant 1} \frac{1}{p_n} = +\infty$$

Etapes du raisonnement.

Soit $x > 0$; on appelle $N_j(x)$ le nombre des entiers $n \leqslant x$ $(n \geqslant 2)$ dont tous les facteurs premiers sont d'indice $\leqslant j$, et on montre

$$1^\circ \quad N_j(x) \leqslant 2^j \sqrt{x} \qquad (1)$$

pour ce faire on écrit $n = (n_1)^2 n_2$ (tous les exposants des facteurs premiers dans n_2 étant 1 ou 0), puis on montre que le nombre des valeurs possibles pour n_1 est $\leqslant \sqrt{x}$, et le nombre des valeurs possibles pour n_2 est $\leqslant 2^j$.

$$2^\circ \quad x - N_j(x) \leqslant \frac{x}{p_{j+1}} + \frac{x}{p_{j+2}} + \ldots \quad , \quad \text{d'où}$$

$$1 - \frac{N_j(x)}{x} \leqslant \sum_{n > j} \frac{1}{p_n}$$

D'après 1° , $\lim_{x \to \infty} \frac{N_j(x)}{x} = 0$, d'où à la limite $\sum_{n > j} \frac{1}{p_n} \geqslant 1$.

Ceci étant vrai pour tout j , prouve la divergence de la série.

Calcul du plus grand commun diviseur à partir de la décomposition en facteurs premiers.

Soient a et $b \neq 0$:

$$\begin{cases} a = \pm \prod_{p} p^{k(p)} \\ b = \pm \prod_{p} p^{k'(p)} \end{cases}$$

Alors $(a, b) = \prod_{p} p^{\inf(k(p),\, k'(p))}$.

Exercice : plus petit commun multiple.

Généralités sur les anneaux intègres.-

Définition : Soit A un anneau intègre. Un élément $a \in A$ est dit irréductible si

(i) a est $\neq 0$ et n'est pas inversible ;

(ii) a n'est pas le produit de deux éléments non-inversibles.

La condition (i) exprime que l'idéal principal (a) n'est pas réduit à zéro et e distinct de A. La condition (ii) exprime que si $a = bc$, on a $(a) = (b)$ ou $(a) = (c)$.

Proposition 1. Pour que $a \in A$ soit irréductible, il faut et il suffit que l'idéal p cipal (a) soit $\neq 0$ et soit maximal dans l'ensemble des idéaux principaux $\neq A$. (Démonstration laissée à titre d'exercice).

Théorème 1. Soit $a \in A$, $a \neq 0$; si l'idéal principal (a) est premier, a est irréductible.

Rappelons qu'un idéal I (dans un anneau commutatif A à élément-unité, intègre non) est dit premier si l'anneau-quotient A/I est intègre. Il revient au même de dir que :

1º $1 \notin I$;

2º $(x \in A,\ y \in A$ et $xy \in I) \Longrightarrow x \in I$ ou $y \in I$.

Démontrons le théorème ; il suffit de prouver que si $a \neq 0$ n'est pas irréductib l'idéal (a) n'est pas premier. Il y a deux cas à examiner :

- cas où a est inversible ; alors $(a) = A$, donc (a) n'est pas premier ;

- cas où a est non-inversible, $a = bc$, b et c non inversibles. Alors $b \notin$ sinon il existerait x tel que $b = ax$, d'où $a = a \times c$, d'où $1 = x\, c$ (puisque A

intègre), et c serait inversible contrairement à l'hypothèse. De même, $c \notin (a)$. Or $bc \in (a)$; donc l'idéal (a) n'est pas premier. C.Q.F.D.

Il faut prendre garde que la réciproque du théorème est fausse en général ; on verra plus loin (dans la théorie des entiers des corps quadratiques) l'exemple d'un anneau intègre A qui possède un élément irréductible a tel que l'idéal (a) ne soit pas premier.

Néanmoins la réciproque est vraie pour une large catégorie d'anneaux, les anneaux factoriels (cf. ci-dessous).

Introduisons un axiome :

Axiome α : dans A, l'intersection de deux idéaux principaux est un idéal principal.

Par exemple, il est évident que si A est un anneau principal, A satisfait à l'axiome α (puisque tous les idéaux sont principaux).

Soient a et b deux éléments non nuls d'un anneau intègre A satisfaisant à l'axiome (α). Il existe $m \in A$, $m \neq 0$, tel que

$$(1) \qquad (a) \cap (b) = (m),$$

et un tel m est unique à un facteur inversible près [c'est l'idéal (m) qui est unique]. La relation (1) signifie :

Les multiples communs à a et b sont exactement les multiples de m.

Alors m s'appelle le plus petit commun multiple (p.p.c.m.) de a et b ; il est unique à un facteur inversible près.

L'axiome α signifie donc que deux éléments non nuls quelconques ont un p.p.c.m.

Proposition 2. Si a et b non nuls ont un p.p.c.m., soit m, les diviseurs communs à a et b sont exactement les diviseurs de $\frac{ab}{m}$.

Démonstration : si $d \neq 0$ divise a et b, $\frac{ab}{d} = \frac{a}{d} \cdot b = a \cdot \frac{b}{d}$ est un multiple commun à a et b, donc est un multiple de m, donc ab est un multiple de md, et $\frac{ab}{m}$ est un multiple de d. Réciproquement, si d divise $\frac{ab}{m}$, alors m divise $\frac{ab}{d}$, donc $\frac{ab}{d}$ est un multiple commun à a et b, et par suite $\frac{b}{d}$ et $\frac{a}{d}$ sont dans A ;

donc d divise b et a.

Corollaire : les diviseurs communs à a et b ($a \neq 0$, $b \neq 0$) sont exactement les diviseurs de l'un d'entre eux (à savoir $\frac{ab}{m}$). On l'appelle le plus grand commun diviseur (p.g.c.d.) de a et b ; comme le p.p.c.m., le p.g.c.d. est unique à un facteur inversible près.

On a donc une théorie du p.g.c.d. dans tout anneau intègre A qui satisfait à l'axiome α.

Si d est un p.g.c.d. de a et b, et si m est un p.p.c.m. de a et b, on a

$$dm = \varepsilon\, a\, b, \tag{2}$$

où ε est inversible.

Notons (a, b) le p.g.c.d. de a et b (défini à un facteur inversible près). On a la relation

$$\boxed{(ac, bc) = (a, b) \cdot c} \tag{3}$$

(Si on multiplie par c un p.g.c.d. de a et b, on obtient un p.g.c.d. de ac et bc).

Démonstration de (3) : Soit m un p.p.c.m. de ac et bc ; alors m est divisible par c, et $\frac{m}{c}$ est un p.p.c.m. de a et b. Réciproquement, si $\frac{m}{c}$ est un p.p.c.m. de a et b, m est un p.p.c.m. de ac et bc. D'après la relation (2), un p.g.c.d. de ac et bc est

$$\frac{(ac)\cdot(bc)}{m} = \frac{a\,b\,c^2}{m},$$

et un p.g.c.d. de a et b est $\frac{a\,b}{\left(\frac{m}{c}\right)} = \frac{a\,b\,c}{m}$. D'où la relation (3). C.Q.F.D.

Définition : On dit que $a \neq 0$ et $b \neq 0$ sont premiers entre eux si $(a, b) = 1$; autrement dit, si tout diviseur commun à a et b est inversible. Il revient au même de dire que tout multiple commun à a et b est un multiple du produit ab.

Lemme d'Euclide-Gauss. Soit A un anneau intègre satisfaisant à l'axiome α. Soient a, b, c trois éléments $\neq 0$ de A. Si a divise le produit bc, et si a et b

sont premiers entre eux, alors a divise c.

Démonstration. a divise bc et ac, donc a divise le p.g.c.d., qui est

$$(b\,c,\ a\,c) = (b,\ a)\,c = c.$$

Théorème 2. Soit A un anneau intègre satisfaisant à l'axiome α. Pour qu'un élément $a \in A$ $(a \neq 0)$ soit irréductible, il faut et il suffit que l'idéal principal (a) soit premier.

Démonstration. On a déjà vu (Théorème 1) que si (a) est premier, a est irréductible (pour cela l'axiome α n'est pas nécessaire). Inversement, supposons a irréductible alors $1 \notin (a)$ puisque a n'est pas inversible. Il reste à montrer que si $bc \in (a)$, alors $b \in (a)$ ou $c \in (a)$. L'idéal du p.g.c.d. (a, b) est (a) ou (1), puisque a est irréductible.

Si c'est (1), a divise bc par hypothèse et est premier avec b, donc a divise c (lemme d'Euclide-Gauss). Si c'est (a), alors a divise b. C.Q.F.D.

Corollaire du théorème 2. Si A satisfait à l'axiome (α), tout idéal principal maximal est premier.

Démonstration. Soit (a) un idéal, maximal dans l'ensemble des idéaux principaux $\neq A$. Si $a = 0$, cela signifie que pour tout élément $b \neq 0$ l'idéal (b) est égal à A, autrement dit que tout élément non nul est inversible ; alors A est un corps, et (0) est bien un idéal premier. Si $a \neq 0$, dire que (a) est maximal dans l'ensemble des idéaux principaux $\neq A$ revient à dire que l'élément a est irréductible, et alors l'idéal (a) est premier d'après le théorème 2.

Considérons, pour un anneau intègre A, l'axiome suivant :

Axiome α'. — Tout idéal principal maximal de A est premier.

D'après ce qui précède, l'axiome α entraîne l'axiome α'.

Proposition 3. Soit A un anneau intègre satisfaisant à l'axiome α'. Alors si un a irréductible divise un produit fini $x_1\,x_2 \cdots x_n$, a divise l'un au moins des x_i.

En effet, cela résulte du fait que (a) est un idéal premier.

On aurait envie que tout élément $\neq 0$ de A puisse s'écrire comme produit d'un

nombre fini d'éléments irréductibles. On va voir qu'il en est bien ainsi lorsque A satisfait à l'axiome suivant :

Axiome β .- Dans l'anneau intègre A, toute suite croissante d'idéaux principaux es stationnaire.

Ceci signifie que si on a une suite infinie

$$(a_1) \subset (a_2) \subset (a_3) \ldots \subset (a_n) \subset \ldots ,$$

alors $(a_n) = (a_{n+1})$ pour n assez grand . tous les idéaux de la suite sont égaux à partir d'un certain rang.

Exemple. Un anneau principal A satisfait toujours à l'axiome β . En effet, la réu de la suite croissante des idéaux (a_n) est évidemment un idéal. Cet idéal est princ soit (b). Alors l'élément b, qui par hypothèse appartient à la réunion des idéaux (a_n) , appartient à l'un d'eux. Or si $b \in (a_n)$, on a $(b) \subset (a_n)$, et comme (b) cont chacun des (a_p) pour $p \geq n$, on voit que

$$(b) = (a_n) = (a_{n+1}) = \ldots .$$

C.Q.F.D.

Remarque : un anneau A tel que toute suite croissante d'idéaux soit stationnaire s'appelle un anneau noethérien . On en verra des exemples plus tard. Ainsi : tout ann noethérien satisfait à l'axiome (β) [la réciproque est fausse].

Exercice. Tout anneau principal est noethérien.

Théorème 3. Si un anneau intègre A satisfait à l'axiome β, alors tout élément a et non-inversible est égal à un produit (fini) d'éléments irréductibles.

On prouve d'abord un :

Lemme : Si $a \neq 0$ n'est pas inversible, il existe un b irréductible qui divise a.

Démonstration du lemme: Si a est irréductible, il suffit de prendre b = a.

Sinon, (a) n'est pas maximal dans l'ensemble des idéaux principaux $\neq A$, et il existe a_1 tel que

$$(a) \subset (a_1) , (a) \neq (a_1) , (a_1) \neq A .$$

a_1 n'est pas inversible ; si a_1 est irréductible, on prend $b = a_1$. Sinon on a

$$(a_1) \subset (a_2), \quad (a_1) \neq (a_2), \quad (a_2) \neq A.$$

Si a_2 est irréductible, on prend $b = a_2$. Sinon on recommence. Or ces opérations ont une fin, sinon on aurait une suite infinie

$$(a) \subsetneq (a_1) \subsetneq (a_2) \subsetneq \cdots \subsetneq (a_n) \subsetneq \cdots ,$$

ce qui contredit l'axiome β. Donc, au bout d'un nombre fini d'opérations, on trouve un diviseur irréductible de a, ce qui prouve le lemme.

Prouvons maintenant le théorème 3. Etant donné $a \neq 0$, a non-inversible, a possède un diviseur irréductible b_1 (d'après le lemme). D'où $a = b_1 c_1$.
Si c_1 est inversible, a est irréductible, et le théorème est démontré. Sinon, on a de même

$$c_1 = b_2 c_2,$$

où b_2 est irréductible. Si c_2 est inversible, $b_2 c_2 = c_1$ est irréductible, et a est produit de deux facteurs irréductibles. Sinon, on a

$$c_2 = b_3 c_3 ,$$

avec b_3 irréductible. Si c_3 est inversible, on a $a = b_1 b_2 c_2$, produit de trois éléments irréductibles. Sinon, on recommence. Ces opérations ont une fin, sinon on aurai une suite infinie

$$(a) \subsetneq (c_1) \subsetneq (c_2) \subsetneq \cdots \subsetneq (c_n) \subsetneq \cdots ,$$

ce qui est contraire à l'axiome β. Donc le théorème est démontré.

Dans le théorème 3, si on a

$$a = b_1 b_2 \cdots b_n$$

($b_1, \ldots, b_n$ irréductibles), on a aussi

$$(a) = (b_1) (b_2) \cdots (b_n) ,$$

où dans le second membre on a un produit d'idéaux principaux : par définition, le produit $(b)(c)$ de deux idéaux principaux est l'idéal principal engendré par le produit bc. Il ne change pas si on multiplie b et c par des éléments inversibles ; le produit $(b)(c)$ ne dépend donc que des idéaux (b) et (c).

Théorème 4. Soit A un anneau intègre satisfaisant à l'axiome α'. Si on a une éga entre produits d'idéaux principaux:

$$(*) \qquad \prod_{i \in I} (b_i) = \prod_{j \in J} (c_j) \ ,$$

où les ensembles d'indices I et J sont finis, et où les $b_i \in A$ et les $c_i \in A$ sont irréductibles, alors il existe une bijection φ de I sur J telle que

$$(b_i) = (c_{\varphi(i)}) \quad \text{pour tout } i \in I.$$

Démonstration. Par récurrence sur le cardinal de I. C'est évident si I est vide, car alors l'idéal du membre de gauche de (*) est A, ce qui exige que J soit vide La récurrence se fait comme suit : prenons un $i_o \in I$; d'après (*), b_{i_o} divise le p duit $\prod_{j \in J} c_j$, donc (prop. 3) b_{i_o} divise l'un des c_j, soit c_{j_o} ; et comme c_{j_o} est irréductible, on a $(b_{i_o}) = (c_{j_o})$. La relation (*) donne alors, par division :

$$\prod_{i \in I - \{i_o\}} (b_i) = \prod_{j \in J - \{j_o\}} (c_j) \ ,$$

et on applique l'hypothèse de récurrence. C.Q.F.D.

Si maintenant on met ensemble les théorèmes 3 et 4, on obtient :

Théorème 5. Soit A un anneau intègre satisfaisant aux axiomes α' et β. Alors tout idéal principal (a) se met sous la forme d'un produit fini

$$(a) = \prod_{i \in I} (b_i) \ ,$$

où les b_i sont irréductibles, et cette décomposition est unique (à l'indexation près de la famille des (b_i)).

[L'existence résulte du théorème 3, et l'unité résulte du théorème 4].

Ceci nous amène à définir les anneaux factoriels.

Définition. On appelle anneau factoriel un anneau (commutatif à l'élément unité) A, intègre, tel qu'il existe un sous-ensemble (fini ou infini) $P \subset A$ jouissant de la pr priété suivante : pour tout $a \in A$ tel que $a \neq 0$, il existe une application $p \longmapsto k(p)$ de P dans l'ensemble $\mathbb{N}$ des entiers naturels ≥ 0, telle que

(1) $k(p) = 0$ sauf pour un nombre fini d'éléments $p \in P$;

(ii) on ait

$$(1) \qquad a = u \prod_{p \in P} p^{k(p)} \quad ,$$

où $u \in A$ est inversible. En outre, un tel système d'entiers $k(p)$ est unique (et u est donc unique) lorsque a est donné.

Remarque: le sens à donner au produit $\prod_{p \in P} p^{k(p)}$ est clair : tous ses facteurs sont égaux à 1 sauf un nombre fini ; c'est donc un produit fini.

Soit A un tel anneau factoriel ; on notera $k_a(p)$ les exposants qui figurent dans le second membre de (1) (ils dépendent de a).

On a évidemment

$$k_{ab}(p) = k_a(p) + k_b(p).$$

On en déduit aussitôt : pour que a divise c, il faut et il suffit que $k_a(p) \leq k_c(p)$ pour tout $p \in P$. Par conséquent, les multiples communs à a et b sont les multiples de

$$m = \prod_{p \in P} p^{\sup(k_a(p),\, k_b(p))} \quad ;$$

ce qui prouve que l'intersection $(a) \cap (b)$ est égale à l'idéal principal (m). Donc un anneau factoriel satisfait à l'axiome (α). On voit de même qu'un p.g.c.d. de a et b est

$$d = \prod_{p \in P} p^{\inf(k_a(p),\, k_b(p))} \quad .$$

Par ailleurs, si on a une suite croissantes d'idéaux principaux

$$(1) \qquad (a_1) \subset (a_2) \subset \ldots \subset (a_n) \subset \ldots \quad ,$$

alors, pour chaque $p \in P$, la suite des entiers

$$k_{a_1}(p) \ , \ k_{a_2}(p), \ldots, k_{a_n}(p), \ldots$$

est décroissante, donc stationnaire. Et comme $k_{a_1}(p) = 0$ sauf pour un nombre fini de valeurs de p, on voit que la suite (1) elle-même est stationnaire. Donc un anneau factoriel satisfait à l'axiome β.

Montrons que, réciproquement, tout anneau intègre A qui vérifie les axiomes α et β est factoriel. Il suffit de montrer que si A vérifie les axiomes α' et β,

A est factoriel. Or A satisfait à la propriété énoncée au théorème 5. Il suffit donc de voir que la propriété du théorème 5 exprime que A est factoriel.

Pour cela, choisissons, dans chaque idéal principal maximal, un élément qui l'engendre (c'est un élément irréductible). Appelons P la collection des représentants ainsi choisis. Dans le théorème 5, on peut alors supposer que les b_i appartiennent à P, et la relation

$$(a) = \prod_{i \in I} (b_i)$$

s'écrit $$a = u \cdot (\prod_{i \in I} b_i), \quad \text{où } u \text{ est inversible.}$$

Les b_i qui interviennent au second membre sont en nombre fini, mais pas nécessairement distincts ; le second membre est donc de la forme

$$u \cdot \prod_{p \in P} p^{k(p)} \quad ,$$

et une telle écriture de a est unique d'après le théorème 5. C.Q.F.D.

En résumé :

Pour qu'un anneau intègre soit factoriel, il faut et il suffit qu'il satisfasse aux axiomes α et β, ou, ce qui est équivalent, aux axiomes α' et β.

Remarque. Dans la définition d'un anneau factoriel A, on voit que les $p \in P$ sont des éléments irréductibles, et que tout élément irréductible de A est "équivalent" à $p \in P$ et à un seul (deux éléments $\neq 0$ étant dits équivalents s'ils ne diffèrent que par un facteur inversible).

On a vu que tout anneau principal vérifie les axiomes α et β. Donc :

Théorème 7. Tout anneau principal est factoriel.

Remarque 1. Puisque $\mathbb{Z}$ est un anneau principal, on retrouve le fait que $\mathbb{Z}$ est un anneau factoriel (décomposition d'un entier $\neq 0$ en produit de puissances de nombres premiers).

Remarque 2. On a vu que, dans un anneau principal, on a une identité de Bezout : le p.g.c.d. (a, b) de deux éléments est de la forme

$x\,a + y\,b$

(i.e. appartient à l'idéal engendré par a et b). Il n'en est plus toujours de même dans un anneau factoriel. Par exemple, on verra que l'anneau des polynômes $k[X, Y]$ à deux indéterminées X et Y, à coefficients dans un corps commutatif k, est un anneau factoriel ; les diviseurs communs au polynôme X et au polynôme Y sont les polynômes constants $\neq 0$; 1 est donc un p.g.c.d. de X et Y ; mais 1 n'est pas de la forme $XP + YQ$, où P et Q sont des polynômes !

Exemples d'anneaux factoriels.

$k[X]$, anneau des polynômes à une indéterminée X ; c'est un espace vectoriel sur le corps k, ayant une base $\{1\ ,\ X,\ X^2, \ldots\}$ avec comme table

de multiplication : $X^p X^q = X^{p+q}$.

Théorème : L'anneau $k[X]$ des polynômes à une indéterminée est factoriel.

Démonstration : En fait, cet anneau est principal. On le voit en utilisant la division des polynômes.

Rappels sur la division des polynômes :

Si B est un polynôme non identiquement nul, alors pour tout polynôme A, il existe des polynômes Q et R, uniques, tel que :

$$A = BQ + R \quad \text{avec} \quad \deg R < \deg B .$$

Note : le degré d'un polynôme non identiquement nul est le plus grand n tel que le coefficient de X^n soit $\neq 0$.

Degré du polynôme 0 : on peut convenir que c'est -1, ou $-\infty$; c'est un élément strictement plus petit que le degré de tout polynôme non nul.

Montrons que tout idéal de $k[X]$ est principal.

. si $I = \{0\}$, alors I est engendré par 0 donc principal.

. si $I \neq \{0\}$, alors dans I il y a des polynômes $\neq 0$; parmi eux on en prend un de degré minimum : soit B

$$\forall A \in I, \ \exists Q \text{ et } R \ / \quad A = BQ + R \qquad \deg R < \deg B$$

$$R = A - BQ \Rightarrow \left| \begin{array}{l} R \in I \\ \text{et comme } \deg R < \deg B \text{ on conclut } R = 0 . \end{array} \right.$$

donc
I se compose des multiples de B .

C.Q.F.D.

Remarque : on aurait dû d'abord prouver que $k[X]$ est intègre.

Soient deux polynômes non identiquement nuls $(aX^p + \ldots) = A$

$(bX^q + \ldots) = B$

On va montrer que $A \cdot B \neq 0$ et, en fait, que $\deg(A.B) = \deg A + \deg B$.

$AB = abX^{p+q} + \ldots$, et $ab \neq 0$ car $a \neq 0$ et $b \neq 0$

(en effet k est un corps ; il suffirait d'ailleurs que k soit un anneau intègre).

On aura donc dans $k[X]$ la notion de polynôme irréductible.

Qu'est-ce qu'un polynôme inversible ?

Peut-on avoir $BC = 1$? Comme le degré d'un produit est la somme des degrés, il faut $\deg B = \deg C = 0$; donc B se réduit à son terme constant b, qui doit être $\neq 0$. Cela suffit. Ainsi :

Les éléments inversibles de $k[X]$ sont les éléments non nuls de k (considérés comme polynômes de degré 0).

Dans chaque classe de polynômes non nuls, il y a un polynôme unitaire (i.e. : dont le coefficient de la plus haute puissance de X est 1). Donc les polynômes unitaires fournissent un représentant dans chaque classe; comme l'anneau est factoriel, tout polynôme unitaire s'ecrit d'une seule manière comme produit de polynômes unitaires irréductibles.

Comment sont faits les polynômes irréductibles ?

Cela dépend du corps k.

Par exemple pour $k = \mathbb{C}$, il n'y en a pas de degré $\neq 1$: à cause du théorème de d'Alembert, on sait que tout polynôme de $\mathbb{C}(X)$ s'écrit comme un produit de polynômes de degré 1.

$k = \mathbb{R}$: il y a les polynômes de degré 1, comme toujours ; en outre, ceux de degré 2 dont le discriminant est < 0 ; d'après le

théorème de d'Alembert il n'y en a pas d'autres car on fait la décomposition sur $\mathbb{C}$ et on regroupe quand on a deux racines complexes conjuguées.

$k = \mathbb{Q}$: on a des polynômes irréductibles de degré aussi grand que l'on veut : en effet (on verra que) pour tout p premier : $1 + X + X^2 + \ldots + X^{p-1}$ est irréductible, et il y a des nombres premiers aussi grands que l'on veut.

Y-a-t-il des anneaux commutatifs intègres qui soient factoriels sans être principaux ?

La réponse est oui ; en particulier :

Théorème : Si k est un corps commutatif, l'anneau $k[X_1, \ldots, X_n]$ est factoriel, mais pour $n \geqslant 2$ il n'est pas principal.

Démonstration : Si $n = 2$, montrons que $k[X,Y]$ n'est pas principal en trouvant un idéal qui ne soit pas engendré par un seul élément.

Prenons I = idéal des polynômes dont le terme constant est nul ; Cet idéal est engendré par X et Y : il ne peut être engendré par un seul élément ; sinon, si $R(X, Y)$ engendrait I, on aurait

$$\begin{cases} X = R(X,Y)\, P(X,Y) & (1) \\ Y = R(X,Y)\, Q(X,Y) & (2) \end{cases}$$

R n'a pas de terme constant ; soit R_1 la partie de degré 1 de R. On doit avoir $X = R_1(X,Y).P_o$, $Y = R_1(X,Y).Q_o$, où P_o et Q_o sont les termes constants de P et Q. Or X et Y ne sont pas proportionnels, d'où une absurdité.

Démonstration abrégée du fait que $k[X_1, \ldots, X_n]$ est un anneau factoriel.

On observe que tout polynôme $P(X_1, \ldots, X_n)$ peut être considéré comme un polynôme en X_n dont les coefficients sont des polynômes en $X_1, \ldots, X_{n-1}$; d'où un isomorphisme canonique d'anneaux

$$k[X_1,\ldots,X_{n-1},X_n] \approx A[X_n] \ ,$$

où $$A = k[X_1,\ldots,X_{n-1}] \ .$$

Le théorème se prouve alors par récurrence sur n (il est vrai pour $n = 0$, et pour $n = 1$) ; par l'hypothèse de récurrence, $A = k[X_1,\ldots,X_{n-1}]$ est factoriel, et il suffit de prouver le

Lemme : Si A est factoriel, l'anneau $A[X]$ est factoriel.

Voici des indications sur la démonstration de ce lemme : les détails sont laissés au lecteur à titre d'exercice.

D'abord, A étant intègre, $A[X]$ est un anneau intègre. Introduisons le corps des fractions de A, soit K ; on a $A \subset K$, et $A[X]$ s'identifie à un sous-anneau de $K[X]$, qui est principal, donc factoriel. Dans chaque classe d'éléments irréductibles de l'anneau factoriel $K[X]$, choisissons un représentant $P(X)$ à coefficients dans A, ce qui est possible ; de plus on peut choisir P de façon que le plus grand commun diviseur de ses coefficients soit 1 (ceci a un sens, puisque les coefficients sont dans l'anneau A, qui est factoriel). Si on appelle primitif tout élément de $A[X]$, non identiquement nul, et tel que le plus grand commun diviseur de ses coefficients soit 1, on voit que toute classe d'éléments irréductibles de $K[X]$ contient un élément

primitif (unique à un facteur inversible de A près).

Soient P_i les polynômes irréductibles primitifs ainsi choisis. Tout $Q(X)$ à coefficients dans K, non identiquement nul, s'écrit d'une seule manière

$$Q(X) = k.\prod_i P_i(X)^{n_i} ,$$

où les entiers $n_i \geqslant 0$ sont nuls sauf un nombre fini, et $k \in K$ $(k \neq 0)$. En effet ceci exprime que l'anneau $K[X]$ est factoriel.

Je dis que <u>si Q est à coefficients dans A, alors</u> $k \in A$. Cela résulte du <u>lemme de Gauss</u> (qu'on admet provisoirement), et qui dit qu'un produit de polynômes primitifs est primitif ; ici, le polynôme $\frac{1}{k}Q(X)$ est donc primitif. Or si $k = \frac{a}{b}$, $a \in A$, $b \in A$, a et b premiers entre eux (ce qui est possible puisque A est factoriel), on a

$$\frac{b}{a}Q(X) \in A[X] \text{ et primitif ;}$$

si c est l'un quelconque des coefficients de Q, a doit diviser bc, donc a divise c, et il s'ensuit que a est un diviseur commun aux coefficients de Q. Alors les coefficients de $\frac{b}{a}Q(X)$ sont tous divisibles par b, et comme Q est primitif, b est inversible, donc $\frac{a}{b} \in A$.

C.Q.F.D.

Introduisons, dans l'anneau factoriel A, une famille P d'éléments irréductibles de A, telle que tout $a \in A$, non nul, s'écrive d'une seule manière

$$a = u.\prod_{p \in P} p^{k(p)} .$$

Alors on montre facilement que les $p \in P$ (considérés comme polynômes de degré 0) et les $P_i(X)$ forment un système fondamental d'éléments irréductibles de $A[X]$, ce qui prouve enfin que $A[X]$ est factoriel.

<u>Démonstration du lemme de Gauss</u> : il suffit de montrer que si $P_1(X)$ et $P_2(X)$ sont deux polynômes primitifs (à coefficients dans l'anneau fac-

toriel A) , leur produit $P = P_1 P_2$ est primitif. Or soit p un élément irréductible de A qui divise tous les coefficients de P , et considérons l'anneau $B = A/(p)$, qui est intègre. Par l'homomorphisme canonique $\varphi : A \to B$, P, P_1 et P_2 donnent naissance à des polynômes P^φ, P_1^φ et P_2^φ à coefficients dans B , et on a l'identité

$$P^\varphi(X) = P_1^\varphi(X)\, P_2^\varphi(X) .$$

Par hypothèse, les polynômes P_1^φ et P_2^φ ne sont pas identiquement nuls (car si P_1^φ était nul, p diviserait tous les coefficients de P_1). Donc leur produit P^φ n'est pas identiquement nul, car l'anneau $B[X]$ est intègre. Mais puisque p divise les coefficients de P , P^φ est identiquement nul. Contradiction.

Il était donc absurde de supposer que les coefficients de P aient un diviseur commun non inversible. Le lemme de Gauss est démontré.

Remarque importante : pour l'anneau Z , on a montré qu'il existe une infinité de nombres premiers. Il n'en est pas toujours de même pour un anneau principal A . D'abord, si A est un corps, l'ensemble des eléments premiers est vide. Mais même s'il existe des eléments premiers $p_1, p_2, \ldots, p_n$, il n'est pas sûr qu'on puisse en trouver un autre : en effet, dans le cas de Z , on avait considéré

$$a = 1 + p_1 p_2 \ldots p_n$$

et observé que ses facteurs premiers sont $\neq p_1, p_2, \ldots, p_n$. Ce raisonnement marchait parce que a n'était pas inversible (étant ≥ 2), donc admettait au moins un facteur premier. Mais dans le cas général il se peut qu'un tel élément soit inversible, et on ne peut donc pas conclure. Voici un exemple :

Exemple d'un anneau principal A admettant un seul idéal premier.

Soit k un corps commutatif. On note $A = k[[X]]$ l'anneau des séries formelles $\sum_{n\geqslant 0} a_n X^n$; $a_n \in k$.

Cet anneau est intègre.

Quels sont les idéaux ?

Lemme : Si $a_0 \neq 0$, alors $\sum_{n\geqslant 0} a_n X^n$ est inversible dans A .

Démonstration : on peut supposer $a_0 = 1$. Alors $\sum_{n\geqslant 0} a_n X^n = 1 - u$, u étant une série formelle sans terme constant.

$(1-u)^{-1} = 1 + u + u^2 + u^3 + \ldots$: ceci est une série formelle. Donc $(1-u)$ a un inverse.

Soit $a_p X^p + a_{p+1} X^{p+1} + \ldots$ une série formelle quelconque $(a_p \neq 0)$; on l'écrit $\underbrace{X^p(a_p + a_{p+1} X + \ldots)}$; on en déduit que toute série formelle non nulle s'écrit sous la forme uX^p , $p \geqslant 0$, u inversible.

Il s'ensuit que l'anneau $k[[X]]$ est principal, et que ses idéaux sont (1), (X), (X^2), (X^p), ... Le seul idéal premier est (X) .

C.Q.F.D.

Les entiers de Gauss.

$\mathbb{C} \supset \mathbb{Z}$ (i) , qui se compose des $\{a + ib\}/a \in \mathbb{Z}$ et $b \in \mathbb{Z}$.

Ceci est un anneau, car

$(a+bi)(c+di) = ac - bd + i(ad+bc)$.

Dans le plan on obtient l'ensemble des points à coordonnées entières.

Rappel : Le conjugué de $a + bi$ est $a - bi$

$N(a+bi) = (a+bi)(a-bi) = a^2 + b^2$ s'appelle la norme de $a + bi$. Si a et b sont entiers non nuls tous deux $N(a+bi)$ est un entier $\geqslant 1$.

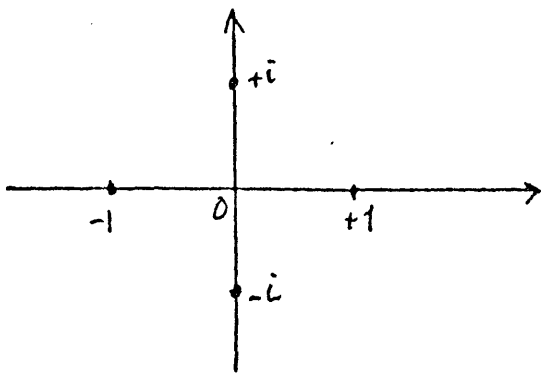
On a $N(\alpha\beta) = N(\alpha).N(\beta)$.

$A = \mathbb{Z}(i)$ est un anneau commutatif, intègre, à élément unité.

1. Quels sont les éléments inversibles de cet anneau ?

Si $\alpha\beta = 1$, on a

$N(\alpha\beta) = N(1) = 1$. Donc $N(\alpha).N(\beta) = 1$, ce qui exige, puisque $N(\alpha)$ et $N(\beta)$ sont entiers $\geqslant 1$, $N(\alpha) = N(\beta) = 1$. Donc α est l'un des 4 nombres $+ 1$, $- 1$, $+ i$, $- i$ de norme 1 .



Les éléments inversibles de cet anneau sont $\pm i$ et ± 1 .

Ils forment un groupe (cyclique) pour la multiplication.

Deux éléments α et β de $\mathbb{Z}(i)$ sont dits équivalents si leur quotient est inversible. C'est la condition nécessaire et suffisante pour l'égalité des idéaux principaux (α) et (β) .

Dans chaque classe d'équivalence, il existe un représentant α et un seul tel que :

$$0 \leqslant \arg \alpha < \frac{\pi}{2} .$$

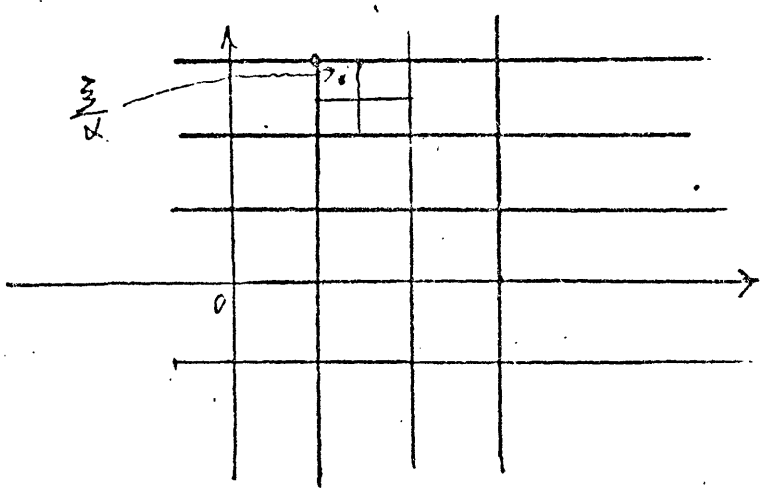
Théorème : L'anneau $\mathbb{Z}(i)$ des entiers de Gauss est un anneau principal.

La démonstration utilise le :

Lemme (division) : Soit $\alpha = a+ib \in A$, $\alpha \neq 0$;

$\forall \xi \in A$, $\exists \eta$ et $\rho \in A$ tels que $\xi = \alpha\eta + \rho$ avec $N(\rho) < N(\alpha)$.

Nous allons montrer en fait que $N(\rho) \leqslant \frac{1}{2}N(\alpha)$. $\frac{\xi}{\alpha}$ est un nombre complexe : $\frac{\xi}{\alpha} = a + ib$, $a, b \in \mathbb{Q}$.



Il existe un des sommets du réseau $\mathbb{Z}(i)$ dont la distance à $\frac{\xi}{\alpha}$ est minimum (il peut en exister plusieurs). Si η est un tel sommet, on a :

$$\left.\begin{array}{l} \mathrm{Re}(\eta - \frac{\xi}{\alpha}) \leqslant \frac{1}{2} \\ \mathrm{Im}\,(\eta - \frac{\xi}{\alpha}) \leqslant \frac{1}{2} \end{array}\right\} \Rightarrow \quad N(\eta - \frac{\xi}{\alpha}) \leqslant \frac{1}{4} + \frac{1}{4} = \frac{1}{2}$$

Or $\frac{\xi}{\alpha} - \eta = \frac{\rho}{\alpha}$, d'où $N(\frac{\rho}{\alpha}) \leqslant \frac{1}{2}$, $N(\rho) \leqslant \frac{1}{2}N(\alpha)$.

C.Q.F.D.

Démonstration du théorème :

Soit I un idéal de l'anneau A .

- Si $I = \{0\}$, l'idéal est principal : (0)

- Si $I \neq \{0\}$: soit $\alpha \in I$ un point de I dont la norme est minimum (parmi les éléments de I de norme non nulle).

Alors :

$\xi = \alpha\eta + \rho$, $\quad N(\rho) < N(\alpha)$

$\xi \in I \Rightarrow \rho \in I$ et $N(\rho) < N(\alpha) \Rightarrow \rho = 0$.

Ainsi $\alpha | \xi$, et l'idéal I se compose des multiples de α , donc est principal.

Note : si α est un générateur de I , les autres générateurs possibles sont $-\alpha$, $\pm i\alpha$.

Corollaire : $\mathbb{Z}(i)$ est factoriel.

Car on a vu que tout anneau principal est factoriel.

2. Comment est fait un nombre premier dans $\mathbb{Z}(i)$?

Il y en a de deux sortes :

1) ceux qui ont un représentant réel > 0 ,

2) ceux $(a+bi)$ pour lesquels $a \neq 0$ et $b \neq 0$.

Lemme 1 : soit $p \in \mathbb{Z}$, $p > 0$; si p est premier dans $\mathbb{Z}(i)$, alors p est premier dans $\mathbb{Z}$.

Car si $p = n_1 n_2$, n_1 et n_2 entiers non inversibles, on a $n_1 \in \mathbb{Z}(i)$, $n_2 \in \mathbb{Z}(i)$ non inversibles, donc p n'est pas premier dans $\mathbb{Z}(i)$.

Remarque : il y a des p premiers dans $\mathbb{Z}$, non premiers dans $\mathbb{Z}(i)$. Par exemple $\begin{cases} 2 = (1+i)(1-i) = i(1-i)^2 \\ 5 = (2+i)(2-i) \end{cases}$.

Lemme 2 : si p premier dans $\mathbb{Z}$, est divisible par $(a+ib)$, $a \neq 0$ et $b \neq 0$, alors $p = a^2+b^2$ et $(a+bi)$ est premier dans $\mathbb{Z}(i)$.

Démonstration : $p = (a+bi)(c+di)$, $c \in \mathbb{Z}$ et $d \in \mathbb{Z}$.

Alors $0 = ad + bc$, d'où $(*)\ \frac{c}{a} = \frac{-d}{b}$. Or a et b sont premiers entre eux ; en effet si $d > 0$ divise a et b , on a $d|a + bi$, donc $d|p$; alors p est divisible par $d(\frac{a}{d} + i\frac{b}{d})$, donc la norme est strictement plus grande que la norme de d . Donc $d < p$, et par suite $d = 1$ puisque p est premier. Ainsi a et b sont premiers entre eux ; la relation $(*)$ entraîne alors

$c = \lambda a$, $d = -\lambda b$, $\lambda \in \mathbf{Z}$. D'où

$p = \lambda(a+bi)(a-bi) = \lambda(a^2+b^2)$.

Comme p est premier, et $a^2 + b^2 > 1$, ceci exige $\lambda = 1$ et $a^2 + b^2 = p$.

Montrons maintenant que $(a+bi)$ est premier dans $\mathbf{Z}(i)$.

Supposons $(a+bi) = (u+vi)(u'+v'i)$. Alors $p = a^2+b^2 = (u^2+v^2)(u'^2+v'^2)$. Puisque p est premier, l'un des facteurs vaut 1 ; par exemple : $u'^2 + v'^2 = 1$; donc $u' + v'i$ est inversible ; ainsi si $(a+bi)$ est le produit de deux éléments l'un est inversible. Ceci exprime bien que $a + bi$ est premier.

Corollaire : soit p un nombre premier dans $\mathbf{Z}$. Alors

(p non premier dans $\mathbf{Z}(i)$) $\Leftrightarrow$ p est de la forme a^2+b^2 ,

$a \in \mathbf{Z}$, $b \in \mathbf{Z}$, $a \neq 0$ et $b \neq 0$.

Démonstration : si p n'est pas premier dans $\mathbf{Z}(i)$, il a un diviseur non inversible qui ne lui est pas équivalent. Ce diviseur ne peut être dans $\mathbf{Z}$, donc p est divisible par $a + bi$, $a \neq 0$ et $b \neq 0$, on applique alors le lemme 2. Réciproquement, supposons $p = a^2 + b^2$, a et b entiers $\neq 0$, $a^2 + b^2 = (a+bi)(a-ib)$; ces facteurs sont non inversibles, donc p n'est pas premier dans $\mathbf{Z}(i)$.

Lemme 3 : si $a + bi$ $(a \neq 0, b \neq 0)$ est premier dans $\mathbf{Z}(i)$ alors $a^2 + b^2$ est premier dans $\mathbf{Z}$.

Démonstration : la decomposition d'un entier en facteurs premiers dans $\mathbb{Z}$ donne :

$$a^2+b^2 = p_1 p_2 \dots p_n \ , \quad p_i \text{ premiers (distincts ou non)}$$

$$a^2+b^2 = (a+bi)(a-bi) \Rightarrow a+bi \mid p_1 p_2 \dots p_n \quad (\text{dans } \mathbb{Z}(i))$$

mais $\mathbb{Z}(i)$ est principal (donc factoriel) ; puisque $a+bi$ est premier et divise un produit de facteurs, il divise l'un d'entre eux, p_1 par exemple: $a+bi \mid p_1$.

Le lemme 2 dit qu'alors $p_1 = a^2+b^2$. C.Q.F.D.

Conclusions : les classes de nombres premiers dans $\mathbb{Z}(i)$ sont :

1) les classes des p premiers dans $\mathbb{Z}$ qui ne sont pas de la forme a^2+b^2 ;

2) les classes des $a+bi$ $(a \neq 0 \ , \ b \neq 0)$ tels que a^2+b^2 soit premier dans $\mathbb{Z}$.

Remarque 1 : Un p premier dans $\mathbb{Z}$ s'écrit au plus d'une manière sous la forme a^2+b^2 (ce qui veut dire : si $a^2+b^2 = c^2+d^2$ est premier, alors

$$\begin{cases} a = \pm c \\ b = \pm d \end{cases} \quad \text{ou} \quad \begin{cases} a = \pm d \\ b = \pm c \end{cases}$$

Démonstration : d'après le lemme 2, $a+bi$, $a-bi$, $c+di$, $c-di$ sont premiers dans $\mathbb{Z}(i)$. D'après l'unicité de la décomposition en facteurs premiers la relation $(a+bi)(a-bi) = (c+di)(c-di)$ entraîne que $c+di$ est équivalent à $a+bi$ ou à $(a-bi)$; dans le premier cas, $c+di = u(a+bi)$, avec $u = \pm 1$ ou $\pm i$; dans le second cas $c+di = u(a-bi)$. D'où la conclusion .

Remarque 2 : si p premier dans $\mathbb{Z}$ n'est pas premier dans $\mathbb{Z}(i)$ (c'est-à-dire $p = a^2+b^2$) , les deux facteurs de $p = (a-bi)(a+bi)$ sont-ils équivalents ? On doit avoir l'une des relations :

$a + bi = \pm (a-bi)$, $a + bi = \pm i(a-bi)$, avec $a \neq 0$, $b \neq 0$, a et b premiers entre eux. La première relation est impossible ; la seconde relation entraîne $a = b$ ou $a = -b$. Donc $a + bi = \pm 1 \pm i$ et $\boxed{p = 2}$. Donc 2 est le seul entier premier qui se décompose, dans $\mathbf{Z}(i)$, en produits de facteurs premiers équivalents entre eux.

La question qui se pose maintenant est de reconnaître quand un p , premier dans $\mathbf{Z}$, est une somme de deux carrés.

Théorème : Pour que p , premier dans Z , soit de la forme $a^2 + b^2$ ($a \in Z$, $b \in Z$), il faut et il suffit que

$p = 2$ ou $p \equiv 1$ (modulo 4).

Démonstration :

. $2 = 1 + 1$ est bien une somme de deux carrés.

Reste à examiner le cas de p premier impair.

- Observation n° 1 : $\begin{pmatrix} p \text{ impair} \\ p = a^2+b^2 \end{pmatrix} \Rightarrow p \equiv 1 \pmod 4$

En effet, a et b n'ont pas la même parité ; par exemple $a = 2a'$, $b = 2b'+1$

$a^2 + b^2 = 4a'^2 + 4b'^2 + 4b' + 1 \Rightarrow p \equiv 1 \pmod 4$.

- On va maintenant montrer : (p premier, $p \equiv 1 \pmod 4$) $\Rightarrow$ p non premier dans $\mathbf{Z}(i)$ (ce qui équivaut, on le sait par le corollaire au lemme 2, à la condition : p est somme de deux carrés). On admet provisoirement le lemme suivant :

Lemme : soit p premier dans $\mathbf{Z}$, $p \equiv 1 \pmod 4$; il existe $x \in \mathbf{Z}$ tel que $x^2+1 \equiv 0 \pmod p$.

[Ce lemme sera prouvé au § suivant, consacré aux restes quadratiques (mod p)] .

Donc si $p \equiv 1 \pmod 4$, on a

$$p \mid x^2+1 \Rightarrow p \mid (x+i)(x-i) \quad \text{dans } \mathbf{Z}(i) \ .$$

p ne peut pas être premier dans $\mathbf{Z}(i)$, sinon p diviserait l'un des facteurs, par ex. $p \mid x+i$ alors $x + i = p(a+bi)$

$$x + i = pa + pbi$$

On obtient $pb = 1$, avec b entier ; mais ceci est impossible

C.Q.F.D.

Corollaire du théorème : Les p premiers de $\mathbf{Z}$ qui sont premiers dans $\mathbf{Z}(i)$ sont ceux tels que $p \equiv -1 \pmod 4$.

Exemple : 3, 7, 11, 19, 23, 31, ...

Par ailleurs : 2, 5, 13, 17, 29, ... sont non premiers (sont sommes de deux carrés) : $2 = 1+1$, $5 = 4+1$, $13 = 4+9$, $17 = 16+1$, $29 = 25+4$.

RESTES QUADRATIQUES MODULO p (p premier dans $\mathbf{Z}$).

Considérons l'anneau $\mathbf{Z}/p\mathbf{Z}$.

Théorème : $A = \mathbf{Z}/p\mathbf{Z}$ est un corps.

Première démonstration :

A est intègre car p est premier.

Notons A* l'ensemble des éléments $\neq 0$ de A , et soit $a \in A^*$; l'application $\begin{cases} A^* \xrightarrow{f} A^* \\ x \longmapsto ax \end{cases}$ est une application injective de A* dans A* (A* est fini, avec p-1 éléments) ; or on sait qu'une application injective d'un ensemble fini dans lui-même est bijective.

Donc $\exists x / ax = 1$, donc a est inversible ; il s'ensuit que l'anneau

est un corps.

Notation : le corps $\mathbb{Z}/p\mathbb{Z}$ se note $\mathbb{F}_p$. Il a p éléments.

Deuxième démonstration : (valable pour tout anneau principal).

Soit A un anneau principal ; soit $p \in A$, $p \neq 0$, (p) premier.

Théorème : $A/(p)$ est un corps.

Montrons que si un idéal I contient (p) , on a $I = (p)$ ou $I = A$.

En effet, comme l'anneau est principal : $I = (a)$; $a \mid p$ car $(p) \subset (a)$, donc soit $a \sim p$ $(\Rightarrow (a) = (p))$, soit a est inversible $(\Rightarrow (a) = A)$.

Donc (p) est un idéal maximal, au sens de la définition suivante :

> Un idéal I d'un anneau commutatif A est maximal si $I \neq A$ et s'il n'y a pas d'idéal contenant I et différent de l'anneau A .

Le théorème à démontrer est une conséquence du résultat général suivant:

Le quotient A/I d'un anneau commutatif A par un idéal maximal I est un corps.

Montrons-le : si I est un idéal quelconque d'un anneau commutatif A, l'application canonique $A \to A/I$ établit une correspondance bijective entre les idéaux de A/I et les idéaux de A contenant I . Dire que I est maximal équivaut à dire que dans $B = A/I$ les seuls idéaux sont $\{0\}$ et B , et que $B \neq \{0\}$. Or ceci exprime que B est un corps.

Exemple : Soit k un corps commutatif ; on a vu que l'anneau $k[X]$ est principal. Soit $P \in k[X]$ un polynôme irréductible. L'idéal (P) est premier, donc l'anneau quotient $k[X]/(P)$ est un corps. Par exemple

$k = \mathbb{R}$, $P(X) = X^2+1$, $k[X]/(X^2+1)$ est un corps :

c'est le corps des nombres complexes.

est un corps.

Notation : le corps $\mathbb{Z}/p\mathbb{Z}$ se note $\mathbb{F}_p$. Il a p éléments.

Deuxième démonstration : (valable pour tout anneau principal).

Soit A un anneau principal ; soit $p \in A$, $p \neq 0$, (p) premier.

Théorème : $A/(p)$ est un corps.

Montrons que si un idéal I contient (p) , on a $I = (p)$ ou $I = A$.

En effet, comme l'anneau est principal : $I = (a)$; $a|p$ car $(p) \subset (a)$, donc soit $a \sim p$ $(\Rightarrow (a) = (p))$, soit a est inversible $(\Rightarrow (a) = A)$.

Donc (p) est un idéal maximal, au sens de la définition suivante :

> Un idéal I d'un anneau commutatif A est maximal si $I \neq A$ et s'il n'y a pas d'idéal contenant I et différent de l'anneau A .

Le théorème à démontrer est une conséquence du résultat général suivant:

Le quotient A/I d'un anneau commutatif A par un idéal maximal I est un corps.

Montrons-le : si I est un idéal quelconque d'un anneau commutatif A, l'application canonique $A \to A/I$ établit une correspondance bijective entre les idéaux de A/I et les idéaux de A contenant I . Dire que I est maximal équivaut à dire que dans $B = A/I$ les seuls idéaux sont $\{0\}$ et B , et que $B \neq \{0\}$. Or ceci exprime que B est un corps.

Exemple : Soit k un corps commutatif ; on a vu que l'anneau $k[X]$ est principal. Soit $P \in k[X]$ un polynôme irréductible. L'idéal (P) est premier, donc l'anneau quotient $k[X]/(P)$ est un corps. Par exemple

$k = \mathbb{R}$, $P(X) = X^2+1$, $\mathbb{R}[X]/(X^2+1)$ est un corps :

c'est le corps des nombres complexes.

Etude de $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$.

Définition : $n \in \mathbb{Z}$ est reste quadratique modulo p si $\exists y \in \mathbb{Z} / y^2 \equiv n \pmod p$.

Il revient au même de dire que la classe x de n dans le corps $\mathbb{F}_p$ est un carré (i.e. est le carré d'un élément de $\mathbb{F}_p$). Il est clair que 0 est un carré ; désormais, on s'intéresse aux carrés $\neq 0$.

$\mathbb{F}_p^* = \mathbb{F}_p - \{0\}$ est un groupe pour la multiplication ; il possède $(p-1)$ éléments. L'ensemble des carrés de $\mathbb{F}_p^*$ est évidemment un sous-groupe G_p ; c'est l'image de l'application

$$u = \mathbb{F}_p^* \longrightarrow \mathbb{F}_p^* \text{ définie par } u(x) = x^2 ,$$

qui est un endomorphisme car $(yz)^2 = y^2 z^2$.

- pour $p = 2$: le seul élément non nul est 1 et c'est un carré ; on a $G_2 = \mathbb{F}_2^*$.

- supposons désormais p premier <u>impair</u> .

$$N = \ker u = \{x \in \mathbb{F}_p^* / x^2 = 1\} .$$

N contient déjà $+1$ et -1 , qui sont distincts puisque $p \neq 2$.

N ne contient pas d'autre élément : en effet, $X^2 - 1$ est un polynôme du second degré à coefficients dans le corps $\mathbb{F}_p$, donc il a au plus deux racines distinctes. Directement, $x^2 - 1 = (x+1)(x-1)$ ne peut être nul que si l'un des facteurs est nul.

Cela dit, l'homomorphisme u induit un isomorphisme

$G_p \approx \mathbb{F}_p^*/N$. Donc

$\mathrm{Card}(G_p) = \mathrm{Card}(\mathbb{F}_p^*)/\mathrm{Card}\ (N)$, or $\mathrm{card}\ N = 2$, donc

$$\boxed{\mathrm{Card}\ G_p = \frac{p-1}{2}} .$$

On peut dire que, dans $\mathbb{F}_p^*$, un élément sur deux est un carré. On veut caractériser simplement ces éléments.

Théorème : Soit p un nombre premier impair, et soit G_p le sous-groupe multiplicatif des carrés dans $\mathbb{F}_p^*$. Alors, pour $x \in \mathbb{F}_p^*$, on a

$$(x \in G_p) \iff x^{\frac{p-1}{2}} = 1 .$$

Rappels : Dans un groupe abélien fini, on appelle ordre d'un élément x le cardinal du sous-groupe cyclique qu'il engendre ; c'est le plus petit des entiers $n > 0$ tels que $nx = 0$ (en notation additive), $x^n = 1$ (en notation multiplicative). L'ordre est 1 si et seulement si x est l'élément neutre.

L'ordre d'un élément x divise l'ordre du groupe G (ou Card G) ; autrement dit, on a $\boxed{x^{\text{card } G} = 1 \text{ pour tout } x \in G}$.

(En effet, l'ordre d'un sous-groupe de G divise l'ordre de G).

Dans le cas qui nous intéresse, G est le groupe multiplicatif $\mathbb{F}_p^*$. On a donc $\boxed{x^{p-1} = 1 \text{ pour tout } x \in \mathbb{F}_p^*}$.

L'application $v : \mathbb{F}_p^* \longrightarrow \mathbb{F}_p^*$ définie par $v(x) = x^{\frac{p-1}{2}}$ est un endomorphisme.

$\ker v = \{x \in \mathbb{F}_p^* / x^{\frac{p-1}{2}} = 1\}$.

On a $\ker v \supset G_p$; car si $x = y^2$, alors $x^{\frac{p-1}{2}} = y^{p-1} = 1$. Par ailleurs, le polynôme $X^{\frac{p-1}{2}} - 1$ a au plus $\frac{p-1}{2}$ racines dans le corps $\mathbb{F}_p$, donc $\text{Card}(\ker v) \leqslant \frac{p-1}{2}$. Comme $\ker v \supset G_p$ et $\text{Card } G_p = \frac{p-1}{2}$, on conclut

$$\boxed{\ker v = G_p}$$

On a donc caractérisé G_p comme étant le noyau de v, ce qui prouve le théorème.

Remarque : pour p premier impair, les $x \in \mathbb{F}_p^*$ qui ne sont pas des carrés sont ceux tels que $x^{\frac{p-1}{2}} = -1$.

En effet, pour tout $x \in F_p^*$, on a $x^{\frac{p-1}{2}} = \pm 1$, puisque $(x^{\frac{p-1}{2}})^2 = 1$.

En résumé, pour un entier n non divisible par p (premier impair), on a : (n est reste quadratique modulo p) $\Leftrightarrow n^{\frac{p-1}{2}} \equiv 1 \pmod p$

(n est non reste quadratique mod p) $\Leftrightarrow n^{\frac{p-1}{2}} \equiv -1 \pmod p$.

Exemple : cherchons quand -1 est reste quadratique (mod p). La condition est $(-1)^{\frac{p-1}{2}} = 1$; elle exprime que $\frac{p-1}{2}$ est pair, autrement dit :

$$\boxed{p \equiv 1 \pmod 4}.$$

Alors ~~Donc~~ (-1) est reste quadratique modulo p ; donc $\exists n / n^2 = -1 \ (p)$ $\Leftrightarrow n^2 + 1 \equiv 0 \ (p)$.

Ceci est précisément le lemme que nous avions admis pour montrer que si p est premier et $\equiv 1 \pmod 4$, p n'est pas premier dans $\mathbb{Z}(i)$.

Calcul de $2^{\frac{p-1}{2}} \pmod p$, p premier impair.

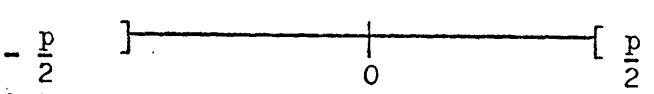
Remarque préliminaire :

1) soit n un entier, $n = qp + r$, $0 \leqslant r < p$.

Chaque entier non nul et non divisible par p a un reste unique, donc sa classe (mod p) a un représentant unique dans l'intervalle $]0, p[$. Il y a aussi un représentant unique dans l'intervalle $]-\frac{p}{2}, +\frac{p}{2}[$ ($\frac{p}{2}$ n'est pas entier).

2) soit $n > 0$ donné non divisible par p. Considérons la suite des multiples entiers de n : $n, 2n, 3n, \ldots, \frac{p-1}{2}n$.

Considérons la suite des $\frac{p-1}{2}$ représentants de ces entiers dans $]-\frac{p}{2}, +\frac{p}{2}[$



. Ils sont distincts, car si $kn \equiv k'n \pmod p$, on a $k \equiv k' \pmod p$ puisque p ne divise pas n, et ceci est impossible si k et k' sont distincts et dans l'intervalle $[1, \frac{p-1}{2}]$, car $|k-k'| \leqslant p-1$.

. Ces représentants ne sont jamais opposés ; ce qui veut dire que la somme de deux d'entre eux n'est jamais congrue à $0 \pmod p$. En effet $kn + k'n$ n'est jamais $\equiv 0 \pmod p$, car ceci exigerait $k + k' \equiv 0 \pmod p$; or $k + k'$ est dans l'intervalle $[1, p-1]$.

. Les valeurs absolues des représentants sont donc distinctes ; il y en a $\frac{p-1}{2}$; donc ce sont exactement les entiers $1, 2, \ldots, \frac{p-1}{2}$.

Chaque entier $1, 2, \ldots, \frac{p-1}{2}$ est donc, au signe près, le représentant d'un des entiers $n, 2n, \ldots, \frac{p-1}{2}n$. Le problème qui se pose maintenant est de trouver le signe du représentant.

Soit ν le nombre des représentants < 0 ; alors le produit

$(n)(2n) \ldots (\frac{p-1}{2}n)$ est congru (mod p) à

$(-1)^\nu 1.2\ldots(\frac{p-1}{2})$.

Ainsi $n^{\frac{p-1}{2}} (\frac{p-1}{2})! \equiv (-1)^\nu (\frac{p-1}{2})! \pmod p$

mais $(\frac{p-1}{2})!$ n'est pas divisible par p, car aucun des facteurs de cette factorielle n'est divisible par p ; on peut alors diviser la congruence ; on obtient

$$\boxed{n^{\frac{p-1}{2}} \equiv (-1)^\nu \pmod p},$$

ν étant le nombre des représentants < 0 situés dans $]-\frac{p}{2}, +\frac{p}{2}[$.

Autre interprétation de ν : prenons maintenant les représentants dans $]0, p[$; les représentants qui étaient > 0 ne changent pas, ceux qui étaient < 0 sont augmentés de p : ce sont ceux de l'intervalle $]\frac{p}{2}, p[$.

ν est donc le nombre des représentants qui sont $> \frac{p}{2}$ quand on prend les représentants dans $]0, p[$.

On applique ceci au cas $n = 2$. On a la suite $2, 4, \ldots, p-1$ des nombres pairs $\geqslant 2$ et $\leqslant p-1$. Ils sont leurs propres représentants dans $]0, p[$. ν est le nombre de ceux qui sont $> \frac{p}{2}$. Donc $2\nu = (p-1) - (\text{le plus grand des nombres pairs } < \frac{p}{2})$.

Or le plus grand nombre pair $< \frac{p}{2}$ est $\frac{p-1}{2}$ ou $\frac{p-3}{2}$, suivant la parité de $\frac{p-1}{2}$.

1er cas : $\frac{p-1}{2}$ est pair.

$$2\nu = (p-1) - (\tfrac{p-1}{2}) \implies \nu = \tfrac{p-1}{4} .$$

2ème cas : $\frac{p-3}{2}$ est pair

$$2\nu = (p-1) - (\tfrac{p-3}{2}) \implies \nu = \tfrac{p+1}{4} .$$

Récapitulons : pour que 2 soit reste quadratique (mod p), p premier impair, il faut et il suffit que ν soit pair, c'est-à-dire :

- si $p \equiv 1 \pmod 4$, il faut et il suffit que $p \equiv 1 \pmod 8$.
- si $p \equiv -1 \pmod 4$, il faut et il suffit que $p \equiv -1 \pmod 8$.

En résumé : les p premiers tels que 2 soit reste quadratique modulo p sont ceux tels que $\boxed{p \equiv \pm 1 \ (8)}$

Remarque :

On a $2^{\frac{p-1}{2}} \equiv (-1)^{\frac{p^2-1}{8}} \pmod p$.

En effet, $\frac{p^2-1}{4}$ est le produit des deux entiers consécutifs $\frac{p-1}{2}$ et $\frac{p+1}{2}$, dont un seul est pair ; donc $\frac{p^2-1}{8}$ est pair si et seulement si $\frac{p-1}{2}$ ou $\frac{p+1}{2}$ est divisible par 4 .

Quand un entier est-il somme de 2 carrés ?

On a déja résolu ce problème pour un entier p premier :

$$p = a^2 + b^2 \iff p = 2 \quad \text{ou} \quad p \equiv 1\ (4)\ .$$

On se pose maintenant la question pour un entier $n > 0$ quelconque. Autrement dit, quand n peut-il s'écrire sous la forme $N(\alpha)$, α étant un entier de Gauss ?

Remarque préliminaire : Si n_1 et n_2 sont sommes de 2 carrés, alors $n_1 n_2$ est somme de 2 carrés (ceci découle de la multiplication de 2 nombres complexes : si $n_1 = N(\alpha_1)$ et $n_2 = N(\alpha_2)$, alors $n_1 n_2 = N(\alpha_1 \alpha_2)$.

Considérons $E = \{n > 0\ ,\ n$ est somme de 2 carrés$\}$.

E est stable par multiplication. Or nous connaissons déjà des éléments de E.

. les carrés $\in E$,

. 2, les p premiers congrus à $1 \pmod 4$ $\in E$,

Théorème : $n \in E \iff$ dans la décomposition de n en facteurs premiers, les exposants des $p \equiv -1(4)$ sont pairs.

Démonstration :

$\Longleftarrow$

Supposons $n = a^2 b$, où b n'a pas de facteurs premiers $\equiv -1\ (4)$. Il suffit de montrer que b est une somme de 2 carrés. Or b est un produit de nombres premiers dont chacun appartient à E ; donc $b \in E$.

$\Longrightarrow$

Soit $n = a^2 + b^2$ $(a \neq 0\ ,\ b \neq 0)$. Soit $d = (a,b)$, $a = da'$; $b = db'$ avec $(a',b') = 1$, $a^2 + b^2 = d^2(a'^2 + b'^2)$.

Soit p un diviseur premier de $a'^2 + b'^2$; alors p n'est pas premier ans l'anneau $Z(i)$ des entiers de Gauss, car :

$p|a'^2 + b'^2 \Longrightarrow p|(a' + b'i)(a' - b'i) \Longrightarrow p|a' + b'i$ par exemple.

$\Longrightarrow p|a'$ et $p|b'$; or $(a', b') = 1$, donc il y a contradiction.

Les seuls facteurs premiers possibles de $a'^2 + b'^2$ sont ceux qui e sont pas premiers dans $Z(i)$; donc ce sont ceux qui ne sont pas $\equiv -1 \pmod 4$.

Ainsi tous les p premiers congrus à $-1(4)$ sont forcément ceux ui figurent dans la décomposition de d^2 en facteurs premiers ; leurs exposants ont pairs.

C.Q.F.D.

Remarque : L'ensemble $\{a,b\}$ des entiers $a \geqslant 0$ et $b \geqslant 0$ tels que $= a^2 + b^2$ n'est pas toujours unique (contrairement à ce qui a lieu lorsque n est remier).

Exemple : $65 = 5 \times 13 \quad (5 = 4 + 1 , \ 13 = 9 + 4)$

$= (2+i)(2-i)(3+2i)(3-2i)$

$= [(2+i)(3-2i)]\,[(2-i)(3+2i)] = (8-i)(8+i) = (64+1)$

$= [(2+i)(3+2i)]\,[(2-i)(3-2i)] = (4+7i)(4-7i) = (16+49)$.

Digression sur les sommes de 4 carrés.

Théorème : Tout entier $n > 0$ s'écrit sous la forme

$a^2 + b^2 + c^2 + d^2$, a, b, c, d entiers $\geqslant 0$.

La démonstration découle de la conjonction des 2 propositions suivantes:

Proposition 1 : l'ensemble F des sommes de 4 carrés est able pour la multiplication.

Proposition 2 : tout entier premier est somme de 4 carrés.

Il reste à démontrer ces 2 propositions ; auparavant, voici quelques notions sur les quaternions.

Notes sur le corps des quaternions.

Un quaternion est un couple (α, β) avec $\alpha \in \mathbb{C}$ et $\beta \in \mathbb{C}$

$$+ : (\alpha, \beta) + (\gamma, \delta) = (\alpha + \gamma, \beta + \delta)$$

$$\times : (\alpha, \beta)(\gamma, \delta) = (\alpha\gamma - \bar{\beta}\delta , \beta\gamma + \bar{\alpha}\delta) ,$$

où $\bar{\alpha}$ désigne le nombre complexe conjugué de α . On note $\mathbb{H}$ l'anneau ainsi défin Admettons que la multiplication est associative (le vérifier !) : voici comment on peut retenir cette formule. D'abord, on a $(\alpha, 0)(\gamma, 0) = (\alpha\gamma, 0)$, donc on peut id tifier l'ensemble des $(\alpha, 0)$ au corps $\mathbb{C}$ des nombres complexes. Ensuite on a

$$(0, 1)(\alpha, 0) = (0, \alpha) , \quad (\alpha, 0)(0, 1) = (0, \bar{\alpha}) .$$

Notons j le quaternion $(0, 1)$. On a, en identifiant $(\alpha, 0) = \alpha$

$$j\alpha = (0, \alpha) , \quad \alpha j = j\bar{\alpha} .$$

Alors (α, β) s'écrit $(\alpha, 0) + (0, \beta) = \alpha + j\beta = \alpha + \bar{\beta}j$.

De plus on vérifie que

$$\boxed{j^2 = -1} .$$

On peut maintenant retrouver la formule de multiplication, en utilis l'associativité, et la distributivité de la multiplication par rapport à l'addition

$$\begin{aligned}(\alpha+j\beta)(\gamma+j\delta) &= \alpha\gamma + j\beta j\delta + j\beta\gamma + \alpha j\delta \\ &= \alpha\gamma + j^2\bar{\beta}\delta + j\beta\gamma + j\bar{\alpha}\delta \\ &= (\alpha\gamma-\bar{\beta}\delta) + j(\beta\gamma+\bar{\alpha}\delta) .\end{aligned}$$

En résumé : tout quaternion s'écrit sous la forme $\alpha + j\beta$, $\alpha \in \mathbb{C}$ $\beta \in \mathbb{C}$; la règle de multiplication est donnée par les règles de calcul

$$j^2 = -1 , \quad j\beta = \bar{\beta}j ,$$

jointes à l'associativité de la multiplication, et la distributivité de la multiplication par rapport à l'addition.

Remarque : la correspondance $\alpha + j\beta \longleftrightarrow (\alpha, \beta)$ identifie $\mathbb{H}$ à $\mathbb{C} \times \mathbb{C}$ comme espace vectoriel à droite sur $\mathbb{C}$ (espace de dimension deux sur $\mathbb{C}$). En revanche, le produit de $\alpha + j\beta$ à gauche par $\gamma \in \mathbb{C}$ est $\gamma\alpha - j\bar{\gamma}\beta$.

$\mathbb{H}$ est un $\mathbb{C}$-espace vectoriel à droite, de base $\{1, j\}$

(1, i, j, ji) forment une base de $\mathbb{H}$ sur les réels.

On pose $\boxed{ji = -k}$.

Opérations sur la $\mathbb{R}$-base $(1, i, j, k)$:

. $i^2 = j^2 = k^2 = -1$ (verification facile).

. $ij = -ji = k$, $jk = -kj = i$, $ki = -ik = j$ (le vérifier).

Centre de $\mathbb{H}$: si un quaternion $x + yi + zj + tk$ commute avec tout quaternion, alors $y = z = t = 0$ (écrire qu'il commute avec i , avec j, et avec k). Le centre de $\mathbb{H}$ se compose des "quaternions réels" : on l'identifie à $\mathbb{R}$.

Conjugué d'un quaternion.

$$\overline{(x + yi + zj + tk)} = x - yi - zj - tk \quad .$$

En employant l'autre écriture :

$$\overline{\alpha + j\beta} = \bar{\alpha} - j\beta$$

$$\overline{\overline{\alpha + j\beta}} = \alpha + j\beta \quad .$$

Propriété fondamentale : soit $u = \alpha + j\beta$. On définit $N(u) = u\bar{u}$.

On a $N(u) = (\alpha+j\beta)\overline{(\alpha+j\beta)} = (\alpha+j\beta)(\bar{\alpha}-j\beta) = \alpha\bar{\alpha} + \beta\bar{\beta} + j(\beta\bar{\alpha}-\bar{\alpha}\beta)$

$$(\alpha+j\beta)\overline{(\alpha+j\beta)} = \alpha\bar{\alpha} + \beta\bar{\beta} = \text{nombre réel} \geqslant 0$$

$$\alpha\bar{\alpha} + \beta\bar{\beta} = 0 \Longleftrightarrow \left\{\begin{matrix}\alpha\bar{\alpha} = 0 \\ \beta\bar{\beta} = 0\end{matrix}\right\} \Longleftrightarrow \alpha = \beta = 0 \quad .$$

Ainsi, si on note $\bar{u}$ le conjugué d'un quaternion u, on a

$$N(u) = u\bar{u} = \bar{u}u = N(u) \geqslant 0 \text{ , et si } u \neq 0 \text{ on a } u\bar{u} > 0 .$$

Les quaternions forment un corps(non commutatif).

En effet, si $u \neq 0$, $u\bar{u} = a > 0$ commute avec tout quaternion, donc

$$u(\frac{1}{a}\bar{u}) = \frac{1}{a}(u\bar{u}) = 1 ,$$

et par suite u est inversible, son inverse étant $\frac{1}{a}\bar{u}$.

Exercice : vérifier les formules ; u et v étant 2 quaternions :

$\overline{u+v} = \bar{u} + \bar{v}$, $\overline{uv} = \bar{v}.\bar{u}$, $N(uv) = N(u).N(v)$.

[noter que $N(uv) = uv\bar{v}\bar{u} = (v\bar{v})u\bar{u}$] .

Le problème qui nous préoccupait avant la parenthèse sur les quaternions était de montrer que tout $n > 0$ s'écrit sous forme de 4 carrés.

Or $(a+bi+cj+dk)(a-bi-cj-dk) = a^2 + b^2 + c^2 + d^2$.

Dans le cas où a, b, c, d sont des entiers naturels ($\in \mathbb{Z}$) , c'est-à-dire où α et β sont des entiers de Gauss ($\in \mathbb{Z}(i)$) alors :

$$u\bar{u} = N(u) = a^2 + b^2 + c^2 + d^2 = \Sigma \text{ 4 carrés.}$$

Ainsi, pour qu'un entier soit somme de 4 carrés il faut et il suffit qu'il soit égal à la norme $N(u)$ d'un quaternion $u = \alpha + j\beta$, où α et β sont des entiers de Gauss (un tel u s'appelle un quaternion entier).

Nous pouvons maintenant démontrer la proposition 1 énoncée plus haut :

Si deux entiers n et n' sont des sommes de 4 carrés, alors leur produit aussi.

En effet, si $n = N(u)$, $n' = N(u')$, on a $nn' = N(uu')$; or le produit de deux quaternions entiers est un quaternion entier.

Remarque : soit $n = x_1^2 + x_2^2 + x_3^2 + x_4^2$, $n' = x_1'^2 + x_2'^2 + x_3'^2 + x_4'^2$. Le produit des quaternions $x_1 + x_2 i + x_3 j + x_4 k$ et $x_1' + x_2' i + x_3' j + x_4' k$ fournira explicitement des entiers z_1, z_2, z_3, z_4 tels que $nn' = z_1^2 + z_2^2 + z_3^2 + z_4^2$.

On va maintenant prouver la proposition 2 annoncée plus haut :

Tout entier premier p est la norme d'un quaternion entier

Avant de commencer la démonstration, commençons par des exemples :

$2 = 1 + 1 + 0 + 0$, $3 = 1 + 1 + 1 + 0$,

$5 = 1 + 4 + 0 + 0$, $7 = 1 + 1 + 1 + 4$.

Soit donc p premier, en général. On peut supposer p impair, car la proposition à démontrer est vraie pour $p = 2$.

Lemme : soit p un nombre premier impair ; il existe des entiers $x \in Z$ et $y \in Z$, $x \geqslant 0$, $y \geqslant 0$ tels que :

$1 + x^2 + y^2 \equiv 0 \pmod p$, $1 + x^2 + y^2 < p^2$.

Démonstration : On donne à x et y respectivement toutes les valeurs entières de 0 à $\frac{p-1}{2}$. Alors x^2 prend $\frac{p+1}{2}$ valeurs distinctes modulo p, car $(x_1)^2 - (x_2)^2 = (x_1-x_2)(x_1+x_2)$ n'est pas $\equiv 0 \pmod p$ si $x_1 \neq x_2$.

De même, y^2 prend $\frac{p+1}{2}$ valeurs distinctes mod p.; et par suite $-(1+y^2)$ prend $\frac{p+1}{2}$ valeurs distinctes mod p .

Les valeurs prises par x^2 et par $-(1+y^2)$ ne sont pas toutes distinctes mod p, car il y en a $p+1$.

Donc $\exists (x,y)$ tel que $p \mid 1 + x^2 + y^2$, $0 \leqslant x \leqslant \frac{p-1}{2}$, $0 \leqslant y \leqslant \frac{p-1}{2}$.

On a $x^2 + y^2 \leqslant 2 \left(\frac{p-1}{2}\right)^2 = \frac{(p-1)^2}{2}$

$1 + x^2 + y^2 \leqslant 1 + \frac{(p-1)^2}{2} < \frac{p^2}{2}$.

Recherche des entiers de $\mathbb{Q}(\sqrt{d})$.

$X^2 - 2aX + (a^2 - d\,b^2)$ est à coefficients entiers

$$\Longleftrightarrow \quad (1) \quad \left|\begin{array}{l} 2a \in \mathbb{Z} \\ a^2 - d\,b^2 \in \mathbb{Z} \end{array}\right| \quad \text{(Pour } b = 0\text{, ceci exprime bien que } a \in \mathbb{Z}\text{)}.$$

$$\Longrightarrow \left\{\begin{array}{l} 4a^2 \in \mathbb{Z} \\ 4(a^2 - d\,b^2) \equiv 0 \pmod 4 \end{array}\right\} \Longrightarrow \quad 4\,d\,b^2 \in \mathbb{Z}$$

$$\Longrightarrow \quad d(2b)^2 \in \mathbb{Z}\ .$$

Posons $b' = 2b$.

Montrons $\quad \underline{d\,b'^2 \in \mathbb{Z} \Longrightarrow b' \in \mathbb{Z}}$

en effet : $\left\{\begin{array}{ll} b' = \frac{\alpha}{\beta} & d\alpha^2 = \beta^2 n \\ (\alpha,\beta) = 1 & \text{les facteurs premiers de } \beta \text{ sont dans } d\text{, et} \\ \alpha,\beta \in \mathbb{Z} & \text{y apparaissent avec un exposant pair, ce qui implique} \\ & \text{contradiction s'il y en a.} \end{array}\right.$

Donc β n'a pas de facteur premier $\Longrightarrow \beta = \pm 1 \Longrightarrow b' \in \mathbb{Z}$.

D'où : $\left\{\begin{array}{l} 2a \in \mathbb{Z} \\ 2b \in \mathbb{Z} \end{array}\right. \Longrightarrow \left\{\begin{array}{l} a = \frac{u}{2} \\ b = \frac{v}{2} \end{array}\right.$ avec u et $v \in \mathbb{Z}$.

On veut de plus : $a^2 - d\,b^2 \in \mathbb{Z}$, soit :

$u^2 - d\,v^2 = 4(a^2 - d\,b^2) \equiv 0 \pmod 4$. Cherchons ces couples u, v.

1er cas : u pair ; $u^2 - dv^2 \equiv 0 \pmod 4 \Longrightarrow dv^2 \equiv 0 \pmod 4$

comme d est sans facteur carré, v doit être pair. Donc a et $b \in \mathbb{Z}$.

2ème cas : u impair ; il faut v impair, d'où

$$\left\{\begin{array}{l} u^2 \equiv 1 \ (4) \\ v^2 \equiv 1 \ (4) \end{array}\right. \Longrightarrow u^2 - dv^2 \equiv 1 - d\text{, d'où } d \equiv 1 \pmod 4.$$

Réciproquement, si $d \equiv 1 \pmod 4$, u et v impairs, on a $u^2 - dv^2 \equiv 0 \pmod 4$. Résumons :

Théorème : Les entiers de $\mathbb{Q}(\sqrt{d})$ sont les suivants :

. si $d \equiv 2$ ou $3 \pmod 4$: ce sont les nombres $a + b\sqrt{d}$, où a et $b \in \mathbb{Z}$;

. si $d \equiv 1 \pmod 4$: ce sont les nombres $a + b\sqrt{d}$, où $2a$, $2b$ et $a + b \in \mathbb{Z}$.

L'ensemble des entiers de $\mathbb{Q}(\sqrt{d})$ est un $\mathbb{Z}$-module qui a une base

$\begin{cases} (1, \sqrt{d}) & \text{si } d \equiv 2 \text{ ou } 3 \pmod 4 \\ (1, \frac{1+\sqrt{d}}{2}) & \text{si } d \equiv 1 \pmod 4 \end{cases}$.

C'est donc un module libre. [Un module est comme un e.v., sauf que les coefficients ne sont pas nécessairement dans un corps : ici les coefficients sont dans $\mathbb{Z}$] .

Les entiers de $\mathbb{Q}(\sqrt{d})$ forment un sous-anneau noté $\mathbb{Z}(\sqrt{d})$ dans le 1er cas, $\mathbb{Z}(\frac{\sqrt{d}+1}{2})$ dans le second. Il suffit de vérifier ce que donne le produit sur les éléments de base : $1 \times \sqrt{d} = \sqrt{d}$, $\sqrt{d}.\sqrt{d} = d$; $(\frac{1+\sqrt{d}}{2})^2 = \frac{1+\sqrt{d}}{2} + \frac{d-1}{4}$, et $\frac{d-1}{4}$ est bien entier, puisque $d \equiv 1 \pmod 4$.

Exemples : . $d = -1 \Rightarrow d \equiv 3 \ (4)$

Les entiers sont $a + bi$, avec a et $b \in \mathbb{Z}$. On retrouve l'anneau des entiers de Gauss.

. $d = 2 \Rightarrow d = 2 \ (4)$

Les entiers sont les $a + b\sqrt{2}$, avec a et $b \in \mathbb{Z}$.

. $d = -3 \Rightarrow d = 1 \ (4)$

Les entiers sont les $a + b(\frac{1+i\sqrt{3}}{2})$, où $a, b \in \mathbb{Z}$.

Notion de norme : $x \in \mathbb{Q}(\sqrt{d}) \Rightarrow x = a + b\sqrt{d}$ avec a et $b \in \mathbb{Q}$.

Norme de $x = N(x) = a^2 - db^2 = (a+b\sqrt{d})(a-b\sqrt{d}) \in \mathbb{Q}$.

$N(xy) = N(x)\ N(y)$

$N(x) = 0 \iff x = 0$

$N(1) = 1$.

La norme d'un entier est un entier (on a vu en effet que $a^2 - db^2 \in \mathbb{Z}$ si $a + b\sqrt{d}$ est entier).

Recherche des éléments inversibles de l'anneau des entiers de $\mathbb{Q}(\sqrt{d})$

$$\begin{cases} xy = 1 \\ x \text{ entier} \\ y \text{ entier} \end{cases} \Rightarrow \begin{cases} N(x)\ N(y) = 1 \\ N(x) \in \mathbb{Z} \\ N(y) \in \mathbb{Z} \end{cases} \Rightarrow \begin{cases} N(x) = \pm 1 \\ N(y) = \pm 1 \end{cases}$$

Donc $x = a + b\sqrt{d}$ doit être un entier de norme ± 1 . Réciproquement, si un entier $a + b\sqrt{d}$ est tel que $N(a + b\sqrt{d}) = (a + b\sqrt{d})(a - b\sqrt{d}) = \varepsilon = \pm 1$, alors $a + b\sqrt{d}$ a pour inverse $\varepsilon(a - b\sqrt{d})$, qui est un autre entie

Ainsi : Théorème : soit x un entier de $\mathbb{Q}(\sqrt{d})$; x est inversible dans l'anneau des entiers $\iff N(x) = \pm 1$.

Les éléments inversibles de l'anneau des entiers s'appellent les unités du corps $\mathbb{Q}(\sqrt{d})$.

Théorème : les unités forment un groupe pour la multiplication.

Démonstration : 1 est une unité ; vérifier que l'inverse d'une unité est une unité, le produit de deux unités est une unité.

. α est une unité $\Rightarrow -\alpha$ est une unité car ($N(\alpha) = N(-\alpha)$). Les unités α telle que $N(\alpha) = +1$ forment un sous-groupe du groupe multiplicatif des unités ; ce sous-groupe est soit tout, soit d'indice 2 (on verra des exemples plus loin).

Recherche du groupe des unités de $Z(\xi)$, pour $\xi = \sqrt{d}$ ou $\frac{1+\sqrt{d}}{2}$ (suivant que $d \equiv 2, 3$ ou $d \equiv 1 \pmod 4$).

(1) Cas d'un corps quadratique imaginaire ($d < 0$). Posons

$d = -d'$; $N(a+ib\sqrt{d'}) = a^2 + d'b^2$

$d \equiv 2$ ou $3 \pmod 4 \Rightarrow \begin{cases} d' \equiv 1 \text{ ou } 2 \pmod 4 \\ a \text{ et } b \in \mathbb{Z} \end{cases}$

On cherche a et $b \in \mathbb{Z}$ tels que $a^2 + d'b^2 = 1$

. si $d' \geqslant 2$, $a^2 + d'b^2 = 1 \Rightarrow \begin{cases} a = \pm 1 \\ b = 0 \end{cases}$ Il y a 2 unités : ± 1 .

. si $d' = 1$, $a^2 + b^2 = 1 \Rightarrow \begin{cases} a = \pm 1 \\ b = 0 \end{cases}$ ou $\begin{cases} a = 0 \\ b = \pm 1 \end{cases}$ Il y a 4 unités : ± 1, $\pm \sqrt{d}$.

$d \equiv 1 \pmod 4 \Rightarrow \begin{cases} d' \equiv 3 \pmod 4 \\ a = \frac{u}{2},\ b = \frac{u}{2},\ u+v \equiv 0 \pmod 2 \\ a^2 + d'b^2 = 1 \end{cases} \Rightarrow \begin{cases} d' > 0 \text{ et } d' \equiv 3 \pmod 4 \\ u^2 + d'v^2 = 4 \\ u + v \equiv 0 \pmod 2 \end{cases}$

. si $d' > 3 \Rightarrow d' \geqslant 7$ puisque $d' \equiv 3 \pmod 4$

$\Rightarrow \begin{cases} v = 0 \\ u = \pm 2 \end{cases} \Rightarrow \begin{cases} a = \pm 1 \\ b = 0 \end{cases}$ Il y a 2 unités : ± 1 .

. si $d' = 3 \Rightarrow \begin{cases} u^2 + 3v^2 = 4 \\ u + v \equiv 0 \pmod 2 \end{cases} \Rightarrow \begin{cases} u = \pm 1 \\ v = \pm 1 \end{cases}$ ou $\begin{cases} u = \pm 2 \\ v = 0 \end{cases}$

Il y a six unités, qui sont les racines sixièmes de 1 dans $\mathbb{C}$: ± 1 et $\frac{\pm 1 \pm i\sqrt{3}}{2}$

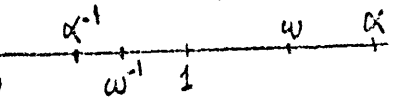
(2) Cas où $d > 0$.

Traitons d'abord un exemple : $d = 2$.

$\omega = 1 + \sqrt{2}$ est une unité, car $N(\omega) = 1 - 2 = -1$.

Lemme : ω est la plus petite des unités $\alpha > 1$.

En effet $\alpha \geqslant \omega$ équivaut à $\alpha^{-1} \leqslant \omega^{-1}$, et aussi à



$\alpha - \alpha^{-1} \geqslant \omega - \omega^{-1}$ (exercice !).

On a $\omega - \omega^{-1} = 1 + \sqrt{2} - (\sqrt{2} - 1) = 2$. Il suffit donc de montrer que $\alpha - \alpha^{-1} \geqslant 2$ pour toute unité $\alpha > 1$. Soit

$$\alpha = a + b\sqrt{2} ;$$

je dis que $a > 0$, $b > 0$; en effet α est le plus grand des 4 nombres $\pm \alpha$, $\pm \alpha^{-1}$, qui sont :

$$\pm a \pm b\sqrt{2} .$$

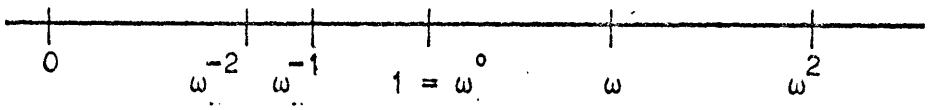
On a $\alpha^{-1} = \pm (a - b\sqrt{2})$, suivant que $a^2 - 2b^2 = \pm 1$. D'où :

$$\alpha - \alpha^{-1} = 2b\sqrt{2} \text{ ou } 2a ,$$

et comme $a \geqslant 1$, $b \geqslant 1$, ceci est $\geqslant 2$. C.Q.F.D.

Théorème : Les unités de l'anneau $Z(\sqrt{2})$ sont les nombres $\pm \omega^n$ $(n \in Z)$, où ω désigne toujours $1 + \sqrt{2}$.

Démonstration : tous ces nombres sont des unités, puisque ± 1 sont des unités, ainsi que les puissances ω^n (n entier $\geqslant 0$) et leurs inverses. Il reste à montrer qu'il n'y a pas d'autre unité. Il suffit de montrer que toute unité $\alpha > 0$ est de la forme ω^n. Considérons, sur la demi-droite réelle positive, la suite (infinie dans les deux sens) des ω^n :



Si α était distinct de tous les points de cette suite, il existerait un $n \in Z$ tel que

$$\omega^n < \alpha < \omega^{n+1} \qquad (n \geqslant 0 \text{ ou } < 0) .$$

Alors $1 < \alpha\omega^{-n} < \omega$, et comme $\alpha\omega^{-n}$ est une unité, on trouve une contradiction avec le lemme. Le théorème est démontré.

Remarque importante : la recherche des unités de $\mathbb{Z}(\sqrt{2})$ est celle des solutions entières de l'équation $|x^2 - 2y^2| = 1$. L'unité $\omega = 1 + \sqrt{2}$ est une solution de $x^2 - 2y^2 = -1$. La propriété multiplicative de la norme montre que :

Les solutions entières de $x^2 - 2y^2 = +1$ sont $x + y\sqrt{2} = \pm\, \omega^{2n}$

Les solutions entières de $x^2 - 2y^2 = -1$ sont $x + y\sqrt{2} = \pm\, \omega^{2n+1}$

avec $\omega = 1 + \sqrt{2}$.

Cas général :

Théorème : $d > 0$ sans facteur carré. Le groupe multiplicatif des unités de l'anneau des entiers du corps $\mathbb{Q}(\sqrt{d})$ se compose des éléments : $\pm\, \omega^n$, $n \in \mathbb{Z}$ où $\omega > 1$ est la plus petite unité > 1 .

ω est appelée unité fondamentale.

Démonstration : Ce qui est difficile, c'est de montrer qu'il existe effectivement des unités autres que ± 1 . Nous l'admettrons (cela résulte, en fait, d'un théorème très général, le "théorème de Dedekind" ; voir le chapitre 4 du livre de Samuel).

Supposons donc qu'on ait prouvé qu'il y a des unités $\alpha \neq \pm 1$; alors l'un des quatre nombres distincts $\pm\, \alpha$, $\pm\, \alpha^{-1}$ est > 1 . Donc il existe des unités > 1 . On va montrer : l'ensemble U (non vide) des unités $\alpha > 1$ possède un plus petit élément. Sinon, il existerait une suite strictement décroissante

$$\alpha_1 > \alpha_2 > \ldots > \alpha_n > \ldots .$$

d'unités toutes > 1 . Cette suite aurait une limite $\beta \geqslant 1$.

Alors $\lim_{n \to \infty} \frac{\alpha_n}{\alpha_{n+1}} = 1$ (*)

Or $\frac{\alpha_n}{\alpha_{n+1}} = \beta_n$ est une unité > 1 ; et toute unité $\beta > 1$ satisfa à $\beta - \beta^{-1} \geqslant 1$.

En effet, $\beta = a + b\sqrt{d}$ (2a et 2b entiers, a+b entier), avec $\beta^{-1} = \pm (a - b\sqrt{d})$; si $\beta > 1$, a et b sont > 0 , donc $\geqslant \frac{1}{2}$, et

$$\beta - \beta^{-1} = 2a \quad \text{ou} \quad 2b\sqrt{d} \geqslant 1 \ .$$

Donc $\beta \geqslant \frac{1+\sqrt{5}}{2}$ (racine > 1 de l'équation $x^2 - x - 1 = 0$), et par suite $\frac{\alpha_n}{\alpha_{n+1}} \geqslant \frac{1+\sqrt{5}}{2}$, ce qui contredit (*) .

Soit alors $\omega > 1$ le plus petit élément de l'ensemble U . On montre (comme dans le cas $d = 2$) , que toute unité est de la forme $\pm \omega^n$.

. si $N(\omega) = +1$: $\forall n$, $N(\pm \omega^n) = 1$. En particulier l'équation en entiers : $x^2 - dy^2 = -1$ n'a pas de solution.

. si $N(\omega) = -1 \Rightarrow \begin{cases} N(\alpha) = +1 \iff \alpha = \pm \omega^{2n}, \ n \in \mathbb{Z} \\ N(\alpha) = -1 \iff \alpha = \pm \omega^{2n+1}, \ n \in \mathbb{Z} \end{cases}$

- Exemple: $d = 3$: l'équation $x^2 - 3y^2 = -1$ n'a pas de solution entière ; en effet $x^2 - 3y^2 = -1 \Rightarrow x^2 \equiv -1 \pmod 3$; absurde car :

$$\forall x : x \equiv \begin{vmatrix} 0 \\ \pm 1 \end{vmatrix} \pmod 3 \Rightarrow x^2 \equiv \begin{vmatrix} 0 \\ 1 \end{vmatrix} \pmod 3 \ .$$

Ainsi, pour $d = 3$, on a $N(\omega) = +1$. En fait, on a $\boxed{\omega = 2 + \sqrt{3}}$ Car ω est bien une unité ; et si α est une unité > 1 , on a $\alpha = a + b\sqrt{3}$ avec a et b entiers > 0 , d'où $\alpha^{-1} = a - b\sqrt{3}$, $\alpha - \alpha^{-1} = 2b\sqrt{3} \geqslant 2\sqrt{3} = \omega - \omega^{-1}$.

Problème : si $d \equiv 1 \pmod 4$, ω est-elle à coefficients entiers

. si oui, toutes ses puissances aussi ; par exemple, pour $d = 17$

si $a + b\sqrt{17}$ est une unité, on a nécessairement $a, b \in \mathbb{Z}$; en effet, si $a = \frac{u}{2}$, $b = \frac{v}{2}$, u et v entiers impairs, il est impossible que $u^2 - 17v^2 = \pm 4$, car on a $u \equiv \pm 1 \pmod 4$, $v \equiv \pm 1 \pmod 4$, d'où $u^2 \equiv 1$ et $v^2 \equiv 1 \pmod 8$, et $u^2 - 17v^2 \equiv -16 \equiv 0 \pmod 8$. Dans ce cas $(d = 17)$, si $\alpha = a + b\sqrt{17}$ est une unité > 1 , on a $a^2 = 17b^2 \pm 1 \geqslant 16$, donc $a \geqslant 4$, et

$$\alpha - \alpha^{-1} = 2a \quad \text{ou} \quad 2b\sqrt{17} \text{ , donc } \geqslant 8 \text{ .}$$

Il s'ensuit que $\omega = 4 + \sqrt{17}$ est la plus petite unité > 1 , car $\omega - \omega^{-1} = 8$.

. <u>si non</u> : $N(\omega) = \varepsilon = \pm 1 = (x + \frac{y}{2})^2 - \frac{dy^2}{4}$ (x et y entiers)

$\omega = x + \frac{y}{2} + \frac{y}{2}\sqrt{d}$, y impair.

$\omega^2 = \frac{+2\varepsilon + dy^2}{2} + \frac{y(2x+y)}{2}\sqrt{d}$ n'est pas à coefficients entiers.

$\omega^3 = (2x+y)\frac{\varepsilon + dy^2}{2} + y\sqrt{d}\,\frac{3\varepsilon + dy^2}{2}$ est à coefficients entiers.

Alors les solutions entières de $x^2 - dy^2 = \pm 1$ sont $\pm \omega^{3n}$; si en outre $N(\omega) = -1$, les solutions entières de $x^2 - dy^2 = 1$ sont $\pm \omega^{6n}$.

<u>Exemple</u> : traiter le cas $d = 5$.

<u>Divisibilité dans l'anneau A des entiers de $\mathbb{Q}(\sqrt{d})$.</u>

Rappelons que $\begin{cases} A = \mathbb{Z}(\sqrt{d}) & \text{si } d \equiv 2 \text{ ou } \equiv 3 \pmod 4, \\ A = \mathbb{Z}(\frac{1+\sqrt{d}}{2}) & \text{si } d \equiv 1 \pmod 4. \end{cases}$

Il sera toujours sous-entendu que d <u>est sans facteur carré</u>.

On va d'abord donner une condition <u>suffisante</u> pour que l'anneau A soit <u>principal</u> (donc factoriel).

Définition : on dit que A possède une division euclidienne si, pour tout $\alpha \neq 0$ de A, et pour tout $\xi \in A$, il existe $\eta \in A$ et $\rho \in A$ tels que

$$\xi = \alpha\eta + \rho \ , \ |N(\rho)| < |N(\alpha)| .$$

Pour cela, il faut et il suffit que pour tout $\zeta \in \mathbb{Q}(\sqrt{d})$, il existe $\alpha \in A$ tel que $|N(\zeta-\alpha)| < 1$ (le lecteur est prié de le prouver).

Proposition 1.- Si A possède une division euclidienne, A est un anneau principal.

La démonstration est analogue à celle donnée pour l'anneau des entiers de Gauss ($d = -1$). Soit I un idéal de A ; si $I = \{0\}$, I est principal. Si $I \neq \{0\}$, l'ensemble des $|N(\alpha)|$, où α parcourt l'ensemble des éléments non nuls de I, est un ensemble d'éléments > 0 de $\mathbb{Z}$; il possède donc un plus petit élément. Soit $\alpha \in I$ tel que $|N(\alpha)|$ ait cette valeur minimum ; pour tout $\xi \in I$, on a $\xi = \alpha\eta + \rho$, $\eta \in A$, $\rho \in A$, $|N(\rho)| < |N(\alpha)|$. Comme $\rho \in I$, on conclut, d'après le choix de α, que $\rho = 0$. Donc tout $\xi \in I$ est divisible par α, et I est l'idéal principal engendré par α.

C.Q.F.D.

Exemples d'entiers d pour lesquels l'anneau A des entiers de $\mathbb{Q}(\sqrt{d})$ possède une division euclidienne :

$$d = -1, -2, -3, -7, -11,$$

$$d = 2, 3, 5, 6, 7,$$

(Pour la démonstration, cf. le livre de Hardy et Wright). Bornons-nous à faire ici la démonstration pour les valeurs suivantes de d : -1, -2, -3, -7, -11, 2 et 3.

Le cas $d = -1$ a déjà été traité (entiers de Gauss).

Cas où $d = -2$: les entiers sont les $a+ib\sqrt{2}$, avec $a \in \mathbb{Z}$, $b \in \mathbb{Z}$. Il s'agit de montrer que si x et $y \in \mathbb{Q}$, il existe a et $b \in \mathbb{Z}$ tels que

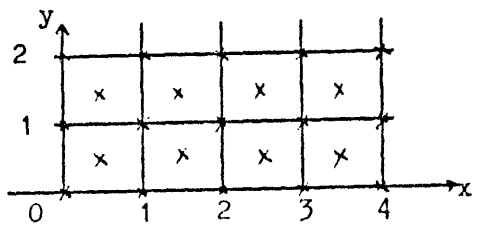
$$(x-a)^2 + 2(y-b)^2 < 1 .$$

Or il existe évidemment a et b $\in \mathbb{Z}$ tels que

$$|x-a| \leqslant 1/2 \ , \ |y-b| \leqslant 1/2,$$

ce qui entraîne $(x-a)^2 + 2(y-b)^2 \leqslant 3/4$. C.Q.F.D.

Cas où $d = -3, -7$ ou -11. Alors $d \equiv 1 \pmod 4$, et les entiers $a+b\sqrt{d}$ correspondent aux couples (a,b) du réseau suivant : on réunit l'ensemble des points du plan à coordonnées entières et son translaté par $(1/2, 1/2)$:



Si $(x,y) \in \mathbb{Q} \times \mathbb{Q}$, on voit qu'il existe un (a,b) du réseau tel que $|y-b| \leqslant 1/4$; puis, ayant choisi b , on peut choisir a de façon que $|x-a| \leqslant 1/2$, le point (a,b) étant toujours dans le réseau. Alors $N(a+b\sqrt{d}) = (x-a)^2 + d'(y-b)^2$, avec $d' = -d$, donc $N(a+b\sqrt{d}) \leqslant \frac{1}{4} + \frac{d'}{16}$, et ceci est bien < 1 si d' est l'un des entiers 3, 7 et 11. C.Q.F.D.

Cas où $d = 2$ ou 3 : les entiers sont les $a+b\sqrt{d}$, avec a et b $\in \mathbb{Z}$. Etant donnés x et y $\in \mathbb{Q}$, il existe a et b $\in \mathbb{Z}$ tels que

$$|x-a| < 1/2 \ , \ |y-b| \leqslant 1/2 \ , \text{ d'où :}$$

$$|N(x-a + (y-b)\sqrt{d})| = |(x-a)^2 - d(y-b)^2| \leqslant \sup((x-a)^2 \ , \ d(y-b)^2) \ ;$$

or $(x-a)^2 \leqslant 1/4$, et $d(y-b)^2 \leqslant 3/4$ si $d = 2$ ou 3 , d'où

$$|N(x-a + (y-b)\sqrt{d})| < 1 \ . \qquad \text{C.Q.F.D.}$$

Remarque : la proposition 1 dit que l'existence d'une division euclidienne est suffisante pour que A soit principal ; mais cette condition n'est pas nécessaire (cf. Hardy-Wright). De plus, on peut prouver que si A est factoriel, alors A est principal.

Désormais, nous allons développer une théorie de la divisibilité dans l'anneau A dans le cas général (sans supposer que A soit factoriel).

Proposition 2.- L'anneau A satisfait à l'axiome β (cf. page 16)

En effet, s'il existait une suite strictement croissante d'idéaux

principaux (α_n), la suite des entiers $|N(\alpha_n)|$ serait strictement décroissante, ce qui est absurde.

Corollaire : tout élément non nul de A s'écrit comme produit d'une famille finie d'éléments irréductibles de A (cf. page 16, théorème 3).

Mais attention : si A n'est pas factoriel, cette décomposition n'est pas unique (même à des facteurs inversibles près). On en verra un exemple dans un instant.

Proposition 3.- Si $\alpha \in A$, et si $|N(\alpha)|$ est > 1 et n'est pas de la forme $|N(\beta)|.|N(\gamma)|$, avec $\beta \in A$, $\gamma \in A$, $|N(\beta)| > 1$, $|N(\gamma)| > 1$, alors α est irréductible dans A.

C'est évident.

Corollaire : si l'entier $N(\alpha)$ est premier dans $\mathbb{Z}$, α est irréductible.

Proposition 4.- Soit p premier dans $\mathbb{Z}$. Alors :

(p est irréductible dans A) $\iff$ (p n'est pas de la forme $|N(\alpha)|$, avec $\alpha \in A$).

Démonstration : si $p = |N(\alpha)| = \pm \alpha \bar{\alpha}$, α et $\bar{\alpha}$ sont non-inversibles, donc p n'est pas irréductible dans A.

Inversement, si $p = \alpha\beta$, α et β non-inversibles dans A, on a $p^2 = N(p) = N(\alpha).N(\beta)$, et comme $N(\alpha)$ et $N(\beta)$ sont des entiers > 1, on conclut $N(\alpha) = p$.

Exemple : d = 5.- Soit $A = \mathbb{Z}(i\sqrt{5})$. Les entiers 2 et 3 ne sont pas de la forme a^2+5b^2 ($a \in \mathbb{Z}$, $b \in \mathbb{Z}$), car $a^2 + 5b^2 \equiv 0$, 1 ou $-1 \pmod 5$. Donc 2 et 3 sont irréductibles dans A. D'autre part,

$\alpha = 1 \mp i\sqrt{5}$ est irréductible, puisque $N(\alpha) = 6$ n'est pas le produit de normes de deux éléments non-inversibles de A (cf. prop. 3). Donc 6 s'écrit de deux manières comme produit d'éléments irréductibles :

$6 = 2.3$, $6 = (1+i\sqrt{5})(1-i\sqrt{5})$,

et les idéaux (2), (3), $(1+i\sqrt{5})$, $(1-i\sqrt{5})$ sont distincts (puisque leurs normes sont distinctes). Il s'ensuit que l'axiome α est faux pour l'anneau $\mathbb{Z}(i\sqrt{5})$, qui n'est donc pas factoriel.

Etude des classes d'idéaux principaux dans A .- Elles sont a priori de deux sortes :

(i) les classes des entiers $n \in \mathbb{Z}$;

(ii) les classes (α), où $\alpha \in A$ n'est pas équivalent à un élément de $\mathbb{Z}$.

On se propose de chercher quand un idéal principal (α) est premier . Commençons par le cas où l'idéal (α) est de la sorte (ii).

Théorème 1.- Soit $\alpha \in A$, $\alpha \neq 0$, α non équivalent à un élément de $\mathbb{Z}$, Alors :

(α est premier dans A) $\Leftrightarrow$ ($|N(\alpha)|$ est premier dans $\mathbb{Z}$)

Démonstration : supposons α premier dans A , et montrons que $|N(\alpha)|$ est premier dans $\mathbb{Z}$. A priori, on a $\pm \alpha \bar{\alpha} = p_1 p_2 \cdots p_n$, produit de facteurs premiers de $\mathbb{Z}$ (distincts ou non). Si α est premier dans A , α divise l'un des p_i , par exemple p_1 ; d'où $p_1 = \alpha\beta$, avec β non-inversible (puisque α , par hypothèse, n'est pas équivalent à un élément de $\mathbb{Z}$). Prenons les normes :

$$(p_1)^2 = N(\alpha).N(\beta),$$

d'où l'on conclut comme plus haut :

$$|N(\alpha)| = p_1 .$$

C.Q.F.D.

Montrons inversement que si $|N(\alpha)|$ est premier dans $\mathbb{Z}$, alors α est premier dans A . Supposons donc $|N(\alpha)| = p$ (premier dans $\mathbb{Z}$) , alors p appartient à l'idéal αA engendré par α . L'anneau quotient $A/\alpha A$ est un

vrai quotient de A/pA . Or A s'écrit comme un quotient

$$\mathbb{Z}[X]/(P),$$

où (P) désigne l'idéal principal engendré par le polynôme minimal P de $\sqrt{d}$ (resp. de $\frac{1+\sqrt{d}}{2}$), suivant la congruence de d (mod 4). Il s'ensuit que A/pA s'identifie au quotient de l'algèbre des polynômes $\mathbb{F}_p[X]$ (à coefficients dans le corps $\mathbb{F}_p$ des entiers mod p) par l'idéal, noté encore (P), engendré par le polynôme P (considéré comme ayant ses coefficients dans $\mathbb{F}_p$). Comme P est un polynôme de degré 2, un vrai quotient de $\mathbb{F}_p[X]/(P)$ est nécessairement de la forme $\mathbb{F}_p[X]/(Q)$, où Q est un facteur de degré un de P . Un tel polynôme Q est irréductible (donc premier) dans l'anneau principal $F_p[X]$, et par suite le quotient est intègre ; il est d'ailleurs isomorphe à F_p . Ainsi $A/\alpha A$ est un corps, ce qui implique que l'idéal engendré par α est premier.

C.Q.F.D.

Demandons-nous maintenant quand un p premier dans $\mathbb{Z}$ engendre un idéal premier de A .

Lemme.- Pour que $p \in \mathbb{Z}$, premier dans $\mathbb{Z}$, soit non premier dans A, il faut et il suffit qu'il existe un $\alpha \in A$, non nul, tel que : α soit non-divisible par p, mais $N(\alpha)$ soit divisible par p .

Démonstration : la condition est suffisante, car si p est premier dans A et divise $\alpha\bar{\alpha}$, p divise α ou $\bar{\alpha}$. Montrons que la condition est nécessaire : supposons qu'on ait $\alpha\beta \equiv 0 \pmod{p}$, $\alpha \not\equiv 0 \pmod{p}$, $\beta \not\equiv 0 \pmod{p}$ alors, en prenant les normes, on trouve que $N(\alpha).N(\beta) \equiv 0 \pmod{p}$, donc l'un des entiers $N(\alpha)$ et $N(\beta)$ est divisible par p .

Ce lemme étant prouvé, nous allons montrer le :

Théorème 2.- Pour qu'un entier p premier impair dans A soit non premier dans A, il faut et il suffit que d soit reste quadratique (mod p).

Pour la démonstration, distinguons deux cas :

Premier cas : $d \not\equiv 1 \pmod 4$. S'il existe $\alpha = x+y\sqrt{d}$, $x \in \mathbb{Z}$, $y \in \mathbb{Z}$, x ou y non divisible par p , tels que $x^2-dy^2 \equiv 0 \pmod p$, alors y n'est pas divisible par p (sinon x le serait aussi) ; donc, dans le corps $\mathbb{F}_p$, la classe de y (notée encore y) est non nulle, et par suite a un inverse. Si on calcule dans $\mathbb{F}_p$, on peut donc écrire

$$(x/y)^2 = d ,$$

ce qui prouve que d est reste quadratique (mod p). Réciproquement, s'il existe $x \in \mathbb{Z}$ tel que $x^2-d \equiv 0 \pmod p$, alors $\alpha = x + \sqrt{d}$ n'est pas divisible par p , tandis que $N(\alpha)$ l'est, donc p n'est pas premier dans A .

Deuxième cas : $d \equiv 1 \pmod 4$. Pour que p soit non-premier dans A , il faut et il suffit (d'après le lemme ci-dessus, et la caractérisation des entiers de $\mathbb{Q}(\sqrt{d})$) qu'il existe deux entiers x et $y \in \mathbb{Z}$, de même parité, non tous deux divisibles par p , tels que $x^2-dy^2 \equiv 0 \pmod{4p}$. Utilisons ici l'hypothèse $p \neq 2$; en calculant dans $\mathbb{F}_p$, ceci s'écrit

$$(x/2)^2 - d(y/2)^2 = 0 ;$$

il s'ensuit que $y/2 \neq 0$ dans $\mathbb{F}_p$, d'où $(x/y)^2 = d$, ce qui montre que d est reste quadratique (mod p). Réciproquement, s'il existe $x \in \mathbb{Z}$ tel que $x^2-d \equiv 0 \pmod p$, alors $\alpha = x+\sqrt{d}$ est un élément de A non divisible par p , mais $N(\alpha)$ est divisible par p ; donc p est non-premier dans A . Ceci achève de prouver le théorème 2.

Corollaire : s'il existe un p premier impair tel que :

$$\begin{cases} d \text{ soit reste quadratique (mod p)} , \\ p \text{ ne soit pas de la forme } |N(\alpha)| \quad (\text{avec } \alpha \in A), \end{cases}$$

alors l'anneau A n'est pas factoriel.

(En effet, p est irréductible dans A d'après la prop. 4, mais n'est pas premier dans A d'après le th. 2).

Exemples : $d = 10$, $p = 3$ (10 est évidemment reste quadratique mod 3 ; il est impossible que l'on ait des entiers x et $y \in \mathbb{Z}$ tels que $x^2-10\,y^2 = \pm 3$, car le premier membre est congru à 0 , 1 ou -1 (mod 5), tandis que le second membre est congru à ± 2 (mod 5)). En conséquence, l'anneau $\mathbb{Z}(\sqrt{10})$ n'est pas factoriel.

Le théorème 2 permet de reconnaître quand un entier premier p impair est premier dans A. Reste le cas où $p = 2$; ce cas est réglé par le :

Théorème 2 bis.- Pour que 2 soit premier dans A , il faut et il suffit que $d \equiv 5 \pmod 8$.

Démonstration : si $d \not\equiv 1 \pmod 4$, 2 n'est pas premier dans A , car 2 divise $d^2-d = (d-\sqrt{d})(d+\sqrt{d})$, mais 2 ne divise ni $d-\sqrt{d}$ ni $d+\sqrt{d}$ (d'après la forme des éléments de A).

Si $d \equiv 1 \pmod 4$, la condition nécessaire et suffisante pour que 2 soit non-premier dans A est (d'après le lemme ci-dessus) qu'il existe x et $y \in \mathbb{Z}$ impairs tels que, si l'on pose

$\alpha = \frac{x+y\sqrt{d}}{2}$, la norme $N(\alpha)$ soit divisible par 2. Ceci exprime que $x^2-dy^2 \equiv 0 \pmod 8$. Une telle condition implique $1-d \equiv 0 \pmod 8$, car on a $x^2 \equiv 1$ et $y^2 \equiv 1 \pmod 8$, puisque x et y sont impairs. Réciproquement, si $d \equiv 1 \pmod 8$, il suffit de prendre $x = 1$, $y = 1$, donc 2 est non premier dans A .

Il résulte alors de l'examen des cas ci-dessus que la condition nécessaire et suffisante pour que 2 soit non-premier dans A est que :

$d \equiv 1 \pmod 4$, ou bien $d \equiv 1 \pmod 8$.

Par passage au complémentaire, la condition $d \equiv 5 \pmod 8$ est nécessaire et suffisante pour que 2 soit premier dans A .

C.Q.F.D.

Voici une application du théorème 2 bis : si $d \not\equiv 5 \pmod 8$ et si 2 n'est pas de la forme $|N(\alpha)|$, avec $\alpha \in A$, alors l'anneau A des entiers de $\mathbb{Q}(\sqrt{d})$ n'est pas factoriel (démonstration analogue à celle du corollaire du th. 2).

Exemple : supposons $d < 0$, et posons $d = -d'$; si $d' \not\equiv 3 \pmod 8$, la seule possibilité pour que 2 soit de la forme $\alpha\bar{\alpha}$ est que $d' = 2$ ou $d' = 7$. Donc si $d' > 0$ est $\not\equiv 3 \pmod 8$ et distinct de 2 et 7, l'anneau des entiers de $\mathbb{Q}(i\sqrt{d'})$ n'est pas factoriel (c'est le cas pour $d' = 5$, 6, 10, 13, 14, 15, 17, etc....).

Exercices.- En application des théorèmes 2 et 2 bis, ainsi que la "loi de réciprocité quadratique" (voir plus loin, p. 103), caractériser les p premiers de $\mathbb{Z}$ qui ne sont pas premiers dans l'anneau A des entiers du corps $\mathbb{Q}(\sqrt{d})$, dans chacun des cas suivants :

Cas où $d = 2$: ce sont $p = 2$ et les $p \equiv \pm 1 \pmod 8$; ce sont aussi ceux qui sont de la forme $|a^2-2b^2|$ ($a \in \mathbb{Z}$, $b \in \mathbb{Z}$) [utiliser la prop. 4 et le fait que A est factoriel].

Cas où $d = -3$: ce sont $p = 3$ et les $p \equiv 1 \pmod 3$; ce sont aussi les p de la forme a^2+ab+b^2 ($a \in \mathbb{Z}$, $b \in \mathbb{Z}$).

Cas où $d = 5$: ce sont $p = 5$ et les $p \equiv \pm 1 \pmod 5$; en admettant que l'anneau $\mathbb{Z}\left(\frac{1+\sqrt{5}}{2}\right)$ est factoriel, montrer que ce sont aussi les p de la forme a^2+ab-b^2 ($a \in \mathbb{Z}$, $b \in \mathbb{Z}$).

Compléments :

Que peut-on dire quand l'anneau A des entiers du corps $\mathbb{Q}(\sqrt{d})$ n'est pas principal ? Pour cette question et d'autres, voir le livre de P. SAMUEL. Donnons ici simplement quelques indications.

Soit K le corps des fractions de A . On appelle idéal fractionnaire toute partie $I \subset K$ telle que :

1° $(x \in I \text{ et } y \in I) \Rightarrow x+y \in I$,

2° $x \in I$ et $a \in A \Rightarrow ax \in I$,

3° $\exists a \in A\ (a \neq 0)$ tel que $aI \subset A$

(les conditions 1° et 2° expriment que I est un A-module ; la condition 3° exprime qu'il existe un dénominateur commun pour toutes les fractions qui appartiennent à I).

Deux idéaux fractionnaires I et J sont équivalents s'il existe $k \in K$ $(k \neq 0)$ tel que $J = kI$. On notera que les idéaux principaux sont ceux qui sont équivalents à A . On peut démontrer le

Théorème : il n'y a qu'un nombre fini de classes d'équivalence d'idéaux fractionnaires. [Dire qu'il y a une seule classe, c'est dire que l'anneau est principal].

On définit une multiplication dans l'ensemble des idéaux fractionnaires : si I et J sont deux tels idéaux, IJ est l'ideal engendré par les produits xy, où $x \in I$, $y \in J$. L'idéal $(1) = A$ est élément neutre pour cette multiplicatio On démontre : si $I \neq \{0\}$, I possède un inverse : c'est un idéal J tel que $IJ = \{1\}$. Les idéaux $\neq \{0\}$ forment donc un groupe pour la multiplication. On démontre tout idéal $I \neq \{0\}$ s'écrit d'une seule manière comme produit $P_1^{\alpha_1} P_2^{\alpha_2} \ldots P_k^{\alpha_k}$, où les $P_i \subset A$ sont des idéaux premiers, et les exposants α_i soht des entiers $\geqslant 0$ ou $\leqslant 0$. Les idéaux contenus dans A sont ceux dont les "exposants" α_i sont $\geqslant 0$.

Théorie élémentaire des corps commutatifs. Corps finis.

Si k, K, ... désignent des corps, on désignera par k^*, K^*, ... les groupes multiplicatifs des éléments non nuls de k, K, ... De plus, on supposera toujours que les corps sont commutatifs.

Théorème : dans un corps k, il n'y a pas d'autre idéal que $\{0\}$ et k

Démonstration : soit I un idéal de k ;

- $I = \{0\} \Rightarrow$ terminé
- $I \neq \{0\} \Rightarrow \exists \alpha \in I$, $\alpha \neq 0$. Alors I contient 1, car l'inverse de α existe et $\in k$, soit $\alpha^{-1} \Rightarrow \alpha\alpha^{-1} = 1 \in I$ $\Rightarrow I = k$.

Théorème réciproque : un anneau commutatif $A \neq \{0\}$ dans lequel $\{0\}$ et A sont les seuls idéaux est un corps.

Démonstration : soit $a \in A$, $a \neq 0$. Alors par hypothèse l'idéal $(a) = \{0\}$ ou A. Si $a \neq 0$, alors $(a) = A$, donc $1 \in (a) \Leftrightarrow \exists x \in A : 1 = xa$ $\Leftrightarrow a$ est inversible. Donc A est un corps.

Soient A et B deux anneaux : un homomorphisme d'anneaux $\rho : A \to B$ est une application telle que

- $\rho(1_A) = 1_B$
- $\rho(a+a') = \rho(a) + \rho(a')$
- $\rho(aa') = \rho(a)\,\rho(a')$

Proposition 1 : tout homomorphisme de corps $\rho : k \to K$ est injectif.

Démonstration : si $\rho : A \to B$ est un homomorphisme d'anneaux, on sait que $\operatorname{Ker}\rho$ est un idéal de A. Donc dans le cas d'un homomorphisme de corps, $\operatorname{Ker}\rho = \{0\}$ ou $\operatorname{Ker}\rho = A$.

. si $\mathrm{Ker}\ \rho = \{0\}$, alors ρ est bien injectif

. si $\mathrm{Ker}\ \rho = k$, alors nécessairement $\rho = 0$; mais on sait que $f(1_k) = 1_K \neq 0$. Contradiction.

Un tel homomorphisme ρ identifie k à un sous-corps de K .

Caractéristique d'un corps.

1) Théorème : soit A un anneau commutatif unitaire. Alors il existe un homomorphisme et un seul de l'anneau $\mathbb{Z}$ dans A .

Démonstration : du point de vue additif, $\mathbb{Z}$ est le sous-groupe engendré par 1 : $\rho : \mathbb{Z} \to A$ doit, par définition, envoyer $1 \in \mathbb{Z}$ dans 1_A ; ainsi l'homomorphisme ρ est entièrement déterminé. On a $\rho(0) = 0$,

$$\rho(n) = n(1_A) = \begin{cases} 1_A + \ldots + 1_A & n \text{ fois si } n > 0 \\ -(1_A + \ldots + 1_A) \ (-n \text{ fois}) & \text{si } n < 0 \end{cases}$$. Il reste à montrer que cet homomorphisme respecte la multiplication :

$$\rho(pq) = p\rho(q) = p(q.1_A) = (pq).1_A .$$

2) Soit k un corps commutatif, et soit $\rho : \mathbb{Z} \to k$ l'unique homomorphisme d'anneaux. Etudions $\mathrm{Ker}\ \rho$ qui est un idéal de $\mathbb{Z}$.

a) $\mathrm{Ker}\ \rho = \{0\}$. ρ est alors une injection de l'anneau $\mathbb{Z}$ dans k . Alors il existe un homomorphisme g et un seul de $\mathbb{Q} \to k$ qui prolonge ρ . Construisons cet homomorphisme : si on veut que g soit un homomorphisme, il est nécessaire que $g(\frac{a}{b}) = \frac{g(a)}{g(b)} = \frac{\rho(a)}{\rho(b)}$; puisque $\frac{a}{b} \in \mathbb{Q}$, on a $a \in \mathbb{Z}$, $b \in \mathbb{Z}$, $b \neq 0$.

$\mathrm{Ker}\ \rho = \{0\}$ et $b \neq 0 \implies \rho(b) \neq 0 \Rightarrow g(b) \neq 0$.

Il faut montrer que la définition de g ne dépend pas de la façon d'écrire la fraction $\frac{a}{b}$.

Supposons $\frac{a}{b} = \frac{a'}{b'}$. A-t-on $\frac{\rho(a)}{\rho(b)} = \frac{\rho(a')}{\rho(b')}$?

$\frac{\rho(a)}{\rho(b)} = \frac{\rho(a')}{\rho(b')} \Leftrightarrow \rho(a)\rho(b') = \rho(b)\rho(a') \Leftrightarrow \rho(ab') = \rho(ba')$

$\Leftrightarrow \rho(ab'-ba') = 0 \Leftrightarrow ab' - ba' = 0$ puisque $\mathrm{Ker}\ \rho = \{0\}$

$\Leftrightarrow \frac{a}{b} = \frac{a'}{b'}$ C.Q.F.D.

En posant par définition $g(\frac{a}{b}) = \frac{\rho(a)}{\rho(b)}$, on peut vérifier que g est un homomorphisme de $\mathbb{Q}$ dans k .

$\mathbb{Q}$ et k étant des corps, g est une injection de $\mathbb{Q}$ dans k qui permet d'identifier $\mathbb{Q}$ à un sous-corps de k : on dit alors que k est une <u>extension</u> du corps $\mathbb{Q}$.

<u>Définition</u> : on dit que le corps k est <u>de caractéristique</u> 0 si ρ est une injection, ou encore s'il existe une injection (nécessairement unique) du corps $\mathbb{Q}$ dans le corps k .

b) $\mathrm{Ker}\ \rho \neq \{0\}$. $\mathrm{Ker}\ \rho$ est donc un idéal non nul de $\mathbb{Z}$. On sait alors qu'il est principal : $\exists p \neq 0$, $p \in \mathbb{Z}$: $\mathrm{Ker}\ \rho = (p)$. ρ induit alors un homomorphisme φ de $\mathbb{Z}/(p)$ dans k qui est injectif. Donc φ identifie l'anneau des entiers modulo p à un sous-anneau du corps k ; ce sous-anneau est intègre puisque k est intègre. Ceci signifie que l'idéal engendré par p est premier, et donc que $p \in \mathbb{Z}$ est <u>premier</u>.

Nous savons alors que $\mathbb{Z}/(p) = \mathbb{F}_p$ est le <u>corps</u> des restes modulo p . On trouve un homomorphisme injectif et un seul de $\mathbb{F}_p$ dans k , qui identifie $\mathbb{F}_p$ à un sous-corps de k (sous-corps fini à p éléments).

<u>Par définition</u> : on dit alors que k est un <u>corps de caractéristique</u> p (p <u>premier</u>).

Calcul dans un corps de caractéristique p .

. $(-1)^p = -1$ (1)

. $(a+b)^p = a^p + b^p \qquad \forall a, b \in k$ (2)

. $(a-b)^p = a^p - b^p \qquad \forall a, b \in k$ (3)

(1) $(-1)^p = -1$: si $p \neq 2$, c'est évident ; si $p = 2$, alors $(-1)^2 = 1 = -1$, car dans $\mathbb{F}_2$, $1 = -1$.

(2) et (3) Il faut montrer que le coefficient binomial C_p^k de $a^k b^{p-k}$ est congru à 0 (modulo p) , pour $1 \leqslant k \leqslant p-1$.

$$C_p^k = \frac{p\,!}{k\,!\,(p-k)!} = \frac{p(p-1)\ldots(p-k+1)}{1 \times 2 \times \ldots \times k} \in \mathbb{N} \ .$$

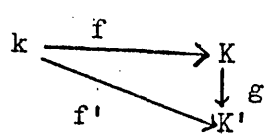
Donc $k\,!$ divise $p(p-1)\ldots(p-k+1)$, mais $1 \leqslant k \leqslant p-1 \Rightarrow k\,!$ et p sont premier entre eux. Donc $k\,!$ divise $(p-1)\ldots(p-k+1)$.

On a donc $C_p^k = p \times \dfrac{(p-1)(p-2)\ldots(p-k+1)}{k\,!} = p \times a$, $a \in \mathbb{Z}$. Donc $C_p^k = 0 \pmod p$ pour $1 \leqslant k \leqslant p-1$. C.Q.F.D.

Remarque : On peut recommencer les opérations (2) et (3) et on en déduit que : $a, b \in \mathbb{F}_p$, $n = p^k \Rightarrow (a+b)^n = a^n + b^n$, $(a-b)^n = a^n - b^n$.

Lorsqu'on a un sous-corps k d'un corps K , on dit que K est une extension de k . Si de plus f est un homomorphisme de k dans K , on dira aussi que f définit K comme extension de k .

Définition : Soient K et K' deux extensions d'un même corps k . On appelle k-homomorphisme de K dans K' un homomorphisme g de K dans K' tel que le diagramme



soit commutatif, c'est-à-dire que $f' = g \circ f$.

Remarques :

1) En caractéristique 0 , tout corps K est une extension de $\mathbb{Q}$, et tout homomorphisme g de K dans un corps K' de caractéristique 0 est automatiquement un $\mathbb{Q}$-homomorphisme au sens précédent.

2) En caractéristique $p \neq 0$, tout corps K est une extension de $\mathbb{F}_p$, et tout homomorphisme g de K dans un corps K' de caractéristique p est automatiquement un $\mathbb{F}_p$-homomorphisme au sens précédent.

Proposition : L'inclusion $k \subset K$ définit sur K une structure d'espace vectoriel sur le corps k :

- le groupe additif étant le groupe additif de K ,
- la multiplication par les scalaires étant définie par

$(\alpha, a) \longmapsto \alpha a$ pour $\alpha \in k$, $a \in K$.

On peut alors vérifier que tous les axiomes des espaces vectoriels sont satisfaits.

Plus généralement, si $f : k \to K$ est un homomorphisme de corps, alors $(\alpha, a) \longmapsto f(\alpha).a$ définit sur K une structure de k-espace vectoriel.

Proposition : tout k-homomorphisme est k-linéaire et réciproquement (démonstration : exercice).

Définition et notation : soit K une extension d'un corps k . On appelle degré de l'extension et on note $[K : k]$ la dimension de K en tant que k-espace vectoriel

$$[K : k] = \dim_k K \ .$$

Exemple : on sait que $(1, \sqrt{2})$ forme une base de $\mathbb{Q}(\sqrt{2})$ en tant qu'espace vectoriel sur le corps $\mathbb{Q} \Rightarrow [\mathbb{Q}(\sqrt{2}) : \mathbb{Q}] = 2$.

Théorème : soient k, K et L trois corps tels que $k \subset K \subset L$, et supposons que les entiers $[L : k]$, $[L : K]$ et $[K : k]$ soient finis.

On a alors : $[L : k] = [L : K]\,[K : k]$.

Démonstration : Soit $(a_1, \ldots, a_n)$ une k-base de K ; $(b_1, \ldots, b_p)$ une K-base de L . L possède donc deux structures d'espace vectoriel : c'est un K-espace vectoriel et un k-espace vectoriel.

Considérons tous les produits $a_j b_j$ $(1 \leqslant j \leqslant n \ , \ 1 \leqslant i \leqslant p)$ et montrons qu'ils forment une k-base de L .

Soit $x \in L$; on sait que x s'écrit de façon unique sous la forme :

$$x = \sum_{i=1}^{p} y_i b_i \qquad y_i \in K \ .$$

On sait que $y_i \in K$ s'écrit de façon unique sous la forme

$$y_i = \sum_{j=1}^{n} z_{ij} a_j \qquad \text{ou} \quad z_{ij} \in k \ .$$

On en déduit que x s'écrit de façon unique sous la forme :

$$x = \sum_{i=1}^{p} \sum_{j=1}^{n} z_{ij} a_j b_i$$

et par conséquent les $a_j b_i$ forment une k-base de L ; or ils sont en nombre np .

Proposition : si $[K : k] < \infty$, tout k-endomorphisme σ de K dans lui-même est un automorphisme.

Démonstration :

1) σ est injectif puisque c'est un homomorphisme de corps ;

2) σ est surjectif, car σ est une application k-linéaire injective d'un espace vectoriel K de dimension finie dans lui-même, ce qui nous permet de conclure que σ est bijectif.

Soient k et K deux corps commutatifs avec $k \subset K$; K est alors un espace vectoriel sur le corps k .

Soit $x \in K$, et considérons le sous-corps engendré par x et k, c'est-à-dire (par définition) le plus petit sous-corps contenant x et k : c'est l'intersection de tous les sous-corps de K qui contiennent x et k. On le notera $k\langle x \rangle$.

Etude du corps $k\langle x \rangle$.

Soit P un élément de $k[X]$; faisons-lui correspondre sa valeur en x : l'application $P \longmapsto P(x)$ est une application f_x de $k[X]$ dans K. C'est un homomorphisme d'anneaux, et en même temps une application k-linéaire.

$f_x : k[X] \to K$ est l'unique homomorphisme d'anneaux qui envoie X sur x et laisse fixes les éléments de k.

L'image de $k[X]$ sera un sous-anneau de K qui contient k et x, et est contenu dans $k\langle x \rangle$.

Etudions le noyau $\operatorname{Ker} f_x$, qui est un idéal de $k[X]$.

1er cas - $\operatorname{Ker} f_x = \{0\}$. Alors on peut identifier $k[X]$ à un sous-anneau de K, puisque f_x est une injection : $P(x) = 0 \iff P = 0$.

Introduisons le corps des fractions de l'anneau intègre $k[X]$: c'est le corps des fractions rationnelles à coefficients dans k, qu'on note $k(X)$.

Alors f_x se prolonge d'une seule manière en un homomorphisme $g_x : k(X) \to K$. En effet, soient $P \in k[X]$, $Q \in k[X]$, $Q \neq 0 \Rightarrow \frac{P}{Q} \in k(X)$; posons $g_x\left(\frac{P}{Q}\right) = \frac{f_x(P)}{f_x(Q)} = \frac{P(x)}{Q(x)}$; ceci a un sens puisque $Q(x) \neq 0$, f_x étant injectif. Il reste à vérifier que si $\frac{P}{Q} = \frac{R}{S}$, on a $\frac{P(x)}{Q(x)} = \frac{R(x)}{S(x)}$. Or $\frac{P}{Q} = \frac{R}{S} \iff PS = QR$ $\Rightarrow f_x(PS) = f_x(QR)$, soit $f_x(P)\, f_x(S) = f_x(Q)\, f_x(R)$, puisque f_x est un homomorphisme. Ceci s'écrit encore $P(x)\, S(x) = Q(x)\, R(x)$, soit $\frac{P(x)}{Q(x)} = \frac{R(x)}{S(x)}$

C.Q.F.D.

On vérifie enfin facilement que g_x est un homomorphisme. g_x étant un homomorphisme de corps, c'est une injection, et par conséquent g_x identifie $k(X)$ à un sous-corps de K qui est le sous-corps engendre par x et k.

Résumé et définition : Lorsque l'application $f_x : k[X] \to K$ qui, à P, fait correspondre $P(x)$, est injective; elle se prolonge d'une seule manière en un homomorphisme injectif $g_x : k(X) \to K$ dont l'image est le sous-corps $k < x >$: on dit alors que x est transcendant sur k.

Définition : un élément x de K est transcendant sur le sous-corps k de K si le sous-corps qu'il engendre s'identifie à $k(X)$.

2ème cas - $\boxed{\text{Ker } f_x \neq \{0\}}$. Alors Ker f_x étant un idéal d'un anneau $k[X]$ principal, il est principal. De plus, on sait que tout polynôme est équivalent à un polynôme unitaire. Donc il existe un unique polynôme unitaire $P \in k[X]$ tel que Ker $f_x = (P)$.

Par passage au quotient, f_x induit un homomorphisme injectif de $k[X]_{/(P)}$ dans K. Puisque $k[X]_{/(P)}$ se plonge dans un corps, c'est un sous-anneau d'un corps et par conséquent il est intègre. On en déduit que (P) est un idéal premier de $k[X]$, et donc que P est un polynôme irréductible de $k[X]$. On sait alors que (P) est un idéal maximal et par conséquent que $k[X]_{/(P)}$ est un corps.

L'image de l'homomorphisme f_x est un sous-corps de K qui contient x, c'est $k < x>$ qui est isomorphe à $k[X]_{/(P)}$.

Rappel : si P est irréductible, l'anneau $k[X]_{/(P)}$ est un corps ; ou encore, si $k[X]_{/(P)}$ est intègre, c'est un corps. Démonstration : $k[X]_{/(P)}$ est un anneau A qui est aussi un espace vectoriel de dimension finie sur le corps k.

Soit donc $a \in k[X]/_{(P)}$, $a \neq 0$ et $b \in k[X]/_{(P)}$. Considérons l'application $b \longrightarrow ab$ de A dans A qui est k- linéaire. C'est une application k-linéaire de A dans lui-même ; elle est injective puisque A est intègre ; elle est donc bijective, et par conséquent 1_A appartient à l'image : $\exists\ b \in k[X]/_{(P)}$ tel que $1_A = ab$. Donc a est inversible, et $A = k[X]/_{(P)}$ est bien un corps.

Rappel : soit k un corps commutatif. Une k-algèbre A est un anneau et aussi un espace vectoriel dans lequel l'addition est k-linéaire :

$\lambda \in k \Longrightarrow \lambda a + \lambda b = \lambda (a + b)$, et la multiplication est telle que

$\lambda \in k \Longrightarrow (\lambda a)b = \lambda(ab)$ et $a(\lambda b) = \lambda(ab)$. Il en résulte alors que l'application b $b \longrightarrow ab$ est k-linéaire (c'est ce qui nous a servi dans la démonstration précédente).

Toute k-algèbre intègre de dimension finie sur k est un corps.

Résumé et définition : si $\mathrm{Ker}\ i_x \neq 0$, (P) est l'idéal des polynômes dont la valeur en x est nulle :

$Q(x) = 0 \Longleftrightarrow$ Q est un multiple de P $\Longrightarrow$ $\begin{cases} Q = 0 \text{ ou} \\ \deg Q \geqslant \deg P \end{cases}$

Si en outre Q est un polynôme unitaire, alors deg Q = deg P $\Longrightarrow$ Q = P, donc P est le polynôme unitaire de plus petit degré qui s'annule en x.

Définition : on dit alors que x est algébrique sur le corps k. P est le polynôme minimal de x : c'est le polynôme unitaire de plus petit degré tel que P(x) = 0. Tous les polynômes Q tels que Q(x) = 0 sont alors des multiples de P. P est un polynôme irréductible de k[X], et on a un isomorphisme g_x entre $k\langle x\rangle$ et $k[X]/_{(P)}$.

Conséquences :

1] $[k\langle x\rangle : k] = \dim_k k[X]/_{(P)} = \deg P = p$

2] Tout élément de $k[X]/_{(P)}$ a un représentant et un seul qui est une combinaison linéaire de 1, X, X^2, ...X^{p-1} à coefficients dans k. Les coefficients de cette combinaison sont déterminés de façon unique.

c] Tout élément de k $\langle x \rangle$ s'écrit d'une seule manière comme une combinaison linéaire $\sum_{i=0}^{p-1} \lambda_i x^i$, avec $\lambda_i \in k$.

A retenir :

degré du corps engendre par x algébrique = degré du poly. minimal de x.

Exercice :

Calculons l'inverse de x dans k $\langle x \rangle$;

$P\langle x \rangle = x^p + a_1 x^{p-1} + \ldots + a_p = 0$, avec $a_i \in k$ et $a_p \neq 0$ (sinon P ne serait pas irréductible)

D'où $x(x^{p-1} + a_1 x^{p-2} + \ldots + a_{p-1}) = -a_p$

Soit $(-a_p)^{-1}$ l'inverse de $(-a_p)$ dans k $\langle x \rangle$; alors

$x(x^{p-1} + a_1 x^{p-2} + \ldots + a_{p-1})(-a_p)^{-1} = 1$. Donc l'inverse de x dans k$\langle x \rangle$ est $(-a_p)^{-1}(x^{p-1} + a_1 x^{p-2} + \ldots + a_{p-1})$.

Applications :

1 - Soit k un corps commutatif donné et soit P un polynome irréductible de k[X].

Proposition :

Il existe un surcorps K de k qui contient un élément x de K tel que le polynôme minimal de x soit P. Si de plus K est engendré par x et par k, alors K est k- isomorphe à $k[X]/_{(P)}$.

Démonstration :

a] Existence : il suffit de prendre $K = k[X]/_{(P)}$ et de prendre x égal à la classe de X.

b] Unicité : si K est une solution et si K est engendré par x et k, on sait qu'on a unique injection de $k[X]/_{(P)}$ dans K qui envoie la classe de X sur x ; cette injection est un isomorphisme si K est engendré par x et k.

Terminologie :

Le corps dont la proposition précédente affirme l'existence, et qui est unique à un k-isomorphisme près, s'appelle le corps obtenu par adjonction à k d'une racine du polynôme irréductible $P(X)$.

2 - Exemples :

a] $k = \mathbb{R}$, $P(X) = X^2 + 1$.

Si on adjoint à $\mathbb{R}$ une racine de $P(X)$, on obtient le corps

$\mathbb{C} = \mathbb{R}(X)/(X^2 + 1)$; la classe de X est souvent notée i.

On a dim $\mathbb{C}$ = deg $(X^2 + 1) = 2$; tout élément de C s'écrit sous la forme a + bi, avec $a \in \mathbb{R}$, $b \in \mathbb{R}$.

b] $k = \mathbb{F}_p$, $P(X) = X^2 + 1$. Existe-t-il $n \in \mathbb{F}_p$ tel que $x^2 + 1 = 0$, i.e. $x^2 = -1$; ou encore -1 est-il reste quadratique modulo p ?

- si $p \neq -1 \pmod 4$, alors $P(X)$ n'est pas irréductible dans $\mathbb{F}_p(X)$;
- si $p = -1 \pmod 4$, alors $P(X) = X^2 + 1$ est irréductible sur $\mathbb{F}_p(X)$.

On considère alors $\mathbb{F}_p(X)/(X^2 + 1)$; on pourra encore noter i la classe de X. Le corps obtenu sera de dimension 2 sur $\mathbb{F}_p$, et tout élément s'écrira a + bi, $a \in \mathbb{F}_p$, $b \in \mathbb{F}_p$: on trouve un corps à p^2 éléments.

c] $k = \mathbb{Q}$, $P(X) = X^4 - 2$. On montrera que $P(X)$ est irréductible sur $\mathbb{Q}[X]$. Si on adjoint à $\mathbb{Q}$ une racine de $X^4 - 2$, on obtient un nouveau corps K dont tout élément s'écrit sous la forme $a + b\alpha + c\alpha^2 + d\alpha^3$, avec $a, b, c, d \in \mathbb{Q}$, $\alpha^4 = 2$. Le degré de K sur $\mathbb{Q}$ est 4. On définit un $\mathbb{Q}$-homomorphisme de K dans $\mathbb{R}$ en envoyant α sur $\sqrt{2} \in \mathbb{R}$. Dans K, on a

$X^4 - 2 = (X - \alpha)(X + \alpha)(X^2 + \alpha^2)$, et $X^2 + \alpha^2$ est irréductible dans $K[X]$, car il l'est dans $\mathbb{R}[X]$.

Autre problème :

Soit K le corps par adjonction à k d'une racine d'un polynôme irréductible $P \in k[X]$. Soit K' un corps muni d'un homomorphisme $\varphi : k \longrightarrow K'$.

On cherche les k-homomorphismes de K dans K', c'est-à-dire les homomorphismes qui prolongent φ :

Supposons le problème résolu : considérons un homomorphisme $\Phi : K \longrightarrow K'$ qui prolonge φ. $\Phi : k[X]/_{(P)} \longrightarrow K'$; Φ provient donc d'un homomorphisme Ψ de $k[X]$ dans K' qui est tel que $\Psi(P) = 0$, et qui prolonge φ. Or soit $Q(X) \in k[X]$, $Q(X) = a_0 + a_1X + \ldots + a_kX^k$; on doit avoir $\Psi(a_0 + a_1X + \ldots + a_kX^k) = \varphi(a_0) + \varphi(a_1)\,\Psi(X) + \ldots + \varphi(a_k)\,\Psi(X^k)$ puisque les $a_i \in k$; Ψ étant un homomorphisme, on a $\Psi(X^j) = [\Psi(X)]^j$.

Donc $\Psi(a_0 + a_1X + \ldots + a_kX^k) = \varphi(a_0) + \varphi(a_1)\,\Psi(X) + \ldots + \varphi(a_k)\,[\Psi(X)]^k$.

Donc pour déterminer Ψ il suffit de connaître $\Psi(X) = x$; la donnée d'un élément x de K' déterminera ainsi Ψ. Mais il faut exprimer que $\Psi(P) = 0$.

Or posons $Q^{\varphi}(x) = \varphi(a_0) + \varphi(a_1)X + \ldots + \varphi(a_k)X^k$. On aura $\Psi(Q) = Q^{\varphi}(x)$, et la condition cherchée est $\Psi(P) = P^{\varphi}(x) = 0$.

Conclusion :

Les homomorphismes $\Psi : k[X] \longrightarrow K'$ cherchés qui prolongent φ sont en correspondance bijective avec les racines (dans K') du polynôme P^{φ} transformé du polynôme P par l'homomorphisme φ.

Cas particulier :

Si $k \subset K$ et $k \subset K'$, alors $Q^{\varphi} = Q$; donc ce qui détermine Ψ, c'est la donnée d'une racine $x \in K'$ du polynôme $P(X)$.

Conséquence :

Une condition nécessaire et suffisante pour que Ψ existe est que le polynôme P admette au moins une racine dans K'.

Soit toujours K obtenu par adjonction à k d'une racine de P irréductible sur k[X]. On a alors $[K : k] = \deg P < \infty$; cherchons les k-automorphismes de K. Nous savons que tout k-endomorphisme de K est un k-automorphisme de K, puisque le degré de l'extension est fini. Or ce qui détermine un k-endomorphisme de K, c'est la donnée d'une racine de P dans K. Choisissons $\alpha \in K$ tel que $P(\alpha) = 0$; alors, pour toute racine $\beta \in K$ du polynôme P, il existe un unique k-automorphisme $\sigma : K \longrightarrow K$ tel que $\sigma(\alpha) = \beta$, et on obtient ainsi tous les k-automorphismes de K. Ils forment un groupe, dont l'ordre est égal au nombre des racines distinctes du polynôme P dans le corps K.

Cas particulier connu :

Soit $\mathbb{C}$ le corps obtenu par adjonction au corps $\mathbb{R}$ d'une racine du polynôme $P = X^2 + 1$. Dans $\mathbb{C}[X]$, $X^2 + 1 = (X + i)(X - i)$.

Prenons $\alpha = i$; alors il existe un seul automorphisme qui envoie i en i : c'est l'identité ; et il existe un seul automorphisme σ qui envoie i sur -i : c'est la conjugaison.

Définition :

Soit K une extension de k ($k \subset K$) ; K est algébrique sur k si et seulement si tout élément de K est algébrique sur k.

Proposition (condition suffisante pour qu'une extension soit algébrique) :

Si le degré d'une extension K sur k est fini, alors K est algébrique sur k. (La réciproque est fausse).

Démonstration :

1ère méthode : soit $x \in K$, et soit $k\langle x\rangle$ le sous-corps de K engendré par x et k

on a : $[K : k] = [K : k\langle x\rangle] \times [k\langle x\rangle : k]$

($k\langle x\rangle$ est un sous-k-espace vectoriel de K)

$\Longrightarrow$ $[k\langle x\rangle : k]$ (divise) $[K : k]$ qui est fini

$\Longrightarrow$ $[k\langle x\rangle : k]$ est fini

$\Longleftrightarrow$ x est algébrique.

2ème méthode : posons $d = \dim_K k\langle x\rangle = [k\langle x\rangle : k]$.

Considérons $1, x, \ldots x^d$ (ce sont des éléments de $k\langle x\rangle$) :

on a $(d + 1)$ éléments d'un espace vectoriel de dimension d, ils sont donc linéairement dépendants.

$\Longleftrightarrow$ $\exists$ une relation linéaire à coefficients dans k entre $1, \ldots x^d$;

$\Longleftrightarrow$ $\exists$ un polynôme de degré d non identiquement nul dont x est racine ;

$\Longleftrightarrow$ x est algébrique.

Corollaire :

Si x est algébrique sur k $\Longrightarrow$ $k\langle x\rangle$ est algébrique sur k.

dém : x algébrique sur k $\Longrightarrow$ $[k\langle x\rangle : k]$ est fini.

Théorème important :

Soit k une extension algébrique de k. Alors tout k-endomorphisme de K est un k-automorphisme.

remarque : si $[K : k] < \infty$, on a déjà établi le résultat.

dém : - soit σ un k-endomorphisme de K.

σ est injectif (c'est un endormorphisme de corps)

Il reste à montrer que σ est surjectif ($\Longleftrightarrow \forall x \in K, \Longrightarrow x \in \mathrm{Im}\sigma$)

- soit $P(X) \in k[X]$ le polynôme minimal de x (il est bien défini puisque x est algébrique sur k) ; il est irréductible.

soit $(x_i)_{i \in I}$ l'ensemble des racines distinctes de P dans K (il a au moins une racine dans K, à savoir x ; x est l'un des x_i).

Alors $\sigma(x_i) = x_j$ (d'après ce qui précède).

et σ induit donc une application de l'ensemble E des racines dans lui-même.

or σ est injective et card E est fini, puisque card E $\leq$ n = deg P.

σ est donc bijective.

En particulier x (x $\in$ E) est dans l'image de K, ce qu'on voulait montrer.

Notation et définition.

On note G(K, k) le groupe des k-automorphismes de K lorsque K est algébrique sur k.

C'est le groupe de Galois de K sur k.

Exemple : $G(\mathbb{C}, \mathbb{R}) = \{\text{identité, conjugaison}\}$.

Problème :

Soit k donné, et P $\in$ k [X] irréductible ou non. On veut construire K, extension de k, telle que :

1° P se décompose en un produit de polynômes du premier degré à coefficients dans K (on dit alors que P a toutes ses racines dans K) ;

2° K soit engendré par k et les racines de P. On dira qu'un tel K est obtenu par adjonction à k de toutes les racines de P.

Théorème fondamental :

Un tel K existe.

De plus : $\begin{cases} [K : k] < +\infty \\ K \text{ est unique à un k-isomorphisme près.} \end{cases}$

1° existence :

On va raisonner par récurrence sur le degré de P ; la récurrence portera sur tous les corps k possibles.

Soit n = deg P

* $n = 1$.

k est donné, et P est un polynôme du 1er degré à coefficients dans k.

Alors il suffit de prendre comme extension $K = k$.

* Supposons la proposition vraie pour un corps k quelconque et pour deg $P < n$ $(n \geqslant 2)$.

Soit maintenant deg $P = n$.

- 1er cas : P est réductible dans k.

Alors $P = P_1 P_2$, P_1 et $P_2 \in k[X]$, deg $P_1 < n$ et deg $P_2 < n$. On peut appliquer l'hypothèse de récurrence à P_1 et k :

soit k_1 une extension de k telle que P_1 se décompose dans k_1 et que k_1 soit engendré par k et les racines de P_1. Appliquons la encore à P_2 et k_1 : soit k_2 une extension de k_1 telle que P_2 se décompose dans k_2 et que k_2 soit engendré par k_1 et les racines de P_2.

Alors on a trouvé une extension de k, à savoir k_2, telle que :

$$\begin{cases} P \text{ se décompose dans } k_2 ; \\ k_2 \text{ est engendré par k et les racines de P.} \end{cases}$$

- 2è cas : P est irréductible dans k.

On sait qu'on peut trouver une extension k_1 de k telle que :

$$\begin{cases} P \text{ a au moins une racine } \alpha \in k_1 \\ k_1 \text{ est engendré par k et } \alpha. \end{cases}$$

Alors P a au moins un facteur du 1 er degré dans k_1 <==> il est réductible dans k_1, et on est ramené au cas précédent.

2° $[K : k] < +\infty$

On suppose donc que K est une extension de k, telle que P se décompose dans K,

que K soit engendré par k et les racines de P.

Soient $x_1 \ldots x_n$ les racines distinctes de P (dans K)

et soient : $k_1 = k\langle x_1\rangle$

$k_2 = k_1\langle x_2\rangle$

$k_n = K = k_{n-1}\langle x_n\rangle$.

On n'est pas sûr que ces corps soient tous distincts, mais peu importe.

On a alors une suite $k_1 \subset k_2 \ldots \subset k_n = K$ de corps emboîtés (distincts ou non) et telle que $[k_{i+1} : k_i]$ soit fini.

En effet $k_{i+1} \equiv k_i\langle x_{i+1}\rangle$, et x_{i+1} est racine d'un polynôme non identiquement nul de $k[X]$ (donc de $k_i[X]$)

$\Longleftrightarrow$ x_{i+1} est algébrique sur k_i

$\Longrightarrow$ $[k_{i+1} = k_i\langle x_{i+1}\rangle : k_i]$ est fini

Mais $[K: k] = \prod_{i=0}^{n-1} [k_{i+1} : k_i]$, donc $[K : k]$ est fini.

3° unicité à un k-isomorphisme près.

- Soient 2 solutions K et K' ; cherchons à définir un k-homomorphisme de K dans K'.

* On a l'injection $i : k \longrightarrow K'$, et on va chercher à la prolonger en un homomorphisme $\varphi_1 : k_1 \longrightarrow K'$; on sait que cela est possible si et seulement Q, le polynôme minimal de x_1 sur k, a une racine dans K'.

* Or $P(x_1) = 0$ puisque $x_1 \in \{x_i\}_{i \in I}$; donc $Q \mid P$ dans $k[X]$, et a fortiori dans $K'[X]$, or P est un produit de facteurs du premier degré dans $K'[X]$. Donc Q est un produit de facteurs du 1er degré dans $K'[X]$, et comme son degré n'est pas nul, il a moins une racine dans K', qui définira l'homomorphisme φ_1 cherché.

* En faisant le même raisonnement, on prolongera φ_1 en un homomorphisme φ_2 de k_2 dans K'.

De proche en proche, on obtiendra un homomorphisme φ de K dans K' qui prolongera i,

Ce sera un k-homomorphisme de K dans K'.

- De même, on obtiendrait un k-homomorphisme τ de K' dans K. Alors $\tau \circ \varphi$ est un k-endomorphisme de K, soit σ ; or $[K : k]$ est fini, donc σ est un k-automorphisme ; de même on montre que $\varphi \circ \tau = s$ est un k-automorphisme

Donc : φ et τ sont des k-isomorphismes et par suite K et K' sont k-isomorphes.

C.Q.F.D.

Exemple :

- soit $k = \mathbb{Q}$, et $P(X) = X^4 - 2$.

P est irréductible sur $\mathbb{Q}$: en effet si P(X) était égal à un produit $P_1(X)\ P_2(X)$ à coefficients dans $\mathbb{Q}$ (deg $P_1 > 0$, deg $P_2 > 0$), cette décomposition serait valable dans $\mathbb{R}$ [X]. Or dans $\mathbb{R}[X]$ les facteurs irréductibles de $X^4 - 2$ sont $X - 2^{\frac{1}{4}}$, $X + 2^{\frac{1}{4}}$ et $X^2 + \sqrt{2}$; l'un des facteurs P_1 ou P_2 devrait être l'un de ces 3 polynômes ; or aucun n'est à coefficients dans $\mathbb{Q}$.

Soit $k_1 \supset \mathbb{Q}$ le corps obtenu par adjonction d'une racine α du polynôme irréductible $X^4 - 2$.

Je dis que k_1 est $\mathbb{Q}$-isomorphe à un sous-corps de $\mathbb{R}$. En effet k_1 est une extension de $\mathbb{Q}$, $\mathbb{R}$ aussi, et on sait qu'il existe un $\mathbb{Q}$-homomorphisme φ de k_1 dans $\mathbb{R}$ si et seulement si P a une racine dans $\mathbb{R}$. Or P a une racine dans $\mathbb{R}$, par exemple $\sqrt[4]{2}$.

Donc φ existe, et comme il est injectif, il identifie k_1 à un sous-corps de $\mathbb{R}$.

On a $k_1 = \mathbb{Q}(\sqrt[4]{2})$, avec $[k_1 : \mathbb{Q}] \times \deg P = 4$.

Dans $k_1[X]$, on peut écrire $P(X) = (X - \alpha)\ (X + \alpha)\ (X^2 + \alpha^2)$. Mais le polynôme $X^2 + \alpha^2$ est irréductible dans $\mathbb{R}$, et comme k_1 est un sous-corps de $\mathbb{R}$, il est a fortiori irréductible dans k_1.

Il va donc falloir adjoindre $i\alpha$ ou $-i\alpha$ à k_1, pour obtenir un corps k_2 dans lequel se décompose.

Pour cela, il suffit d'adjoindre à k_1 une racine de $X^2 + 1$, c'est-à-dire $\pm i$.

On obtiendra alors K qui sera le corps cherché avec $[K : k_1] = 2$ = degré du polynô

$X^2 + 1$, donc $[K : k] = 4.2 = 8$.

Définition.

On se donne k et $P \in k[X]$;

Le corps obtenu en adjoignant à k les racines de P s'appelle le corps de décomposition de P sur k.

Il est unique à un k-isomorphisme près.

Problème plus général : théorème de Steinitz.

- Soit k un corps, on cherche s'il existe une estension K de k telle que :

1° tout polynôme à coefficients (dans k) se décompose dans K[X] en produit de polynômes du 1er degré.

2° K soit engendré par k et toutes les racines de tous les polynômes.

(c'est-à-dire que K soit algébrique sur k).

- On démontre (et c'est le théorème de Steinitz) que ce problème a une solution K, et que 2 solutions sont k-isomorphes. De plus, si K est un tel corps, on montre que tout polynôme K[X] se décompose dans K[X] en produit de facteurs du 1er degré. On dit que K est algébriquement clos.

K s'appelle la clôture algébrique de k (unique à un k-isomophisme près).

Par exemple, le théorème de d'Alembert exprime que $\mathbb{C}$ est la clôture algébrique de $\mathbb{R}$.

Cas particulier : corps de décomposition du polynôme $P \in k[X] = X^n - 1$

- Les racines de P dans ce corps de décomposition s'appellent les racines $n^{\text{ièmes}}$ de l'unité. On prend pour k le corps $\mathbb{Q}$ ou l'un des corps $\mathbb{F}_p$ (p premier).

On cherche donc le corps de décomposition du polynôme $X^n - 1$ sur le corps $\mathbb{Q}$ ou $\mathbb{F}_p$.

On l'appelle le corps des racines $n^{\text{ièmes}}$ de l'unité.

- Supposons que la caractéristique soit un nombre premier p.

Ecrivons : $n = p^k n'$, avec $(n', p) = 1$;

on a : $X^n - 1 = (X^{n'} - 1)^{p^k}$.

En effet :

$(X^{n'} - 1)^{p^k} = (X^{n'})^{p^k} - 1 = X^{n'p^k} - 1 = X^n - 1$,

et les racines de $X^n - 1$ sont celles de $X^{n'} - 1$.

On obtiendra donc le corps cherché par adjonction à $\mathbb{F}_p$ des racines de $X^{n'} - 1$.

Désormais on supposera que p ne divise pas n, lorsque la caractéristique p est $\neq 0$.

* Rappel sur la notion d'ordre de multiplicité :

Soit $P \in k[X]$; α racine de $P \iff P(\alpha) = 0$

α racine simple de $P \iff P(\alpha) = 0$ et $P'(\alpha) \neq 0$.

* Dans le corps des racines $n^{\text{ièmes}}$ de l'unité, $X^n - 1$ se décompose en un produit de facteurs du 1er degré ; je dis que les racines de $X^n - 1$ sont toutes simples.

Il suffit de montrer que la dérivée de $(X^n - 1)$ ne s'annule pour aucune des racines. Or si $P(X) = X^n - 1$, on a :

$P'(X) = n.X^{n-1}$.

Soit α une racine de P; montrons que $n.\alpha^{n-1} \neq 0$;

En effet :

- $\alpha^{n-1} \neq 0$, sinon on n'aurait pas $\alpha^n = 1$
- . si le corps est de caractéristique 0 : $n \geqslant 1 \Longrightarrow n \neq 0$

  . s'il est de caractéristique p : on a supposé que p ne divise pas n, c'est-à-dire : n n'estpas multiple de p, donc $n \neq 0$ dans le corps.

Donc dans les 2 cas $n\alpha^{n-1} \neq 0$ (car un corps est un anneau intègre).

Et par suite : dans le corps considéré, chaque racine a est simple.

Donc il y a n racines distinctes.

Notion de racine primitive.

Dans le cas de la caractéristique 0, le corps considéré est engendré par $\mathbb{Q}$ et les racines $n^{\text{ièmes}}$ de l'unité. Il est isomorphe au sous-corps de $\mathbb{C}$ engendré par $\mathbb{Q}$ et $e^{2i\Pi/n}$ (toutes les racines $n^{\text{ièmes}}$ de 1 sont des puissances

de celle-là).

Soit α une racine de $X^n - 1$; considérons la suite des puissances

$\alpha, \alpha^2, \ldots, \alpha^n = 1$.

α est primitive $\Leftrightarrow$ ces puissances sont toutes distinctes ;

$\Leftrightarrow$ n est le plus petit entier $d > 0 / \alpha^d = 1$.

i $\alpha = e^{2ik\frac{\Pi}{n}}$ il faut et il suffit que $k^d = 0 \pmod n$ entraîne $d \equiv 0 \pmod n$,

c'est-à-dire que k soit premier à n.

Il y a donc $\varphi(n)$ racines primitives de l'unité , où $\varphi(n)$ désigne le nombre des entiers de la suite $(1, 2, \ldots, n)$ qui sont premiers à n.

En caractéristique $p \neq 0$, on dira encore qu'une racine $n^{\text{ièmes}}$ de l'unité α est primitive si les puissances $\alpha, \alpha^2, \ldots, \alpha^n$ sont distinctes. Mais il n'est pas évident qu'il existe des racines primitives. On va le prouver tout à l'heure.

Calcul de $\varphi(n)$ (appelé indicateur d'Euler) :

On montre (exercice) que si $(n_1, n_2) = 1$, on a $\varphi(n_1 n_2) = \varphi(n_1)\,\varphi(n_2)$.

Si p est premier, $\varphi(p) = p - 1$.

Si $n = p^\alpha$, on a $\varphi(n) = p^{\alpha - 1}(p - 1)$.

Si $n = \prod_i (p_i)^{\alpha_i}$ $(\alpha_i \geqslant 1)$, on a $\varphi(n) = n \prod_i \frac{p_i - 1}{p_i}$.

Problème :

Y a t-il des racines primitives $n^{\text{ièmes}}$ de l'unité en caractéristique $p \neq 0$?

Polynômes cyclotomiques.

- Choisissons une caractéristique fixée : 0 ou p.

Pour cette valeur, considérons l'ensemble des racines primitives de $X^n - 1$, soit $\{\alpha_i\}$ (il peut être vide a priori).

On définit $P_n(X) = \Pi(X - \alpha_i)$; (c'est le polynôme unitaire qui a pour racines simples toutes les racines primitives de $X^n - 1$.

Et si $\{\alpha_i\} = \emptyset$, alors $P_n(X) = 1$

- Si α est tel que $\alpha^n = 1$, on considère le plus petit entier $d \geqslant 1$ tel que $\alpha^d = 1$. C'est l'ordre de α dans le groupe multiplicatif des éléments non nuls

du corps. Alors d divise n (ordre d'un sous-groupe d'un groupe fini).

Et toute racine $n^{ième}$ de l'unité a un ordre qui divise n.

On remarque que les racines primitives sont celles dont l'ordre est n.

- Pour chaque d qui divise n, on considère les racines dont l'ordre est d, qui sont, par définition, les racines de $P_d(X)$.

En groupant ainsi les racines en paquets, on aura

$$\boxed{X^n - 1 = \Pi_{d|n} P_d(X)}$$

- Cette formule va permettre de calculer explicitement les polynômes P_d, et de montrer qu'ils sont tous à coefficients entiers.

. on a : $P_1(X) = X - 1$ (1est la racine primitive unième de l'unité)

. et $X^2 - 1 = P_1(X) \cdot P_2(X) \Longrightarrow P_2(X) = X + 1$

(-1 est racine carrée primitive de l'unité, et c'est la seule).

. supposons qu'on connaisse les P_d pour $d|n$ et $d<n$.

Alors $X^n - 1 = (\Pi_{d<n} P_d(X)) \cdot P_n(X)$

où $\Pi_{d<n} P_d(X)$ est connu (hypothèse de récurrence); on aura donc P_n par un quotient ; et de plus, par récurrence, on montre que les coefficients de $P_d(X)$ sont entiers (si on est en caractéristique 0 on sait seulement a priori, que ces coefficients sont rationnels).

- Ces formules sont valables en toute caractéristique (pourvu que p ne divise pas n

Alors, comme P_n s'écrit de la même façon en caractéristique p ou 0, et que deg $P_n = \varphi(n)$ en caractéristique 0, on en conclut.:

deg $P_n = \varphi(n)$ pour toute caractéristique

Alors : deg $P_n \neq 0$; donc il y a des racines primitives $n^{ièmes}$ de l'unité.

Définition :

P_n est le polynôme cyclotomique relatif à l'entier n.

Calcul de P_n pour les premiers entiers.

. $P_1(X) = X - 1$

. $P_2(X) = X + 1$

. P_3 ? $\quad X^3 - 1 = P_1 P_3$

$\Longrightarrow P_3(X) = X^2 + X + 1$

. P_4 ? $\quad X^4 - 1 = P_1 P_2 P_4 \Longrightarrow P_4(X) = X^2 + 1$

. P_5 ?

D'une manière générale, si n est 1er : $X^n - 1 = P_1(X) \cdot P_n(X)$

d'où $P_n(X) = \dfrac{X^n - 1}{X - 1}$;

$\Longrightarrow P_5(X) = X^4 + X^3 + X^2 + X + 1$

. P_6 ?

$X^6 - 1 = P_1 P_2 P_3 P_6 \quad \Longrightarrow X^3 + 1 = P_2 P_6$

et $P_1 P_3 = X^3 - 1$

Or $P_2 = X + 1$, donc $P_6(X) = X^2 - X + 1$

. P_7 ?

$P_7(X) = X^6 + X^5 + X^4 + X^3 + X^2 + X + 1$

. $P_{12}(X) = X^4 - X^2 - 1$ (exercice)

Calcul de $\varphi(n) = \deg P_n$

- On décompose n en produit de facteurs premiers.

$n = p_1^{\alpha_1} \ldots p_k^{\alpha_k} \qquad \alpha_1 \geqslant 1, \ldots, \alpha_k \geqslant 1$

Alors : $\varphi(n) = n\left(1 - \dfrac{1}{p_1}\right) \ldots \left(1 - \dfrac{1}{p_k}\right)$

(Exercice !)

- Exemple : n = 12, $12 = 2^2 \cdot 3$, et $\varphi(12) = 12(1 - 1/2)(1 - 1/3) = 4$.

Résumé :

En toute caractéristique p, pourvu que p ne divise pas n, P_n possède dans le corps de décomposition de $X^n - 1$, $\varphi(n)$ racines simples ; ce sont les racines primitives de $X^n - 1$.

Problème : P_n est-il irréductible ?

Soit K le corps obtenu (à partir de $\mathbb{Q}$ ou $\mathbb{F}_p$) par adjonction de toutes les racines de $X^n - 1$.

- Supposons que P_n soit irréductible.

Alors le corps K s'obtient par adjonction à $\mathbb{Q}$ ou $\mathbb{F}_p$ d'une racine α de P_n (en effet, le corps ainsi obtenu contiendra toutes les puissances de α, donc toutes les racines $n^{\text{ièmes}}$ de l'unité puisque α est primitive). Alors $[K : \mathbb{Q}]$, ou $[K : \mathbb{F}_p] = \deg P_n = \varphi(n)$.

- Si P_n n'est pas irréductible, soit Φ un facteur irréductible de P_n.

Alors K est obtenu par adjonction à $\mathbb{Q}$ ou $\mathbb{F}_p$ d'une racine de Φ, d'où :

$[K : \mathbb{Q} \text{ ou } \mathbb{F}_p] = \deg \Phi$.

Le membre de gauche ne dépend pas de Φ, donc celui de droite non plus ; donc :

Tous les facteurs irréductibles de P_n ont le même degré $d = [K : \mathbb{Q} \text{ ou } \mathbb{F}_p]$ et d est un diviseur de $\varphi(n)$.

Théorème d'Eisenstein. (sans démonstration)

En caractéristique 0 (c'est-à-dire sur $\mathbb{Q}$), $P_n(X)$ est irréductible.

Exemple :

Si p est premier : $P_p(X) = X^{p-1} + X^{p-2} + \dots X + 1$ est irréductible sur

Remarque :

Au contraire, en caractéristique p, P_n peut être réductible. On en verra des exemples.

CORPS FINIS (toujours commutatifs).

Exemple : $\mathbb{F}_p$, où p est premier, est un corps fini.

Recherche du cardinal.

Soit K un corps fini.

Il ne peut être de caractéristique 0 (sinon il contiendrait un sous-corps isomorphe à $\mathbb{Q}$ qui est infini).

Sa caractéristique est donc p premier, et par suite K est une extension de $\mathbb{F}_p$. Alors on sait que K est un espace vectoriel sur $\mathbb{F}_p$. Puisqu'il est fini, il est de dimension finie.

Posons : $[K : \mathbb{F}_p] = d$ (c'est un entier)

Alors, tout élément de K sera une combinaison linéaire de d éléments, et chaque coefficient (ils sont au nombre de d) pourra prendre p valeurs.

Donc :

$$\text{card } K = p^d \text{ (une puissance de la caractéristique)}$$

Théorème 1 :

Soit p premier et soit d un entier arbitraire ≥ 1.

Alors, il existe un corps ayant p^d éléments ; en outre, deux corps ayant p^d éléments sont isomorphes.

Dém :

c'est un théorème d'existence et d'unicité. On démontre d'abord l'unicité pour avoir des informations.

1° - unicité (à un isomorphisme près).

- Soit K un corps à p^d éléments ; ses éléments non nuls forment un groupe multiplicatif K* à $p^d - 1$ éléments.

Soit $x \in K^*$; alors $x^{p^d - 1} = 1$, donc $x^{p^d} = x$.

Mais ceci est aussi vrai pour $x = 0$.

D'où $\forall x \in K : x^{p^d} = x$.

- Considérons lepolynôme de degré p^d à coefficients dans $\mathbb{F}_p$: $X^{p^d} - X$; il a p^d racines dans le corps, et ce sont tous les éléments du corps (c'est un exemple de polynôme à coefficients dans un corps fini, qui est nul pour toutes les valeurs de la variable, mais non identiquement nul). A fortiori, K est engendré par ces racines ; donc K est le corps de décompocition de ce polynôme ; il est donc défini à un isomorphisme près.

2° - existence.

- Soit K le corps de décomposition du polynôme $P(X) = X^{p^d} - X$ sur $\mathbb{F}_p$ (on sait qu'un tel K existe). Montrons que card $K = p^d$.

a) les racines de P sont toutes simples.

En effet calculons $P'(X) = p^d X^{p^d-1} - 1$;

mais $p^d = 0$ en caractéristique p,

donc $P'(X) = -1$ pour toutes les valeurs de la variable, et en particulier pour les racines.

Il y a donc p^d racines distinctes de P dans K.

b) il reste à montrer que K ne contient aucun autre élément que les racines (ou encore que l'ensemble de ces racines est un sous-corps, puisque K est le plus petit corps contenant les racines).

Soit E l'ensemble des racines de P;

soient x et $y \in E$ (c'est-à-dire $x^{p^d} = x$ et $y^{p^d} = y$)

calculons :

$$(x - y)^{p^d} = x^{p^d} - y^{p^d} \quad \text{(en caractéristique p)}$$

$$= x - y \text{ , d'où } x - y \in E.$$

$$(xy)^{p^d} = x^{p^d} y^{p^d} = xy, \text{ d'où } xy \in E.$$

Ainsi E est un sous-anneau. Enfin, si $x \in E$ et $x \neq 0$,

on a $x^{-1} \in E$, car :

$$(x^{-1})^{p^d} = x^{-p^d} = (x^{p^d})^{-1} = x^{-1}$$

E est donc un sous-corps de K, etpar suite E = K : le corps de décomposition de P est l'ensemble de ses racines : il a donc p^d éléments.

Notation : Pour tout entier q de la forme p^d (p premier, d entier $\geqslant 1$), on notera $\mathbb{F}_q$ le corps à q éléments. Cette notation est en accord avec la notation $\mathbb{F}_p$.

Théorème :

Le groupe multiplicatif $\mathbb{F}_q^*$ est cyclique (c'est-à-dire engendré par par un de ses éléments.)

Démonstration :

$\mathbb{F}_q^*$ se compose des racines (toutes distinctes) de $X^{q-1} - 1$. Mais on sait qu'il existe une racine primitive $(q-1)^{\text{ième}}$ de l'unité, soit α.

Ce qui s'écrit :

$\exists\, \alpha \in \mathbb{F}_q^* / \alpha, \alpha^2, \ldots, \alpha^{q-1} = 1$ soient toutes distinctes (c'est-à-dire ces puissances donnent une fois et une seule tous les éléments non nuls du corps).

Il y a $\varphi(q-1)$ éléments tels que α.

Application au cas d = 1 ($\Longleftrightarrow$ p = q).

Le groupe multiplicatif $\mathbb{F}_p^*$ des entiers non nuls modulo p est cyclique.

Ce qui s'écrit :

$\exists\, \alpha \in \mathbb{F}_p^* / \alpha, \alpha^2, \ldots, \alpha^{p-1} = 1$ soient des éléments distincts.

α est une racine primitive du polynôme $X^{p-1} - 1$, dont ~~toutes~~ les racines sont exactement les éléments de $\mathbb{F}_p^*$.

Exemple : p = 5

Les éléments non nuls de $\mathbb{F}_5$ sont $\pm 1, \pm 2$.

+ 1 et - 1 ne sont pas des racines primitives $4^{\text{ièmes}}$ de l'unité car

$1^2 = (-1)^2 = 1$

. mais $\alpha = \pm 2 \Longleftrightarrow \alpha^2 = -1 \Longrightarrow \alpha^3 = \pm 2 \Longrightarrow \alpha^4 = 1$, donc + 2 et - 2 sont primiti

Tous les entiers non nuls modulo 5 s'écrivent d'une seule manière comme puissances de ± 2.

Remarque :

Soit p premier impair.

. on a vu : α est carré dans $\mathbb{F}_p^* \Longleftrightarrow \alpha^{\frac{p-1}{2}} = 1$

. mais si α est primitive, alors $\alpha^{\frac{p-1}{2}} = -1$ (puisque p-1 est le plus entier $d > 0$ tel que $\alpha^d = 1$), donc dans ce cas, α n'est pas reste quadratique modulo p.

. cette condition n'est pas suffisante ; il existe des éléments qui sont non reste quadratiques modulo p tout en n'étant pas racines primitives $(p-1)^{\text{ièmes}}$ de l'unité

Théorème de Wilson : $(p-1)! \equiv -1 \ (p)$

C'est un conséquence du fait que $\mathbb{F}_p^*$ est cyclique.

En effet :

Considérons tous les éléments de $\mathbb{F}_p^*$; ils s'écrivent, pour un α convenablement choisi, $\alpha, \alpha^2, \ldots, \alpha^{p-1} = 1$

Leur produit s'écrit : $\alpha^{1+2+\ldots+p-1} = \alpha^{\frac{p(p-1)}{2}}$

. supposons d'abord p impair ; alors $\frac{p-1}{2}$ est entier, donc $\alpha^{\frac{p(p-1)}{2}} = \left(\alpha^{\frac{p-1}{2}}\right)^p$.

Mais α est primitive, donc $\alpha^{\frac{p-1}{2}} = -1$,

d'où $\alpha^{\frac{p(p-1)}{2}} = (-1)^p = -1$ puisque p est impair.

D'autre part, le produit des éléments de $\mathbb{F}_p^*$ peut aussi s'écrire $1.2. \ldots (p-1)$.

On a donc :

$$(p-1)! \equiv -1 \ (p).$$

. cette formule est aussi vraie pour $p = 2$ puisqu'elle s'écrit $1! = 1 \equiv -1 \ (2)$

. d'où le Théorème de Wilson.

Retour à $\mathbb{F}_q$ pour $q = p^d$

* Première interprétation de d et résultats.

Soit α un générateur du groupe multiplicatif $\mathbb{F}_q^*$. (ou encore une racine primitive $(q-1)^e$ de l'unité)

Alors $\mathbb{F}_q^* = \{\alpha, \alpha^2, \ldots, \alpha^{q-1} = 1\}$.

$\mathbb{F}_q$ est engendré par $\mathbb{F}_p$ et α, et de plus $[\mathbb{F}_q : \mathbb{F}_p] = d$.

Mais d est aussi le degré du polynôme minimal de α, qui est un facteur irréductible du polynôme cyclomotique $P_{q-1}(X)$, de degré $\varphi(q-1)$. On voit que tous les facteurs irréductibles de P_{q-1} sont de même degré d, et que d est un diviseur de $\varphi(q-1)$.

* Deuxième interprétation de d comme cardinal du groupe de Galois $G(\mathbb{F}_q, \mathbb{F}_p)$.

On va chercher les automorphismes du corps $\mathbb{F}_q$ (ce sont en fait des $\mathbb{F}_p$-automorphismes de $\mathbb{F}_q$).

Puisque $\mathbb{F}_q$ s'obtient par adjonction à $\mathbb{F}_p$ d'une racine α d'un polynôme irréductible Q, alors il y a une correspondance bijective entre les automorphismes cherchés et les racines du polynôme Q (dont on adjoint une racine) dans $\mathbb{F}_q$. Cette correspondance associe à chaque automorphisme σ la racine $\beta = \sigma(\alpha)$ du polynôme Q.

Il y a alors autant d'automorphismes de $\mathbb{F}_q$ que de racines du polynôme Q.

Mais les racines de Q sont aussi racines du polynôme cyclomotique P_{q-1} ; elles sont donc distinctes.

D'autre part d est le degré de Q, et par suite Q a d racines distinctes dans $\mathbb{F}_q^*$.

D'où le résultat : il y a d automorphismes de $\mathbb{F}_q$, c'est-à-dire :

$$\boxed{\text{Card } G(\mathbb{F}_q, \mathbb{F}_p) = d}$$

* Détermination du groupe de Galois $G(\mathbb{F}_q, \mathbb{F}_p)$. Il est cyclique.

. on va exhiber d automorphismes distincts de $\mathbb{F}_q$: on aura ainsi trouvé les éléments de G.

. l'application σ de $\mathbb{F}_q$ dans $\mathbb{F}_q$ définie par : $x \xrightarrow{\sigma} x^p$ est un endomorphisme du corps $\mathbb{F}_q$.

En effet, pour x et $y \in \mathbb{F}_q$ on a : $x^p + y^p = (x+y)^p$

$$x^p \cdot y^p = (xy)^p$$

D'autre part, $\mathbb{F}_q$ est un espace vectoriel de dimension d finie sur $\mathbb{F}_p$,

et σ est injective en tant qu'homomorphisme de corps, c'est donc un automorphisme de $\mathbb{F}_q$.

. considérons $\sigma^2 = \sigma \circ \sigma$, application de $\mathbb{F}_q$ dans $\mathbb{F}_q$ définie par :

$x \longrightarrow \sigma^2(x) = (x^p)^p = x^{p^2}$.

C'est aussi un automorphisme de $\mathbb{F}_q$.

On obtient ainsi σ, σ^2, ..., σ^k, ..., $\sigma^d = id$ comme automorphismes de $\mathbb{F}_q$ ($\sigma^d = id$ puisque $\forall x \in \mathbb{F}_q \Rightarrow x^{p^d} = x$)

. ces automorphismes sont tous distincts.

En effet, supposons qu'ils ne le soient pas.

Alors, $\exists k_1$ et $k_2 < d$ / $\sigma^{k_1} = \sigma^{k_2}$

$\Longleftrightarrow \exists k < d$ / $\sigma^k = y$

$\Longleftrightarrow \exists k < d$ / $x \in \mathbb{F}_q : \sigma^k(x) = x^{p^k} = x$

et le polynôme $X^{p^k} - X$ aurait p^d racines distinctes ce qui est impossible (il en a au plus p^k).

. on a ainsi trouvé d automorphismes de $\mathbb{F}_q$, à savoir σ, σ^2,...,$\sigma^d = id$. Chacun d'eux est une puissance de l'un d'entre eux σ, automorphisme "élévation à la puissance p", et il n'y en a pas d'autres.

Le groupe $G(\mathbb{F}_q, \mathbb{F}_p)$ est donc cyclique d'ordre d, engendré par l'automorphisme $x \longrightarrow x^p$.

* Détermination des racines d'unfacteur irréductible Q de P_{q-1}.

Soit Q un facteur irréductible (sur $\mathbb{F}_p$) du polynôme cyclotomique P_{q-1}. Son degré est d.

Soit α une racine de Q (α est une racine primitive $(q-1)^{ième}$ de l'unit

Les autres racines de Q sont des éléments de $\mathbb{F}_q$, donc ce sont des puissances de α.

D'autre part, on sait que tout élément du groupe de Galois transforme α en une racine du même polynôme Q. Donc α, α^p, α^{p^2}, ..., $\alpha^{p^{d-1}}$ ($\alpha^{p^d} = \alpha$) sont des

racines distinctes de Q.

Mais Q est de degré d, il a donc au plus d racines distinctes. Donc :

Les d racines de Q sont α, α^p, ..., $\alpha^{p^{d-1}}$.

Exemple : p = 3, d = 2.

- on étudie $\mathbb{F}_9$, dont le groupe multiplicatif a 8 éléments, les racines $8^{\text{ièmes}}$ de l'unité.

- $P_8(X) = X^4 + 1$, P_8 est le polynôme cyclotomique relatif à l'entier 8, ses racines sont les racines primitives $8^{\text{ièmes}}$ de l'unité.

d = 2 est le degré de tout facteur irreductible de P_8. On a, en fait :

$X^4 + 1 = (X^2 + X - 1)(X^2 - X - 1)$

en effet $(X^2 + X - 1)(X^2 - X - 1) = (X^2 - 1)^2 - X^2 = X^4 - 3X^2 + 1$

avec $-3X^2 = 0$ dans $\mathbb{F}_3$.

Choisissons $Q(X) = X^2 - X - 1$.

$\mathbb{F}_9$ est obtenu en adjoignant à $\mathbb{F}_3$ une racine de ce polynôme irréductible, soit α.

Puisque $[\mathbb{F}_9 : \mathbb{F}_3] = \deg Q = d = 2$, on va pouvoir écrire tous les éléments de $\mathbb{F}_9$ comme combinaisons linéaires de 1 et α à coefficients dans $\mathbb{F}_3$, et cela d'une manière unique.

$\Longleftrightarrow \forall z \in \mathbb{F}_9$, $z = x\alpha + y$, avec x et y $\in \mathbb{F}_3$ (x et y = 0 ou $\pm$ 1)

Mais on sait que d'autre part, tout élément de $\mathbb{F}_9^*$ peut s'écrire d'une seule façon comme puissance de α.

Etablissons la correspondance entre les 2 écritures. Il vient :

$\alpha = \alpha$

$\alpha^2 = \alpha + 1$

$\alpha^3 = \alpha^2 + \alpha = 2\alpha + 1 = -\alpha + 1$

$\alpha^4 = -\alpha^2 + \alpha = -1$ (α racine de Q est racine de P_8)

$\alpha^5 = -\alpha$

$\alpha^6 = -\alpha - 1$

$\alpha^7 = \alpha - 1$

$\alpha^8 = 1$

On a ainsi tous les éléments de $\mathbb{F}_9^*$.

L'autre racine de Q est l'image de α par l'élément de $G(\mathbb{F}_9 : \mathbb{F}_3)$ (card G = d = 2) qui n'est pas l'identité, à savoir $\alpha^p = \alpha^3$.

SYMBOLE DE LEGENDRE.

Loi de Réciprocité Quadratique.

Définition :

Soit p premier impair. Soit n un entier quelconque.

On appelle symbole de Legendre et on note $(\frac{n}{p})$:

$$(\frac{n}{p}) = n^{\frac{p-1}{2}} \pmod p$$

. $n \equiv 0 \ (p)$, $(\frac{0}{p}) = 0$

. $n \not\equiv 0 \ (p)$ $\begin{cases} (\frac{n}{p}) = +1 & \text{si n est reste quadratique (mod p)} \\ (\frac{n}{p}) = -1 & \text{si n est non reste quadratique (mod p)} \end{cases}$

Propriétés :

$$(\frac{nn'}{p}) = (\frac{n}{p})\,(\frac{n'}{p}).$$

Par décomposition de n en facteurs premiers, le calcul de $(\frac{n}{p})$ est ramené au problème suivant :

Problème :

Calculer $(\frac{q}{p})$ pour q premier $\neq$ p.

On l'a déjà calculé pour q = 2 :

$$(\frac{2}{p}) = (-1)^{\frac{p^2-1}{8}} = \begin{cases} +1 & \text{si } p \equiv \pm 1 \pmod 8 \\ -1 & \text{si } p \equiv \pm 3 \pmod 8 \end{cases}$$

Théorème : Loi de réciprocité de Gauss.

Soient p et q deux entiers premiers impairs distincts. On a

$$\boxed{\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}} \left(\frac{p}{q}\right)}$$

Ce théorème sera prouvé plus loin.

Remarque : la loi de réciprocité s'énonce encore comme suit :

$\left(\frac{p}{q}\right) = \left(\frac{q}{p}\right)$ si p ou q est congru à 1 (mod 4) ;

$\left(\frac{p}{q}\right) = -\left(\frac{q}{p}\right)$ si p et q sont congrus à -1 (mod 4).

Calcul de $\left(\frac{n}{p}\right)$, à l'aide de la loi de réciprocité.

Il suffit de regarder les n tels que $-\frac{p}{2} < n < \frac{p}{2}$

On doit donc calculer $\left(\frac{\pm n}{p}\right)$ pour $0 < n < \frac{p}{2}$

$\left(\frac{-n}{p}\right) = \left(\frac{-1}{p}\right)\left(\frac{n}{p}\right) = (-1)^{\frac{p-1}{2}}\left(\frac{n}{p}\right)$. On est donc ramené au cas où $n>0$.

Par décomposition de n en facteurs premiers, on est ramené à calculer $\left(\frac{q}{p}\right)$ pour q premier impair $< p$ (et même $< \frac{p}{2}$), puisqu'on connaît déjà $\left(\frac{2}{p}\right)$. Par la loi de réciprocité :

$$\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}}\left(\frac{p}{q}\right),$$

et on est ramené au problème initial, à cela près que p a été remplacé par $q < \frac{p}{2}$. On recommence avec q le même processus, et on obtient ainsi le principe d'un calcul de $\left(\frac{n}{p}\right)$ par récurrence sur p.

Exemple : $\left(\frac{23}{17}\right) = \left(\frac{6}{17}\right) = \left(\frac{2}{17}\right)\left(\frac{3}{17}\right) = \left(\frac{3}{17}\right)$

$$\left(\frac{3}{17}\right) = \left(\frac{17}{3}\right) = \left(\frac{2}{3}\right) = -1$$

donc $\left(\frac{23}{17}\right) = -1$.

Quelques cas particuliers :

(1) $\left(\frac{-3}{p}\right) = (-1)^{\frac{p-1}{2}} \left(\frac{3}{p}\right) = \left(\frac{p}{3}\right) = \begin{cases} 1 \text{ si } p \equiv 1 \pmod 3 \\ -1 \text{ si } p \equiv -1 \pmod 3 \end{cases}$

$\left(\frac{5}{p}\right) = \left(\frac{p}{5}\right)$; or $\left(\frac{\pm 1}{5}\right) = 1$, $\left(\frac{\pm 2}{5}\right) = -1$, d'où

(2) $\left(\frac{5}{p}\right) = \begin{cases} 1 \text{ si } & p \equiv \pm 1 \pmod 5 \\ -1 \text{ si } & p \equiv \pm 2 \pmod 5 \end{cases}$

Démonstration de la loi de réciprocité.

On adjoint au corps $\mathbb{F}_p$ les racines du polynôme $X^q - 1$. Soit K le corps obtenu ; K est un corps fini.

On fait tous les calculs dans K. Il y a dans K des racines primitives $\varphi(q)$. On en prend une α. Toutes les racines sont les puissances de α ; $\alpha, \alpha^2, \ldots, \alpha^q = 1$.

Soit $x \in \mathbb{F}_q$; on peut définir α^x, puisque α^k ne dépend que de la classe $k \pmod q$.

On pose $\boxed{y = \sum_{x \in \mathbb{F}_q} \left(\frac{x}{q}\right) \alpha^x}$ (On fait les calculs dans K, α^0 n'y figure pas en réalité, car son coefficient est $\left(\frac{0}{q}\right) = 0$.

$$y^2 = \left(\sum_{b \in \mathbb{F}_q} \left(\frac{x}{q}\right) \alpha^x\right)\left(\sum_{x' \in \mathbb{F}_q} \left(\frac{x'}{q}\right) \alpha^{x'}\right) = \sum_{x,x'} \left(\frac{xx'}{q}\right) \alpha^{x+x'}$$

Faisons le changement de variable $\begin{cases} x = x \\ x + x' = t \end{cases}$

$$y^2 = \sum_{t \in \mathbb{F}_q} \sum_{x \in \mathbb{F}_q} \left(\frac{x(t-x)}{q}\right) \alpha^t$$

$$y^2 = \sum_{t \in \mathbb{F}_q} c_t \alpha^t \quad , \quad c_t = \sum_{x \in \mathbb{F}_q} \left(\frac{x(t-x)}{q}\right)$$

$x = 0 \Longrightarrow \left(\frac{x(t-x)}{q}\right) = 0$. Donc $c_t = \sum_{x \in \mathbb{F}_q^*} \left(\frac{x(t-x)}{q}\right)$

Cas $t = 0$.

$$c_0 = \sum_{x \in \mathbb{F}_q^*} \left(\frac{-x^2}{q}\right)$$

$$\left(\frac{-x^2}{q}\right) = \left(\frac{-1}{q}\right)\left(\frac{x^2}{q}\right) = \left(\frac{-1}{q}\right) = (-1)^{\frac{q-1}{2}}$$

$$\Longrightarrow c_0 = (-1)^{(q-1)/2}(q-1).$$

Cas $t \neq 0$.

$$c_t = \sum_{x \in \mathbb{F}_q^*} \left(\frac{x(t-x)}{q}\right)$$

$$\left(\frac{x(t-x)}{q}\right) = \left(\frac{-x^2\left(1-\frac{t}{x}\right)}{q}\right) = \left(\frac{-x^2}{q}\right)\left(\frac{1-\frac{t}{x}}{q}\right)$$

$$= (-1)^{\frac{q-1}{2}}\left(\frac{1-\frac{t}{x}}{q}\right)$$

$$c_t = (-1)^{\frac{q-1}{2}} \sum_{x \in \mathbb{F}_q^*} \left(\frac{1-\frac{t}{x}}{q}\right) .$$

Lorsque x parcourt $\mathbb{F}_q^*$, il en est de même de $\frac{1}{x}$, donc de $\frac{t}{x}$, car $t \neq 0$ a un inverse dans $\mathbb{F}_q^*$. Donc $1 - \frac{t}{x}$ parcourt l'ensemble $\mathbb{F}_q - \{1\}$, et on a :

$$c_t = (-1)^{(q-1)/2} \sum_{z \in \mathbb{F}_q - \{1\}} \left(\frac{z}{q}\right) = (-1)^{\frac{q-1}{2}} \left[\sum_{z \in \mathbb{F}_q} \left(\frac{z}{q}\right) - \left(\frac{1}{q}\right) \right]$$

$\sum_{z \in \mathbb{F}_q} \left(\frac{z}{q}\right) = 0$, car il y a $\frac{q-1}{2}$ fois $(+1)$ et $\frac{q-1}{2}$ fois (-1).

$$\Longrightarrow c_t = (-1)^{\frac{q-1}{2}}(-1). \quad \text{Ainsi :}$$

$$y^2 = (-1)^{\frac{q-1}{2}} \left[(q-1) + \sum_{t \in \mathbb{F}_q^*} (-1)\ \alpha^t \right]$$

$$y^2 = (-1)^{\frac{q-1}{2}} \left[q - \sum_{t \in \mathbb{F}_q} \alpha^t \right]$$

$\sum_{t \in \mathbb{F}_q} \alpha^t = 0$, car la somme des racines de $X^q - 1$ est nulle. D'où

(1) $$\boxed{y^2 = (-1)^{\frac{q-1}{2}} q}$$ dans le corps K.

De plus $y^p = \sum_{x \in \mathbb{F}_q} \left(\frac{x}{q}\right) \alpha^{px}$, car $\left(\frac{x}{q}\right)^p = \left(\frac{x}{q}\right)$, puisque $u^p = u$ pour tout $u \in \mathbb{F}_q$

$$\left(\frac{p}{q}\right) y^p = \sum_{x \in \mathbb{F}_q} \left(\frac{px}{q}\right) \alpha^{px} = \sum_{x \in \mathbb{F}_q} \left(\frac{x}{q}\right) \alpha^x = y \quad \text{(car quand x parcourt } \mathbb{F}_q\text{, p x aussi).}$$

Comme $y \neq 0$, on conclut

(2) $$\boxed{\left(\frac{p}{q}\right) y^{p-1} = 1}$$

Or $(p-1)$ est pair, donc

$y^{p-1} = [y^2]^{\frac{p-1}{2}}$. Ainsi (2) et (1) donnent :

$$1 = (\frac{p}{q})\ (y^2)^{\frac{p-1}{2}} = (\frac{p}{q})\ (-1)^{\frac{q-1}{2}\frac{p-1}{2}}\ q^{\frac{p-1}{2}}.$$

Or $q^{\frac{p-1}{2}} = (\frac{q}{p})$ d'après la définition du symbole de Legendre.

Finalement :

$$1 = (-1)^{\frac{p-1}{2}\frac{q-1}{2}}\ (\frac{p}{q})\ (\frac{q}{p}) \quad . \quad \text{C.Q.F.D.}$$

Corollaire.

$$(\frac{-q}{p}) = (-1)^{\frac{p-1}{2}\frac{q+1}{2}}\ (\frac{p}{q}) .$$

En effet $(\frac{-q}{p}) = (\frac{-1}{p})\ (\frac{q}{p}) = (-1)^{\frac{p-1}{2}}\ (-1)^{\frac{p-1}{2}\frac{q-1}{2}}\ (\frac{p}{q})$

$$= (-1)^{\frac{p-1}{2}\frac{q+1}{2}}\ (\frac{p}{q}) .$$

REPARTITION des NOMBRES PREMIERS dans les ENTIERS.

Proposition 1.

$\forall n > 0$, il existe $n-1$ entiers consécutifs dont aucun n'est premier .

Démonstration.

On considère la suite des entiers $n! + 2$, $n! + 3, \ldots, n! + n$. Il y en a $n-1$. Aucun de ces nombres n'est premier, puisqu'ils sont successivement divisibles par 2, 3,..., n.

Problème.

Existe-t-il des entiers n arbitrairement grands tels que $(2n-1)$ et $(2n+1)$ soient premiers ?

Ce problème n'est pas résolu.

Notation I.

Soit p_n le n-ième nombre premier (dans l'ordre croissant) ; par exemple, $p_1 = 2$, $p_2 = 3$, $p_3 = 5$.

$\forall k$, $\exists n$ tel que $p_{n+1} - p_n \geq k$.

Notation II.

Pour n entier on pose : $\pi(x) = \text{Card}\ \{p \mid p \leq x,\ p \text{ premier}\}$.

Exemple : $x = 10$, $\pi(10) = 4$.

Quand $x \longrightarrow \infty$, $\frac{\pi(x)}{x}$ tend vers 0. Ce résultat est une conséquence du "grand théorème des nombres premiers" :

Théorème.

$$\lim_{x \to \infty} \frac{\pi(x) \log x}{x} = 1.$$

Nous ne prouverons pas ce théorème difficile. Il a été démontré en 1896 par Hadamard et par de la Vallée-Poussin par des méthodes analytiques ; puis plus tard par des mét des dites "élémentaires", mais compliquées.

Exercice : Prouver que l'assertion du théorème équivaut à $\lim_{x \to \infty} \frac{p_n}{n \log n} = 1$.

Exercice : Soit k un nombre réel > 1. Prouver que pour tout entier n assez gran il existe au moins un nombre premier p tel que $n < p \leq k\,n$. [On admettra le grand théorème des nombres premiers]. En fait, pour $k = 2$, et pour tout entier $n \geq 1$, existe un nombre premier p tel que $n < p \leq 2n$. (Voir Hardy and Wright, p. 343, th. 418).

Sur les questions relatives à la répartition des nombres premiers, on pourra cons ter le petit livre :

A. Blanchard, Initiation à la théorie analytique des nombres premiers (Dunod 196

Désormais, on va se borner à étudier la :

Répartition des nombres premiers dans les progressions arithmétiques.

Voici le problème dont il s'agit : soient a et m deux entiers > 0 ($m \geq 2$). C veut savoir si la progression arithmétique formée des entiers $\equiv a \pmod m$ contient des nombres premiers.

Si a et m ne sont pas premiers entre eux, autrement dit si le p.g.c.d. $(a, m) > 1$, tout nombre premier $p \equiv a \pmod m$ est divisible par (a, m) ; par sui si (a, m) n'est pas premier, il n'y a aucun tel p, et si (a, m) est premier, c'e l'unique p premier qui soit $\equiv a \pmod m$. Le seul cas intéressant est donc celui o a et m sont premiers entre eux, c'est-à-dire $(a,m) = 1$. On se propose de démontrer loin le

Théorème de Dirichlet. Si $(a, m) = 1$, il existe une infinité de nombres premiers c à a modulo m.

On démontrera même un théorème plus précis (dû à Dirichlet), mais que nous ne sommes pas encore capables d'énoncer.

Remarque : L'entier m étant donné, le nombre des progressions arithmétiques formées d'entiers premiers à m est $\varphi(m)$ (nombre des entiers ≥ 1 et $\leq m$ qui sont premiers à m). En effet, les progressions arithmétiques de raison m ne sont autres que les éléments de $\mathbb{Z} / m\,\mathbb{Z}$ (anneau des entiers modulo m), et celles dont les éléments sont premiers à m correspondent aux éléments de $\mathbb{Z}/m\,\mathbb{Z}$ qui sont inversibles pour la multiplication. Ces éléments forment un groupe (abélien), noté G(m).

1er exemple : Etude des congruences modulo 3.

On va prouver le ;

Théorème : Il existe une infinité de p premiers $\equiv -1 \pmod 3$, et une infinité de p premiers $\equiv +1 \pmod 3$.

Démonstration.

Commençons par les $p \equiv -1 \pmod 3$. Pour tout entier $x \geq 1$, $3x - 1$ possède au moins un facteur premier $\equiv -1 \pmod 3$. En effet, tout facteur premier de $3x - 1$ est $\equiv \pm 1 \pmod 3$, et comme $3x - 1 \equiv -1 \pmod 3$ il n'est pas possible que tous les facteurs premiers soient $\equiv 1 \pmod 3$.

ontrons qu'il y a une infinité p premiers $\equiv -1 \pmod 3$. En effet, quelle que soit a suite finie de nombres premiers $p_1, \ldots, p_n$, tous $\equiv -1 \pmod 3$, posons $= p_1, \ldots, p_n$; alors $3x - 1$ admet au moins un facteur premier $p \equiv -1 \pmod 3$; un el p est nécessairement $\neq p_1, p_2, \ldots, p_n$.

s où $p \equiv 1 \pmod 3$.

utilise les restes quadratiques.

mme : Si un entier x est $\not\equiv 0 \pmod 3$ tous les facteurs premiers de $x^2 + 3$ sont 1 (mod 3).

nonstration.

t p un facteur premier de $x^2 + 3$; -3 est reste quadratique (mod p). Or) = $(\frac{p}{3})$; donc $(\frac{p}{3}) = 1$, c'est-à-dire $p \equiv 1 \pmod 3$. C.Q.F.D.

Si maintenant $p_1, \ldots, p_n$ sont premiers et $\equiv 1 \pmod 3$, posons $x = p_1, \ldots, p_n$;

alors $x^2 + 3$ possède un facteur premier $p \equiv 1 \pmod 3$, et p est distinct de $p_1, \ldots, p_n$, sinon p déviserait 3, ce qui est absurde.

2ème exemple : Etude des congruences (mod 4).

Théorème : Il existe une infinité de p premiers $\equiv -1 \pmod 4$.

Démonstration.

Si x est un entier ≥ 1, $4x - 1$ possède au moins un facteur premier $p \equiv -1 \pmod 4$.

En effet, les facteurs premiers de $4x - 1$ sont tous $\equiv \pm 1 \pmod 4$, et s'ils étaient tous $\equiv +1 \pmod 4$, leur produit $4x - 1$ serait $\equiv 1 \pmod 4$, ce qui est absurde. Si maintenant $p_1, \ldots, p_n$ sont premiers et $\equiv -1 \pmod 4$, soit x le produit $p_1, \ldots, p_n$; sont facteur premier p de $4x - 1$ est distinct de $p_1, \ldots, p_n$. Donc il existe bien une infinité de nombres premiers $\equiv -1 \pmod 4$.

Théorème. Il existe une infinité de p premiers $\equiv 1 \pmod 4$. Pour la démonstration on utilise le

Lemme : Pour tout entier $x \geq 1$, tous les facteurs premiers de $4x^2 + 1$ sont $\equiv 1 \pmod 4$.

Car si $4x^2 + 1 \equiv 0 \pmod p$, -1 est reste quadratique $\pmod p$, et l'on sait que ceci équivaut à $p \equiv 1 \pmod 4$. De là on déduit, toujours par le même procédé, l'existence d'une infinité de nombres premiers $\equiv 1 \pmod 4$.

Cas général.

Le cas général des $p \equiv a \pmod m$, avec $(a, m) = 1$, ne se laisse pas traiter par des méthodes aussi simples. On va avoir besoin d'utiliser la théorie des fonctions analytiques d'une variable complexe.

.../...

FONCTIONS ANALYTIQUES d'une VARIABLE COMPLEXE.

Ce qui suit est un résumé de notions et de résultats, pour lesquels le lecteur est renvoyé aux traités classiques.

I- Séries entières.

Définition 1.

On appelle série formelle une expression $\sum_{n \geq 0} a_n X^n$, où X est une lettre, et les coefficients $a_n \in \mathbb{C}$. Soit $r \geq 0$; considérons $\sum_{n \geq 0} |a_n| r^n$, série à termes ≥ 0. on considère l'ensemble des $r \geq 0$ pour lesquels cette série est convergente. Il est non vide, car il contient $r = 0$. Soit ρ la borne supérieure de ces r. Le cas où $\rho = 0$ ou $\rho = \infty$ n'est pas exclu.

Si ρ est fini, il n'est pas toujours vrai que $\sum_{n \geq 0} |a_n| \rho^n$ soit finie. Le nombre ρ s'appelle le rayon de convergence de la série $\sum a_n X^n$.

Définition 2.

On dit que la série est "convergente" si $\rho \neq 0$. On peut alors remplacer la lettre X par un nombre complexe x, pourvu que $|x| < \rho$. On pose $f(x) = \sum_{n \geq 0} a_n x^n$; c'est la somme d'une série absolument convergente; $x \longmapsto f(x)$ est une fonction continue à l'intérieur du disque de convergence, c'est-à-dire pour $|x| < \rho$. Elle est dérivable au sens complexe, i.e. : pour $|x| < \rho$,

$$\lim_{\substack{h \to 0 \\ h \in \mathbb{C}-\{0\}}} \frac{f(x+h) - f(x)}{h} \quad \text{existe.}$$

Cette limite est notée $f'(x)$.

De plus $f'(x) = \sum_{n \geq 0} n a_n x^{n-1}$.

Le rayon de convergence de la série formelle $\sum n a_n X^{n-1}$ ("série dérivée") est le même que celui de la série initiale. On peut appliquer ceci à la série dérivée, et recommencer. Par suite, f est indéfiniment dérivable au sens complexe. A chaque fois, on dérive terme à terme. La dérivée n-ième est donnée par

$f^{(n)}(x) = n!\, a_n + x(\ldots)$, d'où $f^{(n)}(0) = n!\, a_n$.

Ainsi $a_n = \frac{1}{n!} f^{(n)}(0)$.

Proposition 1.

Les séries convergentes forment un anneau.

(N.B. chacune d'elles a un rayon de convergence > 0, qui dépend de cette série).

Notations.

$\mathbb{C}[X]$: Anneau des polynômes à une indéterminée X ;

$\mathbb{C}[[X]]$: Anneau des séries entières formelles ;

$\mathbb{C}\{X\}$: Anneau des séries convergentes ; c'est un sous-anneau de $\mathbb{C}[[X]]$.

Proposition 2.

Ce sont des anneaux intègres.

C'est bien connu dans le cas de l'anneau des polynômes. Pour l'anneau $\mathbb{C}[[X]]$ des séries formelles, on introduit l'ordre d'une série formelle $\sum a_n X^n$ non identiquement nulle : c'est le plus petit n tel que $a_n \neq 0$; et on montre que l'ordre du produit de deux séries formelles non identiquement nulles est la somme de leurs ordres (donc le produit n'est pas identiquement nul). Enfin, l'anneau $\mathbb{C}\{X\}$, sous-anneau de l'anneau intègre $\mathbb{C}[[X]]$, est intègre.

Remarque. Ces anneaux sont en réalité des algèbres sur le corps $\mathbb{C}$.

Proposition 3.

Un élément de l'anneau $\mathbb{C}[[X]]$, resp. $\mathbb{C}\{X\}$, est inversible si et seulement si le coefficient a_0 est non nul. Les éléments non inversibles forment un idéal de l'anneau. Ce sont les séries pour lesquelles $a_0 = 0$.

Corollaire.

$\mathbb{C}[[X]]$ est $\mathbb{C}\{X\}$ sont des anneaux locaux (i.e. les éléments inversibles forment un idéal ; c'est l'unique idéal maximal).

Soit $f(X)$ une série convergente non identiquement nulle ; on a $f(X) = a_p X^p + \ldots$, $a_p \neq 0$. Donc $f(X) = X^p g(X)$, où $g(X)$ est un élément inversible de l'anneau.

Proposition 4.

Les idéaux de l'anneau $\mathbb{C}\{X\}$ sont les idéaux (X^p) (même énoncé pour $\mathbb{C}[[X]]$).

Démonstration.

Soit I un idéal autre que 0 ; considérons le plus petit des ordres p des $f \in I$ qui ne sont pas nulles. On voit tout de suite que $I = (X^p)$.

Corollaire.

Il y a un seul idéal premier ; c'est l'idéal maximal (X).

Exemples de séries entières.

1) $e^x = \exp(x) = \sum_{n \geq 0} \frac{x^n}{n!}$. Son rayon de convergence est infini.

$\frac{d}{dx} e^x = \sum_{n \geq 0} \frac{x^{n-1}}{(n-1)!} = e^x$

$e^x e^y = e^{x+y}$. En effet :

$$\left(\sum_{p \geq 0} \frac{x^p}{p!}\right)\left(\sum_{q \geq 0} \frac{y^q}{q!}\right) = \sum_{n \geq 0}\left(\sum_{p+q=n} \frac{x^p y^q}{p!q!}\right) = \sum_{n \geq 0} \frac{(x+y)^n}{n!}.$$

2/ Fonction logarithmique : $x \in \mathbb{C}$ étant donné, cherchons les $y \in \mathbb{C}$ tels que $e^y = x$. On a nécessairement $x \neq 0$, car $e^y \cdot e^{-y} = 1$, donc $e^y \neq 0$.

Posons $y = y' + i\,y''$, $y' \in \mathbb{R}$, $y'' \in \mathbb{R}$, $x = e^y = e^{y'} e^{iy''}$. Pour $y'' \in \mathbb{R}$, on a $|e^{iy''}| = 1$; y'' est l'une des valeurs de l'argument de $e^{iy''}$. Ainsi :

$|x| = e^{y'}$, $\arg x = y'' + 2k\pi$ $(k \in \mathbb{Z})$.

On pose donc $\boxed{\log x = \log |x| + i \arg x}$, fonction qui a une infinité de déterminations, puisque $\arg x$ n'est défini que modulo 2π. On va voir maintenant que dans certains cas on peut choisir une de ces déterminations.

Par exemple, si x varie dans le demi-plan $\mathrm{Re}(x) > 0$, il existe une détermination de $\arg x$ telle que $-\frac{\pi}{2} < \arg x < \frac{\pi}{2}$; il lui correspond une détermination de $\log x$, appelée la détermination principale pour $\mathrm{Re}(x) > 0$.

Ceci vaut en particulier lorsque $x = 1 + u$, avec $|u| < 1$. En fait, le détermination principale $\log(1+u)$ est la somme d'une série entière :

$$\log(1+u) = u - \frac{u^2}{2} + \ldots + (-1)^{n+1} \frac{u^n}{n} + \ldots$$

dont le rayon de convergence est 1.

Pour u réel ce développement s'obtient en intégrant

$$\frac{1}{1+u} = 1 - u + u^2 + \ldots + (-1)^n u^n + \ldots .$$

Il faut vérifier que $\begin{cases} e^{\log(1+u)} = 1 + u & \text{pour } |u| < 1, \\ \log e^u = u & \text{pour } u \text{ assez voisin de } 0. \end{cases}$

C'est une question de calcul formel ; comme on sait que c'est vrai pour u réel, c'est que le calcul formel réussit, donc c'est aussi vrai pour u complexe.

II- Fonctions analytiques.

Soit U un ouvert du plan $\mathbb{C}$ de la variable complexe, et soit x_0 un point de U. Considérons un disque ouvert $|x - x_0| < r$ contenu dans U. Soit f une fonction définie dans U, à valeurs complexes. Considérons sa restriction au disque $|x-x_0| < r$.

Définition 1.

On dit que la restriction de f est développable en série entière dans le disque, s'il existe une série entière $\sum_{u \geq 0} a_n X^n$ dont le rayon de convergence soit au moins r, et telle que :

$$f(x) = \sum_{n \geq 0} a_n (x - x_0)^n \qquad \text{pour } |x - x_0| < r.$$

Alors f est continue pour $|x - x_0| < r$, et est même indéfiniment dérivable au sens complexe.

Définition 2.

Soit f une fonction à valeurs complexes. f est analytique dans l'ouvert $U \subset \mathbb{C}$ si $\forall x_0 \in U$, il existe un disque $|x - x_0| < r$ de centre x_0, contenu dans U, tel que la restriction de f à ce disque soit développable en série entière.

Notation.

On note $\mathcal{H}(U)$ l'ensemble des fonctions analytiques dans U.

Proposition 1.

$\mathcal{H}(U)$ est une algèbre sur le corps complexe $\mathbb{C}$.

Proposition 2.

Si f est analytique dans U, f est indéfiniment dérivable dans u. De plus, toutes ses dérivées sont analytiques dans U.

III- Principe du prolongement analytique.

Soit $a \in \mathbb{C}$. Supposons que f soit développable en série entière au voisinage de a. $|x - a| < r \Longrightarrow f(x) = \sum_{n \geq 0} \alpha_n (x-a)^n$. On a, en dérivant, $f^{(n)}(a) = n!\, \alpha_n$. Donc $(f^{(n)}(a) = 0, \forall n \geq 0) \Longrightarrow f(x) = 0$ pour tout x tel que $|x - a| < r$. D'où :

Proposition 1.

Soit f une fonction analytique dans U, soit $a \in U$. Si $f^{(n)}(a) = 0$ pour tout $n \geq 0$, alors f est identiquement nulle dans un voisinage de a.

Proposition 2.

Soit f une fonction analytique dans U.

Soit $E = \{ a \in U \mid f = 0$ dans un voisinage de $a \}$.

Alors E est ouvert et fermé.

Démonstration.

1) E est ouvert.

Soit $a \in E$. D'après la définition de E, il existe r tel que $|x - a| < r \Longrightarrow f(x) = 0$. Donc E contient le disque $|x - a| < r$, et par suite E est ouvert.

2) E est fermé.

Soit b un point adhérent à E. Il existe une suite $\{a_k\}$ de points de E dont b est la limite. Pour tout $n \geq 0$, on a $f^{(n)}(a_k) = 0$. Pour n fixé, on a $f^{(n)}(a_k) = 0$ pour tout k ; comme $f^{(n)}$ est continue, on a $f^{(n)}(b) = 0$ à la limite. Donc f est identiquement nulle au voisinage de b, c'est-à-dire $b \in E$.

Théorème 1. (principe du prolongement analytique).

Soit f une fonction analytique dans un ouvert connexe U. S'il existe $a \in U$ et un voisinage V de a dans lequel f est identiquement nulle, alors f est identiquement nulle dans U. Mieux : s'il existe $a \in U$ telle que $f^{(n)}(a) = 0$ pour tout $n \geq 0$, alors f est identiquement nulle dans U.

Démonstration.

D'après les hypothèses, l'ensemble E des points de U au voisinage desquels f est $\equiv 0$ n'est pas vide. Or E est ouvert et fermé dans U connexe ; donc $E = U$.

Problème.

Soit U un ouvert connexe de C, et V un ouvert non vide contenu dans U. Soit f analytique dans V. Existe-t-il une g analytique dans U dont la restriction à V soit f ? Le théorème précédent montre que si une telle g existe, elle est unique.

Remarque. Pour les fonctions d'une variable complexe il y a équivalence entre être de classe C^∞ et être analytique. Il n'en est plus de même pour les fonctions d'une variable réelle. Par exemple, la fonction $f : \mathbb{R} \longrightarrow \mathbb{R}$ définie par

$$f(x) = \begin{cases} e^{\frac{1}{x^2-1}} & \text{pour } |x| < 1 \\ 0 & \text{pour } |x| \geq 1 \end{cases}$$

est de classe C^∞ mais elle n'est pas analytique.

En effet, elle est identiquement nulle dans un ouvert non vide de $\mathbb{R}$, sans être nulle partout ($\mathbb{R}$ est connexe).

Théorème 2.

Soit f une fonction $U \longrightarrow \mathbb{C}$, U ouvert de $\mathbb{C}$. Si f est de classe C^1 au sens complexe, alors f est analytique et en particulier de classe C^∞. On dit aussi que f est holomorphe. Le théorème 2 se prouve à l'aide du ;

Théorème 3.

Si f est de classe C^1 dans un disque ouvert de centre 0, $|x| < r$, alors f est développable en série entière dans ce disque.

[La démonstration utilise "l'intégrale de Cauchy"].

Corollaire.

La somme d'une série entière est une fonction analytique dans son disque de convergence.

IV- Zéros - Pôles.

Soit f une fonction analytique dans U. Soit $a \in U$ tel que $f(a) = 0$. On a $f(x) = \sum_{n \geq 0} \alpha_n (x-a)^n$ pour $|x-a| < r$ assez petit. La condition $f(a) = 0$ équivaut à $\alpha_o = 0$. Supposons que f ne soit pas identiquement nulle dans un voisinage de a. Soit p tel que $\alpha_p \neq 0$, $\alpha_q = 0 \ \forall q < p$. Alors $f(x) = (x-a)^p g(x)$ où $g(x)$ est développable en série entière :

$$g(x) = \alpha_p + \alpha_{p+1}(x-a) + \ldots + \alpha_n (x-a)^{n-p} + \ldots$$ On a

$$g(a) = \alpha_p \neq 0.$$

Définition 1.

Soit f une fonction analytique dans U. Soit $a \in U$. On dit que a est un zéro d'ordre p pour la fonction analytique f si

$$f(a) = f'(a) = \ldots = f^{(p-1)}(a) = 0 \ , \ f^{(p)}(a) \neq 0.$$

Ces conditions équivalent à :

$f(x) = (x-a)^p g(x)$, $g(a) \neq 0$, $g(x)$ analytique au voisinage de a.

La condition $g(a) \neq 0$ entraîne $g(x) \neq 0$ pour x assez voisin de a, puisque g est continue.

$\Longrightarrow f(x) \neq 0$ pour $0 < |x-a| < \rho$, $\rho > 0$ assez petit . D'où

Proposition.

Soit f une fonction analytique dans U, U connexe . On suppose que f est non identiquement nulle dans U. Soit $a \in U$, tel que $f(a) = 0$. Alors $f(x) \neq 0$ pour $x \neq a$ et suffisamment voisin de a. [En d'autres termes, les zéros de f sont isolés] Soit $E = \{$zéros de $f\}$. On voit que si f n'est pas identiquement nulle dans U connexe, E est un ensemble discret pour la topologie induite.

Définition 2.

Soit f une fonction analytique dans $U - \{a\}$, $a \in U$, où U est un ouvert connexe de $\mathbb{C}$. On suppose f non identiquement nulle dans U. On dit que a est un pôle de f si dans un voisinage de a, a exclu, on a $f(x) = \dfrac{g(x)}{(x-a)^p}$ (p entier ≥ 1), où $g(x)$ est analytique au voisinage de a (a inclus), avec $g(a) \neq 0$. On voit que lorsque x tend vers a (en restant $\neq a$), $|f(x)|$ tend vers l'infini : on peut convenir de donner la valeur ∞ à la fonction f au point a (pôle de f).

Définition 3.

p s'appelle l'ordre de multiplicité du pôle.

Remarque : $(x-a)^p f(x)$ se prolonge en une fonction $g(x)$ holomorphe au point a, $g(a) \neq 0$.

Exemples de pôles.

Soit U un ouvert de $\mathbb{C}$. Soit $a \in \mathbb{C}$. Soient f et g deux fonctions holomorphes au voisinage de a. Si $g \not\equiv 0$ au voisinage de a, le quotient $h(x) = \dfrac{f(x)}{g(x)}$ est défini au voisinage de a (a exclu), puisque $g(x) \neq 0$ pour $0 < |x-a| < \rho$ (ρ assez petit). Si en outre $f \not\equiv 0$, on peut écrire $f(x) = (x-a)^p f_1(x)$, $g(x) = (x-a)^p g_1(x)$ avec $f_1(a) \neq 0$, $g_1(a) \neq 0$. D'où $h(x) = \dfrac{f(x)}{g(x)} = (x-a)^{p-q} \dfrac{f_1(x)}{g_1(x)}$. Posons $h_1(x) = \dfrac{f_1(x)}{g_1(x)}$; c'est une fonction holomorphe au voisinage de a (a inclus), et $h_1(a) \neq 0$. D'où $h(x) = (x-a)^{p-q} h_1(x)$.

.../...

i $p \geq q$, $h(x)$ est holomorphe au voisinage de a ;

i $p > q$, a est zéro de $h(x)$, d'ordre $p-q$;

i $p < q$, $h(x)$ admet un pôle en a, d'ordre $q-p$.

llure de f au voisinage d'un pôle.

Soit $f(x) = \frac{g(x)}{(x-a)^p}$, $g(a) \neq 0$. Le développement en série de g au voisina-

ge de a montre que l'on a

$$g(x) = \alpha_0 + \alpha_1(x-a) + \ldots + \alpha_{p-1}(x-a)^{p-1} + (x-a)^p g_1(x), \quad \text{avec } \alpha_0 \neq 0.$$

D'où :

$$f(x) = \frac{\alpha_0}{(x-a)^p} + \frac{\alpha_1}{(x-a)^{p-1}} + \ldots + \frac{\alpha_{p-1}}{x-a} + g_1(x) ,$$

avec $\alpha_0 \neq 0$ et g_1 holomorphe au voisinage de a (a inclus). La différence $f(x) - g_1(x)$ est ainsi un polynôme de $\frac{1}{x-a}$, de degré p égal à l'ordre de multiplicité du pôle a ; on l'appelle la partie principale de f au pôle a.

Fonctions méromorphes.

Définition.

On appelle fonction méromorphe dans U (U ouvert de $\mathbf{C}$) une fonction f holomorphe dans $U - \Delta$ (où Δ est un sous-ensemble discret de U, qui dépend de f), telle que tout point $a \in \Delta$ soit un pôle de f. On peut convenir de donner la valeur ∞ à f en tout point de Δ.

Principe du prolongement analytique pour les fonctions méromorphes : l'ensemble des $a \in U$ tels que f soit identiquement nulle au voisinage de a, est ouvert et fermé dans U (même démonstration que pour les fonctions holomorphes). Donc si U est connexe, cet ensemble est vide ou égal à U.

.../...

Soit $\mathcal{M}(U)$ l'ensemble des fonctions méromorphes dans U. Si $f_1, f_2 \in \mathcal{M}(U)$, on définit la somme $f_1 + f_2$ et le produit $f_1 f_2$ comme suit : soit Δ_1 l'ensemble des pôles de f_1, et Δ_2 l'ensemble des pôles de f_2 ; dans $U - (\Delta_1 \cup \Delta_2)$, $f_1 + f_2$ est la somme de deux fonctions holomorphes ; si $a \in \Delta_1 \cup \Delta_2$, deux cas sont possibles : ou bien $f_1 + f_2$ est holomorphe au point a (si les "parties principales" de f_1 et f_2 sont opposées), ou bien a est un pôle de $f_1 + f_2$; donc $f_1 + f_2$ est une fonction méromorphe dans U. De même, $f_1 f_2$ est méromorphe dans U.

L'ensemble $\mathcal{M}(U)$ est ainsi muni d'une structure d'anneau.

Proposition 1.

Si U est connexe, l'anneau $\mathcal{M}(U)$ est un corps.

Démonstration.

On doit montrer que si $f \in \mathcal{M}(U)$ et f non identiquement nulle, $\frac{1}{f}$ est méromorphe. Or si a n'est pas un zéro de f, on a $f(x) = \frac{1}{(x-a)^p} g(x)$, g holomorphe au voisinage de a, $g(a) \neq 0$, $p \geq 0$; donc $\frac{1}{f(x)} = (x-a)^p \frac{1}{g(x)}$, où $\frac{1}{g(x)}$ est holomorphe au voisinage de a : donc $\frac{1}{f}$ est holomorphe au voisinage de a. Si a est un zéro de f, f est holomorphe au voisinage de a, et n'est pas identiquement nulle au voisinage de a ; sinon, U étant connexe , f serait identiquement nulle dans U (principe du prolongement analytique), contrairement à l'hypothèse.

Donc a est un zéro isolé de f :

$$f(x) = (x-a)^p f_1(x) \quad , \quad p \geq 0,$$

avec f_1 holomorphe au voisinage de a, $f_1(a) \neq 0$. Donc

$$\frac{1}{f(x)} = \frac{1}{(x-a)^p} \frac{1}{f_1(x)} \ ,$$

avec $\frac{1}{f_1}$ holomorphe au voisinage de a (a inclus) : a est bien un pôle de $\frac{1}{f}$.

C.Q.F.D.

Proposition 2.

Si $f \in \mathcal{M}(U)$, la dérivée f' appartient aussi à $\mathcal{M}(U)$.

Démonstration.

f est holomorphe dans $U - \Delta$ (Δ discret), donc f' aussi, et il reste à montrer que si $a \in \Delta$ est un pôle de f, c'est aussi un pôle de f'. Or

$$f(x) = \frac{1}{(x-a)^p}\, g(x) \quad , \quad \begin{cases} g \text{ holomorphe au voisinage de } a, \\ g(a) \neq 0. \end{cases}$$

$$f'(x) = \frac{1}{(x-a)^p}\, g'(x) - \frac{p}{(x-a)^{p+1}}\, g(x) = \frac{1}{(x-a)^{p+1}}\, h(x),$$

avec $h(x) = (x-a)\, g'(x) - p\, g(x)$, holomorphe au voisinage de a, et $h(a) = -p\, g(a) \neq 0$. On voit que l'ordre de multiplicité du pôle a, pour f', est $p+1$ (si p est l'ordre de multiplicité du pôle a pour f).

Inégalités de Cauchy.

Soit f holomorphe au voisinage de 0. On a le développement en série $f(x) = \sum_{n \geq 0} a_n x^n$ pour $|x| < \rho$, ρ désignant le rayon de convergence de la série. Rappelons que ρ est le plus grand des $r > 0$ tels que f soit holomorphe dans le disque $|x| < r$.

Fixons r tel que $0 < r < \rho$. Sur le disque compact $|x| \leq r$, f est continue, donc bornée ; soit $M(r) = \sup_{|x| \leq r} |f(x)|$.

Posons $x = r\, e^{i\theta}$; on a $f(r\, e^{i\theta}) = \sum_{n \geq 0} a_n r^n e^{in\theta}$. On peut intégrer cette série terme à terme à cause de la convergence uniforme ; plus précisément :

$$e^{-ip\theta} f(r\, e^{i\theta}) = \sum_{n \geq 0} a_n r^n e^{i(n-p)\theta}.$$

$$\frac{1}{2\pi} \int_0^{2\pi} e^{-ip\theta} f(r\, e^{i\theta})\, d\theta = \sum_{n \geq 0} a_n r^n \frac{1}{2\pi} \int_0^{2\pi} e^{i(n-p)\theta}\, d\theta .$$

Or $\frac{1}{2\pi} \int_0^{2\pi} e^{i(n-p)\theta}\, d\theta = 0$ si $n \neq p$, $= 1$ si $n = p$. D'où :

$$\frac{1}{2\pi} \int_0^{2\pi} e^{-ip\theta} f(r\, e^{i\theta})\, d\theta = a_p r^p. \quad \text{Ainsi}$$

$$|a_p| \leq \frac{1}{2\pi r^p} \int_0^{2\pi} |f(r\, e^{i\theta})|\, d\theta \leq \frac{1}{2\pi r^p} \times 2\pi\, M(r) .$$

Finalement, récrivant n au lieu de p, on obtient $\boxed{|a_n| \leq \frac{M(r)}{r^n}}$ (inégalité de Cauchy).

Remarque. a_o est la valeur moyenne de la fonction $f(x)$ sur le cercle $|x| = r$.

Théorème de Liouville.

Soit $f(x)$ une fonction holomorphe dans tout le plan et bornée. Alors f est constante.

Démonstration.

Pour $n \geq 1$ l'inégalité de Cauchy montre, lorsque $r \longrightarrow +\infty$, que $a_n \to 0$. Donc $f(x) = a_o$. C.Q.F.D.

VII- Limites de fonctions holomorphes.

Théorème de Weierstrass.

Soit U un ouvert de $\mathbf{C}$. Soit $\{f_n\}$ une suite infinie de fonctions holomorphes dans U. On suppose que les f_n ont une limite f au sens de la convergence uniforme locale (cf. définition ci-dessous).

Alors f est holomorphe dans U. De plus $f'(x) = \lim_{p \to \infty} f'_p(x)$, la limite étant uniforme au sens de la convergence uniforme locale.

Définition.

Soit $\{f_n\}$ une suite de fonctions ayant une limite f. La limite est uniforme au sens de la convergence uniforme locale si : $\forall\ a \in U, \exists$ un voisinage $V(a)$ de a dans lequel la suite converge uniformément, c'est-à-dire : $\forall\ \varepsilon > 0, \exists\ p \in \mathbb{N}$ tel que $\forall x \in V(a)$ et $\forall\ n \geq p$, on ait $|f(x) - f_n(x)| \leq \varepsilon$.

Lemme.

La convergence uniforme locale entraîne la convergence uniforme sur tout compact $K \subset U$; réciproquement, la convergence uniforme sur tout compact entraîne la convergence uniforme locale.

Démonstration.

Soit $a \in K$. Il existe un voisinage de a, $V(a)$ dans lequel la convergence est uniforme.

On peut choisir les $V(a)$ ouverts.

On a un recouvrement ouvert de K. On peut en extraire un sous-recouvrement fini.

Soient a_i, $i \in I$ (I fini) tels que les $V(a_i)_{i \in I}$ recouvrent K.

$\forall \varepsilon > 0$, $\exists\ p_i$ tel que $k \geqslant p_i \Rightarrow |f(x) - f_k(x)| \leqslant \varepsilon$, $\forall x \in V(a_i)$.

Soit $p = \sup(p_i)$; p existe et est fini car les p_i sont en nombre fini.

$\forall \varepsilon > 0$, $k \geqslant p \Rightarrow |f(x) - f_k(x)| \leqslant \varepsilon \quad \forall x \in K$.

La réciproque est vraie : si la suite (f_k) converge uniformément sur tout compact de U, tout point de U possède un voisinage compact, donc la convergence est uniforme sur ce voisinage.

Démonstration du théorème

1) Montrons que f est holomorphe. Il suffit de le prouver au voisinage de chaque point.

Soit $|x - a| < \rho$ un disque ouvert contenu dans U. Dans ce disque les f_k sont holomorphes, donc développables en séries entières.

Supposons $a = 0$ (changer x en $x - a$) ; f_k est holomorphe dans le disque $|x| < \rho$.

$f_k(x) = \sum_{n \geqslant 0} a_{n,k}\ x^n$ pour $|x| < \rho$.

Fixons un r tel que $0 < r < \rho$.

Le disque $\{x \mid |x| \leqslant r\}$ est compact. Sur ce compact, la convergence de la suite (f_k) est uniforme par hypothèse :

$\forall \varepsilon > 0, \exists\ p, k \geqslant p, k' \geqslant p \Rightarrow |f_k(x) - f_{k'}(x)| \leqslant \varepsilon$ pour $|x| \leqslant \rho$.

$f_k(x) - f_{k'}(x) = \sum_n (a_{n,k} - a_{n,k'})\ x^n$.

D'après Cauchy, $|a_{n,k} - a_{n,k'}| \leqslant \frac{\varepsilon}{r^n}$ dès que k et k' sont $\geqslant p$.

Ceci montre que, pour n fixé, la suite des $a_{n,k}$ (k variable) est une suite de Cauchy ; donc elle a une limite. Soit $a_n = \lim_{k \to \infty} a_{n,k}$.

Considérons la série $\sum_{n\geqslant o} a_n x^n$. Montrons qu'elle converge pour $|x| < \rho$ et que sa somme est $f(x) = \lim_{k\to\infty} f_k(x)$.

En vertu de la convergence uniforme sur le disque $|x| \leqslant r$, il existe M tel que $|f_k(x)| \leqslant M$ quel que soit x $(|x| \leqslant r)$ et quel que soit k .

D'après les inégalités de Cauchy, on a

$$|a_{n,k}| \leqslant \frac{M}{r^n} \quad \text{quel que soit } k .$$

Soit r' tel que $o < r' < r < \rho$.

Il suffit de montrer la convergence de la série limite sur le disque fermé de rayon r' . Or

$$|a_n| \leqslant \frac{M}{r^n} \quad \text{à la limite, d'où}$$

$$|a_n x^n| \leqslant M \left(\frac{r'}{r}\right)^n \quad \text{lorsque } |x| \leqslant r' .$$

Le second nombre est le terme général d'une progression géométrique de raison $\frac{r'}{r} < 1$. Donc la série converge absolument. Comme r' peut être choisi arbitrairement $< \rho$ (on choisit alors r entre r' et ρ) , on voit que la série $g(x) = \sum a_n x^n$ converge pour $|x| < \rho$.

Il reste à montrer que $g(x) = f(x)$.

$$g(x) - f_k(x) = \sum_{n\geqslant o} (a_n - a_{n,k}) x^n$$

$$= \sum_{o\leqslant n<p} (a_n - a_{n,k}) x^n + \sum_{n\geqslant p} (a_n - a_{n,k}) x^n$$

Majorons cette différence pour $|x| \leqslant r' < r < \rho$.

$$|g(x) - f_k(x)| \leqslant \sum_{o\leqslant n<p} |a_n - a_{n,k}| r'^n + \sum_{n\geqslant p} |a_n| r'^n + \sum_{n\geqslant p} |a_{n,k}| r'^n .$$

$$\sum_{n\geqslant p} |a_n| r'^n + \sum_{n\geqslant p} |a_{n,k}| r'^n \leqslant 2M \sum_{n\geqslant p} \left(\frac{r'}{r}\right)^n = \frac{2M \left(\frac{r'}{r}\right)^p}{1 - \left(\frac{r'}{r}\right)}$$

On <u>choisit</u> p de telle sorte que $\dfrac{2M \left(\frac{r'}{r}\right)^p}{1 - \frac{r'}{r}} \leqslant \frac{\varepsilon}{2}$.

Alors $\exists h$ tel que $k \geqslant h \Rightarrow \sum_{o \leqslant n < p} |a_n - a_{n,k}| \, r'^n \leqslant \frac{\varepsilon}{2}$.

Conclusion : dès que $k \geqslant h$, $|g(x) - f_k(x)| \leqslant \varepsilon$ pour tout x tel que $(x) \leqslant r'$.

Sur le disque fermé de rayon r' , g est donc limite de la suite des f_k . Donc $g = f$, et f est bien holomorphe dans U .

2) $f(x)$ étant holomorphe, est dérivable au sens complexe dans U .

Montrons que

$$f'(x) = \lim_{k \to \infty} f'_k(x) \ ,$$

uniformément sur tout compact contenu dans U .

On sait que la suite $f - f_k$ tend vers zéro uniformément sur tout compact. On veut montrer que $f' - f'_k$ tend vers zéro uniformément sur tout compact.

On est donc ramené à démontrer ceci :

Si une suite de fonctions f_k holomorphes converge vers o uniformément sur tout compact, alors la suite des dérivées converge uniformément vers zéro sur tout compact.

On va le prouver dans le disque $|x| < \rho$. Soit $r < \rho$. Soit $|f(x)| \leqslant M$ sur le disque $|x| \leqslant r$; on va majorer $f'(x)$ sur tout disque de rayon $r' < r$.

Soit $f(x) = \sum_{n \geqslant o} a_n r^n$, $|a_n| \leqslant \frac{M}{r^n}$.

$$\left| \sum_{n \geqslant o} n \, a_n \, x^{n-1} \right| \leqslant \sum_{n \geqslant o} n \, \frac{M}{r^n} \, r'^{n-1} \quad \text{pour } |x| \leqslant r' \ ,$$

$$\leqslant \frac{M}{r} \left[\sum_{n \geqslant o} n \, \left(\frac{r'}{r}\right)^{n-1} \right] = \frac{M}{r} \, \frac{1}{\left(1 - \frac{r'}{r}\right)^2} = M$$

λ indépendant de M , ne dépend que de r et r').

En effet, $\sum_{n\geqslant o} t^n = \frac{1}{1-t}$; la série est uniformément convergente pour $|t| < 1$; on peut donc dériver terme à terme :

$$\sum_{n\geqslant o} n\, t^{n-1} = \frac{d}{dt}\left(\frac{1}{1-t}\right) = \frac{1}{(1-t)^2} \quad .$$

Soit alors $M_k = \sup |f_k(x)|$ pour $|x| \leqslant r$; on a $\sup |f_k'(x)| \leqslant \lambda M_k$ pour $|x| \leqslant r'$; si $\lim M_k = o$, on voit que la suite (f_k') converge uniformément vers 0 sur $|x| \leqslant r'$.

C.Q.F.D.

VIII - Produit infini de fonctions holomorphes -

Définition

On dit que la série $\sum_n u_n(x)$ converge normalement sur un ensemble A si elle est majorée sur A pour une série numérique convergente

$\Longleftrightarrow \quad \forall\, x \in A\ ,\ |u_n(x)| \leqslant \varepsilon_n$, avec $\sum_n \varepsilon_n < +\infty$.

Ceci revient à dire que si l'on pose

$||u_n||_A = \sup_{x\in A} |u_n(x)|$, la série $\sum_n ||u_n||_A$ est convergente (série des "normes").

La convergence normale entraîne évidemment la convergence uniforme.

Théorème

Soit $f_k(x)$, une suite de fonctions holomorphes dans un ouvert $U \subset \mathbb{C}^n$, telles que :

$$\forall\, x \in U\ ,\ |f_k(x)| < 1\ .$$

Si la série $\sum_{k\geqslant o} f_k(x)$ converge normalement sur tout compact contenu dans U , alors $\prod_{k=1}^{n} (1 - f_k(x))$ a une limite quand $n \to \infty$; cette limite est holomorphe dans U et partout non nulle. On la note $\prod_{k=1}^{\infty} (1-f_k(x))$.

De plus $\prod_{k=1}^{\infty} (1-f_k(x)) = \exp\left(\sum_{k=1}^{\infty} \log\,(1-f_k(x))\right)$, où $\log\,(1-u)$ désigne la détermination principale du logarithme pour $|u| < 1$.

Démonstration.

Soit

$$P_n(x) = \prod_{k=1}^{n} (1-f_k(x)) .$$

On a

$$(1) \qquad P_n(x) = \exp \Big(\sum_{k=1}^{n} \log (1 - f_k(x)) \Big).$$

Si on montre que la série $\sum_{k=1}^{\infty} \log (1 - f_k(x))$ converge normalement sur tout compact de U, sa somme $g(x)$ sera holomorphe dans U, et on aura $P(x) = \lim_{n \to \infty} P_n(x) = \exp g(x)$, ce qui prouvera le théorème.

On va donc, sur tout compact $K \subset U$, majorer

$$\log (1 - f_k(x)).$$

Or, par hypothèse, $\exists$ série convergente $\sum_k \varepsilon_k$ à termes > 0, telle que

$$|f_k(x)| \leqslant \varepsilon_k \quad \text{pour} \quad x \in K .$$

On a

$$- \log (1 - f_k(x)) = f_k(x) + \frac{1}{2} (f_k(x))^2 + \ldots + \frac{1}{n} (f_k(x))^n + \ldots$$

$$| \log (1 - f_k(x)| \leqslant \varepsilon_k + \frac{1}{2} (\varepsilon_k)^2 + \ldots + \frac{1}{n} (\varepsilon_k)^n + \ldots$$

$$\leqslant \frac{\varepsilon_k}{1 - \varepsilon_k} ,$$

terme général d'une série convergente.

C.Q.F.D.

DEFINITION ET PROPRIETES DE LA FONCTION $\zeta(s)$

Résultats sur les nombres premiers

Soit P l'ensemble de tous les nombres premiers naturels. Soit P' une partie finie de P. Ecrivons

$$\frac{1}{1 - \frac{1}{p}} = 1 + \frac{1}{p} + \frac{1}{p^2} + \ldots + \frac{1}{p^k} + \ldots$$

$$\prod_{p \in P'} \frac{1}{1 - \frac{1}{p}} = \sum_{p_1, \ldots p_k \in P'} \frac{1}{p_1^{h_1} \ldots p_k^{h_k}} = \sum_{n \in M} \frac{1}{n} ,$$

où M est l'ensemble des entiers > 0 dont tous les facteurs premiers appartiennent à P'.

Cette série est convergente (produit d'un nombre fini de séries convergentes).

Si l'ensemble des nombres premiers était fini, la série $\sum_{n\geqslant 1} \frac{1}{n}$ (étendue à tous les entiers > 0) serait convergente, ce qui est faux.

En effet :

$$\sum_{k<n\leqslant 2k} \frac{1}{n} > \frac{1}{2k} \times n = \frac{1}{2}, \text{ donc } \sum \frac{1}{n}, \text{ par regroupement de termes, est somme d'une infinité de nombres } > \frac{1}{2}, \text{ et par suite est infini.}$$

Conclusion : l'ensemble des nombres premiers est infini (ceci est une nouvelle preuve). Soit p_k le k-ième nombre premier.

Lorsque k augmente indéfiniment, $\prod_{i=1}^{k} \frac{1}{1-\frac{1}{p_i}}$ augmente indéfiniment

car la limite est $\sum_{i=1}^{\infty} \frac{1}{n}$.

Donc $\lim_{k\to\infty} \prod_{i=1}^{k} (1-\frac{1}{p_i}) = 0$. On va en déduire :

Théorème (Euler)

La série des inverses de tous les nombres premiers est divergente.

Démonstration : on a

$$\log\left(\frac{1}{1-\frac{1}{p}}\right) = -\log\left(1-\frac{1}{p}\right) = \frac{1}{p} + \frac{1}{2p^2} + \ldots + \frac{1}{np^n} + \ldots$$

$$= \log\left(1-\frac{1}{p}\right) - \frac{1}{p} \leqslant \frac{1}{p^2}\left[\frac{1}{2} + \frac{1}{3p} + \ldots + \frac{1}{np^{n-2}} + \ldots\right]$$

$$\leqslant \frac{1}{2p^2}\left(1 + \frac{1}{p} + \frac{1}{p^2} + \ldots\right) \leqslant \frac{1}{p^2}$$

Or, $\sum_{n\geqslant 0} \frac{1}{n^2}$ est convergente.

$\Longrightarrow \sum_{p\in P} \frac{1}{p^2}$ est convergente.

$\Longrightarrow \sum_{p\in P} \left(-\log\left(1-\frac{1}{p}\right) - \frac{1}{p}\right)$ converge.

Donc $\sum_{i=1}^{k} \left(-\log\left(1-\frac{1}{p_i}\right)\right) - \sum_{i=1}^{k} \frac{1}{p_i}$ tend vers une limite finie

quand $k \to \infty$.

Or $\log \dfrac{1}{\prod_{i=1}^{k}\left(1-\frac{1}{p_i}\right)} \longrightarrow \infty$. Donc

$\sum_{i=1}^{k} \frac{1}{p_i} \longrightarrow \infty$. C.Q.F.D.

II - Rappels

Définition 1. -

Soit x réel positif, soit s complexe.

$$x^s = e^{s \log x} \; ; \; |x^s| = x^{\mathrm{Re}\,(s)} \; .$$

$$\frac{d}{ds}\,(x^s) = \log x \, . \, e^{s \log x} = x^s \log x \; .$$

Théorème.

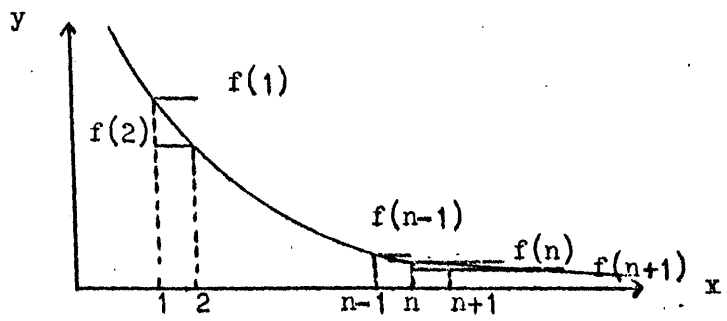
La série $\sum_{n \geq 1} \frac{1}{n^\alpha}$ (α réel positif) est :

- convergente si $\alpha > 1$,
- divergente si $\alpha \leqslant 1$.

Démonstration

Posons $f(x) = \frac{1}{x^\alpha}$, $x > 0$.

f est une fonction décroissante car $\alpha > 0$.



Or pour n'importe quelle fonction décroissante f définie pour $x > 0$, on a

$$\sum_{n=2}^{\infty} f(n) \leqslant \int_1^{\infty} f(x)\,dx < \sum_{n=1}^{\infty} f(n) \; .$$

Donc la série $\sum f(n)$ converge en même temps que l'intégrale $\int_1^{\infty} f(x)\,dx$.

On applique ceci à $f(x) = \frac{1}{x^\alpha}$:

Si $\alpha \neq 1$, $\int_1^\infty \frac{dx}{x^\alpha} = \lim_{a \to \infty} \frac{1}{1-\alpha} \left| \frac{1}{x^{\alpha-1}} \right|_1^a$, d'où :

si $\alpha > 1$, $\int_1^\infty \frac{dx}{x^\alpha} = \frac{1}{\alpha - 1}$,

si $\alpha < 1$, l'intégrale est divergente.

Si $\alpha = 1$, $\int_1^\infty \frac{dx}{x^\alpha} = \lim_{a \to \infty} |\log x|_1^a$, et

l'intégrale est divergente.

III - Définition de la fonction de Riemann

Considérons $\sum_{n=1}^{\infty} \frac{1}{n^s}$, s complexe.

$$\left| \frac{1}{n^s} \right| = \frac{1}{n^{Re(s)}} .$$

Si $Re(s) > 1$, la série converge absolument, et sa somme est une fonction holomorphe. En effet, d'après le théorème de Weierstrass, il suffit de démontrer que cette série converge normalement sur tout compact.

On va montrer que la série converge normalement dans tout demi-plan, $Re(s) \geqslant \alpha$, quel que soit $\alpha > 1$. On a en effet

$$\left| \frac{1}{n^s} \right| \leqslant \frac{1}{n^\alpha} \quad \text{si} \quad Re(s) \geqslant \alpha ,$$

et $\sum \frac{1}{n^\alpha}$ est convergente pour $\alpha > 1$.

Définition

On pose $\boxed{\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s}}$ fonction de Riemann ;

$\zeta(s)$ est holomorphe dans le demi-plan $Re(s) > 1$.

Théorème

Le produit infini $\prod_{p \in P} \frac{1}{1 - \frac{1}{p^s}}$, étendu à tous les nombres premiers p,

est convergent pour $Re(s) > 1$, et on a

$$\boxed{\zeta(s) = \prod_{p \in P} \frac{1}{1 - \frac{1}{p^s}} \quad \text{pour} \quad Re(s) > 1}$$

Démonstration

1) Pour voir que le produit est convergent, il suffit de vérifier que la série $\sum_{p\in P} \frac{1}{p^s}$ converge normalement dans toute bande

$$\mathrm{Re}(s) \geqslant \alpha \quad (\alpha > 1) \ .$$

Or, $\frac{1}{|p^s|} \leqslant \frac{1}{p^\alpha}$;

$\sum_{p\in P} \frac{1}{p^\alpha}$ converge, car la série $\sum_{n\geqslant 0} \frac{1}{n^\alpha}$ est convergente. D'où le résultat.

2) Soit P' une partie finie de P . On a

$$\prod_{p\in P'} \frac{1}{1-\frac{1}{p^s}} = \prod_{p\in P'} \left(1 + \frac{1}{p^s} + \ldots + \frac{1}{p^{ks}} + \ldots\right)$$

$$= \sum_{n\in M} \frac{1}{n^s} \ , \text{ où}$$

M est l'ensemble des entiers $\geqslant 1$ dont tous les facteurs premiers appartiennent à P'.

Quand on prend des parties finies P' de plus en plus grandes, le produit tend vers $\prod_{p\in P} \frac{1}{1-\frac{1}{p^s}}$, et le second membre tend vers $\sum_{n\geqslant 1} \frac{1}{n^s}$ (le démontrer).

D'où le théorème.

opriétés de $\zeta(s)$

Proposition 1 -

$\psi(s) = \log \zeta(s) - \sum_{p\in P} \frac{1}{p^s}$, qui est holomorphe pour $\mathrm{Re}(s) > 1$, se se prolonge en une fonction holomorphe dans le demi-plan $\mathrm{Re}(s) > \frac{1}{2}$.

Démonstration

Il faut d'abord préciser la détermination de $\log \zeta(s)$ choisie pour $\mathrm{Re}(s) > 1$.

Puisque $\zeta(s) = \prod_{p \in P} \frac{1}{1 - \frac{1}{p^s}}$, on prend pour $\log \zeta(s)$ la somme de la série $\sum_{p \in P} \left(- \log\left(1 - \frac{1}{p^s}\right)\right)$.

Ainsi

$$\psi(s) = \sum_{p \in P} \left[- \log \left(1 - \frac{1}{p^s}\right) - \frac{1}{p^s} \right] = \sum_{p \in P} \psi_p(s) \text{ , avec}$$

$$\psi_p(s) = - \log \left(1 - \frac{1}{p^s}\right) - \frac{1}{p^s} = \frac{1}{2p^{2s}} + \ldots + \frac{1}{kp^{ks}} + \ldots$$

Cette série converge normalement pour $\mathrm{Re}(s) \geqslant \alpha$ $(\alpha > 0)$, comme on va le voir ; donc $\psi_p(s)$ est holomorphe pour $\mathrm{Re} > 0$. En effet $\left| \frac{1}{p^{ks}} \right| \leqslant \frac{1}{p^{k\alpha}}$ si $\mathrm{Re}(s) \geqslant \alpha > 0$, et la série $\sum \frac{1}{k} \frac{1}{p^{k\alpha}}$ est évidemment convergente.

On voit de plus que $|\psi_p(s)| \leqslant \sum_{k \geqslant 2} \frac{1}{k} p^{-k\alpha}$ pour $\mathrm{Re}(s) \geqslant \alpha > 0$.

Or,

$$\sum_{k \geqslant 2} \frac{1}{k} p^{-k\alpha} \leqslant \frac{1}{2} p^{-2\alpha} \left(1 + p^{-\alpha} + p^{-2\alpha} + \ldots + p^{-(k-2)\alpha} + \ldots\right)$$

$$\Longrightarrow \quad |\psi_p(s)| \leqslant \frac{1}{2} p^{-2\alpha} \frac{1}{1 - p^{-\alpha}} \; ;$$

or $p \geqslant 2$. Prenons désormais $\alpha > \frac{1}{2}$; alors $p^{-\alpha} \leqslant \frac{1}{\sqrt{p}} \leqslant \frac{1}{\sqrt{2}}$, d'où

$$\Longrightarrow \frac{1}{1 - p^{-\alpha}} \leqslant \frac{1}{1 - \frac{1}{\sqrt{2}}} < 4 \; .$$

Donc $|\psi_p(s)| \leqslant 2p^{-2\alpha}$.

Or $\alpha > \frac{1}{2} \Longrightarrow 2\alpha > 1$. Donc la série $\sum_{p \in P} p^{-2\alpha}$ est convergente.

$\Longrightarrow \sum_{p \in P} \psi_p(s)$ est une série normalement convergente pour $\mathrm{Re}(s) \geqslant \alpha > \frac{1}{2}$.

Conclusion

$\psi(s) = \sum_{p \in P} \psi_p(s)$ est normalement convergente dans toute bande de $\mathrm{Re}(s) \geqslant \alpha > \frac{1}{2}$. Donc $\psi(s)$ est holomorphe dans la bande ouverte $\mathrm{Re}(s) > \frac{1}{2}$. La proposition 1 est démontrée.

Proposition 2 -

La fonction $\psi(s) = \zeta(s) - \frac{1}{s-1}$, qui est holomorphe pour $\mathrm{Re}(s) > 1$, se prolonge en une fonction holomorphe dans le demi plan $\mathrm{Re}(s) > 0$.

Démonstration. Supposons d'abord $\mathrm{Re}(s) > 1$.

On a $\frac{1}{s-1} = \int_1^\infty \frac{dx}{x^s}$ (calculer une primitive de $\frac{1}{x^s}$) . Donc

$$\psi(s) = \sum_{n=1}^{\infty} \frac{1}{n^s} - \int_1^\infty \frac{dx}{x^s} = \sum_{n=1}^{\infty} \left[\frac{1}{n^s} - \int_n^{n+1} \frac{dx}{x^s} \right] .$$

Ceci a un sens car l'intégrale converge uniformément.

$$\psi(s) = \sum_{n=1}^{\infty} \left[\int_n^{n+1} \left(\frac{1}{n^s} - \frac{1}{x^s} \right) dx \right] .$$

Soit $f(x) = \frac{1}{x^s}$ pour $n \leqslant x \leqslant n+1$. On a

$|f(x) - f(n)| \leqslant \sup_{n \leqslant x \leqslant n+1} |f'(x)|$. Or

$f'(x) = -s\, x^{-s-1} \Longrightarrow |f'(x)| \leqslant |s|\, x^{-\mathrm{Re}(s)-1} \leqslant \frac{|s|}{n^{\mathrm{Re}(s)+1}}$

$\Longrightarrow |f(x) - f(n)| \leqslant \frac{|s|}{|n^{s+1}|}$

Ainsi $\left|\frac{1}{n^s} - \frac{1}{x^s}\right| \leqslant \frac{|s|}{|n^{s+1}|}$ pour $n \leqslant x \leqslant n+1$.

Posons $\varphi_n(s) = \int_n^{n+1} \left[\frac{1}{n^s} - \frac{1}{x^s}\right] dx$. C'est une fonction holomorphe de s pour $\mathrm{Re}(s) > 0$.

$|\varphi_n(s)| \leqslant \frac{|s|}{|n^{s+1}|} = \frac{|s|}{n^{\mathrm{Re}(s)+1}}$

Cette série converge normalement pour $\mathrm{Re}(s) \geqslant \alpha$, si $\alpha > 0$. Donc $\zeta(s) - \frac{1}{s-1}$ est somme d'une série de fonctions holomorphes pour $\mathrm{Re}(s)$ qui converge normalement dans toute bande $\mathrm{Re}(s) \geqslant \alpha > 0$. La somme est donc holomorphe pour $\mathrm{Re}(s) > 0$, et la proposition 2 est démontrée.

Conséquence

$\varphi(s)$ est holomorphe pour $\mathrm{Re}(s) > 0$, $\frac{1}{s-1}$ est holomorphe pour $s \neq 1$.

Donc $\frac{1}{s-1} + \varphi(s)$ est méromorphe pour $\mathrm{Re}(s) > 0$, avec l'unique pôle simple $s = 1$, de résidu égal à 1.

Par suite $\zeta(s)$ se prolonge en une fonction méromorphe pour $\mathrm{Re}(s) > 0$, avec l'unique pôle simple $s = 1$, de résidu 1 .

[En fait, on peut montrer que $\zeta(s)$ se prolonge en une fonction méromorphe dans tout le plan complexe, avec l'unique pôle $s = 1$.]

Utilisation des propositions 1 et 2 -

D'après la proposition 2 , on a

$$\zeta(s) = \frac{1}{s-1} + \varphi(s) = \frac{1}{s-1} \left[1 + (s-1)\,\varphi(s)\right] .$$

Pour s voisin de 1 , on peut prendre le log d'une fonction voisine de 1 :

$$\log \zeta(s) = \log \frac{1}{s-1} + \log \left[1 + (s-1)\,\varphi(s)\right] .$$

La deuxième fonction est holomorphe au voisinage de $s = 1$, nulle pour $s = 1$. On a la même détermination pour $\log \zeta(s)$ que lors de la première définition, car dans chacun des cas c'est la détermination qui est réelle pour s réel > 1 . Ainsi $\log \zeta(s) = \log \frac{1}{s-1} + h(s)$, h holomorphe au voisinage de $s = 1$, nulle pour $s = 1$.

Or, d'après la proposition 2 , on a

$$\log \zeta(s) = \psi(s) + \sum_{p \in P} \frac{1}{p^s} .$$

Par différence, on voit que

$$\sum_{p \in P} \frac{1}{p^s} - \log \frac{1}{s-1} \quad \text{est holomorphe au voisinage de } s = 1 .$$

En particulier, $\lim\limits_{\substack{s \to 1 \\ \mathrm{Re}(s)>1}} \left(\sum_{p \in P} \frac{1}{p^s} - \log \frac{1}{s-1} \right)$ existe.

On en déduit :

$$(*) \qquad \boxed{\lim_{\substack{s \to 1 \\ \mathrm{Re}(s)>1}} \frac{1}{\log\left(\frac{1}{s-1}\right)} \left[\sum_{p \in P} \frac{1}{p^s} \right] = 1 .}$$

Définition

Soit P' une partie (finie ou infinie) de l'ensemble P des nombres premiers. On suppose que $\frac{1}{\log(\frac{1}{s-1})}\left[\sum_{p\in P'}\frac{1}{p^s}\right]$ a une limite ρ quand s tend vers 1 ($Re(s)$ restant > 1) .

ρ est alors appelée la densité du sous-ensemble P' de P .

D'après la relation (*), on a toujours $\rho \leqslant 1$. D'autre part, si P' est fini, il est évident que la densité de P' est nulle.

Répartition des nombres premiers.

I - Théorème de Dirichlet -

On se donne un entier $m \geqslant 2$.

Soit p premier. Il se trouve dans l'une des progressions arithmétiques de raison m ; elles sont au nombre de m .

p définit un élément de $\mathbb{Z}/m\mathbb{Z}$.

1er cas -

Si p ne divise pas m , les classes p , $2p$,..., mp sont distinctes ; il y en a m .

p est un générateur du groupe cyclique $\mathbb{Z}/m\mathbb{Z}$ (additif).

2ème cas -

Si p divise m , p est le seul nombre premier dans la progression arithmétique de raison m qui contient p .

Car si q premier , $q = p + k\,m$, on a $q = p$.

Considérons la progression arithmétique de raison m qui commence par a (a donné) .

Cherchons s'il existe p premier tel que $p \equiv a \pmod m$.

Si $(a , m) = d$, on a $p \equiv 0 \pmod d \Longrightarrow d = 1$ ou $p = d$.

Donc si $d > 1$, il y a au plus un nombre premier $p \equiv a \pmod m$.

Exemple

$a = 6 \qquad m = 8$

On cherche p premier, tel que $p \equiv 6 \pmod 8$

Le p.g.c.d. est 2 .

Le seul p possible est $p = 2$.

Le seul cas intéressant concerne donc la recherche des nombres premiers dans une progression (mod m) dont les termes sont premiers à m . Ces progressions sont en nombre $\varphi(m)$.

Théorème de Dirichlet -

Soient a et m deux entiers > 0 tels que $(a , m) = 1$.

On note $P_{a, m} = \{p \in P \mid p \equiv a \pmod m\}$.

Alors la densité de $P_{a, m}$ est $\frac{1}{\varphi(m)}$.

$$\Longleftrightarrow \lim_{\substack{s \to 1 \\ Re(s) > 1}} \left[\frac{1}{\log \frac{1}{s-1}} \sum_{p \in P_{a, m}} \frac{1}{p^s} \right] = \frac{1}{\varphi(m)} \quad .$$

(P désigne l'ensemble de tous les nombres premiers).

Corollaire : Si $(a, m) = 1$, l'ensemble $P_{a, m}$ est infini .

La démonstration sera donnée plus tard.

II - Générateurs du groupe cyclique $\mathbb{Z}/m\mathbb{Z}$ -

Proposition

$\alpha \in \mathbb{Z}/m\mathbb{Z}$ est un générateur $\Longleftrightarrow$ α est inversible pour la multiplication.

Démonstration

Si α est un générateur, $\alpha \beta = o \Longrightarrow \beta = o$ car α est premier à m .

L'application $\beta \longmapsto \alpha \beta$ est donc injective de $\mathbb{Z}/m\mathbb{Z}$ dans $\mathbb{Z}/m\mathbb{Z}$; par suite, elle est bijective.

Donc 1 est dans l'image ; il existe β tel que $\alpha \beta = 1$, et α est inversible. La réciproque est évidente.

Exemple

$m = 8$;

1, 3, 5, 7, sont premiers à m ; dans ce cas particulier, ils sont leur propre inverse.

Définition :

On note $G(m)$ le groupe multiplicatif des éléments inversibles de $\mathbb{Z}/m\mathbb{Z}$.

Exercice

Structure de $G(m)$

1) $\underline{m = p^\alpha}$, p premier , $p \neq 2$.

Alors $G(m)$ est cyclique d'ordre $p^{\alpha-1}(p-1)$.

Il y a $\varphi(p^{\alpha-1}(p-1))$ générateurs, soit $p^{\alpha-2}(p-2)\varphi(p-1)$.

Il faut en trouver effectivement un.

Exemples :

$\underline{m = 9}$ $\qquad G(m) = \{\pm 1, \pm 2, \pm 4\}$.

2 est générateur :

$2,\ 2^2 = 4,\ 2^3 = 8 = -1,\ 2^4 = -2,\ 2^5 = -4,\ 2^6 = 1$.

$\underline{m = 27}$ $\qquad G(m) = \{\pm 1, \pm 2, \pm 4, \pm 5, \pm 7, \pm 8, \pm 10, \pm 11, \pm 13\}$.

2 est générateur

$2,\ 2^2 = 4,\ 2^3 = 8,\ 2^4 = -11,\ 2^5 = +5,\ 2^6 = 10,\ 2^7 = -7,\ 2^8 = +13,$

$2^9 = -1, \ldots, 2^{18} = 1$.

$\underline{m = 3^\alpha}$

$\forall\, \alpha$, 2 engendre le groupe multiplicatif $G(3^\alpha)$.

On montre que pour chaque p premier impair, il existe un entier dont la classe (mod p^α) engendre le groupe multiplicatif $G(p^\alpha)$, $\forall\, \alpha$.

2) $\underline{m = 2^\alpha}$

. $m = 2$, $G(2) = \{1\}$.

. $m = 4$, $G(4)$ = groupe cyclique d'ordre 2 engendré par la classe de (-1) .

. $m = 2^\alpha$, $\alpha > 3$.

Alors $G(2^\alpha)$ est isomorphe au produit d'un groupe cyclique d'ordre 2 (engendré par la classe de (-1)) et d'un groupe d'ordre $2^{\alpha-2}$ (engendré par la classe de 3 (mod 2^α)) .

3) $\underline{m = m' m''}$, $(m' , m'') = 1$.

Alors $G(m)$ est isomorphe à $G(m') \times G(m'')$.

Exercice. Montrer que si $G(m)$ est cyclique et non réduit à l'élément neutre, on a :

- ou bien $m = 4$,
- ou bien $m = p^{\alpha}$ (p premier impair, $\alpha \geqslant 1$)
- ou bien $m = 2p^{\alpha}$ (p premier impair, $\alpha \geqslant 1$).

Théorème (sans démonstration).

Tout groupe abélien fini G est isomorphe à un produit de groupes cycliques dont les ordres sont des puissances de nombres premiers. Le nombre de ces groupes cycliques, ainsi que leurs ordres, sont déterminés de façon unique. (On n'aura pas à utiliser ce théorème).

aractères des groupes abéliens finis G (notés multiplicativement).

1.- Un caractère χ est un homomorphisme de G dans le groupe multiplicatif $\mathbb{C}^*$.

2.- Conséquence : les $\chi(x)$, où $x \in G$, sont des racines de l'unité car si = Card G, alors $(\chi(x))^n = \chi(x^n) = \chi(1) = 1$.

3.- Si χ_1 et χ_2 sont deux caractères de G, on définit leur produit $\chi_1\chi_2$ ar la formule : $(\chi_1 \chi_2)(x) = \chi_1(x) \cdot \chi_2(x)$. Alors $\chi_1 \chi_2$ est un caractère de (évident).

ette loi de composition dans l'ensemble $\hat{G}$ des caractères de G est commutative et ssociative ; elle possède un élément neutre qui est le caractère trivial egal à 1 ur tout élément de G ; on le note 1.

onséquence : $\hat{G}$ est un groupe abélien, car $\forall\ \chi \in \hat{G}$, $\exists\ \chi' \in \hat{G}$ tels que $\chi\chi' =$ ' est défini par $\forall x \in G$, $\chi'(x) = \frac{1}{\chi(x)}$.

éfinition : le groupe $\hat{G}$ s'appelle le dual du groupe G.

4.- Proposition.

Si G est un groupe cyclique d'ordre n, alors $\hat{G}$ est aussi cyclique d'ordre n.

émonstration :

Soit a un générateur de G ; alors $G = \{a, a^2, \ldots, a^n = 1\}$, les autres générateurs de G étant les a^k tels que $(k, n) = 1$. Dans ce cas, un caractère χ de est entièrement déterminé quand on connait $\chi(a)$, car $\forall p$, $\chi(a^p) = (\chi(a))^p$. On $\chi(a) \in \mathbb{C}^*$; quelles valeurs a-t-on le droit de donner à $\chi(a)$? Une condition écessaire est que $[\chi(a)]^n = \chi(a^n) = \chi(1) = 1$, i.e. que $\chi(a)$ soit une racine -ième de l'unité.

outrons que cette condition est suffisante :

Soit u une racine n-ième de l'unité, et posons $\chi(a^k) = u^k$. Le second membre dépend que de la classe de k (modulo n) car $u^n = 1$ par hypothèse ; donc la lation précédente définit bien une fonction χ ; on vérifie que χ est bien un ractère, et on a bien $\chi(a) = u$. Ainsi l'ensemble des caractères du groupe cyclique est en correspondance bijective avec l'ensemble des racines n-ièmes de l'unité.

---/---

Si $\chi_1(a) = u_1$, et $\chi_2(a) = u_2$, alors $(\chi_1 \chi_2)(a) = u_1 u_2$; donc la correspondance précédente est un isomorphisme de groupes. Le groupe $\hat{G}$ est <u>cyclique</u>, car le groupe multiplicatif des racines n-ièmes de l'unité est cyclique (engendré par une racine <u>primitive</u> n-ième de l'unité).

5.- Soient G et G' deux groupes finis et soit $\varphi : G \longrightarrow G'$ un homomorphisme. Soit $\hat{G}$ le dual de G, $\hat{G}'$ celui de G'. Un élément $\chi' \in \hat{G}'$ est un homomorphisme $\chi' : G' \longrightarrow \mathbb{C}^*$; si nous composons χ' et φ, nous obtenons un caractère $\chi = \chi' \circ \varphi \in \hat{G}$. L'application

$$\hat{\varphi} : \begin{cases} \hat{G}' \longrightarrow G \\ \chi' \longmapsto \chi = \chi' \circ \varphi \end{cases}$$

ainsi définie est un <u>homomorphisme de groupes</u> (vérification évidente).

<u>Conclusion</u>.

A tout homomorphisme $\varphi : G \longrightarrow G'$ on associe l'homomorphisme

$$\hat{\varphi} : \hat{G}' \longrightarrow \hat{G} .$$

Si on a trois groupes G, G', G'' et deux homomorphismes $\varphi : G \longrightarrow G'$, $\psi : G' \longrightarrow G''$, alors on a les trois groupes $\hat{G}$, $\hat{G}'$, $\hat{G}''$ et deux homomorphismes $\hat{\varphi} : \hat{G}' \longrightarrow \hat{G}$, $\hat{\psi} : \hat{G}'' \longrightarrow \hat{G}'$

$$G \xrightarrow{\varphi} G' \xrightarrow{\psi} G''$$

$$\hat{G}'' \xrightarrow{\hat{\psi}} \hat{G}' \xrightarrow{\hat{\varphi}} \hat{G}$$

et on vérifie que $\boxed{\widehat{\psi \circ \varphi} = \hat{\varphi} \circ \hat{\psi}}$ (attention à l'ordre !).

On dit alors que le dual $\hat{G}$ de G est défini comme <u>foncteur contravariant</u> de G (cf. les espaces vectoriels : le dual E^* d'un espace vectoriel E est un foncteur contravariant de E).

<u>Etude du dual d'un produit $G \times G'$</u>.

Soit χ un caractère de $G \times G'$; χ est un homomorphisme $G \times G' \longrightarrow \mathbb{C}^*$. Si $(x, x') \in G \times G'$, on a $(x, x') = (x, 1) \cdot (1, x')$. Donc $\chi(x, x') = \chi(x, 1) \cdot \chi(1, x')$. Considérons l'application $x \longmapsto \chi(x, 1)$ de G dans $\mathbb{C}^*$: c'est un homomorphisme car $\chi(x_1 x_2, 1) = \chi[(x_1, 1)(x_2, 1)] = \chi(x_1, 1) \cdot \chi(x_2, 1)$. Cette application est donc un caractère de G.

a donc $\chi(x, 1) = \chi_1(x)$, où $\chi_1 \in \hat{G}$

$\chi(1,x') = \chi_2(x')$, où $\chi_2 \in \hat{G'}$.

a $\chi(x, x') = \chi_1(x)\ \chi_2(x')$, où $\chi_1 \in \hat{G}$ et $\chi_2 \in \hat{G'}$ sont déterminés par la donnée

caractère χ.

résumé, si on note par i l'application canonique de G dans $G \times G'$ définie par

x) = (x, 1) et par $i' : G' \longrightarrow G \times G'$ (définie par $i'(x') = (1, x')$, on a les

hémas suivants :

$$\left.\begin{array}{l} G \xrightarrow{i} G \times G' \xrightarrow{\chi} \mathbb{C}^* \\ x \longrightarrow (x, 1) \longrightarrow \chi_1(x) \\ G' \xrightarrow{i'} G \times G' \xrightarrow{\chi} \mathbb{C}^* \\ x' \longrightarrow (1, x') \longrightarrow \chi_2(x') \end{array}\right\} \quad \text{on a} \quad \begin{array}{ccc} \widehat{G \times G'} & \xrightarrow{\hat{i}} & \hat{G} \\ \downarrow \hat{i}' & & \\ \hat{G'} & & \end{array}$$

éorème. Soit $\widehat{G \times G'} \longrightarrow \hat{G} \times \hat{G'}$ l'homomorphisme défini par $\hat{i}$ et $\hat{i}'$, à

voir $\chi \longmapsto (\hat{i}(\chi), \hat{i}'(\chi))$. Cet homomorphisme est un <u>isomorphisme de</u> $\widehat{G \times G'}$ sur

$\times \hat{G'}$.

<u>monstration.</u>

On définit un homomorphisme de $\hat{G} \times \hat{G'}$ dans $\widehat{G \times G'}$ par :

$$(\chi_1, \chi_2) \longmapsto \left[(x, x') \longmapsto \chi_1(x)\ \chi_2(x')\right].$$

on compose cette application avec l'homomorphsime de $\widehat{G \times G'}$ dans $\hat{G} \times \hat{G'}$ défini

ns l'énoncé, on trouve l'identité dans un sens comme dans l'autre ; donc les deux

nomorphismes sont des isomorphismes, réciproques l'un de l'autre.

<u>nclusion.</u>

Le groupe dual d'un produit $G \times G'$ s'identifie au produit des duaux de G et

<u>arque</u> : Il ne faut pas croire que si G et G' sont cycliques, $G \times G'$ soit

lique!

<u>actères d'un groupe quotient</u> G/H.

t p la projection canonique de G dans G/H ; on a alors l'homomorphisme

$\widehat{G/H} \longrightarrow \hat{G}$; $\hat{p}$ s'explicite ainsi : à un caractère χ de G/H elle associe

caractère de G défini par la composition $G \xrightarrow{p} G/H \xrightarrow{\chi} \mathbb{C}^*$.

a) Montrons que l'homomorphisme $\hat{p}$ est une <u>injection</u>, c'est-à-dire que son noyau est réduit à l'élément neutre. Or si χ est tel que $\chi \circ p = 1$, alors $\chi = 1$ car p est surjective : C.Q.F.D.

On a ainsi la <u>suite exacte</u> $\{1\} \longrightarrow \widehat{G/H} \xrightarrow{\hat{p}} \hat{G}$.

b) Quels sont les caractères de G qu'on obtient dans l'image de $\hat{p}$?

Le caractère $\chi \circ p$ prend la valeur 1 sur H. Réciproquement, soit χ' un caractère de G tel que, $\forall x \in H$, $\chi'(x) = 1$; alors on peut passer au quotient et χ' induit un homomorphisme $\chi : G/H \longrightarrow \mathbb{C}^*$, et on a la relation $\chi' = \chi \circ p$. Donc si on note $\hat{i}$ l'application canonique : $\hat{G} \longrightarrow \hat{H}$ on a la suite exacte

$$\{1\} \longrightarrow \widehat{G/H} \xrightarrow{\hat{p}} \hat{G} \xrightarrow{\hat{i}} \hat{H}, \quad \text{puisque } \operatorname{Im} \hat{p} = \operatorname{Ker} \hat{i}.$$

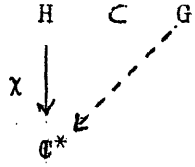
c) Montrons que $\hat{i}$ est <u>surjectif</u>.

Par définition, $\hat{i}(\chi) = \chi|H$. Dire que $\hat{i}$ est surjectif, c'est dire que tout caractère de H provient par restriction à H d'un caractère de G, ou encore :

<u>Proposition.</u> <u>Tout caractère de</u> H <u>peut se prolonger en un caractère de</u> G.

<u>Démonstration.</u>

Soit H un sous-espace de G, et soit χ un caractère de H. On cherche un homomorphisme $\dashrightarrow$ de G dans $\mathbb{C}^*$ prolongeant χ.



Si $G = H$, alors χ répond à la question.

Si $G \neq H$, alors il existe $x \in G$ tel que $x \notin H$; x et H engendrent un sous-groupe G_1 de G : $H \subset G_1 \subset G$. Pour résoudre le problème, il suffit de montrer qu'on peut prolonger χ à G_1, car si $G_1 \neq G$ alors on recommence avec $H \subset G_1 \subset G_2 \subset G$. Comme G est fini, on ne fera qu'un nombre fini de fois cette opération.

On va donc supposer que $G = G_1$ et on appellera encore χ un prolongement cherché de χ à G.

Il faut donc définir $\chi(x)$. Or la classe de x dans G/H est d'ordre fini. Il en existe donc une puissance qui soit l'élément neutre dans G/H : soit n le plus

petit entier n tel que $x^n \in H$ (i.e. $\hat{x}^n = e$) ; alors $(\chi(x))^n = \chi(x^n)$ est déjà connu. Soit donc $\alpha \in \mathbb{C}^*$ tel que $\alpha^n = \chi(x^n)$. Montrons qu'il existe un caractère χ et un seul de G qui prolonge χ sur H et qui satisfait à $\chi(x) = \alpha$.

En effet tout élément de G s'écrit sous la forme $g = x^p h$, où $h \in H$ et $p \in \mathbb{N}$. Posons alors

$$\chi(x^p h) = \alpha^p \chi(h) \quad ;$$

ceci définit χ, à condition que la valeur du deuxième membre ne dépende pas de la manière d'écrire g sous la forme $x^p h$; vérifions-le. Pour cela montrons que si $x^p h = 1$ dans G, alors $\alpha^p \chi(h) = 1$ dans $\mathbb{C}^*$. Or

$x^p h = 1 \Longrightarrow x^p \in H \Longrightarrow p = kn \Longrightarrow \alpha^p = (\alpha^n)^k = (\chi(x^n))^k \Longrightarrow h = x^{-kn}$

$\Longrightarrow \alpha^p \chi(h) = [\chi(x^n)]^k \chi(x^{-kn}) = \chi(1) = 1$, car χ est un caractère sur H. χ étant ainsi bien défini, on vérifie facilement que χ est un homomorphisme de G dans $\mathbb{C}^*$, qui prolonge bien le caractère χ donné sur H ; C.Q.F.D.

Conséquence de cette proposition : on a la suite exacte

$$\{1\} \longrightarrow \widehat{G/H} \xrightarrow{\hat{p}} \hat{G} \xrightarrow{\hat{i}} \hat{H} \longrightarrow \{1\}$$

Théorème. Si G est un groupe abélien fini, on a $\operatorname{Card} \hat{G} = \operatorname{Card} G$.

Démonstration.

On fait une récurrence sur l'ordre (= cardinal) de G.

a) Si $\operatorname{Card} G = 1$, alors $\operatorname{Card} \hat{G} = 1$.

b) Si G est cyclique, nous savons que le théorème est vrai.

c) Si G n'est pas cyclique, soit $y \neq 1$, $y \in G$; y engendre un sous-groupe cyclique H de G.

Considérons la suite exacte : $\{1\} \longrightarrow H \longrightarrow G \longrightarrow G/H \longrightarrow \{1\}$. On a $\operatorname{Card} G/H < \operatorname{Card} G$. H étant cyclique, on a $\operatorname{Card} H = \operatorname{Card} \hat{H}$, et par l'hypothèse de récurrence, $\operatorname{Card} G/H = \operatorname{Card} \widehat{G/H}$. Considérant la suite exacte $\{1\} \longrightarrow (G/H)^{\wedge} \longrightarrow \hat{G} \longrightarrow \hat{H} \longrightarrow \{1\}$, on a les relations :

$$\left.\begin{aligned} \operatorname{Card} G &= \operatorname{Card} H \times \operatorname{Card} (G/H) \\ \operatorname{Card} \hat{G} &= \operatorname{Card} \widehat{(G/H)} \times \operatorname{Card} \hat{H} \end{aligned}\right\} \Longrightarrow \operatorname{Card} G = \operatorname{Card} \hat{G}$$

Rappel :

Dans une suite exacte, $\{1\} \longrightarrow G' \longrightarrow G \longrightarrow G'' \longrightarrow \{1\}$, on a toujours

$$\boxed{\text{Card } G = (\text{Card } G') \times (\text{Card } G'')}$$

Etude du bidual $\hat{\hat{G}}$ d'un groupe abélien G fini.

$\hat{\hat{G}}$ est, par définition, le groupe des caractères du groupe $\hat{G}$, qui est lui aussi fini. Si $x \in G$, l'application $\chi \longmapsto \chi(x)$ de $\hat{G}$ dans $\mathbb{C}^*$ est un caractère de $\hat{G}$, car $(\chi_1 \chi_2)(x) = \chi_1(x)\, \chi_2(x)$ (par définition du produit $\chi_1 \chi_2$).

Soit i l'application $G \longrightarrow \hat{\hat{G}}$ définie par

$$x \longmapsto [\chi \longmapsto \chi(x)] :$$

c'est un homomorphisme de groupes, car $x = x_1 x_2 \Longrightarrow \chi(x) = \chi(x_1)\, \chi(x_2)$ pour chaque χ de $\hat{G}$, et par suite le caractère $i(x)$ est le produit des caractères $i(x_1)$ et $i(x_2)$.

Théorème. L'homomorphisme $i : x \longmapsto [\chi \longmapsto \chi(x)]$ de G dans $\hat{\hat{G}}$ est un isomorphisme de groupes.

Démonstration.

a) L'application i est injective ; cherchons en effet son noyau :

$$\text{Ker } i = \{x \in G : \forall \chi \in \hat{G},\ \chi(x) = 1\}.$$

Montrons que $x \in \text{Ker } i \Longleftrightarrow x = 1$, ou encore que si $x \neq 1$, $x \in G$, il existe $\chi \in \hat{G}$ tel que $\chi(x) \neq 1$.

Soit $x \in G$, $x \neq 1$; alors x engendre un sous-groupe cyclique H de G avec Card $H \neq 1$. Alors $\hat{H}$ est engendré par un caractère χ de H dont la valeur sur x est une racine primitive k-ième de l'unité, où k = ordre de x = Card H ; comme $k \neq 1$, on a $\chi(x) \neq 1$. Nous savons que nous pouvons prolonger ce caractère χ de H en un caractère de G qui est bien tel que $\chi(x) \neq 1$. C.Q.F.D.

b) L'application i est surjective.

Utilisons le théorème précédent : Card G = Card $\hat{G}$; en remplaçant G par $\hat{G}$, on a alors Card $\hat{G}$ = Card $\hat{\hat{G}}$, et par conséquent Card G = Card $\hat{\hat{G}}$. Comme $i : G \longrightarrow \hat{\hat{G}}$ est injective, elle est bijective. C.Q.F.D.

Désormais nous identifierons G et $\hat{G}$ au moyen de i : chacun des groupes G et $\hat{G}$ s'identifie au dual de l'autre.

Théorème . Soit χ un caractère de G ; alors

$$\sum_{x \in G} \chi(x) = \begin{cases} 0 & \text{si } \chi \neq 1, \\ \text{Card } G & \text{si } \chi = 1 \end{cases}$$

Démonstration.

1.- Si $\chi = 1$, évident.

2.- Si $\chi \neq 1$, alors $\exists\, y \in G : \chi(y) \neq 1$. Choisissons un tel y. On a $\sum_{x \in G} \chi(x) = \sum_{x \in G} \chi(xy)$; en effet l'application $x \longmapsto xy$ de G dans G étant bijective, xy décrit une fois et une seule G. Or $\chi(xy) = \chi(x)\,\chi(y)$, d'où $\sum_{x \in G} \chi(x) = \chi(y) \left(\sum_{x \in G} \chi(x)\right)$ dans $\mathbb{C}^*$. Comme $\chi(y) \neq 1$, on en déduit :

$$\sum_{x \in G} \chi(x) = 0.$$

Cas particulier :

Soit G un groupe cyclique d'ordre n, et soit a un générateur de G, on va donner une autre démonstration du théorème dans ce cas particulier. On veut calculer $\sum_{k=1}^{n} \chi(a^k) = \sum_{k=1}^{n} [\chi(a)]^k$.

1.- Si $\chi = 1 \Longrightarrow \chi(a) = \chi(a^k) = 1 \Longrightarrow \sum_{k=1}^{n} \chi(a^k) = \text{Card } G = n.$

2.- Si $\chi \neq 1$, $\chi(a) \neq 1$; alors $\chi(a)$ est une racine n-ième ; soit d son ordre qui divise n. On a donc $[\chi(a)]^d = 1$, $d \mid n$, $d \geq 2$.

Il y a d puissances de $\chi(a)$ distinctes et chacune de ces valeurs se retrouve $\frac{n}{d}$ fois $\Longrightarrow \sum_{k=1}^{n} \chi(a^k) = \frac{n}{d} \sum_{k=1}^{d} \chi(a^k)$. Or $\sum_{k=1}^{d} \chi(a^k)$ est la somme de toutes les racines d-ièmes de l'unité, donc la somme des racines du polynôme $X^d - 1 = 0$ pour $d \geq 2$; c'est le coefficient de X^{d-1}, c'est donc nul.

Théorème dual. Soit x un élément donné de G ; alors

$$\sum_{\chi \in \hat{G}} \chi(x) = \begin{cases} 0 & \text{si } x \neq 1 \\ \text{Card } G & \text{si } x = 1 \end{cases}$$

La démonstration de ce théorème est évidente : on applique le théorème précédent en remplaçant G par $\hat{G}$, et $\hat{G}$ par G (compte tenu du fait que $\hat{\hat{G}} \approx G$).

Retour aux entiers modulo m.

On s'intéresse au dual $\widehat{G(m)}$ du groupe multiplicatif G(m) des éléments inversibles de $\mathbb{Z} / m\mathbb{Z}$. On sait que Card G(m) = $\varphi(m)$, donc Card $\widehat{G(m)} = \varphi(m)$. Soit $\chi \in \widehat{G(m)}$; χ est un homomorphisme : $G(m) \longrightarrow \mathbb{C}^*$; on peut relever cette application sur l'ensemble E(m) des entiers premiers à m : on compose χ avec l'application canonique de E(m) sur G(m), et on notera encore χ cette application de E(m) dans $\mathbb{C}^*$.

On a alors $\chi(ab) = \chi(a)\,\chi(b)$, et $\chi(a)$ ne dépend que de la classe de a (modulo m), a étant supposé premier à m.

Définition. On prolonge $\chi : E(m) \longrightarrow \mathbb{C}^*$ en une application $\chi : \mathbb{Z} \longrightarrow \mathbb{C}$, en posant $\chi(a) = 0$ si $(a, m) \neq 1$. On vérifie :

(1) $\chi(a) = 0 \iff (a, m) \neq 1$;

(2) $\chi(ab) = \chi(a)\,\chi(b)$ quels que soient a et $b \in \mathbb{Z}$;

(3) $\chi(a)$ ne dépend que de la classe de a modulo m.

Une telle fonction χ s'appelle un caractère modulo m.

L'ensemble de ces fonctions est en correspondance bijective avec le groupe dual $\widehat{G(m)}$; elles sont en nombre $\varphi(m)$.

Dans toute la suite, m sera fixé et χ désignera un caractère modulo m.

Rappel :

$$\zeta(s) = \sum_{n \geq 1} \frac{1}{n^s} \quad \text{pour} \quad \mathrm{Re}(s) > 1.$$

On pose

$$\boxed{L(s, \chi) = \sum_{n \geq 1} \frac{\chi(n)}{n^s} \quad \text{pour} \quad \mathrm{Re}(s) > 1}$$

Propriétés de $L(s, \chi)$.

1.- On est sûr que la série de somme $L(s, \chi)$ converge normalement dans tout demi-plan $\mathrm{Re}(s) \geq \alpha > 1$; $L(s, \chi)$ est donc holomorphe pour $\mathrm{Re}(s) > 1$; elle dépend évidemment du caractère χ modulo m.

2.- Si on considère le produit infini $\prod_{p \in P} (1 - \frac{\chi(p)}{p^s})$, il est normalement convergent dans tout demi-plan $Re(s) \geq \alpha > 1$; sa valeur est une fonction holomorphe, qui ne s'annule jamais, dans le demi-plan $Re(s) > 0$.

Théorème. On a

(1) $$\boxed{L(s, \chi) = \frac{1}{\prod_{p \in P} (1 - \frac{\chi(p)}{p^s})}}$$

Démonstration.

Soit $P' \subset P$, P' fini ; on a

$$\frac{1}{\prod_{p \in P'} (1 - \frac{\chi(p)}{p^s})} = \prod_{p \in P'} (1 + \frac{\chi(p)}{p^s} + \frac{\chi(p^2)}{p^{2s}} + \ldots)$$

$$\frac{1}{\prod_{p \in P'} (1 - \frac{\chi(p)}{p^s})} = \sum_{p_i \in P'} \frac{\chi(p_1^{k_1} \ldots p_\alpha^{k_\alpha})}{(p_1^{k_1} \ldots p_\alpha^{k_\alpha})^s} = \sum_{n \in \mathcal{P}} \frac{\chi(n)}{n^s} ,$$

où $\mathcal{P} \subset \mathbb{N}$ est l'ensemble des entiers dont tous les facteurs premiers appartiennent à P'.

En passant à la limite on obtient immédiatement le théorème cherché.

Cas particulier.

$\chi = 1$ est le caractère trivial : il est égal à 1 sur les n premiers à m, à 0 sur les autres entiers n. On a alors :

$$L(s, 1) = \sum_{\substack{n \in \mathbb{N} \\ (n,m)=1}} \frac{1}{n^s} = \prod_{\substack{p \in P \\ p \nmid m}} \frac{1}{1 - \frac{1}{p^s}} .$$

On constate que $L(s, 1)$ ne diffère de $\zeta(s)$ que pour un produit fini :

$$\zeta(s) = \left(\prod_{p \mid m} \frac{1}{1 - \frac{1}{p^s}}\right) \cdot L(s,1) ,$$

ou encore

$$\boxed{\frac{\zeta(s)}{L(s,1)} = \prod_{p \mid m} \frac{1}{1 - \frac{1}{p^s}}}$$

Définition.

$$f_\chi(s) = \sum_{p \in P} \frac{\chi(p)}{p^s}$$

Proposition.

(2) $$\sum_{p \in P_a} \frac{1}{p^s} = \frac{1}{\varphi(m)} \sum_{\chi} \chi(a)^{-1} f_\chi(s) \qquad \text{pour} \qquad \mathrm{Re}(s) > 1 ,$$

où $P_a = \{ p \in P : p \equiv a \pmod m \}$, et où la sommation est étendue à tous les caractères modulo m.

Démonstration.

$f_\chi(s)$ est une fonction holomorphe pour $\mathrm{Re}(s) > 1$, car c'est une série partielle de la série $L(s, \chi)$, qui converge normalement dans tout demi-plan $\mathrm{Re}(s) \geq \alpha > 1$. D'autre part, la $\sum_\chi$ est finie.

D'après la définition de la fonction $f_\chi(s)$, on a :

$$\chi(a)^{-1} f_\chi(s) = \sum_{p \in P} \frac{\chi(a)^{-1} \chi(p)}{p^s} = \sum_{p \in P} \frac{\chi(a^{-1} p)}{p^s} .$$

Donc

$$\sum_\chi \chi(a)^{-1} f_\chi(s) = \sum_{p \in P} \Big(\sum_\chi \frac{\chi(a^{-1} p)}{p^s} \Big) \quad ; \quad \text{or} \quad \chi(a^{-1} p) = 0 \quad \text{si}$$

$p \notin G(m)$.

Si $p \in G(m)$, on a, d'après la relation fondamentale des caractères,

$$\sum_\chi \chi(a^{-1} p) = \begin{cases} 0, & \text{si } a^{-1} p \not\equiv 1 \pmod m \\ \text{Card } G(m), & \text{si } a^{-1} p \equiv 1 \pmod m . \end{cases}$$

Or $p \equiv a \pmod m \iff p \in P_a \iff a^{-1} p \equiv 1 \pmod m$

$\Rightarrow \sum_\chi \chi(a^{-1} p) = \text{Card } G(m) = \varphi(m)$ et par conséquent

$$\sum_\chi \chi(a)^{-1} f_\chi(s) = \varphi(m) \sum_{p \in P_a} \frac{1}{p^s} .$$

D'où : $$\sum_{p \in P_a} \frac{1}{p^s} = \frac{1}{\varphi(m)} \sum_\chi \chi(a)^{-1} f_\chi(s) \quad \text{pour} \quad \mathrm{Re}(s) > 1 \qquad \text{C.Q.F.D.}$$

Dans la relation (1) ci-dessus, prenons les logarithmes

$$(1') \qquad \log L(s, \chi) = \sum_{p \in P} - \log \left(1 - \frac{\chi(p)}{p^s}\right) .$$

Dans le second membre, on a pris la détermination principale de $\log(1-u)$ pour $|u| < 1$; la série converge, et sa somme définit la détermination de $\log L(s, \chi)$ pour laquelle la relation (1') est vraie. Les deux membres sont alors des fonctions holomorphes de s pour $\mathrm{Re}(s) > 1$.

Théorème 1. $\log L(s, \chi) - f_\chi(s)$ se prolonge en une fonction $\Psi_\chi(s)$ holomorphe pour $\mathrm{Re}(s) > \frac{1}{2}$.

[En particulier, $\Psi_\chi(s)$ est holomorphe au voisinage de $s = 1$.]

(Démonstration plus loin).

Corollaire. Compte tenu de la proposition ci-dessus (formule (2)), on voit que $\sum_\chi \chi(a)^{-1} \log L(s, \chi) - \varphi(m) \sum_{p \in P_a} \frac{1}{p^s} = \sum_\chi \chi(a)^{-1} \Psi_\chi(s)$ se prolonge en une fonction holomorphe pour $\mathrm{Re}(s) > \frac{1}{2}$.

Conclusion : pour étudier le comportement de $\sum_{p \in P_a} \frac{1}{p^s}$ quand s tend vers 1, il suffira d'étudier le comportement de $\log L(s, \chi)$ lorsque $s \longrightarrow 1$, pour chaque caractère χ.

(1) χ est le caractère trivial ; donc $\chi(a)^{-1} = 1$. On sait que $\zeta(s) = L(s, 1) \prod_{p|m} \frac{1}{1 - \frac{1}{p^s}}$. Donc $\log \zeta(s) = \log L(s, 1) - \sum_{p|m} \log \left(1 - \frac{1}{p^s}\right)$.

Or nous savons que $\log(1 - \frac{1}{p^s})$ est holomorphe pour $\mathrm{Re}(s) > 0$ et par conséquent $\sum_{p|m} \log(1 - \frac{1}{p^s})$ est holomorphe pour $\mathrm{Re}(s) > 0$. D'autre part, $\log \zeta(s) - \log \frac{1}{s-1}$ est holomorphe au voisinage de $s = 1$. Donc $\log L(s, 1) - \log \frac{1}{s-1}$ est holomorphe au voisinage de $s = 1$.

(2) χ n'est pas le caractère trivial.

Théorème 2. Si $\chi \neq 1$, alors $L(s, \chi)$ se prolonge en une fonction holomorphe pour $\mathrm{Re}(s) > 0$, dont la valeur pour $s = 1$ est différente de zéro.

(Démonstration plus loin).

Conséquence : compte tenu du corollaire au théorème 1, on voit que

$\varphi(m)\ (\sum_{p \in P_a} \frac{1}{p^s}) - \log \frac{1}{s-1}$ est holomorphe au voisinage de $s = 1$. D'où

$$\lim_{\substack{s \to 1 \\ Re(s) > 1}} \frac{1}{\log \frac{1}{s-1}} \left(\sum_{p \in P_a} \frac{1}{p^s} \right) = \frac{1}{\varphi(m)} .$$

Or le premier membre est, par définition la densité de P_a. Nous avons donc ainsi démontré le théorème de Dirichlet, en utilisant les théorèmes 1 et 2. Il reste à prouver ces deux théorèmes.

Démonstration du théorème 1.

La démonstration va être analogue à la démonstration (déjà donnée plus haut) du fait que $\log \zeta(s) - \sum_{p \in P} \frac{1}{p^s} = \psi(s)$ est holomorphe pour $Re(s) > \frac{1}{2}$.

On a ici :

$$\log L(s, \chi) = \sum_{p \in P} - \log \left[1 - \frac{\chi(p)}{p^s} \right] .$$

Par hypothèse $\chi \neq 1$. Pour un p donné, si $Re(s) > 0$ on a $\left|\frac{\chi(p)}{p^s}\right| < 1$ et par conséquent

$$- \log\left[1 - \frac{\chi(p)}{p^s} \right] = \frac{\chi(p)}{p^s} + \frac{\chi(p)^2}{2p^{2s}} + \frac{\chi(p)^3}{p^{3s}} + \ldots + \frac{\chi(p)^n}{n\, p^{ns}} + \ldots$$

Donc

$$- \log\left[1 - \frac{\chi(p)}{p^s} \right] - \frac{\chi(p)}{p^s} = \frac{\chi(p)^2}{2p^{2s}} + \frac{\chi(p)^3}{p^{3s}} + \ldots + \frac{\chi(p)^n}{n\, p^{ns}} + \ldots = \psi_p(s),$$

fonction holomorphe pour $Re(s) > 0$.

On va majorer $\psi_p(s)$. Si $Re(s) \geq \alpha > 0$, alors

$$|\psi_p(s)| \leq \frac{1}{2p^{2\alpha}} + \frac{1}{3p^{3\alpha}} + \ldots + \frac{1}{n\, p^{n\alpha}} + \ldots = \frac{1}{2p^{2\alpha}} \left(1 + \frac{1}{p^{\alpha}} + \frac{1}{p^{2\alpha}} + \ldots\right).$$

D'où

$$|\psi_s(s)| \leq \frac{1}{2p^{2\alpha}} \cdot \frac{1}{1 - \frac{1}{p^{\alpha}}} \qquad \text{pour} \quad Re(s) \geq \alpha > 0.$$

Supposons désormais $\alpha > \frac{1}{2}$; alors $\forall p \in P$, $\frac{1}{1 - \frac{1}{p^{\alpha}}} \leq 4$ car $\frac{1}{1 - p^{-\alpha}}$ atteint son maximum pour $p = 2$, $\alpha = \frac{1}{2}$, et $\frac{1}{1 - \frac{1}{\sqrt{2}}} \leq 4$.

Si $\alpha > \frac{1}{2}$, on a donc $|\psi_p(s)| \leq \frac{2}{p^{2\alpha}}$ pour $\mathrm{Re}(s) \geq \alpha$. Pour $\alpha > \frac{1}{2}$, la série $\sum_{p \in P} \frac{2}{p^{2\alpha}}$ converge ; donc la série $\sum_{p \in P} \psi_p(s)$ est normalement convergente pour $\mathrm{Re}(s) \geq \alpha > \frac{1}{2}$; sa somme $\psi(s)$ est donc une fonction holomorphe pour $\mathrm{Re}(s) > \frac{1}{2}$.

Conclusion. $\log L(s, \chi) - \sum_{p \in P} \frac{\chi(p)}{p^s}$ est holomorphe pour $\mathrm{Re}(s) > \frac{1}{2}$, ce qui démontre le théorème 1.

Démonstration du théorème 2. On va prouver deux choses :

a) première assertion : si $\chi \neq 1$, alors $L(s, \chi)$ est holomorphe pour $\mathrm{Re}(s) > 0$.

Pour cela, on utilise le :

Lemme 1.

Si on a une série $\sum_{n \geq 1} \frac{a_n}{n^s}$, où les $a_n \in \mathbb{C}$ vérifient la condition :

$$\forall u, v \in \mathbb{N}, \quad \left| \sum_{n=u+1}^{v} a_n \right| \leq A \quad \text{fixe},$$

alors la série $\sum_{n \geq 1} \frac{a_n}{n^s}$ converge pour $\mathrm{Re}(s) > 0$, et converge uniformément sur tout compact K contenu dans la bande $\mathrm{Re}(s) > 0$.

La somme de cette série est donc une fonction holomorphe pour $\mathrm{Re}(s) > 0$.

Démonstration.

Soit $u \in \mathbb{N}$, et posons $\sigma_u(s) = \sum_{n=1}^{u} \frac{a_n}{n^s}$. Soit $v \in \mathbb{N}$, $u < v$; alors :

$$\sigma_v(s) - \sigma_u(s) = \sum_{n=u+1}^{v} \frac{a_n}{n^s}.$$

Si toutes ces sommes partielles tendent uniformément vers zéro quand u et $v \to +\infty$, alors d'après le critère de Cauchy, on aura démontré la convergence uniforme de la série.

On pose

$$A_{u,v} = \sum_{n=u+1}^{v} a_n$$

Par hypothèse, on a $|A_{u,v}| \leq A$. Or (transformation d'Abel)

$$(1)\quad \sigma_v(s) - \sigma_u(s) = \sum_{n=u+1}^{v-1} A_{u,n}\left(\frac{1}{n^s} - \frac{1}{(n+1)^s}\right) + A_{u,v}\frac{1}{v^s} .$$

On va majorer $\left|\frac{1}{n^s} - \frac{1}{(n+1)^s}\right|$ pour $\mathrm{Re}(s) \geqslant \alpha > 0$. On a

$$\frac{1}{n^s} - \frac{1}{(n+1)^s} = s\int_n^{n+1} \frac{dx}{x^{s+1}} \quad , \quad \frac{1}{n^\alpha} - \frac{1}{(n+1)^\alpha} = \alpha\int_n^{n+1} \frac{dx}{x^{\alpha+1}} \quad , \text{ d'où :}$$

$$\left|\frac{1}{n^s} - \frac{1}{(n+1)^s}\right| \leqslant \frac{|s|}{\alpha}\left(\frac{1}{n^\alpha} - \frac{1}{(n+1)^\alpha}\right) \leqslant \frac{|s|}{\alpha}\frac{1}{n^\alpha} .$$

On déduit alors de (1) :

$$(2)\quad |\sigma_v(s) - \sigma_u(s)| \leqslant A\left(\frac{|s|}{\alpha} + 1\right).\frac{1}{u^\alpha} ,$$

quel que soit $v > u$, et quel que soit s tel que $\mathrm{Re}(s) \geqslant \alpha$.

Comme $\alpha > 0$, $\sigma_v(s) - \sigma_u(s)$ tend vers 0 quand $u \to +\infty$; si s appartient à un compact K contenu dans $\mathrm{Re}(s) > 0$, il existe $\alpha > 0$ et $k > 0$ tels que $\mathrm{Re}(s) \geqslant \alpha$ et $|s| \leqslant k$, donc (2) prouve la convergence uniforme, et le lemme 1 est prouvé. .

Pour prouver la "première assertion", il reste à vérifier que la série

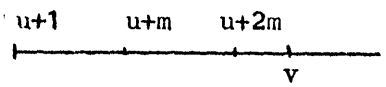
$$L(s, \chi) = \sum_{n \geq 1} \frac{\chi(n)}{n^s}$$ satisfait à l'hypothèse du lemme.

Ici $a_n = \chi(n)$. Il s'agit de majorer $\left| \sum_{n = u+1}^{v} \chi(n) \right|$ par une constante A indépendante de u et v .

Pour cela, utilisons la relation des caractères : $\chi(n)$ ne dépend que du reste de n (modulo m). Regardons d'abord ce qui se passe quand on somme sur une péricde :

$\sum_{n = u+1}^{u+m} \chi(n) = \sum_{n \in G_m} \chi(n) = 0$ puisque $\chi \neq 1$ par hypothèse.

Donc quand on considère $\sum_{n = u+1}^{v} \chi(n)$, c'est égal à une somme de moins de m termes consécutifs, et par conséquent une somme qui a au plus $\varphi(m)$ termes non nuls ; comme chacun d'eux est de valeur absolue un,



On a $\left| \sum_{n = u+1}^{v} \chi(n) \right| \leq \varphi(m)$, qui est la constante A cherchée.

Conclusion. La somme de la série $\sum_{n \geq 1} \frac{\chi(n)}{n^s}$ est une fonction $L(s, \chi)$ holomorphe pour $Re(s) > 0$, sous l'hypothèse que $\chi \neq 1$.

b) Deuxième assertion : si $\chi \neq 1$, alors $L(1, \chi) \neq 0$ (ici, $L(1, \chi)$ désigne la valeur, pour $s = 1$, de la fonction $L(s, \chi)$ qui, on vient de le voir, est holomorphe pour $Re(s) > 0$).

Démonstration.

Considérons $\zeta_m(s) = \prod_\chi L(s, \chi)$, le produit étant étendu à tous les caractères modulo m. C'est un produit de $\varphi(m)$ termes dont l'un, celui relatif à $\chi = 1$, admet un pôle simple en $s = 1$ (avec résidu égal à 1).

On sait aussi que $L(s, \chi)$ est holomorphe pour $Re(s) > 0$ si $\chi \neq 1$. Donc dire que $L(1, \chi) \neq 0$ pour tout $\chi \neq 1$, c'est dire que $\zeta_m(s)$, qui est méromorphe pour $Re(s) > 0$ comme produit de $\varphi(m) - 1$ fonctions holomorphes et d'une fonction méromorphe, a effectivement un pôle au point $s = 1$, ou encore que $\zeta_m(s)$ n'est pas holomorphe pour $Re(s) > 0$. C'est ce qui nous reste à démontrer.

Or $\zeta_m(s)$ est un produit fini de produits infinis :

$$\zeta_m(s) = \prod_\chi \prod_{p \in P} \left[1 - \frac{\chi(p)}{p^s}\right]^{-1} \qquad \text{pour } Re(s) > 1.$$

On peut échanger l'ordre des produits : on a

$$\zeta_m(s) = \prod_{p \in P} \prod_\chi \left[1 - \frac{\chi(p)}{p^s}\right]^{-1} = \prod_{\substack{p \in P \\ p \nmid m}} \prod_\chi \left[1 - \frac{\chi(p)}{p^s}\right]^{-1},$$

car $\chi(p) = 0$ si p divise m.

Considérons le polynôme en une indéterminée X : $\prod_\chi [1 - \chi(p)\, X]$.

C'est un polynôme $P(X)$ de degré $\varphi(m)$.

Lemme 2.

Si $p \nmid m$, alors $P(X) = \left[1 - X^{f(p)}\right]^{g(p)}$, où $f(p)$ est l'ordre de p dans le groupe $G(m)$, et où $g(p) = \frac{\varphi(m)}{f(p)}$.

Démonstration du lemme 2.

$P(X) = \prod_\chi [1 - \chi(p)\, X]$, où χ parcourt le dual de $G(m)$; $\chi(p)$ est une racine $f(p)$-ième de 1. On va montrer que lorsque χ parcourt $\widehat{G(m)}$, $\chi(p)$ prend $g(p)$ fois chaque racine $f(p)$-ième de 1.

Dans $G(m)$, la classe de p engendre un groupe cyclique G' d'ordre $f(p)$, par définition de $f(p)$.

oit G'' le groupe quotient $G(m)/G'$. On a alors la suite exacte

$$1) \longrightarrow G' \longrightarrow G(m) \longrightarrow G'' \longrightarrow (1),$$

et on en déduit la suite exacte :

$$(1) \longrightarrow \hat{G}'' \longrightarrow \widehat{G(m)} \longrightarrow \hat{G}' \longrightarrow (1).$$

L'homomorphisme $\widehat{G(m)} \longrightarrow \hat{G}'$ est celui qui, à chaque caractère χ de $G(m)$, ssocie sa restriction à G'. Dans le noyau $\hat{G}''$, il y a $g(p)$ éléments ; donc our chaque caractère de G' il y a $g(p)$ caractères de $G(m)$ qui l'induisent. insi : quelle que soit la racine $f(p)$-ième de l'unité θ, il existe exactement (p) caractères χ tels que $\chi(p) = \theta$. Donc

$$P(X) = \prod_{\chi} [1 - \chi(p)\, X] = \Big[\prod_{\theta} (1 - \theta\, X) \Big]^{g(p)}.$$

Il reste à vérifier que

$$\prod_{\theta} (1 - \theta\, X) = 1 - X^{f(p)}.$$

Or on sait que $\prod_{\theta} (X - \theta) = X^{f(p)} - 1$. Faisons le changement de variable $X \longrightarrow \frac{1}{Y}$ et il vient $\prod_{\theta} (\frac{1}{Y} - \theta) = \frac{1}{Y^{f(p)}} - 1$. Il suffit alors de multiplier les deux membres par $Y^{f(p)}$.

Dans l'identité du lemme 2, remplaçons maintenant X par $\frac{\chi(p)}{p^s}$; on obtient :

$$\zeta_m(s) = \prod_{p \nmid m} \Big[\prod_{\chi} (1 - \frac{\chi(p)}{p^s})^{-1} \Big] = \prod_{p \nmid m} \frac{1}{\big[1 - (\frac{1}{p^s})^{f(p)}\big]^{g(p)}}.$$

Si on développe en série $\Big[1 - (\frac{1}{p^s})^{f(p)}\Big]^{g(p)}$, on trouve

$$(1 - p^{-f(p)s})^{-g(p)} = 1 + \sum_{k \geq 1} \frac{b_{k,p}}{\big[p^{f(p)s}\big]^k},$$

où les coefficients $b_{k,p}$ sont des entiers ≥ 0. Si on multiplie toutes ces séries pour $p \nmid m$, terme à terme, on trouve une série de la forme $\zeta_m(s) = \sum_{n \geq 1} \frac{a_n}{n^s}$, où $a_1 = 1$, et où beaucoup de a_n sont nuls ; mais c'est une série <u>à coefficients entiers</u> ≥ 0. C'est le développement en série de Dirichlet de la fonction $\zeta_m(s)$. n sait que cette série converge pour $\mathrm{Re}(s) > 1$, car tous les calculs précédents ont licites pour $\mathrm{Re}(s) > 1$.

Proposition.

La série $\sum_{n \geq 1} \frac{a_n}{n^s}$ de $\zeta_m(s)$ ne converge pas pour toutes les valeurs réelles >0 de s.

Démonstration.

Il suffit de trouver une autre série $\sum_{n \geq 1} \frac{b_n}{n^s}$, où $b_n \leq a_n$, et qui diverge pour certains réels > 0. Pour cela développons par une autre méthode $\left[\frac{1}{1-p^{-f(p)s}}\right]^{g(p)}$

$$\left(\frac{1}{1-p^{-f(p)s}}\right)^{g(p)} = (1 + p^{-f(p)s} + p^{-2f(p)s} + \ldots)^{g(p)}$$

$$\leq (1)^{g(p)} + (p^{-f(p)s})^{g(p)} + (p^{-2f(p)s})^{g(p)} .$$

On voit que les coefficients $b_{k,p}$ sont majorés par ceux de cette série qui n'est autre que

$$1 + \frac{1}{p^{\varphi(m)s}} + \frac{1}{p^{2\varphi(m)s}} + \ldots + \frac{1}{p^{k\varphi(m)s}} + \ldots ,$$

puisque $f(p)\, g(p) = \varphi(m)$.

Quand on fait le produit des séries relatives aux $p \nmid m$, les coefficients a_n sont majorés par ceux de la série :

$$\prod_{p \nmid m} \frac{1}{1 - p^{-\varphi(m)s}} = \sum_{n \in \mathcal{N}} \frac{1}{n^{\varphi(m)s}} ,$$

où $\mathcal{N} = \{n \in \mathbb{N} \mid (n, m) = 1\}$.

Mais on verra (cf. remarque ci-dessous) que cette dernière série diverge pour $s = \frac{1}{\varphi(m)}$, qui est un réel > 0.

Donc a fortiori la série $\sum_{n \geq 1} \frac{a_n}{n^s}$ (qui représente $\zeta_m(s)$ pour $\mathrm{Re}(s) > 1$) diverge pour $s = \frac{1}{\varphi(m)}$. C.Q.F.D.

On va maintenant utiliser ce résultat pour prouver ce qu'on désire, à savoir :

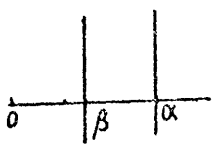
$\zeta_m(s)$ n'est pas holomorphe pour $\mathrm{Re}(s) > 0$.

Pour cela, nous utiliserons le lemme suivant :

Lemme 3.

Si on a une série de Dirichlet $f(s) = \sum_{n \geq 1} \frac{a_n}{n^s}$, à coefficients $a_n \geq 0$, qui converge pour $Re(s) > \alpha$, et si sa somme $f(s)$, qui est holomorphe pour $Re(s) > \alpha$, se prolonge en une fonction holomorphe dans une bande $Re(s) > \beta$ ($\beta < \alpha$), alors la série converge aussi pour $Re(s) > \beta$.

a) Démonstration du lemme.



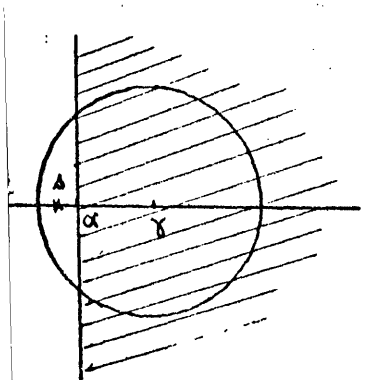
On se place sur l'axe réel puisque $|n^s| = n^{Re(s)}$ et $|\frac{a_n}{n^s}| = \frac{a_n}{n^{Re(s)}}$. Par hypothèse $\sum_{n \geq 1} \frac{a_n}{n^s}$ converge sur $]\alpha, +\infty[$.

Imaginons que $\sum_{n \geq 1} \frac{a_n}{n^s}$ converge pour $Re(s) > \beta'$ et que sa somme $f(s)$ soit holomorphe en s au voisinage de β' ; alors la série converge aussi pour $s \geq \beta' - \varepsilon$ ($\varepsilon > 0$) ; ou encore :

Si la série converge pour $s > \alpha$ et si $f(s)$ est holomorphe au voisinage de $s = \alpha$, alors elle converge pour $s > \alpha - \varepsilon$ ($\varepsilon > 0$). Ceci est une assertion qu'il s'agit de prouver, et qui entraîne évidemment le lemme 3. Quant à cette assertion, elle résulte de la :

Proposition.

Soit $f(s) = \sum_{n \geq 1} \frac{a_n}{n^s}$ ($a_n \geq 0$) une série qui converge pour $s > \alpha$. Si sa somme, qui est holomorphe pour $Re(s) > \alpha$, se prolonge en une fonction holomorphe dans un disque ouvert centré en γ réel ($\gamma > \alpha$) et contenant α, alors la série converge en tout point réel s intérieur au disque.



Démonstration.

On peut supposer $\gamma = 0$ (par translation sur s).

Ecrivons le développement de Taylor de la fonction dans le disque :

(1) $$f(s) = \sum_{p \geq 0} \frac{1}{p!} f^{(p)}(0)\, s^p .$$

On sait qu'il converge dans tout le disque où f est holomorphe.

Pour calculer les dérivées successives de f au point 0, on peut dériver terme à terme la série $\sum_{n \geq 1} \frac{a_n}{n^s}$ (puisqu'elle converge uniformément au voisinage de 0). Il vient

$$f^{(p)}(0) = \sum_{n \geq 1} \frac{a_n (-\log n)^p}{1} , \quad \text{car} \quad n^{-s} = e^{-s \log n} ,$$

Soit

$$(-1)^p f^{(p)}(0) = \sum_{n \geq 1} a_n (\log n)^p .$$

Supposons donc s réel négatif, mais s dans le disque, et posons $s = -t$, $t \in \mathbb{R}^+$. (1) devient

$$f(-t) = \sum_{p \geq 0} (-1)^p \frac{t^p}{p!} f^{(p)}(0) = \sum_{p \geq 0} \sum_{n \geq 1} \frac{t^p}{p!} a_n (\log n)^p .$$

C'est une série double à termes ≥ 0, on peut donc sommer par rapport à l'indice n d'abord :

$$f(-t) = \sum_{n \geq 1} a_n \left(\sum_{p \geq 0} \frac{t^p}{p!} (\log n)^p \right).$$

$\sum_{p \geq 0} \frac{t^p}{p!} (\log n)^p$ est la série de Taylor de la fonction n^t, série qui converge pour toute valeur de t. Donc $\sum_{p \geq 0} \frac{t^p}{p!} (\log n)^p = n^t$, et par suite

$$f(-t) = \sum_{n \geq 1} a_n n^t ;$$

faisant le changement de variable $t \longmapsto -s$, il vient $f(s) = \sum_{n \geq 1} \frac{a_n}{n^s}$,

et $\sum_{n \geq 1} \frac{a_n}{n^s}$ est bien convergente lorsque s est à gauche de α et intérieur au disque.

<u>Nous avons donc bien démontré la proposition et par suite le lemme 3.</u>

Ceci nous permet d'en déduire que $\zeta_m(s)$ n'est pas holomorphe pour $\mathrm{Re}(s) > 0$, car en vertu du lemme 3 la série de $\zeta_m(s)$ devrait converger pour tout s réel > 0

or on a vu qu'elle diverge pour $s = \frac{1}{\varphi(m)}$.

On a donc enfin prouvé la "deuxième assertion", et le théorème 2 est démontré.

Remarque :

Démontrons de deux façons différente que $\sum_{n \in \mathcal{N}'} \frac{1}{n^{\varphi(m)s}}$ diverge pour $s = \frac{1}{\varphi(m)}$, où $\mathcal{N}' = \{ n \in \mathbb{N} : (n, m) = 1 \}$.

Ceci s'exprime encore ainsi $\sum_{\substack{n \in \mathbb{N} \\ (n,m)=1}} \frac{1}{n} = +\infty$.

a) On sait que $\sum_{p \in P} \frac{1}{p} = +\infty$. Or $\sum_{\substack{p \in P \\ p \nmid m}} \frac{1}{p}$ n'en diffère que par un nombre fini de termes.

De plus $\sum_{\substack{p \in P \\ p \nmid m}} \frac{1}{p} \leq \sum_{\substack{n \in \mathbb{N} \\ (n,m)=1}} \frac{1}{n}$, d'où le résultat .

b) $\sum_{(n,m)=1} \frac{1}{n^s}$ pour $\mathrm{Re}(s) > 1$. On a

$$\zeta(s) = \left(\prod_{\substack{p \in P \\ p \nmid m}} \frac{1}{1 - \frac{1}{p^s}} \right) \left(\prod_{\substack{p \in P \\ p \mid m}} \frac{1}{1 - \frac{1}{p^s}} \right)$$

Soit $\zeta(s) = \sum_{(n,m)=1} \frac{1}{n^s} \times$ (produit fini).

Or lorsque $s \longrightarrow 1$, $\zeta(s) \longrightarrow \infty$, et par conséquent $\sum_{(n,m)=1} \frac{1}{n^s} \longrightarrow \infty$ quand $s \longrightarrow 1$.

c) [3e démonstration] - On considère les n qui ne contiennent aucun des facteurs premiers $p_1, \ldots, p_k$. Soit q le produit $p_1 \ldots p_k$. Tout entier de la forme $tq - 1$ (où t est entier ≥ 1) est de ce type-là. Donc

$$\sum_{n \mid (n,m)=1} \frac{1}{n} \geq \sum_{t=1}^{\infty} \frac{1}{tq-1} \geq \sum_{t=1}^{\infty} \frac{1}{tq} = \frac{1}{q} \left(\sum_{t=1}^{\infty} \frac{1}{t} \right) = +\infty.$$

THEORIE de GALOIS . Applications.

k : corps de base. Rappelons (sans démonstration) le :

Théorème de Steinitz : $\exists\ K \supset k$, K algébrique sur k, tel que tout polynôme $\in k[X]$ se décompose dans $K[X]$.

Alors tout polynôme $\in K[X]$ se décompose dans $K[X]$. Cette dernière propriété s'exprime en disant que K est algébriquement clos. Dans la suite on supposera $k \subset \Omega$ algébriquement clos .(Il n'est pas nécessaire que supposer que Ω soit une extension algébrique de k). Dans les applications que nous ferons, on prendra $\Omega = \mathbb{C}$ (corps des nombres complexes).

Définition. Soit $x \in \Omega$, x algébrique sur k. Les conjugués de x sont, par définition, les racines de $P(X)$ dans Ω, où P désigne le polynôme minimal de x sur k. La relation de conjugaison est une relation d'équivalence, car

y conj. de $x \iff P(y) = 0 \iff P$ est le polynôme minimal de y (puisque P est irréductible), d'où :

Deux éléments sont conjugués $\iff$ ils sont algébriques sur k et ont le même polynôme minimal sur k.

Soit $P \in k[X]$ irréductible ; alors P se décompose dans $\Omega[X]$, et P est polynôme minimal de chacune de ses racines. Question : P peut-il avoir des racines multiples ? Voici la réponse :

Soit P' le polynôme dérivé. Les racines multiples de P sont les racines du p.g.c.d. (P, P'). Puisque P est irréductible, ce p.g.c.d. est P ou 1. Si $P' \not\equiv 0$, $\deg(\text{p.g.c.d.}) < \deg P$, donc le p.g.c.d. est 1, toutes les racines de P sont simples. Si $P' \equiv 0$, toutes les racines de P sont multiples.

Exemple : En caractéristique 0, $\begin{cases} P(X) = X^n + \dots, \\ P'(X) = n X^{n-1} + \dots \text{ n'est pas identiquement nul} \\ \text{car } n \neq 0. \end{cases}$

Définition : Soit K une extension algébrique de k ; on dit que $x \in K$ est séparable sur k si les racines du polynôme minimal P de x sont toutes simples. Il en est toujours ainsi en caractéristique 0.

Examinons maintenant le cas de la caractéristique p (p premier).

$$P(X) = \sum_{k=0}^{n} a_k X^k , \quad a_n = 1, \quad P \text{ irréductible sur } k.$$

$$P'(X) = n X^{n-1} + (n-1) a_{n-1} X^{n-2} + \dots$$

$$P'(X) = 0 \iff a_k = 0 \text{ pour } p \nmid k \ ;$$

mais alors $P(X) = P_1(X^p)$, et P_1 est évidemment irréductible (Réciproque fausse: par exemple, $P_1(Y) = Y$ est irréductible, mais $P(X) = X^p$ ne l'est pas). $P_1(X)$ a-t-il des racines multiples ? On est ramené au même problème pour P_1. Par récurrence, on voit que $P(X) = Q(X^{p^r})$, où Q est un polynôme irréductible dont toutes les racines sont simples. Dans $\Omega[X]$, Q se décompose : $Q(Y) = \prod_i (Y - b_i)$, les $b_i \in \Omega$ étant tous distincts. On a donc $P(X) = \prod_i (X^{p^r} - b_i)$. Comme Ω est algébriquement clos, $\exists\, a_i \in \Omega$ tel que $(a_i)^{p^r} = b_i$. Alors $X^{p^r} - b_i = X^{p^r} - (a_i)^{p^r} = (X - a_i)^{p^r}$, d'où $P(X) = (\prod_i (X - a_i))^{p^r}$, les a_i étant distincts. Les a_i sont les racines de $P(X)$; chacune d'elles est d'ordre égal à p^r.

Remarque : si $k \subset k_1 \subset K$, $x \in K$, x séparable sur $k \implies x$ séparable sur k_1 (car le polynôme minimal P_1 de x sur k_1 est un diviseur du polynôme minimal P de x sur k ; si les racines de P sont simples, celles de P_1 sont simples).

Rappel. Soit $k \subset K$, $x \in K$, algébrique sur k, tel que $K = k\langle x \rangle$, sous-corps engendré par k et x. Soit $P(X)$ le polynôme minimal de x sur k.

Problème : Trouver les homomorphismes $K \to \Omega$ qui laissent fixes les éléments de k (ou, comme on dit, les k-homomorphismes $K \to \Omega$). On a vu qu'un tel homomorphisme Φ est défini par l'élément $\Phi(x) \in \Omega$, qui est une racine arbitraire du polynôme $P(X)$. Ainsi les homomorphismes cherchés sont en correspondance bijective avec les racines du polynôme P dans Ω. Leur nombre est égal au degré de P si et seulement si x est séparable sur k ; en général leur nombre est un diviseur du degré de P, puisque les racines de P ont toutes le même ordre de multiplicité.

Problème : Soit plus généralement $k \subset K$, avec $[K : k] < +\infty$ ($\Rightarrow$ K est une extension algébrique de k). Soit i l'injection de k dans Ω. On cherche les homomorphismes : $\sigma : K \longrightarrow \Omega$ qui prolongent i.

Solution. Puisque le degré $[K : k]$ est fini, il existe une suite d'éléments $x_1, \ldots, x_n \in K$ tels que $k_1 = k\langle x_1 \rangle$, $k_2 = k_1\langle x_2 \rangle, \ldots, k_n = k_{n-1}\langle x_n \rangle$, avec $k_n = K$.

Soit :

d_1 = degré du polynôme minimal P_1 de x_1 sur k,

d_1' = nombre des racines distinctes de P_1 dans Ω.

d_2 = degré du polynôme minimal P_2 de x_2 sur k_1,

d_2' = nombre des racines distinctes de P_2 dans Ω.

d_n = degré du polynôme minimal P_n de x_n sur k_{n-1},

d_n' = nombre des racines distinctes de P_n dans Ω.

d_1' divise d_1, et lui est égal si et seulement si x_1 est séparable sur k ; de même pour d_2', d_2, etc.... Il y a exactement d_1' homomorphismes $k_1 \longrightarrow \Omega$ qui prolongent i ; pour chacun d'eux il y a d_2' prolongements $k_2 \longrightarrow \Omega$; etc... Donc il y a $d_1' \ldots d_n'$ prolongements de i en un homomorphisme $K \longrightarrow \Omega$.

Or $d_1' \ldots d_n'$ divise $d_1 \ldots d_n$, et d'autre part

$$d_1 \ldots d_n = [k_1 : k][k_2 : k_1] \ldots [k_n : k_{n-1}] = [K : k].$$

[N.B. : le nombre des homomorphismes cherchés est indépendant du choix de $x_1, \ldots, x_n$].

Si $x_1, \ldots, x_n$ sont séparables sur k , alors $\begin{cases} x_1 \text{ est séparable sur } k, \\ x_2 \text{ est séparable sur } k_1, \\ \text{etc...} \end{cases}$

donc $d_1' \ldots d_n' = d_1 \ldots d_n = [K : k]$.

S'il existe un x non séparable sur k, alors le nombre des homomorphismes est $< [K : k]$; car on peut choisir $x_1, \ldots, x_n$ de façon que $x_1 = x$, et alors $d_1' < d_1$, donc $d_1' \ldots d_n' < [K : k]$.

.../...

Définition. Soit K une extension algébrique de k. On dit que K est séparable sur k si $\forall\, x \in K$, x est séparable sur k. On vient de voir que si K est engendré par un nombre fini d'éléments séparables sur k, alors K est séparable sur k. Ce qui précède fournit une démonstration du théorème suivant :

Théorème : Soit K une extension de k, $[K : k] < +\infty$. Le nombre des, k-homomorphismes $K \longrightarrow \Omega$ est un diviseur du degré $[K : k]$; il est égal au degré si et seulement si K est séparable sur k.

Transitivité des extensions séparables : soit $k \subset K \subset K'$, $[K' : k] < +\infty$. Si K est séparable sur k et K' séparable sur K, alors K' est séparable sur k.

Démonstration : d'après le théorème précédent, les homomorphismes $K \longrightarrow \Omega$ qui prolongent l'injection $i : k \longrightarrow \Omega$ sont en nombre $[K . k]$; chacun de ces prolongements se prolonge de $[K' : K]$ façons en un homomorphisme $K' \longrightarrow \Omega$. Donc il y a $[K : k] . [K' : K]$ prolongements $K' \longrightarrow \Omega$ de $i : k \longrightarrow \Omega$. Or $[K : k][K' : K] = [K' : k]$. D'après le théorème précédent (appliqué à k et K') il s'ensuit que K' est séparable sur k.

Remarque : Soit $x \in K$. Soit P(X) le polynôme minimal de x sur k. Pour toute racine du polynôme P(X), il existe un homomorphisme $k\langle x\rangle \longrightarrow \Omega$ qui prolonge $i : k \longrightarrow \Omega$. Par le théorème de Zorn, on voit que l'homomorphisme $k\langle x\rangle \longrightarrow \Omega$ peut lui-même se prolonger en un homomorphisme $K \longrightarrow \Omega$; on a donc prouvé la proposition suivante :

Proposition. Si K est une extension algébrique de k, si $x \in K$, et si $y \in \Omega$ est une racine quelconque du polynôme minimal P de x sur k, il existe au moins un k-homomorphisme $\sigma : K \longrightarrow \Omega$ tel que $\sigma(x) = y$.

Problème. Soit $[K : k] < \infty$. On cherche s'il existe un élément $x \in K$ qui, avec k, engendre K.

Condition nécessaire. Considérons les $\sigma : K \longrightarrow \Omega$ qui prolongent $i : k \longrightarrow \Omega$; si x engendre K sur k, alors les éléments $\sigma(x)$ sont distincts.

[En effet, si x engendre K, la connaissance de l'élément $\sigma(x)$ détermine l'homomorphisme σ]

On va montrer que cette condition nécessaire est suffisante lorsque K est séparable sur k :

Si les $\sigma(x)$ sont distincts et si K est séparable sur k, alors $K = k\langle x\rangle$.

Pour le prouver :

Lemme : si $[K : k] < \infty$, K séparable sur k, et si $x \in K$ est tel que les éléments $\sigma_1(x)$ et $\sigma_2(x)$ correspondant à deux k-homomorphismes distincts $\sigma_1 : K \longrightarrow \Omega$ et $\sigma_2 : K \longrightarrow \Omega$ soient distincts, alors $K = k\langle x\rangle$.

Démonstration. Puisque K est séparable sur k, les σ sont en nombre $[K : k]$; les $\sigma(x)$ étant distincts, ils sont aussi en nombre $[K : k]$. Or, d'après la proposition précédente, les $\sigma(x)$ sont exactement les racines du polynôme minimal de x. Comme ses racines sont simples, il est de degré $[K . k]$, et par suite $[k\langle x\rangle : k] = \deg P = [K . k]$.

Puisque $k \subset k\langle x\rangle \subset K$, il s'ensuit que $k\langle x\rangle = K$. C.Q.F.D.

Théorème de l'élément primitif.

Théorème. Soit K une extension de k, $[K : k] < +\infty$, K séparable sur k. Alors il existe $x \in K$ tel que $K = k\langle x\rangle$.

Démonstration :

1er cas : k est fini ; alors K est fini. On sait alors que K est engendré par un seul élément (si $q = \text{Card } K$, K est engendré par une racine primitive de l'équation $X^{q-1} - 1 = 0$).

2ème Cas : k est infini. De toute façon, K est engendré sur k par un nombre fini d'éléments. Il suffira donc de montrer que si K est engendré sur k par α et β, alors K peut être engendré sur k par un seul élément.

Faisons parcourir à σ l'ensemble des k-homomorphismes $K \longrightarrow \Omega$. On cherche un $c \in k$ tel que les $\sigma(\alpha + c\beta) = \sigma(\alpha) + c\,\sigma(\beta)$ soient tous distincts (alors $\alpha + c\beta$ engendrera K sur k). Or supposons que $\sigma_i(\alpha) + c\,\sigma_i(\beta) = \sigma_j(\alpha) + c\,\sigma_j(\beta)$ pour $i \neq j$ (*) ; pour un couple (i,j) donné, il existe au plus une valeur de c satisfaisant à cette relation : car si

$\sigma_i(\beta) = \sigma_j(\beta)$, on a $\sigma_i(\alpha) \neq \sigma_j(\alpha)$. [sinon on aurait $\sigma_i = \sigma_j$, puisque K est engendré par α et β], et alors (*) n'a lieu pour aucune valeur de c ; si au contraire $\sigma_i(\beta) \neq \sigma_j(\beta)$, (*) n'a lieu que pour $c = \dfrac{\sigma_i(\alpha) - \sigma_i(\alpha)}{\sigma_i(\beta) - \sigma_j(\beta)}$.

Ainsi, mises à part des valeurs de c en nombre fini, on a $\sigma_i(\alpha + c\beta) \neq \sigma_j(\alpha + c\beta)$ quels que soient i et j distincts. Comme le corps K est infini par hypothèse, on peut choisir c en dehors de cet ensemble fini.

C.Q.F.D.

Corollaire : Soit K une extension algébrique séparable de k. Supposons qu'il existe un entier n tel que, $\forall x \in K$, x annule un polynôme unitaire de $k[X]$ de degré au plus n. Alors $[K : k] \leq n$.

Démonstration : Il suffit de montrer que tout corps K' tel que $k \subset K' \subset K$ et que $[K' : k] < +\infty$ satisfait à $[K' : k] \leq n$. Or, K' étant donné, $\exists\, x \in K'$ tel que $K' = k\langle x \rangle$ (théorème de l'élément primitif). D'après l'hypothèse, le polynôme minimal de x sur k est de degré $\leq n$, donc $[K' : k] \leq n$. C.Q.F.D.

Extensions normales.

Définition. Soit $k \subset K$ une extension algébrique. On dit que K est une extension normale de k si P irréd$\in k[X]$ a une racine dans $K \Rightarrow P$ se décompose en facteurs de premier degré dans $K[X]$. Il revient au même de dire que si $x \in K$, le polynôme minimal de x sur k se décompose dans $K[X]$.

Exemple : si K est algébriquement clos et algébrique sur k, alors K est normal sur k.

Soient $k \subset k_1 \subset K$.

Proposition. K normal sur $k \Rightarrow K$ normal sur k_1. En effet, soit

$$\begin{cases} P & \text{le polynôme } k_1\text{-minimal de } x \in K; \\ Q & \text{le polynôme } k\text{-minimal de } x \in K ; \end{cases}$$

alors P divise Q.

Par hypothèse, Q se décompose dans K (K étant normal sur k) ; donc P se décompose dans K. C.Q.F.D.

Soit toujours K une extension algébrique de k. Choisissons un k-homomorphisme de K dans Ω, qui identifie K à un sous-corps de Ω. Pour que K soit une extension normale de k, il faut et il suffit que le conjugué (par rapport à k) de tout élément de K soit dans K (a priori, ce conjugué est un élément de Ω). Ceci résulte aussitôt de la définition d'une extension normale.

Mais on sait, d'après une proposition antérieure (page 162) que si $y \in \Omega$ est k-conjugué d'un $x \in K$, il existe un k-homomorphisme $\sigma : K \to \Omega$ tel que $\sigma(x) = y$. On en déduit aussitôt :

Proposition.- Pour que K, extension algébrique de k, plongée dans Ω, soit une extension normale, il faut et il suffit que tout k-homomorphisme de K dans Ω envoie K dans K (donc soit un automorphisme de K : cf. théorème de la page 84).

Exemple : $Q(X) \in k[X]$. Adjoignons à k toutes les racines de Q ; on obtient le "corps de décomposition" K de Q sur k. Je dis que K est une extension normale de k. En effet, soit $\sigma : K \to \Omega$ un k-homomorphisme. Soient (x_i) les racines de $Q(X)$ dans K. Puisque $\sigma(x_i)$ est une racine de $Q(X)$, on a $\sigma(x_i) \in K$; et comme K est engendré par k et les x_i, on a $\sigma(K) \subset K$. Donc K est normal sur k.

Cas particulier : Supposons $[K : k] = 2$; alors K est une extension normale de k, car $K = k(x)$, où x est racine d'un $P(X) = x^2 + bx + c$ $(b, c \in k)$; l'autre racine est $-b - x \in K$, et par suite K est corps de décomposition de $P(X)$.

Attention : on n'a pas de transitivité pour les extensions normales (contrairement à ce qui a lieu pour les extensions séparables). Autrement dit, il se peut qu'on ait $k \subset K \subset K'$, K normal sur k, K' normal sur K, mais K' non normal sur k.

Exemple : $k = \mathbb{Q}$, $K = \mathbb{Q}(\sqrt[4]{2}) \subset \mathbb{R}$

$\sqrt[4]{2}$ est racine de $X^2 - \sqrt{2}$; donc $\mathbb{Q}(\sqrt[4]{2})$ s'obtient

en adjoignant à $\mathbb{Q}(\sqrt{2})$ une racine α de $X^2 - \sqrt{2}$, et on a

$$[\mathbb{Q}(2^{1/4}) : \mathbb{Q}] = [\mathbb{Q}(2^{1/4}) : \mathbb{Q}(\sqrt{2})] \cdot [\mathbb{Q}(\sqrt{2}) : \mathbb{Q}] = 4$$

$\mathbb{Q}(2^{1/4})$ est donc une extension normale (quadratique) d'une extension (normale quadratique) de $\mathbb{Q}$. Or $\mathbb{Q}(2^{1/4})$ n'est pas une extension normale de $\mathbb{Q}$, car le polynôme $\mathbb{Q}$-irréductible $X^4 - 2$ a une racine $2^{1/4}$ dans $\mathbb{Q}(2^{1/4})$, mais la racine $2^{1/4}i$ n'est pas dans $\mathbb{Q}(2^{1/4})$.

Problème. Soit $k \subset K$, $[K : k] < +\infty$. Existe-t-il $K' \supset K$, K' normal sur k, tel que $[K' : k] < +\infty$? (Plongeons $K \subset \Omega$; on va voir qu'il y a effectivement un plus petit sous-corps de Ω satisfaisant à ces conditions.

Soit $\sum$ l'ensemble des k-homomorphismes $K \to \Omega$; soit K' le sous-corps engendré par les corps $\sigma(K)$, lorsque σ parcourt l'ensemble fini $\sum$.

Proposition. Le sous-corps K' de Ω engendré par les $\sigma(K)$ $(\sigma \in \sum)$ est normal sur k, et de degré fini sur k.

Démonstration. Soit (x_i) un système fini d'éléments de K qui engendrent K sur k. Les $\sigma(x_i)$ (où σ parcourt $\sum$) engendrent K' (sur k). Ils sont en nombre fini. Soit $\tau : K' \to \Omega$ un k-homomorphisme. $\tau(K')$ est le sous-corps de Ω engendré par les $\tau(\sigma(K)) = (\tau \circ \sigma)(K)$. Puisque $\tau \circ \sigma$ est un homomorphisme $K \to \Omega$, $\tau \circ \sigma \in \sum$, donc $\tau \circ \sigma(K) \subset K'$. Ainsi $\tau(K') \subset K'$, ce qui montre que K' est normal sur k.

Théorie de Galois.

Notation : si $K \supset k$ est une extension, on note $G(K, k)$ le groupe des k-automorphismes de K (automorphismes de K laissant fixes les éléments de k). On l'appelle le groupe de Galois de K sur k.

Exemple : soit $Q(X) \in k[X]$, et soit K le corps de décomposition du polynôme Q. Tout $\sigma \in G(K, k)$ permute les racines de Q, et σ est déterminé quand on

.../...

connaît la permutation qu'il définit sur les racines (puisque K est engendré par k et les racines de Q). Ainsi G(K, k) s'identifie à un sous-groupe du groupe des permutations des racines de Q ; ce sous-groupe est transitif dans l'ensemble des racines si et seulement si Q(X) est irréductible sur k. (Exercice : le démontrer).

Théorème 1. Soit $K \supset k$, $[K : k] < +\infty$. Pour que l'extension K de k soit normale et séparable, il faut et il suffit que

$$\text{Card } G(K, k) = [K : k].$$

Démonstration. Supposons K normale et séparable. Puisque K est normale l'ensemble des k-automorphismes de K n'est autre que l'ensemble des k-homomorphismes $K \to \Omega$; puisque K est séparable, leur nombre est égal à $[K : k]$.

Réciproquement, si Card $G(K, k) = [K : k]$, le nombre des k-homomorphismes $K \to \Omega$ est $\geq [K : k]$, et comme c'est un diviseur de $[K : k]$, il lui est égal. Ceci signifie que tout k-homomorphisme $K \to \Omega$ est un automorphisme de K, donc K est une extension normale de k. De plus le nombre des k-homomorphismes $K \to \Omega$ étant $[K : k]$, l'extension est séparable. C.Q.F.D.

Remarque : dans tous les cas, le Cardinal de G(K, k) divise $[K : k]$ (Exercice!).

Définition. Soit K un corps. Soit G un groupe d'automorphismes de K. On note K^G l'ensemble des $x \in K$ tels que $\sigma(x) = x$, $\forall \sigma \in G$.

Proposition. K^G est un sous-corps de K (le démontrer). Si on pose $K^G = k$, il est évident que $G(K, k) \supset G$.

Définition. $K \supset k$ est une extension galoisienne $\Leftrightarrow k = K^{G(K, k)}$; autrement dit, tout élément de K invariant par le groupe de Galois G(K, k) appartient à k.

Théorème 2. Soit $K \supset k$, extension de degré fini $[K : k]$. Alors

$$\boxed{\text{K galoisien sur k} \Leftrightarrow \text{K normal et séparable sur k.}}$$

Démonstration. Prouvons d'abord $\Longleftarrow$.

Soit $x \in K$, fixe par G(K, k) ; on veut montrer que $x \in k$. Soit P le polynôme minimal de x ; toutes ses racines sont dans K, et elles sont simples.

Soit y une racine de P ; $\exists\ \sigma \in G(K, k)$ tel que $\sigma(x) = y$. Puisque x est fixe par $G(K, k)$ on a $y = x$. Donc P n'a qu'une racine : il est du premier degré, et par suite $x \in k$.

Prouvons maintenant $\Longrightarrow$. Pour cela, on va utiliser un :

Lemme : Soit G un groupe fini d'automorphismes d'un corps K. Alors K est une extension normale et séparable de $k = K^G$. De plus, si $x \in K$, le degré du polynôme minimal de x sur k est égal au nombre des transformés distincts de x par G.

Démonstration du lemme ; soient (x_i) les transformés distincts de $x \in K$ par G. Alors G permute les x_i. Le polynôme unitaire ayant pour racines simples les x_i est $Q(X) = X^n - p_1 X^{n-1} + p_2 X^{n-2} + \ldots + (-1)^n p_n$, où n désigne le nombre des x_i et où

$$\begin{cases} p_1 = \sum_i x_i \\ p_2 = \sum x_i x_j \\ \text{---------} \\ p_n = x_1 x_2 \ldots x_n \end{cases}$$

(dans $\sum x_i x_j$, par exemple, on somme sur l'ensemble des parties $\{i,j\}$ à deux éléments). Alors $p_1, \ldots, p_n \in K$ sont des éléments invariants par G. Donc $p_i \in k$ pour $i = 1, \ldots, n$, et par suite $Q(X) \in k[X]$. Or $Q(x) = 0$. Q est donc un multiple de polynôme minimal P de x sur k ; mais P doit avoir pour racines les x_i, donc $P = Q$. Ainsi le polynôme minimal de x a toutes ses racines dans K, et elles sont simples. Ceci prouve que K est une extension normale et séparable de k. Le lemme est démontré.

Fin de la démonstration du théorème 2. Supposons K galoisien sur k. Appliquons le lemme au groupe $G(K, k) = G$; alors $K^G = k$ puisque K est galoisien. Le lemme dit alors que K est normal et séparable sur k.

Théorème 3. Soit K un corps, et soit G un groupe fini d'automorphismes de K. Posons $K^G = k$

Alors : (i) K est une extension galoisienne de k ;

(ii) $[K : k] = \text{card } G$;

(iii) $G(K, k) = G$.

Démonstration : on a évidemment $G \subset G(K, k)$. Il s'ensuit que $k = K^{G(K, k)}$, donc K est galoisien sur k (par définition).

D'après le théorème 2 (ou le lemme), K est une extension normale et séparable, donc (théorème 1) $\text{Card } G(K,k) = [K : k]$.

Soit $n = \text{card } G$. D'après le lemme, le degré du polynôme minimal de n'importe quel x est $\leqslant n$.

D'après un résultat antérieur, ceci entraîne $[K : k] \leqslant n$ (parce que K est séparable),

d'où $\text{card } G(K, k) \leqslant \text{card } G$; et comme $G \subset G(K, k)$, on conclut

$$G = G(K, k),$$

et $$[K : k] = \text{card } G .$$

SITUATION GALOISIENNE :

On se place dans la situation suivante :

$k \subset K$, K galoisien sur k , $[K : k] < +\infty$

(k et K sont donnés une fois pour toutes).

Soit k' un corps tel que $k \subset k' \subset K$; alors $\begin{cases} k' \text{ séparable sur } k \\ K \text{ galoisien sur } k' \end{cases}$

[car tout élément de k' est séparable sur k , puisque K est séparable sur k ; de plus K étant normal (resp. séparable) sur k est normal (resp. séparable) sur k'] .

A un tel corps k' nous associons le groupe $G(K, k')$, sous-groupe de $G(K, k)$. Alors le sous-corps de K formé des x invariants par $G(K, k')$ n'est autre que k' , puisque K est galoisien sur k' .

- Soit maintenant G' un sous-groupe de $G(K, k)$; nous lui associons le sous-corps $K^{G'}$ des éléments de K invariants par G' . Le groupe de Galois $G(K, K^{G'})$ est alors G' (théorème 3).

Donc les deux applications qu'on a définies $k' \to G(K, k')$, $G' \to K^{G'}$ sont des bijections (réciproques l'une de l'autre) qui mettent en correspondance bijective l'ensemble des sous-corps k' tels que $k \subset k' \subset K$, et l'ensemble des sous-groupes de $G(K, k)$.

Problème : A quelle condition doit satisfaire le sous-groupe $G' \subset G(K, k)$ pour que le sous-corps correspondant

$$k' = K^{G'}$$

soit une extension normale de k ? Il revient au même de demander que k' soit galoisien sur k (puisque de toute façon k' est séparable sur k) .

Théorème 4 -

Pour que $k' = K^{G'}$ soit normal sur k , il faut et il suffit que G' soit un sous-groupe distingué de $G(K, k)$. S'il en est ainsi, k' est stable par $G(K, k)$, et la restriction de chaque $\sigma \in G(K, k)$ au sous-corps k' induit un homomorphisme

$$G(K, k) \longrightarrow G(k', k)$$

qui est surjectif et a pour noyau $G(K, k')$. Autrement dit, on a une suite exacte

$$(1) \longrightarrow G(K, k') \longrightarrow G(K, k) \longrightarrow G(k', k) \longrightarrow (1)$$

qui identifie $G(k', k)$ au groupe quotient $G(K, k)/G(K, k')$.

Démonstration -

Soient $\sigma \in G(K, k)$, $\tau \in G(K, k')$.

On a $\sigma \tau \sigma^{-1} \in G(K, \sigma(k'))$ (évident) .

Donc si $G(K, k')$ est distingué dans $G(K, k)$, on a

(1) $G(K, \sigma(k')) = G(K, k')$

quel que soit $\sigma \in G(K, k)$. Mais la relation (1) signifie que $\sigma(k') = k'$ (cf. correspondance bijective entre sous-corps et sous-groupes). Autrement dit, k' est stable pour $G(K, k)$, ce qui exprime précisément que k' est une extension normale de k .

Réciproquement, si k' est stable pour $G(K, k)$, l'homomorphisme de restriction $G(K, k) \longrightarrow G(k', k)$ est surjectif, car tout k-homomorphisme $k' \longrightarrow k'$ se prolonge en un k-homomorphisme $K \longrightarrow \Omega$, qui est en fait un k-automorphisme de K (K étant normal sur k). Enfin, le noyau de $G(K, k) \longrightarrow G(k', k)$ est évidemment $G(K, k')$, qui est donc un sous-groupe distingué. Ceci achève la démonstration.

Exemple :

Supposons $[K : k] = p^n$, p premier, K galoisien sur k. Alors il existe $k = k_n \subset k_{n-1} \subset \ldots \subset k_1 \subset k_o = K$, tels que chaque k_i soit galoisien sur k, et $[k_i : k_{i+1}] = p$.

En effet, soit $G = G(K, k)$; on a Card $G = p^n$ (théorème 1).

On sait que ceci entraîne que le centre de G contient un sous-groupe cyclique G_1 d'ordre p. G_1 est distingué, et Card $(G/G_1) = p^{n-1}$. On recommence avec G/G_1 ; donc $\exists\ G_2$, tel que G_2/G_1 soit un sous-groupe cyclique d'ordre p du centre de G/G_1. Alors G_2 est distingué dans G, $\text{Card}(G/G_2) = p^{n-2}$.

Par récurrence on construit ainsi

$(1) = G_o \subset G_1 \subset G_2 \subset \ldots \subset G_n = G$, tous distingués les uns dans les autres, avec G_i/G_{i-1} cyclique d'ordre p.

Il suffit alors de prendre pour $k_1, \ldots, k_n$ les sous-corps associés aux groupes $G_1, \ldots, G_n$.

PROBLEMES DE CONSTRUCTIONS GEOMETRIQUES

On se place dans le plan $\mathbb{R}^2$ (muni de la forme quadratique x^2+y^2).

Soit donné $E \subset \mathbb{R}^2$, un ensemble de points dans le plan euclidien.

Opérations possibles (règle du jeu) :

- tracer la droite passant par 2 points donnés distincts (déjà construits) ;
- tracer le cercle de centre A qui passe par B (A et B = points déjà construits) ;
- construire le point d'intersection de 2 droites déjà tracées (non parallèles) ;
- construire (s'ils existent) les points d'intersection $\begin{cases} \text{d'un cercle et d'une droite} \\ \text{de deux cercles} \end{cases}$ déjà tracés.

Tous les points obtenus à partir des points de E par itération des constructions permises constituent, par définition, l'ensemble des points qu'on peut construire à partir de E avec la règle et le compas.

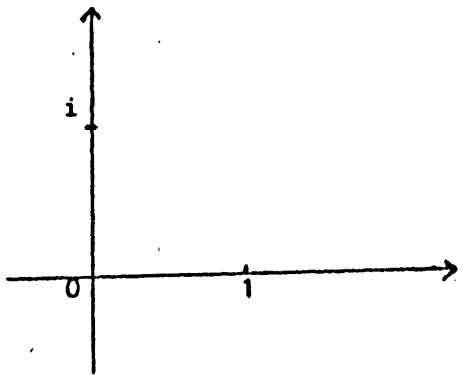
<u>Exemples de problèmes résolubles par les constructions précédentes</u>.

- construire la médiatrice d'un segment ;
- construire le symétrique d'un point par rapport $\begin{cases} \text{à un point,} \\ \text{à une droite;} \end{cases}$
- construire la droite perpendiculaire à une droite donnée D et passant par un point P donné;
- construire la parallèle à D menée par P (cette construction montre que l'usage de l'équerre, que l'on fait glisser le long d'une règle, est licite);
- étant donné deux droites sécantes D_1 et D_2, construire leurs deux bissectrices.

On sait que deux points distincts O et A déterminent une demi-droite : {points de la droite OA qui sont du même côté de A que O}.

On sait distinguer une demi-droite $\Rightarrow$ on sait construire la bissectrice intérieure d'un angle de demi-droites (comme médiatrice d'un segment convenable).

Traduction algébrique.



On se donne deux points dans le plan, notés 0, 1. Ils définissent deux axes de coordonnées rectangulaires ; on oriente le plan en choissant une des demi-droites perpendiculaires en 0 à la droite joignant 0 et 1. Cela fait, on obtient une bijection du plan sur le corps $\mathbb{C}$ des nombres complexes.

Problème : Un ensemble $E \in \mathbb{C}$ étant donné (avec $0 \in E$, $1 \in E$), on se propose de caractériser l'ensemble $K = K(E)$ des points de $\mathbb{C}$ que l'on peut obtenir à partir des points de E par des constructions faites au moyen de la règle et du compas.

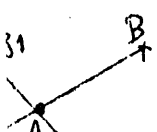
Théorème 1. *K est un sous-corps de $\mathbb{C}$, stable par la conjugaison $z \longmapsto \bar{z}$. De plus, tout polynôme du second degré à coefficients dans K a ses racines dans K.*

Démonstration.

i et $-i \in K$: prendre les points d'intersection du cercle (0, 1) (de centre 0, passant par 1) avec la droite perpendiculaire au point 0, à la droite D joignant 0 et 1.

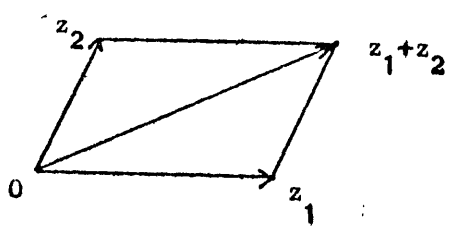
$z \in K \Rightarrow \bar{z} \in K$, car $\bar{z}$ est symétrique de z par rapport à la droite D.

$z \in K \Rightarrow -z \in K$, car $-z$ est symétrique de z par rapport au point 0.



Montrons que $z_1 \in K$, $z_2 \in K \Rightarrow z_1 + z_2 \in K$. Pour cela, on construit le point milieu du segment d'extrémités z_1 et z_2 ; puis on prend le point B, symétrique de 0 par rapport à A.

Remarque : on pourrait aussi construire le parallélogramme

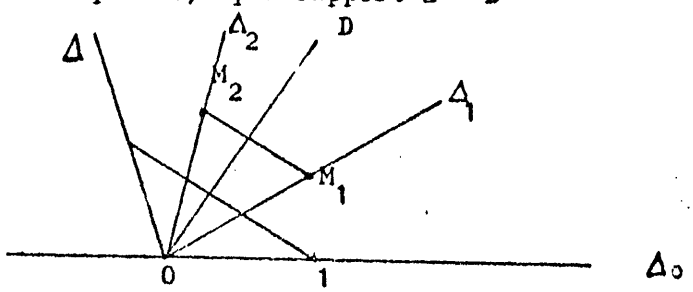


mais cette construction tombe en défaut si les points 0, z_1 et z_2 sont alignés.

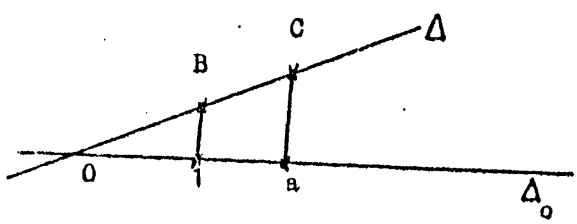
Montrons maintenant que $z_1 \in K$, $z_2 \in K \Rightarrow z_1 z_2 \in K$. Il suffit de le prouver lorsque $z_1 \neq 0$ et $z_2 \neq 0$; tout revient à construire la demi-droite dont l'argument est la somme des arguments de z_1 et de z_2, et à porter sur cette demi-droite

une longueur égale au produit de $|z_1|$ et de $|z_2|$. Voici la solution de ces deux problèmes.

Demi-droite Δ d'origine 0 dont l'argument est la somme des arguments de deux demi-droites Δ_1 et Δ_2 d'origine 0 : on porte sur Δ_1 et Δ_2 des longueurs OM_1 et OM_2 égales à un nombre donné (par exemple 1), on construit la médiatrice D du segment $M_1 M_2$, et on peut la symétrique Δ de la demi-droite Δ_0 (d'origine 0, passant par 1) par rapport à D



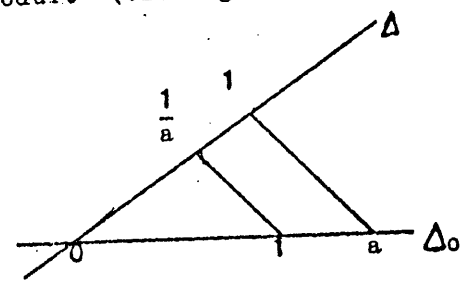
Produit de deux nombres $a > 0$ et $b > 0$: On porte, sur une demi-droite Δ déjà construite (et distincte de la demi-droite Δ_0 d'origine 0, passant par 1), une longueur égale à b, ce qui donne un point B, puis, par le point de Δ_0 d'abscisse a on mène la parallèle à la droite joignant le point 1 de Δ_0 au point B ; elle coupe Δ en un point C ; la longueur OC est égale au produit ab cherché.



Jusqu'à présent, on a prouvé que K est un sous-groupe additif de $\mathbb{C}$, stable pour la multiplication, et contenant $1 \in \mathbb{C}$. Pour montrer que K est un sous-corps il suffit de prouver que : $z \in K - \{0\} \Rightarrow \frac{1}{z} \in K$.

Or le point $\frac{1}{z}$ a un argument opposé à celui de z, et son module est l'inverse de $|z|$. Si Δ est la demi-droite joignant 0 à z, la demi-droite Δ' joignant 0 à $\frac{1}{z}$ est la symétrique de Δ par rapport à Δ_0 ; on peut donc la construire (par exemple en construisant le symétrique du point z par rapport à Δ_0). Il reste alors à porter sur Δ' une longueur égale à $\frac{1}{a}$, où $a = |z|$ est connu.

D'où le problème : <u>construire l'inverse</u> $\frac{1}{a}$ <u>d'un nombre</u> $a > 0$ <u>donné</u>. Pour le résoudre, on procède comme pour le produit (cf. figure)



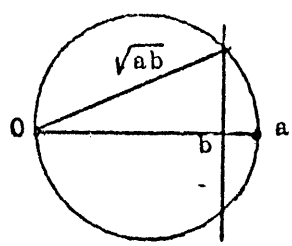
Pour achever la démonstration du théorème 1, il reste à prouver que tout polynôme du second degré à coefficients dans K a ses racines dans K. La formule donnant les racines montre qu'il suffit de montrer ceci :

<u>Si</u> $z \in \mathbb{C}$ <u>est tel que</u> $z^2 \in K$, <u>alors</u> $z \in K$.

Ceci revient à prouver deux choses :

(1) on peut, avec la règle et le compas, construire la droite bissectrice de l'angle de deux demi-droites (or nous savons déjà ceci) ;

(2) on peut, avec la règle et le compas, construire la racine carrée $\sqrt{a}$ d'un nombre réel $a > 0$. Montrons plus généralement que si $a > 0$ et $b > 0$ sont donnés, on peut construire $\sqrt{ab}$; ceci résulte de la figure (en supposant par exemple $b < a$



<u>Corollaire du théorème 1.</u> Soit k le sous-corps de $\mathbb{C}$ engendré par l'ensemble donn $E \subset \mathbb{C}$, et soit $K = K(E)$ le sous-corps formé des points qu'on peut obtenir à partir des points de E par des constructions faites au moyen de la règle et du compas. Supposons qu'on ait une suite de sous-corps de $\mathbb{C}$:

$$k = k_0 \subset k_1 \subset k_2 \subset \dots \subset k_n$$

tels que $[k_i : k_{i-1}] = 2$ pour $1 \leq i \leq n$. <u>Alors</u> k_n <u>est contenu dans</u> K.

<u>Démonstration du corollaire</u> : on le prouve par récurrence sur n. C'est vrai pour $n = 0$, car $k \subset K$ puisque K est un corps (th. 1). Si c'est vrai pour n-1

$(n > 0)$, on a $k_{n-1} \subset K$; d'après le théorème 1, tout polynôme du second degré à coefficients dans k_{n-1} a ses racines dans K ; or tout $x \in k_n$ est racine d'un polynôme du second degré à coefficients dans k_{n-1}, puisque $[k_n : k_{n-1}] = 2$.

Donc $k_n \subset K$. C.Q.F.D.

Théorème 2. (Sorte de réciproque du corollaire).

Soit k un sous-corps de $\mathbb{C}$ contenant $i = \sqrt{-1}$ et stable par $z \mapsto \bar{z}$. Soit $K = K(k)$ le sous-corps de $\mathbb{C}$ formé des points constructibles avec la règle et le compas à partir des points de k. Alors, si $z \in K$, il existe une suite de sous-corps

$$k = k_0 \subset k_1 \subset \cdots \subset k_n$$

tels que

(*) $\qquad z \in k_n, \quad [k_i : k_{i-1}] = 2 \qquad$ pour $\quad 1 \leq i \leq n$.

On peut même faire en sorte que, pour $1 \leq i \leq n$,

$$k_i = k_{i-1}(\sqrt{d_i}) \ ,$$

où $d_i \in k_{i-1}$ est réel > 0.

Avant de prouver le théorème 2, énonçons :

Corollaire des théorèmes 1 et 2. Un sous-corps k de $\mathbb{C}$, stable par $z \mapsto \bar{z}$ étant donné, pour que $z \in K(k)$ (i.e. pour que z soit constructible avec la règle et le compas à partir des points de k), il faut et il suffit qu'il existe une suite de sous-corps

$$k = k_0 \subset k_1 \subset \cdots \subset k_n$$

satisfaisant à la condition (*) du théorème 2.

En effet, c'est suffisant (corollaire du théorème 1). C'est nécessaire : le théorème 2 l'affirme lorsque k contient $i = \sqrt{-1}$: sinon, posons $k_0 = k(i)$; le corps k_0 est stable par $z \mapsto \bar{z}$ (vérification immédiate). D'après le théorème 2, si $z \in K(k)$, on a une suite

$$k \subset k_0 \subset k_1 \subset \cdots \subset k_n$$

telle que

$$z \in k_n, \quad [k_0 ; k] = 2, \quad [k_i : k_{i-1}] = 2 \quad \text{pour} \quad 1 \leq i \leq n.$$

Donc la condition est nécessaire, et le corollaire est prouvé.

Démonstration du théorème 2. Soit k stable par $z \mapsto \bar{z}$, et contenant i. Il est clair que $z = x + iy \in k \iff x \in k$ et $y \in k$. Par définition, un tel point z est dit rationnel sur k.

Définition. On appelle droite rationnelle sur k toute droite d'équation $ux + vy + w = 0$, où $u, v, w \in k$.

Définition. On appelle cercle rationnel sur k tout cercle d'équation $x^2 + y^2 + \alpha x + \beta y + \gamma = 0$, où $\alpha, \beta, \gamma \in k$.

Les assertions suivantes sont immédiates :

- La droite qui joint deux points distincts rationnels sur k est rationnelle sur
- Le cercle de centre P qui passe par Q, lorsque P et Q sont rationnels sur k, est rationnel sur k.
- Le point d'intersection de deux droites (sécantes) rationnelles sur k est rationnel sur k.

Intersection de deux cercles rationnels sur k :

(C) $x^2 + y^2 + \alpha x + \beta y + \gamma = 0$, (C') $x^2 + y^2 + \alpha' x + \beta' y + \gamma' = 0$.

Les points d'intersection sont aussi ceux du cercle (C) et de la droite

(D) $(\alpha - \alpha') x + (\beta - \beta') y + \gamma - \gamma' = 0$ (qui est vide si $\alpha = \alpha'$, $\beta = \beta'$).

On est ramené à étudier les points d'intersection d'un cercle rationnel sur k et d'une droite rationnelle sur k. Pour cela, on doit résoudre une équation du second degré à coefficients dans k. Donc si les points d'intersection existent (i.e. sont réels), ils sont rationnels sur un corps de la forme $k(\sqrt{d})$, où d est un nombre réel > 0 qui appartient à k. Un tel corps $k(\sqrt{d})$ est stable par $z \mapsto \bar{z}$, comme le corps k.

Maintenant, le théorème 2 résulte évidemment des considérations précédentes.

Le corollaire des théorèmes 1 et 2 (cf. ci-dessus) donne une condition nécessaire et suffisante pour que $z \in \mathbb{C}$ puisse être construit avec la règle et le compas à l'aide de points d'un sous-corps k de $\mathbb{C}$, stable par $z \mapsto \bar{z}$. Cette condition n'est pas encore très maniable. On en déduit néanmoins :

ondition nécessaire pour que $z \in K(k)$: c'est que :

(1) z soit algébrique sur k ;

(2) le degré du polynôme minimal de z sur k soit une puissance de 2.

En effet, ce degré est égal à $[k\langle z\rangle : k]$, qui divise $[k_n : k]$, or $[k_n : k] = 2^n$]

n va montrer sur des exemples comment cette condition nécessaire peut être utilisée.

xemple 1 : "quadrature du cercle ".

e problème (classique depuis l'Antiquité) consiste en ceci : construire un disque ont l'aire soit égale à celle d'un carré de côté donné.

On va voir qu'une telle construction n'est pas possible avec la règle et le ompas . En effet, prenons comme unité de longueur le côté du carré. Le rayon du isque cherché est $\frac{1}{\sqrt{\pi}}$, si ce disque pouvait être construit par la règle et le ompas à partir du corps $\mathbb{Q}(i)$, $\frac{1}{\sqrt{\pi}}$ serait algébrique sur $\mathbb{Q}$, donc π serait algébrique sur $\mathbb{Q}$. Or Lindemann a démontré en 1882 que π est transcendant sur $\mathbb{Q}$ il n'est pas question de donner cette démonstration ici). Du même coup se trouve rouvée l'impossibilité de la "quadrature du cercle" (au sens des Grecs).

xemple 2 : "trisection de l'angle".

n se donne $k \subset \mathbb{C}$, stable par $z \mapsto \bar{z}$ puis un $\alpha \in k$ tel que $|\alpha| = 1$. On cherche à construire n $z \in \mathbb{C}$ tel que $\boxed{z^3 = \alpha}$. Si on sait construire un tel z, alors on sait ussi construire jz et j^2z, j et j^2 désignant les deux racines cubiques de 'unité, autres que 1. En effet, j et j^2 sont les racines de l'équation $^2 + X + 1 = 0$, donc peuvent être construits à partir de $\mathbb{Q}$ par la règle et le compas.

. Pour que z soit constructible à partir de k, il faut que le degré de on polynôme minimal (sur k) soit une puissance de 2.

r ce polynôme minimal divise $X^3 - \alpha$; donc il doit être de degré 1 ou 2. Mais 'il est de degré 2, l'une des trois racines a un polynôme minimal de degré 1, onc est dans k.

n résumé, si les racines de l'équation $X^3 = \alpha$ peuvent se construire à partir de k ar la règle et le compas, l'une au moins d'entre elles appartient au corps k.

Réciproquement, si l'une des racines de $X^3 = \alpha$ est dans k, les trois racines sont constructibles par la règle et le compas à partir de k.

Il se pose alors le problème suivant :

Problème : Soit donné un sous-corps k_o de $\mathbb{C}$; donnons-nous un $\alpha \in \mathbb{C}$ tel que $|\alpha| = 1$, et que $k = k_o\langle\alpha\rangle$ soit stable par $z \to \bar{z}$; cherchons si l'équation $X^3 = \alpha$ possède une racine dans le corps $k = k_o\langle\alpha\rangle$ (condition nécessaire et suffisante pour que la donnée de k_o et de α permette de construire les trois racines cubiques de α par la règle et le compas).

Ce problème a ou n'a pas de solution, suivant les valeurs de α. On va se borner à donner des exemples :

Proposition 1. Si ce problème est possible, α est algébrique sur k_o.

Démonstration par l'absurde : supposons α transcendant sur k_o. Alors le corps $k_o\langle\alpha\rangle$ s'identifie au corps des fractions rationnelles $k_o(X)$: chaque élément de $k_o\langle\alpha\rangle$ s'écrit d'une seule manière comme une fraction rationnelle de α, à coefficients dans k_o. Supposons que le polynôme $X^3 - \alpha$ ait une racine dans ce corps : on a donc des polynômes

$$P(X) \in k_o[X] \quad , \quad Q(X) \in k_o[X] \quad , \quad Q \not\equiv 0$$

tels que

$$\left(\frac{P(\alpha)}{Q(\alpha)}\right)^3 = \alpha \quad ,$$

c'est-à-dire

$$(P(\alpha))^3 - \alpha(Q(\alpha))^3 = 0.$$

Puisque α est transcendant sur k_o, ceci implique que le polynôme

$$(P(X))^3 - X(Q(X))^3$$

est identiquement nul. Or le degré de $X(Q(X))^3$ est $\equiv 1 \pmod 3$, et celui de $(P(X))^3$ est $\equiv 0 \pmod 3$. Contradiction !

Supposons désormais α algébrique sur k_o. On va voir que dans certains cas le problème posé a une solution, dans d'autres il n'en a pas.

Exemple 1 : $k_o = \mathbb{Q}$, $\alpha = e^{\frac{2i\pi}{5}}$. Alors $z = \alpha^2$

satisfait à $z^3 = \alpha$, puisque $\alpha^5 = 1$. Le problème a donc une solution : on peut, avec la règle et le compas, partager l'angle $\frac{2\pi}{5}$ en trois parties égales (il suffit de le doubler!).

Exemple 2 : $k_o = \mathbb{Q}$, $\alpha = e^{\frac{2i\pi}{3}}$. Cette fois on a $\alpha^3 = 1$, donc α est bien algébrique. Si l'équation $X^3 - \alpha = 0$ avait une solution z dans $\mathbb{Q}\langle\alpha\rangle$, z pourrait être construit par la règle et le compas à partir de $\mathbb{Q}$, car $[\mathbb{Q}\langle\alpha\rangle : \mathbb{Q}] = 2$. Donc l'un des nombres

$$e^{\frac{2i\pi}{9}} \quad , \quad e^{\frac{8i\pi}{9}} \quad , \quad e^{\frac{14i\pi}{9}}$$

pourrait être construit à partir de $\mathbb{Q}$ par la règle et le compas. Or chacun d'eux est racine primitive 9-ième de l'unité (car 1, 4 et 7 sont premiers à 9). Donc on pourrait construire toutes les racines 9-ièmes de l'unité par la règle et le compas. Or on prouvera plus loin que c'est impossible. La conclusion, ici, est donc qu'on ne peut pas effectuer la trisection de l'angle $\frac{2\pi}{3}$ au moyen de la règle et du compas, à partir du corps $\mathbb{Q}\langle e^{\frac{2i\pi}{3}}\rangle$.

Revenons à la théorie générale : on va chercher une autre condition nécessaire et suffisante pour qu'un $z \in \mathbb{C}$ donné puisse être construit par la règle et le compas à partir d'un corps $k \subset \mathbb{C}$ donné.

Théorème 3. $k \subset \mathbb{C}$ étant donné, pour que (k stable par $z \mapsto \bar{z}$) z puisse être construit par la règle et le compas à partir de k, il faut et il suffit qu'il existe une extension normale k' de k, telle que le degré $[k' : k]$ soit une puissance de 2, et que $z \in k'$.

N.B. : normale $\Leftrightarrow$ galoisienne, car la caractéristique de k étant 0, toutes les extensions sont séparables.

La condition est nécessaire : par hypothèse, on a

$$k = k_0 \subset k_1 \subset \cdots \subset k_q \quad , \quad [k_i : k_{i-1}] = 2 \quad , \quad z \in k_q \ .$$

Si k_q est normale, alors on prend $k' = k_q$; sinon, soit $\sum$ l'ensemble (fini) des k-homomorphismes $k_q \longrightarrow \mathbb{C}$ [en fait, le cardinal de $\sum$ est 2^q] ; pour $\sigma \in \sum$, $\sigma(k_q)$ est un sous-corps de $\mathbb{C}$; soit k' le sous-corps engendré par les $\sigma(k_q)$, lorsque σ parcourt $\sum$. On sait que k' est une extension normale de k, et il reste à prouver que le degré $[k' : k]$ est une puissance de 2. Or soient $x_1 \in k_1$, $x_2 \in k_2, \ldots, x_q \in k_q$ qui engendrent k_q sur k. $\sigma(x_1), \ldots, \sigma(x_q)$ engendrent $\sigma(k_q)$ sur k.

Considérons successivement

$\sigma_1 = Id$, σ_2, $\sigma_3, \ldots$ Ecrivons la suite des éléments

$$x_1, x_2, \ldots, x_q, \ \sigma_2(x_1), \ldots, \sigma_2(x_q), \ \sigma_3(x_1), \ldots, \sigma_3(x_q), \ \ldots$$

Ils engendrent k' sur k. Or chacun d'eux est :

$\left\{ \begin{array}{l} \text{ou quadratique sur le sous-corps engendré par les précédents,} \\ \text{ou appartient à ce sous-corps.} \end{array} \right.$

Donc k' peut s'obtenir à partir de k par une succession d'extensions quadratiques.

$\Longrightarrow$ $[k' : k]$ = puissance de 2.

La condition est suffisante : Soit $z \in k'$, k' extension galoisienne de k, $[k' : k] = 2^n$. On a vu, grâce à la théorie de Galois, que k' s'obtient à partir de k par des extensions quadratiques successives. Prouvons-le à nouveau.

Soit $G = G(k', k)$; on a Card $G = 2^n$.

Lemme : Le centre de G contient un sous-groupe à deux éléments (déjà démontré). Soit G_{n-1}. Il lui correspond k_{n-1}, tel que $k \subset k_{n-1} \subset k'$; k_{n-1} se compose des $x \in k$ laissés fixes par G_{n-1}. On a $[k' : k_{n-1}] = 2$, et k_{n-1} est une extension galoisienne de k, car G_{n-1} est distingué dans G (puisqu'il est contenu dans le centre). De plus $[k_{n-1} : k] = 2^{n-1}$. Donc, par récurrence, on obtient une suite de sous-corps $k = k_0 \subset k_1 \subset \cdots \subset k_{n-1} \subset k'$, chacun étant de degré 2 sur le précédent. Puisque $z \in k'$, il s'ensuit que z peut être construit par la règle et le compas

à partir de k.

Corollaire du théorème 3 : Soit $P(X)$ le polynôme minimal de z sur k. Soit K le corps de décomposition de P (sur k), c'est-à-dire le sous-corps de $\mathbf{C}$ engendré par k et les racines de $P(X)$.

Alors, pour que z puisse être construit par la règle et le compas à partir de k, il faut et il suffit que le degré $[K : k]$ soit une puissance de 2.

Démonstration. K est une extension normale (donc galoisienne) de k ; c'est la plus petite extension normale contenant z. Si $[K : k]$ est une puissance de 2, z est constructible (d'après le théorème 3). Réciproquement, si z est constructible, le corps k' du théorème 3 contient K, donc $[K : k]$ divise $[k' : k]$, et par suite $[K : k]$ est une puissance de 2.

Construction des polygones réguliers de n côtés.

Problème : On se donne le cercle unité. On veut construire les solutions complexes de $X^n - 1 = 0$.

Ici on prend pour k le corps $\mathbb{Q}$ (engendré par 0 et 1). Il suffit de construire une racine primitive, i.e. une racine du polynôme cyclotomique $P_n(X)$, dont le degré est $\varphi(n)$.

Admettons pour un instant le résultat suivant (théorème d'Eisenstein) : le polynôme cyclotomique $P_1(X)$ est irréductible dans $\mathbb{Q}[X]$. Alors si α est une racine primitive n-ième de l'unité (par exemple $\alpha = e^{\frac{2\pi i}{n}}$), le corps $\mathbb{Q}\langle\alpha\rangle$ engendré par α est le corps obtenu par adjonction à $\mathbb{Q}$ d'une racine du polynôme irréductible $P_n(X)$, donc

$$[\mathbb{Q}\langle\alpha\rangle : \mathbb{Q}] = \deg P_n = \varphi(n).$$

D'ailleurs $\mathbb{Q}\langle\alpha\rangle$ est le sous-corps de $\mathbb{C}$ engendré par $\mathbb{Q}$ et toutes les racines de P_n ; donc, d'après le corollaire au théorème 3, la condition

$\varphi(n)$ est une puissance de 2

est nécessaire et suffisante pour que les racines n-ièmes de l'unité puissent être construites à partir de $\mathbb{Q}$ par la règle et le compas.

Démonstration du théorème d'Eisenstein.

Par l'absurde : supposons $P_n(X) = Q_1(X) \cdot Q_2(X)$, Q_1 et Q_2 étant des polynômes unitaires à coefficients dans $\mathbb{Q}$, $\deg Q_1 > 0$, $\deg Q_2 > 0$. Alors, d'après le lemme de Gauss, les coefficients de Q_1 et Q_2 sont enréalité dans $\mathbb{Z}$. Pour chaque p premier, on peut donc considérer les polynômes $Q_1^{(p)}$ et $Q_2^{(p)}$, à coefficients dans $\mathbb{F}_p$, obtenus par réduction modulo p des coefficients de Q_i et

Q_2. On aura

$$P_n^{(p)}(X) = Q_1^{(p)}(X) \cdot Q_2^{(p)}(X).$$

Les racines (complexes) de P_n se répartissent en deux sous-ensembles : les racines de Q_1, et les racines de Q_2. Soient α une racine de Q_1, β une racine de Q_2 ; puisque α et β sont des racines primitives, on a

$$\beta = \alpha^k \quad , \quad k \text{ entier tel que } (k, n) = 1.$$

Soit $k = p_1 p_2 \cdots p_k$ la décomposition de k en facteurs premiers (distincts ou non) ; on a $p_i \nmid n$ pour tout i. Considérons la suite

$$\alpha_1 = \alpha^{p_1} \quad , \quad \alpha_2 = (\alpha_1)^{p_2}, \ldots, \alpha_h = (\alpha_{h-1})^{p_h} = \beta \ ;$$

ce sont des racines de Q_1 ou de Q_2 ; comme la première est racine de Q_1, et la dernière est racine de Q_2, il y a deux termes consécutifs de cette suite, soient γ et γ^p (où p est l'un des p_i) tels que

$$Q_1(\gamma) = 0, \qquad Q_2(\gamma^p) = 0.$$

Observons que p ne divise pas n. Donc les polynômes

$$Q_1(X) \quad \text{et} \quad Q_2(X^p)$$

ont au moins une racine complexe commune ; leur p.g.c.d. (qui est à coefficients dans $\mathbb{Q}$, et même dans $\mathbb{Z}$ à cause du lemme de Gauss) est un polynôme unitaire $R(X)$ de degré ≥ 1. Puisque $R(X)$ divise $Q_1(X)$ et $Q_2(X^p)$ à coefficients entiers, la réduction (mod p) montre que $R^{(p)}(X)$ divise $Q_1^{(p)}(X)$ et $Q_2^{(p)}(X^p)$. Donc $Q_1^{(p)}(X)$ et $Q_2^{(p)}(X^p)$ ont une racine commune (soit u) dans une extension algébrique convenable de $\mathbb{F}_p$. Or

$$0 = Q_2^{(p)}(u^p) = (Q_2^{(p)}(u))^p,$$

donc u est une racine commune à $Q_1^{(p)}$ et $Q_2^{(p)}$, et comme $P_n^{(p)} = Q_1^{(p)} Q_2^{(p)}$, u est racine multiple de $P_n^{(p)}(X)$, et a fortiori de $X^n - 1$. Or les racines de $X^n - 1$ sont simples, puisque n n'est pas multiple de la caractéristique p. D'où une contradiction, ce qui démontre le théorème.

Retour à la construction du polygone régulier de n côtés.

On a trouvé la condition nécessaire et suffisante : $\varphi(n)$ est une puissance de

Explicitons : soit

$$n = 2^{\alpha}\, p_1^{\alpha_1} \cdots p_2^{\alpha_k},$$

$p_1, \ldots, p_2$ étant des nombres premiers impairs distincts, et $\alpha \geq 0$, $\alpha_1 \geq 1, \ldots, \alpha_k \geq 1$. On a

$$\varphi(n) = \begin{cases} 2^{\alpha-1}\, p_1^{\alpha_1-1} \cdots p_k^{\alpha_k-1} (p_1-1)\cdots(p_k-1) & \text{si } \alpha \geq 1 \\ p_1^{\alpha_1-1} \cdots p_k^{\alpha_k-1} (p_1-1)\cdots(p_k-1) & \text{si } \alpha = 0. \end{cases}$$

Pour que $\varphi(n)$ soit une puissance de 2, il faut et il suffit que :

(i) $\alpha_1 = 1, \ldots, \alpha_k = 1$;

(ii) $p_1 - 1, \ldots, p_k - 1$ soient des puissances de 2.

Donc : les p premiers impairs figurant effectivement dans la décomposition de n en facteurs premiers doivent être tels que $p-1$ soit une puissance de 2, et ils figurent alors avec l'exposant 1.

Remarque. Soit $n = n' n''$, n' et n'' premiers entre eux ; pour que n satisfasse à la condition précédente, il faut et il suffit que n' et n'' y satisfassent. En fait, si l'on a déjà construit le polynôme régulier de n' côtés et celui de n'' côtés, on construit celui de n côtés comme suit : soient u et $v \in \mathbb{Z}$ tels que

$$u\, n' + v\, n'' = 1 \quad \text{(Bézout)} ;$$

alors

$$\frac{1}{n} = \frac{v}{n'} + \frac{u}{n''},$$

donc

$$e^{\frac{2i\pi}{n}} = \left(e^{\frac{2i\pi}{n'}}\right)^{v} \cdot \left(e^{\frac{2i\pi}{n''}}\right)^{u}$$

(il suffit d'ajouter deux angles déjà connus).

D'après cette remarque, tout revient à construire les polygones réguliers de p côtés, p étant un nombre premier tel que $p-1$ soit une puissance de 2. Cherchons ces nombres premiers.

Lemme : si $p = 1 + 2^h$ est premier, alors l'entier h est lui-même une puissance de 2.

[Démonstration : sinon $h = h' h''$, avec h' impair ≥ 3. On a

$$2^h + 1 = (2^{h''})^{h'} + 1,$$

qui est divisible par $2^{h''} + 1$ en vertu de l'identité connue

$$X^n + 1 = (X+1)(X^{n-1} - X^{n-2} + X^{n-3} + \ldots + 1) \quad (n \text{ impair})]$$

D'après ce lemme, on a

$$p = 1 + 2^{(2^k)} \quad ;$$

le nombre $1 + 2^{(2^k)}$ se note F_k (k-ième nombre de Fermat). La question est maintenant : pour quelles valeurs de k le nombre F_k est-il premier ? Fermat avait conjecturé que F_k était premier pour tout k ; Gauss a montré que F_5 n'est pas premier, et on conjecture aujourd'hui qu'il n'y a qu'un nombre fini d'entiers k tels que F_k soit premier.

Voici les premiers nombres de Fermat :

$$F_0 = 3, \quad F_1 = 5, \quad F_2 = 17, \quad F_3 = 257, \ldots$$

Ainsi les polygones réguliers de 3, 5, 17, 257,... côtés sont constructibles par la règle et le compas. On va donner maintenant la construction pour 3, 5 et 17.

Groupe de Galois du corps des racines m-ièmes de l'unité.

Soit $K \supset \mathbb{Q}$ le corps de décomposition du polynôme cyclotomique $P_m(X)$; le corps K est le sous-corps de $\mathbb{C}$ engendré par $\mathbb{Q}$ et les racines m-ièmes de l'unité. K est aussi le corps obtenu par adjonction à $\mathbb{Q}$ d'une racine du polynôme irréductible $P_m(X)$, donc

$$[K : \mathbb{Q}] = \deg P_m(X) = \varphi(m).$$

Cherchons le groupe de Galois $G(K, \mathbb{Q})$. Puisque K est une extension normale de $\mathbb{Q}$, c'est une extension galoisienne (car la caractéristique est 0), donc

(1) $$\text{Card } G(K, \mathbb{Q}) = [K : \mathbb{Q}] = \varphi(m).$$

Choisissons une racine primitive α ; toute racine primitive s'écrit alors α^k où k est un entier premier à m, dont la classe (modulo m) est bien déterminé

Donc si $\sigma \in G(K, \mathbb{Q})$, il existe un $k \in G(m)$ et un seul tel que :

$$\sigma(\alpha) = \alpha^k ;$$

soit $k(\sigma)$ cet élément de $G(m)$. On a alors

$$(*) \qquad \sigma(\beta) = \beta^{k(\sigma)}$$

pour toute racine m-ième de l'unité β. L'application $\sigma \longmapsto k(\sigma)$ est un homomorphisme du groupe $G(K, \mathbb{Q})$ dans le groupe multiplicatif $G(m)$, car si $\sigma = \sigma_2 \circ \sigma_1$, on a

$$\sigma(\alpha) = \sigma_2(\sigma_1(\alpha)) = \sigma_2(\alpha^{k(\sigma_1)}) = \alpha^{k(\sigma_1)\cdot k(\sigma_2)},$$

c'est-à-dire $k(\sigma_2 \circ \sigma_1) = k(\sigma_2) \cdot k(\sigma_1)$.

Cet homomorphisme est injectif, car $k(\sigma)$ détermine σ par la formule (*). Comme $G(K, \mathbb{Q})$ et $G(m)$ ont même cardinal d'après (1), il s'ensuit que $\sigma \longmapsto k(\sigma)$ est bijectif, et définit donc un isomorphisme du groupe de Galois $G(K, \mathbb{Q})$ sur le groupe multiplicatif $G(m)$; cet isomorphisme ne dépend pas du choix de la racine primitive α.

Construction du polygone régulier de p côtés, pour p premier tel que :

$$p = 1 + 2^{(2^h)}.$$

On sait que le groupe $G(p) = \mathbb{F}_p^*$ est cyclique d'ordre $p - 1 = 2^{(2^h)}$. Soi σ un générateur de ce groupe (abélien) :

$$G(K, \mathbb{Q}) = \left\{ \sigma, \sigma^2, \ldots, \sigma^{p-2}, \sigma^{p-1} = 1 \right\}.$$

On a la suite de sous-groupes emboîtés (dont chacun est d'indice 2 dans le précéde sous-groupe engendré par $\sigma \supset$ sous-groupe engendré par $\sigma^2 \supset$ sous-groupe engendré par $\sigma^4 \supset \ldots \supset$ sous-groupe engendré par $\sigma^{\frac{p-1}{2}} \supset (1)$.

Par la théorie de Galois, il leur correspond des sous-corps de K :

$$\mathbb{Q} = k_0 \subset k_1 \subset k_2 \subset \ldots \subset k_h = K, \qquad \text{où}$$

$$\begin{cases} k_1 = \{\text{éléments de } K \text{ invariants par } \sigma^2\} \\ k_2 = \{\text{éléments de } K \text{ invariants par } \sigma^{2^2}\}, \text{ etc...,} \end{cases}$$

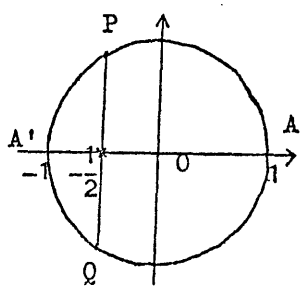
avec $[k_i : k_{i-1}] = 2$.

On va maintenant traiter explicitement les cas $p = 3$, $p = 5$ et $p = 17$.

$p = 3$ $\quad X^3 - 1 = 0, \quad P_3(X) = X^2 + X + 1.$

Les racines de cette équation du second degré sont $\frac{-1 \pm i\sqrt{3}}{2}$, de partie réelle $-\frac{1}{2}$. Ces points sont sur le cercle unité.

Construction : on trace la médiatrice du segment joignant les points $0 = (0, 0)$ et $A' = (0, -1)$, et on prend ses points d'intersection avec le cercle.

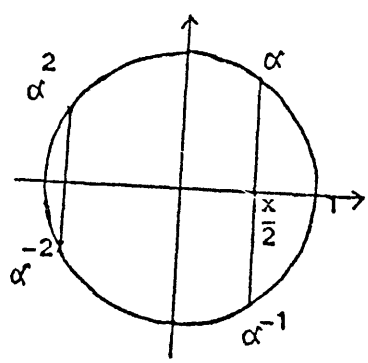


Variante: P et Q sont les points d'intersection du cercle unité et du cercle de centre A' et de rayon 1.

$p = 5$ $\quad X^5 - 1 = 0, \quad P_5(X) = X^4 + X^3 + X^2 + X + 1 = 0.$

Soit $\alpha = e^{\frac{2i\pi}{5}}$; 2 engendre le groupe multiplicatif $\mathbb{F}_5^*$; donc le groupe de Galois est engendré par $\sigma : \alpha \longmapsto \alpha^2$. Les transformés successifs de α par les puissances de σ sont :

$$\begin{cases} \sigma(\alpha) = \alpha^2, \\ \sigma^2(\alpha) = \alpha^4 = \alpha^{-1}, \\ \sigma^3(\alpha) = \alpha^{-2}, \\ \sigma^4(\alpha) = \alpha^{-4} = \alpha. \end{cases}$$



Soient $x = \alpha + \alpha^{-1}$, $x' = \alpha^2 + \alpha^{-2}$. On a $\sigma(x) = x'$, $\sigma(x') = x$, et σ^2 laisse invariants x et x'.

Donc $x + x'$ et xx' sont invariants par le groupe de Galois : ils sont dans $\mathbb{Q}$.

En fait : $\begin{cases} x + x' = \alpha + \alpha^2 + \alpha^{-1} + \alpha^{-2} = -1 \\ xx' = (\alpha + \alpha^{-1})(\alpha^2 + \alpha^{-2}) = \alpha + \alpha^2 + \alpha^{-1} + \alpha^{-2} = -1, \end{cases}$

puisque $\alpha, \alpha^2, \alpha^{-1}, \alpha^{-2}$ sont les quatre racines de l'équation $X^4 + X^3 + X^2 + X + 1 = 0$, dont la somme des racines est -1.

Ainsi x et x' sont les racines de l'équation $X^2 + X - 1 = 0$; ces racines $\quad -1 + \sqrt{5}$

En fait, la figure montre que la racine > 0 est $x = \alpha + \alpha^{-1}$, d'où $x = \frac{\sqrt{5} - 1}{2}$, $x' = -\frac{\sqrt{5} + 1}{2}$. Le corps k_1, formé des éléments invariants par σ^2, est engendré par x et x' ; c'est $\mathbb{Q}(\sqrt{5})$; puis $[K : \mathbb{Q}(\sqrt{5})] = 2$. Observons que

$$\cos \frac{2\pi}{5} = \frac{1}{2} x = \frac{\sqrt{5} - 1}{4}, \quad \cos \frac{4\pi}{5} = \frac{1}{2} x' = -\frac{\sqrt{5} + 1}{4}.$$

Si l'on veut α, la relation $\alpha + \alpha^{-1} = x$ montre que α et α^{-1} sont les racines de l'équation

$$(1) \qquad Y^2 - x\,Y + 1 = 0.$$

De même α^2 et α^{-2} sont les racines de $Z^2 - x' Z + 1 = 0$.

$\alpha = e^{\frac{2\pi i}{5}}$ est la racine de (1) dont la partie imaginaire est > 0 :

$$\alpha = \frac{x + i\sqrt{4 - x^2}}{2} \quad ; \text{ or } \quad 4 - x^2 = 4 - \frac{6 - 2\sqrt{5}}{4} = \frac{5 + \sqrt{5}}{2},$$

d'où $$e^{\frac{2\pi i}{5}} = \frac{\sqrt{5} - 1}{4} + \frac{i}{2}\sqrt{\frac{5 + \sqrt{5}}{2}}.$$

On calculerait de même α^2, α^{-1} et α^{-2}.

Construction : il suffit de construire les points de l'axe réel d'abscisses $\frac{x}{2}$ et $\frac{x'}{2}$; puis par ces points on mène les parallèles à l'axe imaginaire, qui coupent le cercle-unité aux points α, α^{-1}, α^2, α^{-2}. Pour construire $\frac{x}{2}$ et $\frac{x'}{2}$, introduisons l'angle aigu θ tel que

$$\operatorname{tg} 2\theta = 2.$$

La formule classique

$$\operatorname{tg} 2\theta = \frac{2 \operatorname{tg} \theta}{1 - \operatorname{tg}^2 \theta}$$

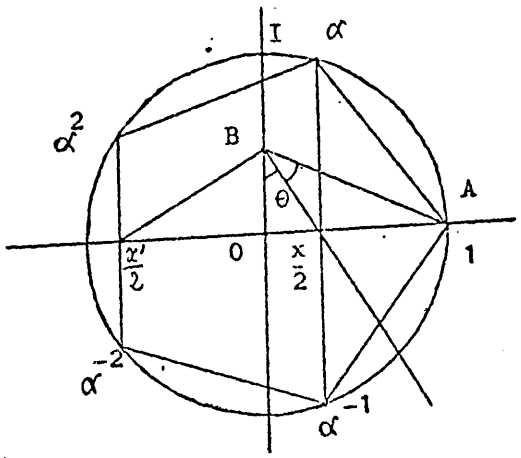
montre que $\operatorname{tg} \theta$ et $-\frac{1}{\operatorname{tg} \theta}$ sont les racines de l'équation

$$\operatorname{tg} 2\theta\,(X^2 - 1) + 2X = 0,$$

c'est-à-dire (puisque $\operatorname{tg} 2\theta = 2$), $X^2 + X - 1 = 0$. On a donc

$$x = \operatorname{tg} \theta, \quad x' = -\frac{1}{\operatorname{tg}\theta} = \operatorname{tg}\left(\theta + \frac{\pi}{2}\right).$$

D'où la construction : soit B le point $(0, \frac{1}{2})$ de l'axe imaginaire ; l'angle $\widehat{OBA}$ est égal à 2θ. On construit ses deux bissectrices, qui coupent l'axe réel aux points cherchés d'abscisses $\frac{x}{2}$ et $\frac{x'}{2}$.



p = 17 $\qquad X^{17} - 1 = 0.$

$P_{17}(X) = X^{16} + X^{15} + X^{14} + \ldots + X + 1 = 0.$

Le groupe de Galois $G(K, \mathbb{Q}) = G$ est cyclique d'ordre 16, isomorphe à $G(17)$.

Or $G(17)$ est engendré par la classe de 3 (mod 17) ; les puissances successives de 3 (mod 17) sont :

$$3^0 = 1,\ 3,\ -8,\ -7,\ -4,\ 5,\ -2,\ -6,$$

$$-1,\ -3,\ 8,\ 7,\ 4,\ -5,\ 2,\ 6.$$

Soit α une racine primitive, par exemple $\alpha = e^{\frac{2\pi i}{17}}$;

le groupe de Galois G est engendré pas l'automorphisme σ tel que $\sigma(\alpha) = \alpha^3$

les transformés de α par les puissances successives de σ (en commençant par σ^0 = identité) sont :

$$\alpha,\ \alpha^3,\ \alpha^{-8},\ \alpha^{-7},\ \alpha^{-4},\ \alpha^5,\ \alpha^{-2},\ \alpha^{-6},$$

$$\alpha^{-1},\ \alpha^{-3},\ \alpha^8,\ \alpha^7,\ \alpha^4,\ \alpha^{-5},\ \alpha^2,\ \alpha^6.$$

Le corps K a pour base (comme expace vectoriel sur $\mathbb{Q}$) :

$$1,\ \alpha,\ \alpha^2, \ldots,\ \alpha^{15},$$

ou encore

$$\alpha,\ \alpha^2,\ \alpha^3, \ldots,\ \alpha^{16}$$

[observer que $1 = -(\alpha + \alpha^2 + \alpha^3 + \ldots + \alpha^{16})$, puisque α annule $P_{17}(X)$]

Tout élément de K s'écrit donc d'une seule manière

$$\sum_{0 \leq i \leq 15} \lambda_i\ \sigma^i(\alpha),$$

où $\lambda_i \in \mathbb{Q}$. On en déduit facilement une caractérisation des éléments des sous-corps $k_1, k_2, k_3, k_4 = K$: k_1 se compose des <u>éléments invariants par</u> σ^2,

c'est-à-dire tels que $\lambda_i = \lambda_{i+2}$ quel que soit i (entier calculé module 16) ce sont les combinaisons linéaires (à coefficients dans $\mathbb{Q}$) des deux éléments suivant :

$$x = \sum_{j=0}^{7} \sigma^{2j}(\alpha), \qquad x' = \sum_{j=0}^{7} \sigma^{2j+1}(\alpha),$$

c'est-à-dire

$$\begin{cases} x = \alpha + \alpha^{-8} + \alpha^{-4} + \alpha^{-2} + \alpha^{-1} + \alpha^{8} + \alpha^{4} + \alpha^{2} \\ x' = \alpha^{3} + \alpha^{-7} + \alpha^{5} + \alpha^{-6} + \alpha^{-3} + \alpha^{7} + \alpha^{-5} + \alpha^{6}. \end{cases}$$

De même, k_2 se compose des combinaisons linéaires (à coefficients dans $\mathbb{Q}$) des quatre éléments :

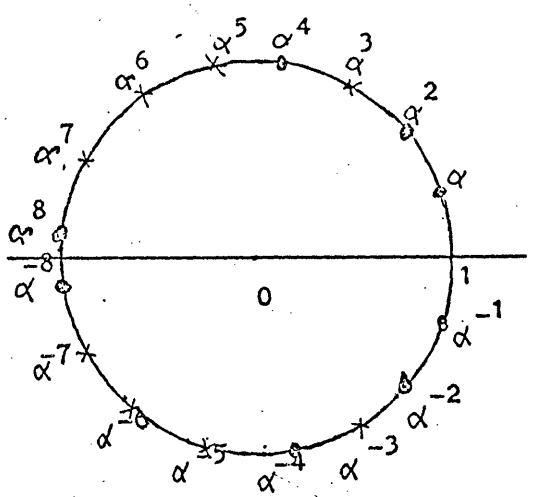
$$y_1 = \alpha + \alpha^{-4} + \alpha^{-1} + \alpha^{4}, \quad y_2 = \sigma^2(y_1) = \alpha^{-8} + \alpha^{-2} + \alpha^{8} + \alpha^{2},$$
$$y_1' = \alpha^{3} + \alpha^{5} + \alpha^{-3} + \alpha^{-5}, \quad y_2' = \sigma^2(y_1') = \alpha^{-7} + \alpha^{-6} + \alpha^{7} + \alpha^{6}.$$

Enfin, k_3 se compose des combinaisons linéaires (à coefficients dans $\mathbb{Q}$) de

$$\alpha + \alpha^{-1}, \quad \alpha^{4} + \alpha^{-4}, \quad \alpha^{3} + \alpha^{-3}, \quad \alpha^{5} + \alpha^{-5},$$
$$\alpha^{-8} + \alpha^{8}, \quad \alpha^{-2} + \alpha^{2}, \quad \alpha^{-7} + \alpha^{7}, \quad \alpha^{-6} + \alpha^{6},$$

dont les moitiés sont les cosinus des angles

$$\frac{2\pi}{17}, \frac{8\pi}{17}, \frac{6\pi}{17}, \frac{10\pi}{17}, \frac{16\pi}{17}, \frac{4\pi}{17}, \frac{14\pi}{17}, \frac{12\pi}{17}.$$



Remarque : Le corps k_3 se compose des éléments de K invariants par σ^8 : o $\sigma^8(\alpha) = \alpha^{-1}$, donc σ^8 transforme toute racine 17-ième de l'unité en son inverse, c'est-à-dire sa conjuguée. On en déduit $\sigma^8(z) = \bar{z}$ pour tout $z \in K$. Les éléments de K invariants par σ^8 ne sont autres que les éléments réels du corps K ; donc $k_3 = K \cap \mathbb{R}$.

Calcul de x et x'. On a $\sigma(x) = x'$, $\sigma(x') = x$; $x + x'$ et xx' sont invariants par G, donc dans $\mathbb{Q}$. En fait $x + x'$ est égal à la somme des racines de l'équation $P_{17}(X) = 0$, c'est-à-dire à -1. Si on calcule le produit xx', on trouve la somme de $8 \times 8 = 64$ termes, dont chacun est une racine primitive 17-ième de l'unité ; par raison de "symétrie", chacune des 16 racines primitives est trouvée 4 fois, donc xx' est égal à 4 fois la somme des racines primitives, c'est-à-dire

$$xx' = -4.$$

Donc x et x' sont les racines de l'équation :

$$X^2 + X - 4 = 0 \quad ;$$

ces racines sont $\frac{-1 \pm \sqrt{17}}{2}$. La figure montre que x est > 0 et $x' < 0$ (x est la somme des racines figurant en gros points sur la figure) ; d'où

$$x = \frac{-1 + \sqrt{17}}{2}, \qquad x' = -\frac{1 + \sqrt{17}}{2}$$

Le corps k_1 est $\mathbb{Q}(\sqrt{17})$.

Calcul de y_1 et y_2. On a évidemment

$$y_2 = \sigma^2(y_1), \quad y_1 = \sigma^2(y_2),$$

donc $y_1 + y_2$ et $y_1 y_2$ sont invariants par σ^2, c'est-à-dire appartiennent à k_1. En fait :

$$y_1 + y_2 = x, \qquad y_1 y_2 = \text{somme des racines de } P_{17}(X) = 0$$
$$= -1.$$

Donc y_1 et y_2 sont racines de l'équation

$$Y^2 - x\,Y - 1 = 0,$$

dont le discriminant est

$$x^2 + 4 = \frac{17 - \sqrt{17}}{2}.$$

Et on a

$$k_2 = \mathbb{Q}\left(\sqrt{17}, \sqrt{\frac{17 - \sqrt{17}}{2}}\right).$$

A ce corps appartiennent aussi y_1' et y_2', qui sont racines de l'équation

$$Y^2 - x'\,Y - 1 = 0,$$

dont le discriminant est $x'^2 + 4 = \frac{17 + \sqrt{17}}{2}$. [On observera que

$$\frac{17 - \sqrt{17}}{2} \cdot \frac{17 + \sqrt{17}}{2} = 17 \times 4 ,$$

d'où

$$\sqrt{\frac{17 + \sqrt{17}}{2}} = \frac{2\sqrt{17}}{\sqrt{\frac{17-\sqrt{17}}{2}}} = \frac{\sqrt{17} + 1}{4}\sqrt{\frac{17 - \sqrt{17}}{2}} \;] \; .$$

Posons ensuite, pour $1 \leq i \leq 8$:

$$z_i = \alpha^i + \alpha^{-i} .$$

On a $z_1 + z_4 = y_1$, $z_1 z_4 = y'_1$;

donc z_1 et z_4 sont les racines de

$$Z^2 - y_1 Z + y'_1 = 0.$$

De même, z_3 et z_5 sont les racines de

$$Z^2 - y'_1 Z + y_2 = 0 \; ; \; \text{etc...}$$

Construction par la règle et le compas. Il suffit de construire les points α^3 et α^5 (voir figure) ; car alors le cercle de centre α^3 passant par α^5 recoupe le cercle-unité au point α . Tout revient donc à construire, sur l'axe réel, les points P et Q d'abscisses

$$\frac{1}{2}(\alpha^3 + \alpha^{-3}) = \frac{1}{2} z_3, \qquad \frac{1}{2}(\alpha^5 + \alpha^{-5}) = \frac{1}{2} z_5 .$$

Introduisons l'angle aigu θ tel que

$$\text{tg } 4\theta = 4.$$

On vérifie que

$$x = 2 \text{ tg } 2\theta \; , \; x' = -\frac{2}{\text{tg } 2\theta} .$$

[En effet, $\text{tg } 2\theta$ et $-\frac{2}{\text{tg } 2\theta}$ sont les racines de l'équation

$$\text{tg } 4\theta \, (X^2 - 1) + 2X = 0 ,$$

c'est-à-dire

$$X^2 + \frac{1}{2} X - 1 = 0 ;$$

les doubles (des) racines sont bien les racines de

$$X^2 + X - 4 = 0 ,$$

c'est-à-dire x et x'] .

Ensuite, y'_1 et y'_2 sont les racines de

$$Y^2 + \frac{2}{\text{tg } 2\theta} Y - 1 = 0 ;$$

ces racines sont $\operatorname{tg}\theta$ et $-\frac{1}{\operatorname{tg}\theta}$ [regarder à nouveau l'expression de $\operatorname{tg} 2\theta$ en fonction de $\operatorname{tg}\theta$]. Sur la figure, on voit que $y'_1 > 0$, $y'_2 < 0$; donc

$$y'_1 = \operatorname{tg}\theta \quad , \quad y'_2 = -\frac{1}{\operatorname{tg}\theta} \ .$$

Enfin, y_1 et y_2 sont les racines de

$$Y^2 - 2\operatorname{tg} 2\theta\, Y - 1 = 0 \ ;$$

cette équation se déduit de la précédente en changeant θ en $\theta + \frac{\pi}{4}$; on a donc

$$y_1 = \operatorname{tg}\left(\theta + \tfrac{\pi}{4}\right) \quad , \quad y_2 = -\frac{1}{\operatorname{tg}(\theta + \frac{\pi}{4})} = \operatorname{tg}\left(\theta - \tfrac{\pi}{4}\right) \ .$$

On a alors

$$z_3 + z_5 = \operatorname{tg}\theta \quad , \quad z_3 z_5 = \operatorname{tg}\left(\theta \pm \tfrac{\pi}{4}\right) \ .$$

Les nombres cherchés $\frac{1}{2} z_3$ et $\frac{1}{2} z_5$, abscisses des points P et Q, ont donc pour demi-somme

$$\frac{1}{2}\left(\frac{z_3}{2} + \frac{z_5}{2}\right) = \frac{1}{4} \operatorname{tg}\theta$$

et pour produit

$$\frac{z_3}{2} \cdot \frac{z_5}{2} = \frac{1}{4} \operatorname{tg}\left(\theta - \tfrac{\pi}{4}\right) = -\frac{1}{4} \operatorname{tg}\left(\tfrac{\pi}{4} - \theta\right) \ .$$

Une fois qu'on aura construit $\frac{1}{4}\operatorname{tg}\theta$ et $\frac{1}{4}\operatorname{tg}\left(\frac{\pi}{4} - \theta\right)$, on pourra donc construire $\frac{z_3}{2}$ et $\frac{z_5}{2}$: le milieu du segment PQ sera le point C d'abscisse $\frac{1}{4}\operatorname{tg}\theta$, et le cercle de diamètre PQ coupera l'axe imaginaire en un point K tel que $\overline{OK}^2 = \frac{1}{4}\operatorname{tg}\left(\frac{\pi}{4} - \theta\right) > 0$.

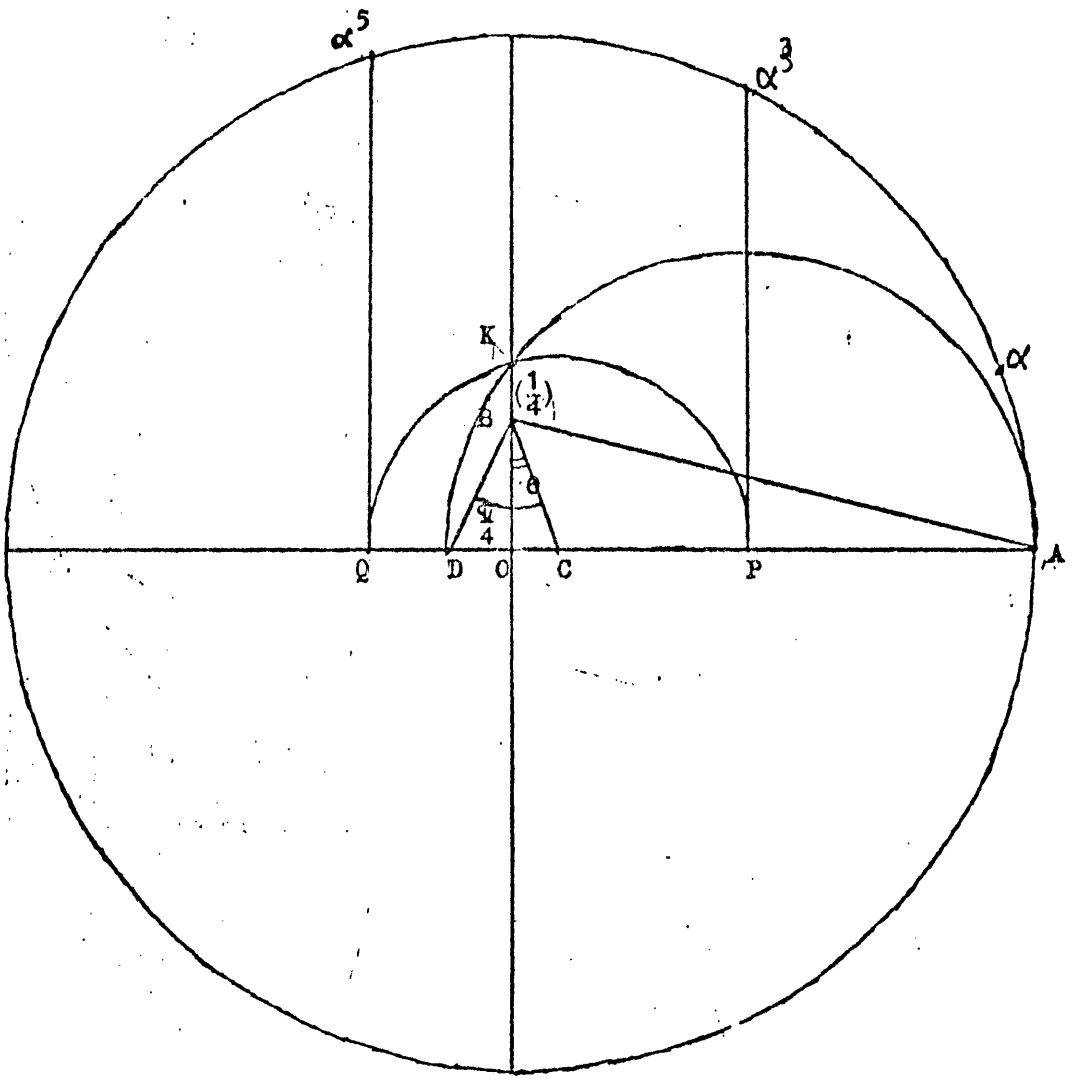
On en déduit la construction suivante : soit A le point de l'axe réel d'abscisse 1, et soit B le point de l'axe imaginaire d'ordonnée $\frac{1}{4}$. L'angle $\widehat{OBA}$ est égal à 4θ ; on en construit le quart (en le partageant deux fois de suite en deux parties égales) ; d'où un point C sur le demi-axe réel positif, tel que $\widehat{OBC} = \theta$. On construit ensuite la demi-droite BD qui fait avec BC l'angle $-\frac{\pi}{4}$: le point D est sur l'axe réel, son abscisse est négative. Le point K cherché (sur l'axe imaginaire) est tel que

$$\overline{OK}^2 = -\overline{OD} \cdot \overline{OA} \ ,$$

donc K est à l'intersection du demi-axe imaginaire >0 avec le cercle de diamètre AD. Ensuite le cercle de centre C qui passe par K coupe l'axe réel

.../...

aux points cherchés P et Q. Les parallèles à l'axe imaginaire passant par P et Q coupent le demi-cercle unité aux points α^3 et α^5 cherchés.



GROUPES CLASSIQUES

On considérera l'espace vectoriel réel $\mathbb{R}^n$ muni de sa base canonique, ainsi que l'espace vectoriel complexe $\mathbb{C}^n$ muni de sa base canonique. On identifiera $\mathbb{R}^n$ à un sous-espace vectoriel réel de $\mathbb{C}^n$.

Les ensembles $\mathrm{End}_{\mathbb{R}}(\mathbb{R}^n)$ et $\mathrm{End}_{\mathbb{C}}(\mathbb{C}^n)$ sont des algèbres, et en particulier des espaces vectoriels ; leur dimension est n^2 :

$$\dim_{\mathbb{R}}(\mathrm{End}_{\mathbb{R}}\ \mathbb{R}^n) = n^2 , \qquad \dim_{\mathbb{C}}(\mathrm{End}_{\mathbb{C}}\ \mathbb{C}^n) = n^2 .$$

On a une structure multiplicative : $(g, f) \longmapsto g \circ f$ (composition des endomorphismes)

1- $(g_1 + g_2) \circ f = g_1 \circ f + g_2 \circ f$

2- $(\lambda g) \circ f = \lambda (g \circ f)$

3- $g \circ (f_1 + f_2) = g \circ f_1 + g \circ f_2$

4- $g \circ (\lambda f) = \lambda (g \circ f)$.

Ces conditions expriment que $g \circ f$ est une fonction bilinéaire du couple (f, g). Soit $f \in \mathrm{End}_{\mathbb{R}}\ \mathbb{R}^n$, et soit $\{e_1, \ldots, e_n\}$ la base canonique de $\mathbb{R}^n$. L'endomorphisme f se représente par une matrice (a_{ij}) à n lignes et n colonnes, qu'on définit en posant

$$f(e_j) = \sum_{i=1}^{n} a_{ij}\, e_i , \quad \text{où} \begin{cases} i = \text{indice de la ligne} \\ j = \text{indice de la colonne.} \end{cases}$$

Soit $x \in \mathbb{R}^n$; alors $x = \sum_{i=1}^{n} x_i\, e_i$, où $x_i \in \mathbb{R}$. Donc

$$f(x) = \sum_{j=1}^{n} x_j\, f(e_j) = \sum_{j=1}^{n} x_j \sum_{i=1}^{n} a_{ij}\, e_i = \sum_{i,j} a_{ij}\, x_j\, e_i \ ;$$

mais $f(x) \in \mathbb{R}^n \Longrightarrow f(x) = \sum_{i=1}^{n} x'_i\, e_i \Longrightarrow x'_i = \sum_{j=1}^{n} a_{ij}\, x_j$.

Par cette correspondance bijective entre $\mathrm{End}_{\mathbb{R}}\ \mathbb{R}^n$ et l'ensemble $M_n(\mathbb{R})$ des matrices réelles à n lignes et n colonnes, on transporte à $M_n(\mathbb{R})$ la structure d'algèbre de $\mathrm{End}\ \mathbb{R}^n$. On trouve :

$$\begin{cases} (a_{ij}) + (b_{ij}) = (a_{ij} + b_{ij}) \\ \lambda (a_{ij}) = (\lambda\, a_{ij}) \\ (a_{ij})(b_{jk}) = (c_{ik}) \quad , \text{ où } \quad c_{ik} = \sum_{j=1}^{n} a_{ij}\, b_{jk} \end{cases}$$

On fait de même pour l'algèbre $M_n(\mathbb{C})$ des matrices complexes à n lignes et n colonnes, en correspondance bijective avec $End_{\mathbb{C}}(\mathbb{C}^n)$; les formules sont les mêmes dans le cas réel que dans le cas complexe.

Groupes linéaires.

Soit $A \in End_{\mathbb{R}}(\mathbb{R}^n)$; A est un endomorphisme de $\mathbb{R}^n$ dans lui-même. Les propriétés suivantes sont équivalentes :

1- A est injectif

2- A est surjectif

3- A est bijectif (c'est-à-dire A est un automorphisme)

4- $\exists$ B tel que $BA = 1$ ($1 = 1_n$ est l'élément unité de l'algèbre)

5- $\exists$ C tel que $AC = 1$ ($1 = 1_n$ est l'élément unité de l'algèbre)

6- $\exists A^{-1}$ tel que $AA^{-1} = A^{-1}A = 1$ ($1 = 1_n$ est l'élément unité de l'algèbre)

7- $\det A \neq 0$.

Définition.

$GL(n, \mathbb{R})$ est l'ensemble des endomorphismes de $\mathbb{R}^n$ vérifiant l'une des conditions ci-dessus ; muni de la multiplication des endomorphismes, c'est un groupe : le groupe linéaire réel à n variables. Il est non-commutatif pour $n \geq 2$.
On a une définition analogue de $GL(n, \mathbb{C})$, groupe linéaire complexe. On identifiera $GL(n, \mathbb{R})$ à un sous-groupe de $GL(n, \mathbb{C})$.
Repère : un élément de $End_{\mathbb{R}} \mathbb{R}^n$ est défini par $f(e_1), \ldots, f(e_n)$; il est inversible si et seulement si $f(e_1), \ldots, f(e_n)$ forment une base de $\mathbb{R}^n$. Une base s'appelle aussi un repère ; on trouve une correspondance bijective entre l'ensemble $GL(n, \mathbb{R})$ et l'ensemble des repères de $\mathbb{R}^n$, comme suit : étant donné un repère r, il existe un unique élément de $GL(n, \mathbb{R})$ qui transforme la base canonique $(e_1, \ldots, e_n)$ de $\mathbb{R}^n$ en le repère r.
Topologie sur $End_{\mathbb{R}} \mathbb{R}^n$.

Il suffit de remarquer que $End_{\mathbb{R}} \mathbb{R}^n$ est isomorphe au produit $\mathbb{R}^n \times \mathbb{R}^n \times \ldots \times \mathbb{R}^n$ (n fois), soit à $\mathbb{R}^{n^2}$ qui est muni de la topologie habituelle.
Le déterminant d'un endomorphisme de $\mathbb{R}^n$ est une application continue de $End_{\mathbb{R}} \mathbb{R}^n$ dans $\mathbb{R}$, et par conséquent $(\det)^{-1}\{0\}$ est un ensemble fermé de $End_{\mathbb{R}} \mathbb{R}^n$.

On en déduit que $GL(n, \mathbb{R}) = (\det)^{-1}\{\mathbb{R} - \{0\}\}$ est un ensemble ouvert de $\mathrm{End}_{\mathbb{R}} \mathbb{R}^n$. Muni de la topologie induite, c'est un groupe topologique : la seule chose à vérifier est que l'inverse d'une matrice inversible est une fonction continue de cette matrice ; or cela résulte de la formule explicite qui donne cet inverse (c'est le quotient d'un polynôme en les éléments de la matrice par l'inverse du déterminant).

Le déterminant d'un endomorphisme injectif de $\mathbb{R}^n$ est une application de $GL(n, \mathbb{R})$ dans $\mathbb{R}^*$; c'est un homomorphisme du groupe $GL(n, \mathbb{R})$ dans le groupe multiplicatif $\mathbb{R}^* \approx GL(1, \mathbb{R})$, car $\det(g \circ f) = (\det g).(\det f)$. L'homomorphisme $\det : GL(n, \mathbb{R}) \longrightarrow \mathbb{R}^*$ est surjectif, car

$$\forall\, d \in \mathbb{R}^*\ ,\ \exists\ M \in GL(n, \mathbb{R}) \quad \text{tel que} \quad \det M = d :$$

il suffit de prendre la matrice $M = \begin{pmatrix} d & & & 0 \\ & 1 & & \\ & & \ddots & \\ 0 & & & 1 \end{pmatrix}$.

On désigne par $SL(n, \mathbb{R})$ le sous-groupe formé des endomorphismes de $GL(n, \mathbb{R})$ dont le déterminant est égal à $+1$. On a alors la suite exacte suivante :

$$(1) \longrightarrow SL(n, \mathbb{R}) \longrightarrow GL(n, \mathbb{R}) \xrightarrow{\det} \mathbb{R}^* \longrightarrow (1).$$

On démontre de la même façon qu'on a la suite exacte

$$(1) \longrightarrow SL(n, \mathbb{C}) \longrightarrow GL(n, \mathbb{C}) \xrightarrow{\det} \mathbb{C}^* \longrightarrow (1)$$

On a d'ailleurs $\mathbb{C}^* = GL(1, \mathbb{C})$.

Proposition. Pour $n \geq 1$, $GL(n, \mathbb{R})$ n'est pas connexe.

Démonstration : pour $n = 1$, $GL(1, \mathbb{R}) = \mathbb{R}^*$ n'est pas connexe mais a deux composantes connexes : l'ensemble ($\mathbb{R}^+$) des $x > 0$ et l'ensemble $\mathbb{R}^-$ des $x < 0$. Pour n quelconque, $(\det)^{-1}(\mathbb{R}^+)$ et $(\det)^{-1}(\mathbb{R}^-)$ sont des ouverts non vides disjoints de $GL(n, \mathbb{R})$, dont la réunion est $GL(n, \mathbb{R})$, qui n'est donc pas connexe.

On note
$$\begin{cases} (\det)^{-1}(\mathbb{R}^+) = GL^+(n, \mathbb{R}) \\ (\det)^{-1}(\mathbb{R}^-) = GL^-(n, \mathbb{R}) \end{cases}$$

Remarque.

$GL^+(n, \mathbb{R})$ est un sous-groupe d'indice 2 (donc distingué) de $GL(n, \mathbb{R})$, car $\mathbb{R}^*/\mathbb{R}^+ \approx \{-1, 1\}$.

Proposition.

$GL^+(n, \mathbb{R})$ est connexe par arcs, et a fortiori connexe.

Démonstration :

1) Rappelons d'abord que si un espace topologique E n'est pas connexe, il n'est pas connexe par arcs. En effet :

Soit E non connexe ; $\exists$ U et V, ouverts non vides de E, tels que $U \cap V = \emptyset$ et $U \cup V = E$. Choisissons $a \in U$ et $b \in V$, et montrons qu'il n'existe pas de chemin de E ayant a pour origine et b pour extrémité. Par l'absurde : supposons qu'on ait un chemin allant de $a \in U$ à $b \in V$, c'est-à-dire une application f de $[0, 1]$ dans E telle que f soit continue, $f(0) = a$, $f(1) = b$. Donc $0 \in f^{-1}(U)$ et $1 \in f^{-1}(V)$; $f^{-1}(U)$ et $f^{-1}(V)$ seraient deux ouverts disjoints non vides de $[0, 1]$ ayant $[0, 1]$ pour réunion, ce qui est absurde car le segment $[0, 1]$ est connexe.

2) $GL^+(n, \mathbb{R})$ est connexe par arcs.

On va le prouver par récurrence sur $n \geq 1$. C'est vrai pour $n = 1$, car $\mathbb{R}^+$ est connexe par arcs. Supposons l'assertion vraie pour $n - 1$ $(n \geq 2)$, et montrons qu'elle est vraie pour n.

Soit $(e_1, \ldots, e_n)$ la base canonique de $\mathbb{R}^n$; un repère $(e'_1, \ldots, e'_n)$ est donné par

$$e'_j = \sum_i a_{ij} e_i ,$$

c'est-à-dire est défini par une matrice $A = (a_{ij})$ telle que $\det A \neq 0$. Il est direct si $\det A > 0$. Il s'agit de montrer que tout repère direct peut être joint au repère canonique $(e_1, \ldots, e_n)$ par un chemin dans l'espace des repères ; ou encore que toute matrice A (à n lignes et n colonnes) telle que $\det A > 0$ peut être jointe à la matrice-unité par un chemin dans l'espace des matrices de déterminant > 0.

1er cas. $a_{11} \neq 0$. On peut alors supposer $a_{11} > 0$; en effet, on passe du repère $(e'_1, e'_2, e'_3, \ldots, e'_n)$ au repère $(-e'_1, -e'_2, e'_3, \ldots, e'_n)$ par un chemin dans l'espace des repères, à savoir

$$(e'_1 \cos\theta - e'_2 \sin\theta, e'_1 \sin\theta + e'_2 \cos\theta, e'_3, \ldots, e'_n)$$

(θ variant de 0 à π). Pour chaque $t \in [0, 1]$, considérons le repère

$$(e'_1,\ e'_2 - t\frac{a_{1,2}}{a_{1,1}}\ e'_1,\ldots,\ e'_n - t\frac{a_{1,n}}{a_{1,1}}\ e'_1)\ ;$$

ceci définit, dans l'espace des repères, un chemin d'origine $(e'_1, e'_2,\ldots, e'_n)$ et d'extrémité $(e'_1, e''_2,\ldots, e''_n)$, avec

$$e''_j = e'_j - \frac{a_{1,j}}{a_{1,1}}\ e'_1 \qquad (2 \leq j \leq n)$$

$e''_2,\ldots, e''_n$ sont combinaisons linéaires de $e_2,\ldots, e_n$, donc la matrice du repère $(e'_1, e''_2,\ldots, e''_n)$ est de la forme

$$B = \begin{pmatrix} a_{11} & 0 & \cdots & 0 \\ a_{21} & & & \\ \vdots & & M & \\ a_{n1} & & & \end{pmatrix}$$

où M est une matrice à (n-1) lignes et (n-1) colonnes. On a

$$\det B = a_{11} \cdot (\det M)\ ;$$

puisque $\det B > 0$ et $a_{11} > 0$, on a $\det M > 0$. De plus la matrice

$$B(t) = \begin{pmatrix} a_{11} & 0 & \cdots & 0 \\ ta_{21} & & & \\ \vdots & & M & \\ ta_{n1} & & & \end{pmatrix}$$

montre qu'il existe un chemin joignant $B = B(1)$ à

$$B(0) = \begin{pmatrix} a_{11} & 0 & \cdots & 0 \\ 0 & & & \\ \vdots & & M & \\ 0 & & & \end{pmatrix}$$

Par l'hypothèse de récurrence, il existe un chemin joignant M à la matrice-unité dans l'espace des matrices inversibles à n-1 lignes et n-1 colonnes. Finalement on arrive à la matrice

$$\begin{pmatrix} a_{11} & 0 & \cdots & 0 \\ 0 & & & \\ \vdots & & I_{n-1} & \\ 0 & & & \end{pmatrix}$$

et il reste à déformer continûment a_{11} en 1, ce qui est possible puisque $a_{11} > 0$.

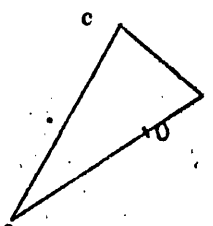
2ème cas. $a_{11} = 0$. Comme les a_{1j} ne sont pas tous nuls, on peut supposer par exemple $a_{12} \neq 0$. Considérons, pour $t \in [0, 1]$, le repère

$$(e'_1 + te'_2, e'_2, \ldots, e'_n) .$$

Pour $t = 1$, on est ramené au cas où $a_{11} \neq 0$, déjà traité.

Théorème. $GL(n, \mathbb{C})$ est connexe par arcs.

La démonstration est analogue à la précédente, par récurrence sur $n \geq 1$. Pour $n = 1$, on doit vérifier que $\mathbb{C} - \{0\}$ est connexe par arcs (plan privé de l'origine 0). Or soient a et b deux points du plan $\mathbb{C}$, distincts de 0 ; si le segment qui joint a et b ne contient pas 0, il fournit un chemin de $\mathbb{C} - \{0\}$ joignant a à b. Sinon, choisissons un point c non aligné avec a et b ; alors la ligne brisée formée du segment joignant a et c et du segment joignant c et b est un chemin d'origine a et d'extrémité b. Donc $\mathbb{C} - \{0\}$ est bien connexe par arcs.



Produits scalaires.

1- Produit scalaire euclidien dans $\mathbb{R}^n$ (ou dans $\mathbb{C}^n$) :

$$\langle x, y \rangle = \sum_{i=1}^{n} x_i \, y_i$$

2- Produit scalaire hermitien dans $\mathbb{C}^n$

$$(x \mid y) = \sum_{i=1}^{n} x_i \, \overline{y_i}$$

On a

a] $(x \mid x) = \sum_i |x_i|^2$; on pose $\|x\| = \sqrt{(x|x)}$

b] $(y \mid x) = \overline{(x \mid y)}$

Remarque.

Le produit scalaire euclidien et le produit scalaire hermitien coïncident sur $\mathbb{R}^n$.

Inégalité de Cauchy-Schwarz :

$$|(x|y)| \leq \|x\| \, \|y\|$$

Démonstration.

$$(\lambda x + \mu y | \lambda x + \mu y) = \lambda\bar{\lambda}\,(x|x) + \mu\bar{\mu}(y|y) + \lambda\,\bar{\mu}(x|y) + \mu\,\bar{\lambda}(y|x)$$

$$= \lambda\bar{\lambda}(x|x) + \mu\bar{\mu}(y|y) + 2\mathcal{R}e[\lambda\,\bar{\mu}(x|y)] \geq 0$$

Soit : $a\,|\lambda|^2 + c\,|\mu|^2 + 2\,\mathcal{R}e(b\,\lambda\,\bar{\mu}) \geq 0$; $a = (x|x)$, $c = (y|y)$, $b = (x|y)$.

Or $a \geq 0$ $c \geq 0 \implies |b| \leq \sqrt{a\,c}$ c.q.f.d.

Inégalité du triangle.

$\|x + y\| \leq \|x\| + \|y\|$: conséquence de Cauchy-Schwarz.

Soit A une matrice (n, n) ou un endomorphisme de $\mathbb{R}^n$, resp. de $\mathbb{C}^n$. Alors

$$\langle Ax, y\rangle = \sum_i (\sum_j a_{ij}\,x_j)\,y_i = \sum_{i,j} a_{ij}\,x_j\,y_i \quad :$$

c'est une forme bilinéaire de $x = (x_1, \ldots, x_n)$ et $y = (y_1, \ldots, y_n)$.

Inversement, si on se donne une forme bilinéaire $f(x, y)$, on a

$$f(x, y) = f(\sum_j x_j\,e_j, \sum_i y_i\,e_i) = \sum_{i,j} f(e_j, e_i)\,x_j\,y_i$$

Si on pose

$$a_{ij} = f(e_j, e_i) \quad \text{et} \quad A = (a_{ij}), \quad \text{on a}$$

$$f(x, y) = \langle Ax, y\rangle$$

Conséquence.

On a une correspondance bijective canonique entre matrices (n, n) et formes bilinéaires : $A \longleftrightarrow$ forme bilinéaire $\langle Ax, y\rangle$

Si on considère $\langle Ax, y\rangle$ et si on fixe y, alors $\langle Ax, y\rangle$ est une forme linéaire $\varphi(x)$; on sait alors qu'il existe un unique z de $\mathbb{R}^n$ tel que $\varphi(x) = \langle x, z\rangle$, i.e. $\varphi(x) = \sum_i x_i\,z_i$. Donc si on fixe y, on a $\langle Ax, y\rangle = \langle x, z\rangle$; il est clair que z dépend linéairement de y. On pose alors $z = {}^tA(y)$, ce qui définit la matrice ${}^tA$. Ainsi $\boxed{\langle Ax, y\rangle = \langle x, {}^tA\,y\rangle}$ quels que soient x et y. Cette relation caractérise la matrice transposée ${}^tA$ de la matrice A. Calculons-la.

Soit ${}^tA = (b_{ij})$; on a

$$\langle x, {}^tA\,y\rangle = \sum_i (\sum_j b_{ij}\,y_j)\,x_i = \sum_{i,j} b_{ij}\,y_j\,x_i = \sum_{i,j} b_{ji}\,y_i\,x_j$$

$$\langle Ax, y\rangle = \sum_i (\sum_j a_{ij}\,x_j)\,y_i = \sum_{i,j} a_{ij}\,y_i\,x_j$$

$$\langle x, {}^tA\, y\rangle = \langle Ax, y\rangle \iff (b_{ji}) = (a_{ij}) \qquad \boxed{b_{ji} = a_{ij}}$$

Ainsi ${}^tA$ se déduit de A par échange des lignes et des colonnes.

Propriétés de la transposition.

$${}^t({}^tA) = A$$

$${}^t(A + B) = {}^tA + {}^tB$$

$${}^t(\lambda A) = \lambda\, {}^tA$$

$${}^t(A\,B) = {}^tB\, {}^tA \quad ;$$ cette dernière relation se vérifie comme suit :

$$\langle AB\,x, y\rangle = \langle Bx, {}^tA\, y\rangle = \langle x, {}^tB\, {}^tA\, y\rangle .$$

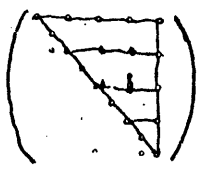
On a enfin $\det({}^tA) = \det A$.

Définition :

On dit qu'une matrice est symétrique si $A = {}^tA$. A symétrique $\iff \langle Ax, y\rangle = \langle x, Ay\rangle$, $\forall x, y \in \mathbb{R}^n$.

Conséquence.

Les matrices symétriques forment un sous-espace vectoriel de $\mathrm{End}_{\mathbb{R}}(\mathbb{R}^n)$, de dimension $\frac{n(n+1)}{2}$. En effet la dimension du sous-espace vectoriel considéré, est égale au nombre d'éléments réels qu'on peut choisir arbitrairement pour former une matrice symétrique



C'est donc

$$1 + 2 + 3 + \ldots + n = \frac{n(n+1)}{2}$$

Considérons maintenant le produit scalaire hermitien $(Ax|y) = \sum_{i,j} a_{ij}\, x_j\, \bar{y}_i$: c'est une fonction $f(x, y)$ qui est linéaire en x et antilinéaire en y :

$$f(\lambda x, y) = \lambda f(x, y), \qquad f(x, \mu y) = \bar{\mu}\, f(x, y).$$

On dit dans ce cas que f est une forme sesquilinéaire. Inversement, si on prend une forme sesquilinéaire f, alors

$$f(x, y) = f\left(\sum_j x_j\, e_j, \sum_i y_i\, e_i\right) = \sum_{i,j} f(e_j, e_i)\, x_j\, \bar{y}_i .$$

Si on pose alors $a_{ij} = f(e_j, e_i)$ et $A = (a_{ij})$, on a

$$f(x, y) = (Ax \mid y).$$

On a donc une correspondance bijective entre les matrices de $\mathrm{End}\ \mathbb{C}^n$ et les formes sesquilinéaires ; cette correspondance est définie par $A \longleftrightarrow (Ax \mid y)$. Alors, comme pour la transposée dans le cas réel, on définit l'adjointe d'une matrice A par $\boxed{(Ax \mid y) = (x, A^* y)}$.

Calcul de l'adjointe :

Si $A^* = (b_{ij})$, alors $b_{ij} = \overline{a}_{ji}$, donc $\boxed{A^* = {}^t\overline{A}}$.

Propriétés.

$(A + B)^* = A^* + B^*$

$(\lambda A)^* = \overline{\lambda}\ A^*$.

$(A\ B)^* = B^*\ A^*$

$(A^*)^* = A$

$\det(A^*) = \overline{(\det A)}$.

Définition.

On dit qu'une matrice est hermitienne si $A = A^*$. A hermitienne $\Longleftrightarrow$ $(Ax \mid y) = (x \mid Ay)$, $\forall\ x, y \in \mathbb{C}^n$.

Propriétés des matrices hermitiennes.

1- Les éléments de la diagonale sont réels.

2- Les matrices hermitiennes forment un sous-espace vectoriel réel de $\mathrm{End}(\mathbb{C}^n)$ dont nous pouvons calculer la dimension sur $\mathbb{R}$. En effet pour former une matrice hermitienne on peut prendre arbitrairement les n éléments réels de la diagonale et les $\frac{n(n-1)}{2}$ éléments complexes qui sont au-dessus de la diagonale, ce qui correspond à $n(n-1)$ nombres réels. Donc en tout $n + n(n-1) = n^2$ réels arbitraires. Soit $H(n)$ le sous-espace vectoriel des matrices hermitiennes de $\mathrm{End}(\mathbb{C}^n)$; on a alors

$$\dim_{\mathbb{R}} H(n) = n^2.$$

3- Si A est hermitienne, alors $(A\,x \mid y) = (x \mid Ay)$. Mais $(x|Ay) = \overline{(Ay|x)}$; on en déduit que pour qu'une matrice A soit hermitienne, il faut et il suffit que la forme sesquilinéaire f associée à A satisfasse à

$$f(x, y) = \overline{f(y, x)}\ ,\ \forall\ x, y \in \mathbb{C}^n$$

Une telle forme s'appelle une forme sesquilinéaire hermitienne. On a donc une correspondance bijective entre matrices hermitiennes et formes sesquilinéaires hermi-

Si f est une forme sesquilinéaire hermitienne, alors $\forall\, x \in \mathbb{C}^n$ on a $f(x, x) \in \mathbb{R}$.

Ceci nous permet de définir une relation d'ordre dans l'espace vectoriel réel des formes sesquilinéaires hermitiennes. On dira que $f \leq g \Longleftrightarrow \forall\, x \in \mathbb{C}^n,\ f(x, x) \leq g(x, x)$.

Définitions.

1- Une forme sesquilinéaire hermitienne f est dite positive si

$$\forall\, x \in \mathbb{C}^n,\quad f(x, x) \geq 0$$

2- Une forme sesquilinéaire hermitienne f est définie positive si

$\forall\, x \in \mathbb{C}^n$ et $x \neq 0$, $f(x, x) > 0$. On écrit alors $f \gg 0$.

Conséquences.

1- A hermitienne est positive $\Longleftrightarrow \forall\, x \in \mathbb{C}^n \quad (Ax \mid x) \geq 0$

2- A hermitienne est $\gg 0 \Longleftrightarrow \forall\, x \in \mathbb{C}^n$ et $x \neq 0$, $(Ax \mid x) > 0$.

Définition.

Une matrice $A \in \mathrm{End}(\mathbb{R}^n)$ est orthogonale si elle conserve le produit scalaire euclidien : A orthogonale $\Longleftrightarrow \forall x, y \in \mathbb{R}^n,\ \langle Ax, Ay\rangle = \langle x, y\rangle$.

Conséquence.

$$\langle Ax, Ay\rangle = \langle x, {}^tAA\, y\rangle = \langle x, y\rangle \quad , \ \forall\, x, y \in \mathbb{R}^n.$$

Si on fixe y alors $\forall x \in \mathbb{R}^n$ $\langle x, {}^tAA\, y\rangle = \langle x, y\rangle$, donc ${}^tAA\, y = y$; ceci doit avoir lieu $\forall\, y$, autrement dit, la relation $\boxed{{}^tAA = 1}$ caractérise les A orthogonales. Ceci entraîne que A est inversible et $\boxed{A^{-1} = {}^tA}$. On en déduit que les transformations orthogonales appartiennent au groupe linéaire $GL(n, \mathbb{R})$.

Proposition.

Les transformations orthogonales de $\mathrm{End}(\mathbb{R}^n)$ forment un sous-groupe de $GL(n, \mathbb{R})$ que l'on note $O(n)$.

Conséquence.

Si $A \in O(n)$, alors ${}^tAA = 1$ donc $(\det A)^2 = 1 \Longrightarrow \det A = \pm 1$. Les matrices orthogonales de déterminant $+1$ forment un sous-groupe $SO(n)$ de $O(n)$, appelé groupe orthogonal spécial

$$SO(n) = O(n) \cap SL(n, \mathbb{R}).$$

$SO(n)$ est un sous-groupe d'indice 2 de $O(n)$.

Remarque.

Un élément de $O(n)$ transforme le repère canonique en un repère orthonormé. Réciproquement, si une transformation transforme un repère orthonormé en un repère orthonormé, c'est une transformation orthogonale.

On a deux nouvelles correspondances bijectives :

1- $O(n) \longleftrightarrow$ repères orthonormés

2- $SO(n) \longleftrightarrow$ repères orthonormés directs.

Proposition. Pour $A \in \mathrm{End}\ \mathbb{R}^n$:

$$A \text{ orthogonale} \iff \forall x \in \mathbb{R}^n,\ \langle Ax, Ax\rangle = \langle x, x\rangle .$$

Démonstration.

La condition est évidemment nécessaire. Supposons-la remplie, et montrons que $\langle Ax, Ay\rangle = \langle x, y\rangle$ quels que soient x et y. Soient $x, y \in \mathbb{R}^n$; on a $\langle x+y, x+y\rangle = \langle x, x\rangle + \langle y, y\rangle + 2\langle x, y\rangle$. Soit $A \in \mathrm{End}_{\mathbb{R}}\ \mathbb{R}^n$; alors

$$\langle A(x+y), A(x+y)\rangle = \langle Ax, Ax\rangle + \langle Ay, Ay\rangle + 2\langle Ax, Ay\rangle .$$

Si $\langle Ax, Ax\rangle = \langle x, x\rangle$ pour tout x, on a

$$\left.\begin{array}{l} \langle x+y, x+y\rangle = \langle A(x+y), A(x+y)\rangle \\ \langle x, x\rangle = \langle Ax, Ax\rangle \\ \langle y, y\rangle = \langle Ay, Ay\rangle \end{array}\right\} \Longrightarrow \langle x, y\rangle = \langle Ax, Ay\rangle$$

C.Q.F.D.

Proposition.

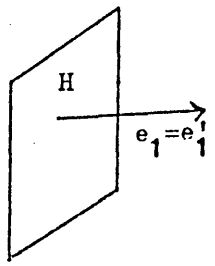
$SO(n)$ est connexe par arcs.

Démonstration.

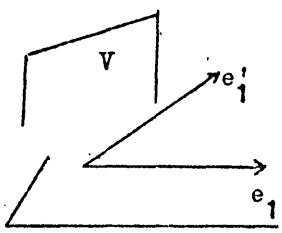
On fait une récurrence sur $n \geq 1$. Si $n = 1$, alors $SO(1) = \{Id\}$: c'est connexe !

Soit $n \geq 2$, et supposons la proposition vraie pour $n - 1$. On prend deux repères orthonormés directs $(e_1, \ldots, e_n)$ et $(e'_1, \ldots, e'_n)$. Il s'agit de les déformer l'un dans l'autre de manière continue en restant dans l'espace des repères orthonormés. Si $e_1 = e'_1$, $(e_2, \ldots, e_n)$ et $(e'_2, \ldots, e'_n)$ sont des repères orthonormés dans

dans l'hyperplan $H = \mathbb{R}^{n-1}$. Par l'hypothèse de récurrence, on peut transformer continûment l'un dans l'autre ces deux repères en restant dans l'espace des repères orthonormés de H. Mais à chaque instant $t \in [0, 1]$, $(e_1, e_2(t), \ldots, e_n(t))$ est orthonormé.



Si $e_1 \neq e_1'$, alors e_1 et e_1' déterminent un plan ; soit V le sous-espace vectoriel orthogonal à ce plan ; V est de dimension n-2. Une rotation autour de V est déterminée par une rotation dans le plan (e_1, e_1') ; il existe une telle rotation, dépendant continûment d'un paramètre, qui varie de l'identité à la rotation α qui transforme e_1' en e_1. Alors α transforme $(e_1', e_2', \ldots, e_n')$ en $(e_1, e_2'', \ldots, e_n'')$,



et on est ramené au cas précédent.

Définition.

Une matrice $A \in \mathrm{End}(\mathbb{C}^n)$ est unitaire si elle conserve le produit scalaire hermitien. A unitaire $\iff \forall x, y \in \mathbb{C}^n$, $(Ax \mid Ay) = (x \mid y)$.

Proposition. Pour $A \in \mathrm{End}\ \mathbb{C}^n$:

A unitaire $\iff \forall x \in \mathbb{C}^n \quad (Ax \mid Ax) = (x \mid x)$.

Démonstration. La condition de droite est évidemment nécessaire ; il reste à montrer qu'elle est suffisante. Or

$$(x+y \mid x+y) = (x|x) + (y|y) + 2\,\mathrm{Re}(x|y)$$

$$(ix+y \mid ix+y) = (x|x) + (y|y) + 2\,\mathrm{Re}(ix|y)$$

$$= (x|x) + (y|y) + 2\,\mathrm{Re}\ i(x|y)$$

$$= (x|x) + (y|y) - 2\ \mathrm{Im}(x|y)$$

Donc

$$(x+y \mid x+y) - i(ix+y \mid ix+y) = (1-i)\left[(x|x) + (y|y)\right] + 2\,(x|y)$$

Donc

$$(x|y) = \frac{1}{2}(x+y \mid x+y) - \frac{i}{2}(i\,x+y \mid ix+y) + \frac{i-1}{2}\left[(x|x) + (y|y)\right].$$

En remplaçant x par Ax et y par Ay, on obtient $(Ax|Ay) =$

$$= \frac{1}{2}(A(x+y)|A(x+y)) - \frac{i}{2}(A(ix+y)|A(ix+y)) + \frac{i-1}{2}\left[(Ax|Ax) + (Ay \mid Ay)\right]$$

Si on suppose que $\forall x \in \mathbb{C}^n$, $(Ax \mid Ax) = (x|x)$, on en déduit que

$$(Ax \mid Ay) = (x|y) \quad , \quad \forall x \text{ et } y \in \mathbb{C}^n.$$

Conséquence : pour $A \in \mathrm{End}\ \mathbb{C}^n$,

A unitaire $\iff \forall x, y \in \mathbb{C}^n \quad (A^*Ax \mid y) = (x|y) \iff A^*A = 1$.

Donc A est inversible, i.e. $A \in GL(n, \mathbb{C})$, et $\boxed{A^{-1} = A^*}$.

Proposition.

L'ensemble des transformations unitaires de $\mathrm{End}(\mathbb{C}^n)$ forme un sous-groupe de $GL(n, \mathbb{C})$, appelé groupe unitaire que l'on note $U(n)$.

Conséquence.

Si $A \in U(n)$, alors $A^* A = 1$, donc $(\det A^*)\ (\det A) = 1$, c'est-à-dire $\overline{(\det A)} \cdot (\det A) = 1 \iff |\det A| = 1$. Les matrices unitaires de déterminant + 1 forment un sous-groupe $SU(n)$ de $U(n)$, appelé groupe spécial unitaire

$$SU(n) = U(n) \cap SL(n, \mathbb{C}).$$

Proposition.- Les quatre groupes $O(n)$, $SO(n)$, $U(n)$, $SU(n)$ sont des groupes compacts.

Démonstration.

Ce sont tous des sous-groupes de $GL(n, \mathbb{C})$, lui-même ouvert dans $\mathrm{End}_{\mathbb{C}}\ \mathbb{C}^n$, espace vectoriel complexe de dimension n^2. Il suffit de montrer que ces sous-groupes sont fermés et bornés dans $\mathrm{End}_{\mathbb{C}}\ \mathbb{C}^n$. Il revient au même de montrer que l'espace des repères réels orthonormés (resp. des repères réels orthonormés directs, resp. des repères complexes orthonormés, resp. des repères complexes orthonormés de déterminant 1) sont des sous-ensembles bornés et fermés dans l'espace $\mathbb{C}^n \times \ldots \times \mathbb{C}^n$ des suites de n vecteurs de $\mathbb{C}^n$. Or ils sont bornés, car formés de vecteurs unitaires. Montrons qu'ils sont fermés : toute limite de repères orthonormés est un repère orthonormé, toute limite de repères réels est un repère réel, toute limite de repères de déterminant 1 est de déterminant 1.

Proposition. Soit $A \in U(n)$. Il existe une base orthonormée de $\mathbb{C}^n$ formée de vecteurs propres pour A, et les valeurs propres sont des nombres complexes λ tels que $|\lambda| = 1$.

Démonstration.

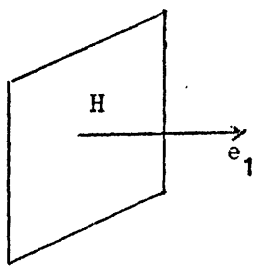
Soit $A \in U(n)$ et soient $\lambda_1, \ldots, \lambda_n$ les valeurs propres (distinctes ou non) de A. Pour chacune de ces valeurs propres λ_i, il existe au moins un vecteur

propre associé, c'est-à-dire un vecteur x_i non nul vérifiant $Ax_i = \lambda_i x_i$.

$A \in U(n) \implies A$ conserve la norme hermitienne $\implies |\lambda_i| = 1$. Toutes les valeurs propres d'une matrice unitaire appartiennent donc au cercle unité.

Montrons qu'il existe une base orthonormée formée de vecteurs propres $e_1, \ldots, e_n$.

En effet il existe un vecteur unitaire e_1 vérifiant $Ae_1 = \lambda_1 e_1$.



On considère alors l'hyperplan H orthogonal à e_1 ; il est stable par A et on recommence l'opération, ce qui donne une démonstration par récurrence sur n.

Corollaire. U(n) est connexe par arcs. Car soit $A \in U(n)$; on va joindre A à 1 par un chemin dans U(n) ; pour cela, prenons une base $(e_1, \ldots, e_n)$ telle que $Ae_i = \lambda_i e_i$; on joint chaque λ_i à 1 par un chemin $t \longmapsto \lambda_i(t)$ à valeurs complexes de module 1. On définit A(t) par $A(t)\, e_i = \lambda_i(t)\, e_i$.

C.Q.F.D.

Décomposition directe de $\mathbb{R}^n$ relative à un $A \in O(n)$.

Soit $A \in O(n)$; comme A conserve la norme euclidienne, toutes les valeurs propres réelles de A sont égales à +1 ou -1. Les autres valeurs propres sont deux à deux imaginaires conjuguées, donc en nombre pair ; et comme O(n) s'identifie naturellement à un sous-groupe de U(n) (à savoir le sous-groupe des A réelles telles que $A^{-1} = A^*$), les valeurs propres imaginaires λ de A satisfont à $|\lambda| = 1$. Pour chaque valeur propre réelle λ de A ($\lambda = \pm 1$), il existe un vecteur $x \in \mathbb{R}^n$, $x \neq 0$, tel que $Ax = \lambda x$; on en déduit l'existence de vecteurs réels, de longueur un, deux à deux orthogonaux, $e_1, \ldots, e_h$ tels que

$$Ae_i = \varepsilon_i e_i, \quad \varepsilon_i = \pm 1, \quad i = 1, 2, \ldots, h$$

avec h = nombre des valeurs propres réelles de A (chacune étant comptée avec son ordre de multiplicité). Soit H le sous-espace de $\mathbb{C}^n$ orthogonal à $e_1, \ldots, e_h$ (orthogonal au sens du produit scalaire hermitien) ; H est stable par A (considéré comme opérant sur $\mathbb{C}^n$), et la restriction U de A à H est unitaire.

H est de dimension complexe égale à n-h ; cette dimension est paire puisque les valeurs propres imaginaires sont deux à deux conjuguées.

Soit donc $n - h = 2t$; et soient $\lambda_1, \overline{\lambda}_1, \ldots, \lambda_t, \overline{\lambda}_t$ les valeurs propres imaginaires. Pour $k \in [1, t]$, on a deux vecteurs h_k et $\overline{h}_k \in \mathbb{C}^n$, non nuls, imaginaires conjugués, tels que

$$(1) \qquad A h_k = \lambda_k h_k, \quad A \overline{h}_k = \overline{\lambda_k}\ \overline{h_k} \ ;$$

posons $h_k = h'_k + i h''_k$, h'_k et h''_k réels, et posons $\lambda_k = \cos \theta_k + i \sin \theta_k$.

Les relations (1) donnent :

$$(2) \qquad \begin{cases} A h'_k = \cos \theta_k h'_k - \sin \theta h''_k \\ A h''_k = \sin \theta_k h'_k + \cos \theta h''_k \end{cases}$$

Comme $(h_k \mid \overline{h_k}) = 0$ (puisque h_k et $\overline{h_k}$ sont des vecteurs propres relatifs à des valeurs propres distincts), on en déduit, en développant :

$$|h'_k| = |h''_k| \ , \quad \langle h'_k, h''_k \rangle = 0 \ ;$$

quitte à multiplier h_k par un scalaire réel convenable, on peut donc supposer que h'_k et h''_k ont pour longueur un et sont orthogonaux. Ils forment une base orthonormée du 2-plan qu'ils engendrent : ce 2-plan est stable par A d'après (2), et A y opère par une rotation d'angle θ_k. En définitive, on a prouvé :

Proposition.

Si $A \in O(n)$, il existe une décomposition directe de $\mathbb{R}^n$ en sous-espaces vectoriels, deux à deux orthogonaux, dont chacun est de dimension 1 ou 2 ; ces sous-espaces sont stables pour A ; dans les sous-espaces de dimension 1, A opère par l'identité $x \longmapsto x$ ou par la symétrie $x \longmapsto -x$; dans chaque sous-espace de dimension 2, A opère par une rotation d'un angle θ qui n'est pas congru à $0 \pmod{\pi}$.

Remarque. Le déterminant de A étant égal au produit des déterminants des actions de A dans chacun des sous-espaces précédents, et le déterminant d'une rotation dans un 2-plan étant égal à +1, on voit que $\det A = +1$ si et seulement si le nombre des sous-espaces de dimension 1 dans lesquels A agit par $x \longmapsto -x$ est pair. C'est aussi l'ordre de multiplicité de la valeur propre -1. Telle est la condition pour que $A = SO(n)$; dans ce cas, la somme directe des sous-espaces de dimension 1

.../...

dans lesquels A agit par $x \longrightarrow -x$ est un sous-espace V, de dimension paire, somme directe de 2-plans dans chacun desquels A agit par une rotation de l'angle π.

Corollaire. On (retrouve le fait que) SO(n) est connexe par arcs ; en effet, si $A \in SO(n)$, l'espace $\mathbb{R}^n$ est somme directe d'un sous-espace W formé de vecteurs laissés fixes par A, et de 2-plans (deux à deux orthogonaux, et orthogonaux à W) dans chacun desquels A agit par rotation ; or une rotation, dans un plan, peut être déformée continûment en l'identité.

Remarque. Si $A \in SO(n)$ et si n est impair, il existe un $x \in \mathbb{R}^n$, $x \neq 0$, tel que $Ax = x$. Si $A \in O(n) - SO(n)$, et si n est pair, il existe un $x \in \mathbb{R}^n$, $x \neq 0$, tel que $Ax = x$ (car si toutes les valeurs propres réelles étaient égales à -1, leur nombre serait pair, et det A serait égal à $+1$).

Groupes linéaires quaternioniens.

Rappelons que le corps $\mathbb{H}$ des quaternions se compose des $\alpha + j\beta$, où $\alpha \in \mathbb{C}$, $\beta \in \mathbb{C}$, avec les règles de calcul :

$$j^2 = -1 , \qquad j\beta = \bar{\beta}\, j .$$

Si $a = \alpha + j\beta \in \mathbb{H}$, le quaternion conjugué est

$$\bar{a} = \bar{\alpha} - j\beta, \text{ et l'on a } \quad a\bar{a} = \bar{a}a = \alpha\bar{\alpha} + \beta\bar{\beta} \in \mathbb{R},$$

qui est ≥ 0, et n'est nul que si $a = 0$ (i.e. $\alpha = 0$ et $\beta = 0$).

$\mathbb{H}$ a deux structures d'espace vectoriel sur $\mathbb{C}$:

- celle qui est définie par la multiplication à droite par un $\lambda \in \mathbb{C}$:

$$(\alpha + j\beta) \longmapsto (\alpha + j\beta)\lambda = \alpha\lambda + j\beta\lambda ;$$

- celle qui est définie par la multiplication à gauche par un $\lambda \in \mathbb{C}$:

$$(\alpha + j\beta) \longmapsto \lambda\,(\alpha + j\beta) = \alpha\lambda + j\beta\bar{\lambda}.$$

La correspondance bijective $\mathbb{H} \approx \mathbb{C} \oplus \mathbb{C}$ définie par $\alpha + j\beta \longmapsto (\alpha, \beta)$ est un isomorphisme de $\mathbb{C}$-espaces vectoriels pour la structure de $\mathbb{C}$-espace vectoriel à droite de $\mathbb{H}$.

Considérons $\mathbb{H}^n = \mathbb{H} \times \ldots \times \mathbb{H}$ (n fois). $\mathbb{H}^n$ a une structure d'espace vectoriel à droite sur $\mathbb{H}$, pour laquelle $(a_1, \ldots, a_n) \cdot b = (a_1 b, \ldots, a_n b)$.

[Il y a aussi une structure d'espace vectoriel à gauche sur $\mathbb{H}$, mais nous ne la considérons pas].

$\mathrm{End}_{\mathbb{H}}(\mathbb{H}^n)$ désignera l'ensemble des applications linéaires $\mathbb{H}^n \longrightarrow \mathbb{H}^n$ pour la structure d'espace vectoriel à droite. C'est un groupe abélien. Soit $A \in \mathrm{End}_{\mathbb{H}}(\mathbb{H}^n)$, et soit $(x_1, \ldots, x_n) \in \mathbb{H}^n$; on vérifie facilement que

$$A(x_1, \ldots, x_n) = (x'_1, \ldots, x'_n) \text{ , où } x'_i = \sum_j a_{ij} x_j \qquad (a_{ij} \in \mathbb{H}).$$

[C'est bien linéaire à droite, car

$$(x'_i \lambda) = \sum_j a_{ij} (x_j \lambda)]$$

Remarque :

Ici on ne peut pas parler de déterminant, car le corps $\mathbb{H}$ n'est pas commutatif.

$GL(n, \mathbb{H})$ désigne l'ensemble des $A \in \mathrm{End}_{\mathbb{H}}(\mathbb{H}^n)$ qui admettent un inverse ; c'est l'ensemble des automorphismes de l'espace vectoriel à droite $\mathbb{H}^n$. C'est un groupe pour la composition des automorphismes.

Produit scalaire quaternionien.

Soient $x \in \mathbb{H}^n$, $y \in \mathbb{H}^n$. On définit le produit scalaire quaternionien par

$$(x, y)_{\mathbb{H}} = \sum_i \overline{y_i} x_i$$

où $\overline{y_i}$ désigne le quaternion conjugué de $y_i \in \mathbb{H}$. Le $\overline{y_i}$ est écrit à gauche de x_i pour que ce produit scalaire soit linéaire à droite par rapport à la variable x.

On a
$$\left.\begin{aligned} (x \lambda, y)_{\mathbb{H}} &= (x, y)_{\mathbb{H}} \lambda \\ (y, x)_{\mathbb{H}} &= \overline{(x, y)_{\mathbb{H}}} \\ \text{d'où} \quad (x, y \lambda)_{\mathbb{H}} &= \overline{\lambda} (x, y)_{\mathbb{H}} \end{aligned}\right\} \text{ C'est la sesquilinéarité quaternionienne.}$$

Adjointe quaternionienne pour une matrice $A \in \mathrm{End}_{\mathbb{H}}(\mathbb{H}^n)$. C'est une matrice A^* définie par

$$(Ax, y)_{\mathbb{H}} = (x, A^* y)_{\mathbb{H}} \quad , \quad \forall x, y \in \mathbb{H}^n$$

Si $A = (a_{ij})$ et $A^* = (b_{ij})$, alors $b_{ij} = \overline{a_{ji}}$.

Matrice symplectique :

C'est une matrice $A \in \mathrm{End}_{\mathbb{H}}(\mathbb{H}^n)$ qui conserve le produit scalaire quaternionien :

$$(Ax, Ay)_{\mathbb{H}} = (x, y)_{\mathbb{H}}, \qquad \forall x, y \in \mathbb{H}^n$$

$\Longleftrightarrow$ $A^* A = 1$.

Donc A est inversible [i.e. $A \in G(n, \mathbb{H})$], et $A^{-1} = A^*$. Les matrices symplectiques forment un sous-groupe de $GL(n, \mathbb{H})$, qu'on note $Sp(n)$.

Exemple : $Sp(1)$.

Une transformation linéaire (à droite) de $\mathbb{H}$ est une transformation $x \longmapsto \lambda$. pour qu'elle appartienne à $Sp(1)$, il faut et il suffit qu'elle conserve le produit scalaire quaternonien, donc que $\lambda \bar{\lambda} = 1$, ou $\| \lambda \|_{\mathbb{H}} = 1$, où $\| \lambda \|_{\mathbb{H}}$ désigne la norme quaternionienne.

Donc $Sp(1)$ est isomorphe au groupe multiplicatif des quaternions de norme 1 ; du point de vue topologique, c'est la sphère S_3 dans $\mathbb{R}^4$.

Identification de $GL(n, \mathbb{H})$ à un sous-groupe de $GL(2n, \mathbb{C})$. Elle va résulter de l'identification $\mathbb{H}^n \approx \mathbb{C}^{2n}$ comme $\mathbb{C}$-espaces vectoriels à droite. Précisons cet isomorphisme : soit $(x_1, \ldots, x_n) \in \mathbb{H}^n$; on a $x_1 = x_1' + j\, x_1'', \ldots, x_n = x_n' + j x_n''$, où $x_1', x_1'', \ldots, x_n', x_n'' \in \mathbb{C}$. Au vecteur $(x_1, \ldots, x_n) \in \mathbb{H}^n$ on associe le vecteur $(x_1', \ldots, x_n', x_1'', \ldots, x_n'') \in \mathbb{C}^{2n}$; tel est l'isomorphisme de $\mathbb{H}^n$ sur $\mathbb{C}^{2n}$. Cet isomorphisme étant $\mathbb{C}$-linéaire, il identifie $GL(n, \mathbb{H})$ à un sous-groupe de $GL(2n, \mathbb{C})$. A quelle condition une transformation $\mathbb{C}$-linéaire est-elle $\mathbb{H}$-linéaire ? Soit $A \in GL(2n, \mathbb{C})$; pour que $A \in GL(n, \mathbb{H})$, il faut et il suffit que $\forall x \in \mathbb{H}^n$ $A(xj) = A(x)\, j$. C'est évident.

Problème : l'identification $GL(n, \mathbb{H}) \subset GL(2n, \mathbb{C})$ identifie le sous-groupe $Sp(n)$ à un sous-groupe de $GL(2n, \mathbb{C})$; on se propose de l'expliciter.

Proposition. Soit $A \in GL(2n, \mathbb{C})$. Si A laisse invariant le produit scalaire quaternionien $(x, y)_{\mathbb{H}}$, alors A est $\mathbb{H}$-linéaire.

Corollaire. $A \in Sp(n) \Longleftrightarrow \begin{cases} A \in GL(2n, \mathbb{C}) \text{ et } A \text{ laisse invariant le produit} \\ \text{scalaire quaternionien.} \end{cases}$

Démonstration de la proposition. On veut prouver que

$$A(x\, j) = A(x) .\, j , \qquad \forall\, x \in \mathbb{H}^n .$$

Or on a, quels que soient $x, y \in \mathbb{H}^n$:

$$(A(xj),\ A(y))_{\mathbb{H}} = (x\ j,\ y)_{\mathbb{H}} = (x,\ y)_{\mathbb{H}} \cdot j,$$

$$(A(x) \cdot j,\ A(y))_{\mathbb{H}} = (A(x),\ A(y))_{\mathbb{H}} \cdot j = (x,\ y)_{\mathbb{H}} \cdot j,$$

d'où

$$(A(x \cdot j),\ A(y))_{\mathbb{H}} = (A(x) \cdot j,\ A(y))_{\mathbb{H}} \quad , \quad \forall\, x,\ y \in \mathbb{H}^n.$$

Fixons x ; lorsque y parcourt $\mathbb{H}^n$, $A(y)$ parcourt $\mathbb{H}^n$ puisque A est inversible par hypothèse ; donc $A(xj)$ et $A(x) \cdot j$ ont même produit scalaire quaternionien avec n'importe quel vecteur $z \in \mathbb{H}^n$. Il s'ensuit que $A(x\,j) = A(x) \cdot j$ quel que soit x. C.Q.F.D.

Lemme. Toute $A \in M_{2n}(\mathbb{C})$ qui laisse invariant le produit scalaire quaternionien est, en fait, dans $GL(2n, \mathbb{C})$, et par suite dans $Sp(n)$. Pour cela explicitons $(x, y)_{\mathbb{H}}$ à l'aide des x'_k, x''_k, y'_k, $y''_k \in \mathbb{C}$ définis par :

$$x_k = x'_k + j\, x''_k \quad , \quad y_k = y'_k + j\, y''_k \ .$$

On a

$$\begin{aligned}(x, y)_{\mathbb{H}} &= \sum_{k=1}^{n} (\overline{y'_k} - j\, y''_k)\ (x'_k + j\, x''_k) \\ &= \sum_{k=1}^{n} x'_k\, \overline{y'_k} + \sum_{k=1}^{n} x''_k\, \overline{y''_k} \\ &\quad - j \left(\sum_{k=1}^{n} x'_k\, y''_k - \sum_{k=1}^{n} x''_k\, y'_k\right) .\end{aligned}$$

Or le produit scalaire hermitien et le produit scalaire euclidien, dans $\mathbb{C}^{2n}$, sont donnés par les formules

$$\begin{cases} (x \mid y) = \sum_{k=1}^{n} x'_k\, \overline{y'_k} + \sum_{k=1}^{n} x''_k\, \overline{y''_k}\ , \\ \langle x, y \rangle = \sum_{k=1}^{n} x'_k\, y'_k + \sum_{k=1}^{n} x''_k\, y''_k\ . \end{cases}$$

Introduisons l'automorphisme $\mathbb{C}$-linéaire J de $\mathbb{C}^{2n}$ défini par :

$$J(x', x'') = (-x'', x') \quad ;$$

on voit que

$$\boxed{(x, y)_{\mathbb{H}} = (x \mid y) - j\, \langle Jx, y \rangle} \ .$$

Donc $A \in M_{2n}(\mathbb{C})$ laisse invariant $(x, y)_{\mathbb{H}}$ si et seulement si A satisfait aux deux conditions suivantes :

(a) A laisse invariant le produit scalaire hermitien $(x \mid y)$;

(b) A laisse invariant $\langle Jx, y\rangle$; autrement dit

(*) $$\boxed{\langle JAx, Ay\rangle = \langle Jx, y\rangle \ , \ \forall\, x, y \in \mathbb{C}^{2n}}$$

La condition (a) exprime que A est unitaire ; on sait que ceci entraîne que A est inversible, ce qui prouve le lemme. On voit de plus que

$$Sp(n) \subset U(2n).$$

Définition. On note $Sp(n, \mathbb{C})$ l'ensemble des $A \in M_{2n}(\mathbb{C})$ qui satisfont à la condition (b), ou, ce qui revient au même, à (*). Observons que :

$$(x, y) \longmapsto \langle Jx, y\rangle$$

est une forme $\mathbb{C}$-bilinéaire alternée des vecteurs x et $y \in \mathbb{C}^{2n}$: en effet

$$\langle Jx, y\rangle = \sum_{k=1}^{n} (x'_k y''_k - x''_k y'_k)$$

est $\mathbb{C}$-linéaire en x, $\mathbb{C}$-linéaire en y, et s'annule pour $x = y$. La condition (*) équivaut à

$$\langle {}^tA\, J\, Ax, y\rangle = \langle Jx, y\rangle \quad , \forall\, x, y \in \mathbb{C}^{2n},$$

ce qui équivaut à

$${}^tA\, J\, A\, x = J\, x, \quad \forall\, x \in \mathbb{C}^{2n} \ ,$$

c'est-à-dire à

(**) $$\boxed{{}^tA\, J\, A = J} \iff A \in Sp(n, \mathbb{C}).$$

Observons que le déterminant de J est un nombre complexe $\neq 0$, puisque son carré est $\det(J^2)$, et que $J^2 = -1_{2n}$, d'où $\det(J^2) = +1$. En prenant les déterminants des deux membres de (**), on trouve donc

$$(\det A)^2 = 1, \quad \text{c'est-à-dire} \quad \det A = \pm 1.$$

[On peut montrer que, en fait, $\det A = 1$]. Donc A est inversible. Autrement dit, $Sp(n, \mathbb{C})$ est contenu dans $GL(2n, \mathbb{C})$; c'est évidemment un sous-groupe de $GL(2n, \mathbb{C})$.

D'après ce qu'on a vu, pour que $A \in M_{2n}(\mathbb{C})$ appartienne à $Sp\ n$, il faut et il suffit que A satisfasse aux conditions (a) et (b) ; on a donc, en définitive :

$$\boxed{Sp\ n = U(2n) \cap Sp(n, \mathbb{C})}$$

Sous forme matricielle, J s'écrit

$$J = \begin{pmatrix} 0_n & -1_n \\ 1_n & 0_n \end{pmatrix}$$

où 0_n désigne la matrice nulle à n lignes et n colonnes, et 1_n la matrice unité à n lignes et n colonnes.

Exercice : écrivons $A = M_{2n}(\mathbb{C})$ sous la forme

$$A = \begin{pmatrix} E & F \\ G & H \end{pmatrix},$$

où $E, F, G, H \in M_n(\mathbb{C})$. Vérifier que la relation ${}^tA\, J\, A = J$, qui exprime que $A \in Sp(n, \mathbb{C})$, équivaut à l'ensemble des conditions suivantes :

$$\begin{cases} {}^tG\, E \quad \text{et} \quad {}^tH\, F \quad \text{sont symétriques} \\ {}^tG\, F - {}^tE\, H = 1_n. \end{cases}$$

Quelques isomorphismes ou homomorphismes particuliers.

(1) $\boxed{SO(2) \approx U(1)}$: cet isomorphisme évident provient du fait qu'une rotation, dans le plan, est définie par un nombre complexe de module 1.

(2) $\boxed{Sp(1, \mathbb{C}) \approx SL(2, \mathbb{C})}$.

En effet $Sp(1, \mathbb{C})$ est le sous-groupe de $GL(2, \mathbb{C})$ formé des transformations qui laissent invariante la forme bilinéaire alternée $x'y'' - y'x''$ [forme bilinéaire du vecteur $x = (x', x'')$ et du vecteur $y = (y', y'')$] ; cette forme n'est autre que le déterminant des vecteurs x et y par rapport à la base canonique. Les transformations de $Sp(1, \mathbb{C})$ sont donc les transformations de $GL(2, \mathbb{C})$ dont le déterminant est égal à 1.

(3) $\boxed{Sp(1) \approx SU(2)}$

En effet, on a vu que

$$Sp(1) = U(2) \cap Sp(1, \mathbb{C}).$$

(4) On définit un homomorphisme de groupes $\varphi : Sp(1) \longrightarrow SO(3)$ de la manière suivante : identifiant $Sp(1)$ au groupe multiplicatif des quaternions de norme 1, associons à $x \in Sp(1)$ la transformation $\mathbb{H} \longrightarrow \mathbb{H}$ définie par $z \longmapsto x\, z\, x^{-1}$ (produit de 3 quaternions). $\mathbb{H}$ étant identifié à $\mathbb{R}^4$, ceci est une transformation $\mathbb{R}$-linéaire qui conserve la distance, car

$$\| x\, z\, x^{-1} \|_{\mathbb{H}} = \| x \|_{\mathbb{H}} \cdot \| z \|_{\mathbb{H}} \cdot \| x^{-1} \|_{\mathbb{H}} = \| z \|_{\mathbb{H}} .$$

C'est donc un élément de $O(4)$. De plus si z est un "quaternion réel" (c'est-à-dire si ses coordonnées dans $\mathbb{R}^4$ sont nulles sauf la première), alors $x\, z\, x^{-1} = z$; donc l'élément de $O(4)$ en question laisse fixe les quaternions réels ; il opère donc dans l'hyperplan orthogonal, qui s'identifie à $\mathbb{R}^3$. Tel est, par définition, l'élément $\varphi(x) \in O(3)$ défini par $x \in Sp\ 1$. En fait, $\varphi(x)$ est dans $SO(3)$, car l'application $\varphi : Sp(1) \longrightarrow O(3)$ est continue, et $Sp(1)$ est connexe (homéomorphe à S^3) ; c'est du reste un homomorphisme de groupes (vérification immédiate). On peut prouver que :

1º φ est surjectif ;

2º le noyau de φ se compose des 2 quaternions $+1$ et -1. D'où la suite exacte de groupes et d'homomorphismes

$$\{1\} \longrightarrow \{\pm 1\} \longrightarrow Sp(1) \longrightarrow SO(3) \longrightarrow \{1\} .$$

On traduit ceci en disant que $Sp(1)$ est un revêtement à deux feuillets de $SO(3)$.

On voit que $SO(3)$, comme espace topologique, s'identifie au quotient de la sphère S^3 par la relation d'équivalence qui identifie les points diamétralement opposés de S^3. Autrement dit, $SO(3)$ est homéomorphe à l'espace projectif réel $P_3(\mathbb{R})$.

(5) On définit un homomorphisme de groupes $\Psi : Sp\ 1 \times Sp\ 1 \longrightarrow SO(4)$ de la manière suivante : à un couple (x, y) de quaternions de norme 1 on associe la transformation $\mathbb{H} \longrightarrow \mathbb{H}$ définie par $z \longmapsto x\, z\, y^{-1}$.

Cette transformation conserve la norme et est $\mathbb{R}$-linéaire ; c'est donc un élément de $O(4)$. On montre comme plus haut que c'est un élément de $SO(4)$. De plus Ψ est un homomorphisme de groupes, est surjectif, et son noyau se compose des deux éléments $\{+1, +1\}$ et $\{-1, -1\}$. Ainsi $Sp(1) \times Sp(1)$ (qui est homéomorphe à $S^3 \times S^3$) est un revêtement à deux feuillets de $SO(4)$. On peut montrer que $SO(4)$ est homéomorphe au produit $S^3 \times P_3(\mathbb{R})$.

Application exponentielle.

Soit $M \in \mathrm{End}_{\mathbb{R}}(\mathbb{R}^n)$. Définissons la norme d'une transformation linéaire M :

$$|M| = \sup_{x \in \mathbb{R}^{n*}} \frac{|M(x)|}{|x|} = \sup_{|x| \leq 1} |M(x)| ,$$

où $|x|$ désigne la norme dans $\mathbb{R}^n$: $|x| = \sqrt{x_1^2 + \ldots + x_n^2}$. La norme, sur l'algèbre $\mathrm{End}\,\mathbb{R}^n$, a les propriétés suivantes :

$$\begin{cases} |\lambda M| = |\lambda| . |M| \\ |M+N| \leq |M| + |N| \\ |M.N| \leq |M| . |N|, \qquad |\mathrm{Id}| = 1. \end{cases}$$

On exprime ces propriétés en disant que $\mathrm{End}\,\mathbb{R}^n$ est une algèbre normée. On peut faire de même avec l'algèbre $\mathrm{End}_{\mathbb{C}}\,\mathbb{C}^n$.

Remarque : On n'a pas nécessairement $|M.N| = |M| . |N|$; par exemple, soit, dans $\mathbb{R}^2$, $\begin{cases} M = \text{projection sur l'axe des } x ; \\ N = \text{projection sur l'axe des } y ; \end{cases}$

on a $MN = 0$, tandis que $|M| = 1$, $|N| = 1$.

Muni de sa norme, $\mathrm{End}_{\mathbb{R}}(\mathbb{R}^n)$ est un espace vectoriel normé complet (car $\mathbb{R}$ est complet), [de dimension finie n^2] ; donc si on a une série dans $\mathrm{End}_{\mathbb{R}}.\mathbb{R}^n$, et si la série des normes converge, alors la série converge ; de plus $\left| \sum_n M_n \right| \leq \sum_n |M_n|$. On dit alors que la série est normalement convergente.

Définition : Considérons la série

$$1 + M + \frac{1}{2} M^2 + \ldots + \frac{1}{n!} M^n + \ldots = \sum_{n \geq 0} \frac{M^n}{n!}$$

Elle est normalement convergente quel que soit M, puisque $\left|\frac{M^n}{n!}\right| \leq \frac{1}{n!} . |M|^n$; le second membre est le terme général d'une série convergente à termes positifs : c'est la série exponentielle.

Donc la série converge. On note $\exp M$ sa somme :

$$\exp M = 1 + M + \ldots + \frac{1}{n!} M^n + \ldots = \sum_{n \geq 0} \frac{M^n}{n!}$$

On a $\begin{cases} \exp M \in \mathrm{End}_{\mathbb{R}}\,\mathbb{R}^n & \text{si } M \in \mathrm{End}_{\mathbb{R}}\,\mathbb{R}^n , \\ \exp M \in \mathrm{End}_{\mathbb{C}}\,\mathbb{C}^n & \text{si } M \in \mathrm{End}_{\mathbb{C}}\,\mathbb{C}^n. \end{cases}$

Proposition. Si M et M' commutent, alors $\exp(M+M') = (\exp M).(\exp M')$.

Démonstration : on utilise le théorème de multiplication des séries normalement convergentes :

$$(\exp M)(\exp M') = \sum_{n\geq 0} \left(\sum_{0\leq p\leq n} \frac{M^p M'^{n-p}}{p!(n-p)!} \right)$$

Or, en développant $(M+M')^n$ et tenant compte de $MM' = M'M$, on trouve

$$\frac{(M+M')^n}{n!} = \sum_{0\leq p\leq n} \frac{M^p M'^{n-p}}{p!(n-p)!} \cdot$$ C.Q.F.D.

Conséquence. $\exp(M).(\exp(-M)) = \exp(0) = 1$, donc $\exp M$ est inversible et a pour inverse $\exp(-M)$.

Ainsi : $\exp M \in GL(n, \mathbb{R})$, resp. $GL(n, \mathbb{C})$.

Soit $t \in \mathbb{R}$; considérons l'application $t \longrightarrow \exp(t M)$; on a $\exp(t_1 M).\exp(t_2 M) = \exp((t_1+t_2) M)$; donc l'application $t \longrightarrow \exp(t M)$ de $\mathbb{R}$ dans $GL(n, \mathbb{R})$ est un homomorphisme du groupe additif $\mathbb{R}$ dans le groupe $GL(n, \mathbb{R})$.

Formulaire.

$$(1) \qquad \begin{cases} \exp(-M) = (\exp M)^{-1} \\ \exp({}^tM) = \sum_{n\geq 0} \frac{({}^tM)^n}{n!} = {}^t(\exp M), \\ \exp(\overline{M}) = \overline{\exp M} \\ \exp(M^*) = (\exp M)^* \end{cases}$$

$$(2) \qquad \det(\exp M) = \exp(\mathrm{Tr}\, M),$$

où Tr M désigne la trace de M, somme des éléments de la diagonale principale. On va démontrer (2). Pour cela, demandons-nous ce qu'on peut dire des valeurs propres de l'exponentielle $\exp M$. On se place dans le domaine complexe ; rappelons que toute matrice peut être rendue triangulaire, par un choix convenable de la base de $\mathbb{C}^n$. En effet, $M \in \mathrm{End}_{\mathbb{C}}\, \mathbb{C}^n$; posons $V = \mathbb{C}^n$, et faisons une démonstration par récurrence sur $\dim_{\mathbb{C}} V$. Soit λ_1 une valeur propre (complexe), racine de $\det(M - \lambda_1 1) = 0$. Alors il y a au moins un vecteur propre $e_1 \neq 0$ tel que $Me_1 = \lambda_1 e_1$ engendre un sous-espace vectoriel V_1 de V, de dimension 1. On considère alors V/V_1 ; M transformant V_1 dans lui-même, M induit un endomorphisme M_1 de V/V_1 ; on applique alors l'hypothèse de récurrence à cet espace de dimension $n-1$.

$$\left.\begin{aligned} M(e_1) &= \lambda_1 e_1, \\ M(e_2) &= \lambda_2 e_2 + \mu_1 e_1, \text{ etc...} \end{aligned}\right\} \Longrightarrow M = \begin{pmatrix} \lambda_1 & \times & \times & \times \\ & \lambda_2 & & \times \\ & 0 & \ddots & \times \\ & & & \lambda_n \end{pmatrix}$$

Calculons exp M :

$$M^2 = \begin{pmatrix} \lambda_1^2 & & & \\ & \ddots & & \\ 0 & & & \\ & & & \lambda_n^2 \end{pmatrix} \quad \cdots\cdots \quad M^k = \begin{pmatrix} \lambda_1^k & & & \\ & \ddots & & \\ 0 & & & \\ & & & \lambda_n^k \end{pmatrix}$$

On a alors $e^M = \sum_{k \geq 0} \frac{M^k}{k!} = \begin{pmatrix} e^{\lambda_1} & & & \\ & \ddots & & \\ 0 & & & \\ & & & e^{\lambda_n} \end{pmatrix}$

Les valeurs propres de exp M sont les exponentielles e^{λ_i} des valeurs propres λ_i de M.

On a donc $\det(\exp M) = e^{\lambda_1} \cdot e^{\lambda_2} \cdots e^{\lambda_n} = e^{\lambda_1 + \lambda_2 + \cdots + \lambda_n} = e^{\mathrm{Tr}M}$. C.Q.F.D.

(Rappelons que la somme des éléments de la diagonale de la matrice représentant M est indépendante du choix de la base).

Conséquence : Si M est réelle, alors $\exp M \in SL(n, \mathbb{R}) \iff \mathrm{Tr}\, M = 0$.

Proposition : $M \longmapsto \exp M$ est une fonction analytique de M, à valeurs dans l'espace vectoriel $\mathrm{End}_{\mathbb{R}} \mathbb{R}^n$, resp. $\mathrm{End}_{\mathbb{C}} \mathbb{C}^n$.

Démonstration. Rappelons la définition de l'analyticité (d'abord) dans le cas complexe.

Soit U un ouvert de V, où V est un $\mathbb{C}$-espace vectoriel de dimension finie. Soit f une fonction définie sur U, à valeurs dans un espace vectoriel complexe de dimension finie W ; $f : U \longmapsto W$. f est analytique (ou holomorphe) signifie qu'elle est analytique au voisinage de chaque point $a_0 \in U$; il reste à dire ce qu'on entend par là.

Or si $a_0 \in U$, on peut, au moyen d'une translation, se ramener au cas où $a_0 = 0$.

Par définition, f est analytique au voisinage de 0 si et seulement si f est développable en série de polynômes homogènes au voisinage de 0, c'est-à-dire

$$f(x) = \sum_{n \geq 0} f_n(x) \quad \text{pour} \quad |x| \leq r \quad (r > 0 \text{ convenable}),$$

f_n étant un polynôme homogène de degré n, et la série étant normalement convergente

pour $|x| \leq r$.

Réciproque: on démontre que la somme d'une série de polynômes homogènes qui converge normalement pour $|x| \leq r$ est analytique dans l'ouvert $\|x\| < r$.

On montre en outre que la composée de deux applications analytiques (quand elle est définie) est analytique.

Exemple : Si $M \in \mathrm{End}_{\mathbb{C}} \mathbb{C}^n$, $\exp M = \sum_{n\geq 0} \frac{M^n}{n!}$ est bien analytique dans toute boule $|M| \leq r$, donc analytique dans tout l'espace $\mathrm{End}_{\mathbb{C}} \mathbb{C}^n$; en effet les coordonnées de la matrice M^n sont des polynômes homogènes de degré n par rapport aux coordonnées de M.

Analyticité dans le cas réel.

On a la même définition d'une fonction analytique. On constate que si f est analytique-complexe dans un ouvert U d'un espace vectoriel complexe V, et si V' est un sous-espace vectoriel réel de V, la restriction de f à $U \cap V'$ est analytique-réelle. Dans le cas qui nous intéresse, $V = \mathrm{End}_{\mathbb{C}} \mathbb{C}^n$, $U = V$, et $V' = \mathrm{End}_{\mathbb{R}} \mathbb{R}^n$; donc $\exp M$ est une fonction analytique-réelle de $M \in \mathrm{End}\, \mathbb{R}^n$.

Autre exemple de fonction analytique. Soit $u \in \mathrm{End}_{\mathbb{C}} \mathbb{C}^n$ tel que $|u| < 1$; la série

$$u - \frac{u^2}{2} + \frac{u^3}{3} + \ldots + (-1)^{k+1} \frac{u^k}{k} + \ldots$$

converge normalement pour $|u| \leq r$, si $r < 1$; donc sa somme est analytique dans la boule $|u| < 1$. Notons $\log(1+u)$ la somme de cette série. On sait donc définir $\log M$, lorsque $M \in \mathrm{End}_{\mathbb{C}} \mathbb{C}^n$ et que $|M-1| < 1$.

$\log M$ est une matrice : nous allons montrer que l'application analytique $M \longmapsto \log M$ est l'inverse de l'application $M \longmapsto \exp M$. D'une façon précise :

(1) $$\boxed{\exp(\log(1+u)) = 1+u \quad \text{pour} \quad |u| < 1}$$

Pour le vérifier, on doit remplacer M par le développement en série de $1+u$ dans $\sum_{n\geq 0} \frac{1}{n!} M^n$, et développer ; c'est un calcul formel, qui marche lorsque u est une variable réelle (résultat classique) ; donc il marche ici. Ce qui prouve (1).

(2) $\log(\exp M) = M$ lorsque $|M|$ est assez petit pour que $|\exp M - 1| < 1$. Le principe de la démonstration de (2) est le même que pour (1) : substitution de séries entières.

On a donc deux applications analytiques :

$f_1 : M \longmapsto \log M$, définie sur un voisinage de 1 dans $\mathrm{End}_{\mathbb{C}}\, \mathbb{C}^n$,

$f_2 : M \longmapsto \exp M$, définie sur $\mathrm{End}_{\mathbb{C}}\, \mathbb{C}^n$ tout entier,

et ces deux applications analytiques sont réciproques l'une de l'autre ; donc la fonction exponentielle induit un isomorphisme analytique d'un voisinage de 0 dans $M_n(\mathbb{C})$ sur un voisinage de 1 dans $GL(n, \mathbb{C})$.

Conséquence : l'application $M \longmapsto \exp M$ est injective dans un voisinage de 0 : si M_1 et M_2 sont assez voisines de 0 et si $\exp M_1 = \exp M_2$, alors $M_1 = M_2$.

Problème :

Où faut-il prendre M pour que son image exp M appartienne à l'un des sous-groupes de $GL(n, \mathbb{C})$ considérés plus haut ? Dans toute la suite, la matrice M sera supposée dans un voisinage V de 0 tel que $M \longmapsto \exp M$ soit injective dans V.

(1) $\boxed{\exp M \in GL(n, \mathbb{R})}$

On veut que $\overline{\exp M} = \exp M$, donc $\exp \overline{M} = \exp M$. Si M et $\overline{M}$ sont dans V, on en déduit que $M = \overline{M}$; donc M est réelle.

Réciproquement si M est réelle, il est évident que $\exp M \in GL(n, \mathbb{R})$.

(2) $\boxed{\exp M \in SL(n, \mathbb{C})}$

On veut donc que $\det M = \exp(\mathrm{Tr}\, M) = 1$. Ceci entraîne que Tr M est un multiple entier de $2\pi i$. Mais si M est assez voisine de 0, on a forcément Tr M = 0. Cette condition est évidemment suffisante pour det M = 1 (que M soit ou non voisine de 0). Ainsi, lorsque M est assez voisine de 0, on a : $\exp M \in SL(n, \mathbb{C}) \iff M \in$ sous-espace vectoriel complexe des matrices de trace nulle.

(3) $\boxed{\exp M \in SL(n, \mathbb{R})} \iff$ M est réelle et Tr M = 0,

du moins si M est assez voisine de 0.

(4) $\boxed{\exp M \in O(n)}$

$\exp M \in O(n) \iff {}^t(\exp M) = (\exp M)^{-1}$, c'est-à-dire $\exp {}^t M = \exp(-M)$. Si M est assez voisine de 0, ${}^tM$ et $-M$ sont voisines de 0 ; on doit donc avoir ${}^tM = -M$, ou encore ${}^tM + M = 0$. Cette condition est évidemment suffisante (que M soit ou non voisine de 0). Donc, pour M assez voisine de 0, on a

$\exp M \in O(n) \iff$ M appartient au sous-espace vectoriel réel des matrices "symétriques-gauches".

Calculons la dimension de cet espace vectoriel : les termes de la diagonale principale d'une telle M sont nuls, ceux qui sont au-dessus de la diagonale sont des nombres réels arbitraires(qui déterminent alors ceux au-dessous de la diagonale). Donc ces M sont des combinaisons linéaires (à coefficients réels arbitraires) de certaines d'entre elles, linéairement indépendantes, en nombre égal à celui des termes situés au-dessus de la diagonale, c'est-à-dire $\frac{n(n-1)}{2}$.

(5) $\boxed{\exp M \in U(n)}$

$\exp M \in U(n) \iff (\exp M)^{*} = (\exp M)^{-1}$, c'est-à-dire

$$\exp M^{*} = \exp(-M) \quad ;$$

ceci, pour M assez voisine de 0, équivaut à

(*) $$M^{*} = -M.$$

Réciproquement, cette relation entraîne $\exp M \in U(n)$, que M soit ou non voisine de 0. Les M satisfaisant à (*) forment un sous-espace vectoriel réel dont on se propose de calculer la dimension. Posons $M = i N$; la condition pour N est

(**) $$N^{*} = N,$$

autrement dit N est hermitienne ; si $N = (a_{ij})$, la condition s'écrit

$$a_{ii} \text{ réel}, \quad a_{ij} = \overline{a_{ji}} \quad \text{pour } i > j.$$

On peut choisir arbitrairement les a_{ii} réels, et les a_{ij} complexes pour $i < j$; la dimension réelle de l'espace vectoriel des N est donc

$$n + 2 \cdot \frac{n(n-1)}{2} = n^{2}.$$

En résumé, pour M assez voisine de 0, on a :

$\exp M \in U(n) \iff M$ est de la forme $i N$, N hermitienne.

(6) $\boxed{\exp M \in Sp(n, \mathbb{C})}$

$$\exp M \in Sp(n, \mathbb{C}) \iff ({}^{t}\exp M)\, J (\exp M) = J$$

$$\iff J^{-1}\, ({}^{t}\exp M)\, J = (\exp M)^{-1}$$

$$\iff J^{-1} (\exp {}^{t}M)\, J = \exp(-M).$$

Or $$J^{-1}(\exp {}^{t}M)\, J = \sum_{n \geq 0} J^{-1} \frac{({}^{t}M)^{n}}{n!} J = \sum_{n \geq 0} \frac{(J^{-1}\, {}^{t}M\, J)^{n}}{n!}$$

$$= \exp (J^{-1}\, {}^{t}M\, J)$$

insi

$$\exp M \in Sp(n, \mathbb{C}) \iff \exp (J^{-1}\, {}^t M\, J) = \exp(-M).$$

onc, pour M assez voisine de 0, on a

$$\exp M \in Sp(n, \mathbb{C}) \iff J^{-1}\, {}^t M\, J = -M \iff {}^t M\, J + J\, M = 0.$$

Réciproquement la condition

(*) $$\boxed{{}^t M\, J + J\, M = 0}$$

entraîne $\exp M \in Sp(n, \mathbb{C})$ quel que soit M (voisin ou non de 0).

La relation (*) définit un espace vectoriel complexe de matrices M. On peut l'expliciter et calculer sa dimension (sur $\mathbb{C}$) : posons

$$M = \begin{pmatrix} A & B \\ C & D \end{pmatrix},$$

A, B, C, D étant dans $M_n(\mathbb{C})$; la condition (*) se traduit par :

$$\begin{cases} B \text{ et } C \text{ symétriques}, \\ D = -{}^t A. \end{cases}$$

La dimension sur $\mathbb{C}$ de l'espace des matrices symétriques (complexes) étant égale à $\frac{n(n+1)}{2}$, et celle de $M_n(C)$ étant n^2, la dimension de l'espace des M satisfaisant à (*) est

$$2 \times \frac{n(n+1)}{2} + n^2 = n(2n+1).$$

En résumé, pour M assez voisine de 0, on a

$$M \in Sp(n,\mathbb{C}) \iff {}^t M\, J + J\, M = 0,$$

et les M satisfaisant à la relation de droite forment un espace vectoriel de dimension complexe égale à $n(2n+1)$.

(7) $$\boxed{\exp M \in Sp\ n}$$

La condition est : $\exp M \in U(2n) \cap Sp(n, \mathbb{C})$. Pour M assez voisine de 0, ceci équivaut à

$$i\,M \text{ hermitienne} \quad \text{et} \quad {}^t M\, J + J\, M = 0.$$

Si on pose

$$M = \begin{pmatrix} A & B \\ C & D \end{pmatrix}$$

on trouve facilement :

$$\begin{cases} A = i\,A' \ , \quad B = i\,B' \ , \quad C = i\,C', \quad D = i\,D', \\ A' \text{ hermitienne}, \quad D' = -{}^t A' \ , \quad B' \text{ symétrique}, \quad C' = B'^* \ , \end{cases}$$

donc la dimension réelle de l'espace vectoriel de ces M est $n^2 + 2\frac{n(n+1)}{2} = n(2n+1)$.

Conclusion finale : dans chacun des 7 cas envisagés, on a associé à un sous-groupe G de $GL(n, \mathbb{C})$ un sous-espace vectoriel V_G de $\mathrm{End}_{\mathbb{C}} \mathbb{C}^n \approx M_n(\mathbb{C})$ (sous-espace vectoriel tantôt réel, tantôt complexe), jouissant des propriétés suivantes :

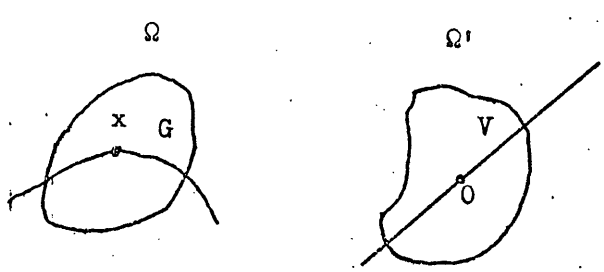
$$\begin{cases} M \in V_G \Longrightarrow \exp M \in G, \\ \text{pour } M \text{ assez voisin de } 0, \ \exp M \in G \Longrightarrow M \in V_G. \end{cases}$$

Dans chaque cas, l'application $M \longmapsto \exp M$ et l'application $A \longmapsto \mathrm{Log}\, A$ définissent des bijections (réciproques l'une de l'autre) d'un voisinage de 0 dans V_G, sur un voisinage de 1 dans G (resp. d'un voisinage de 1 dans G, sur un voisinage de 0 dans V_G).

Théorème. Les groupes G envisagés sont des sous-variétés analytiques (tantôt réelles, tantôt complexes) de $GL(n, \mathbb{C})$.

Avant de démontrer ce théorème, il nous faut définir ce qu'on entend par sous-variété analytique d'un ouvert U d'un espace vectoriel E. [On applique ensuite la définition en prenant $E = \mathrm{End}_{\mathbb{C}} \mathbb{C}^n$, $U = GL(n, \mathbb{C})$].

Définition 1. Soit E un espace vectoriel complexe, et soit $G \subset E$; on dit que G est une sous-variété analytique complexe au voisinage d'un de ses points $x \in G$, si la condition suivante est vérifiée : il existe un "isomorphisme analytique-complexe" f d'un voisinage ouvert Ω de x sur un voisinage ouvert $\Omega' \subset \mathbb{C}^n$ (où $n = \dim_{\mathbb{C}} E$) tel que $f(x) = 0$ et que f induise une bijection de $G \cap \Omega$ sur $V \cap \Omega'$, où V est un sous-espace vectoriel complexe de E



Commentaire. On dit que f est un isomorphisme analytique complexe de Ω sur Ω' si f est une bijection de Ω sur Ω', qui est analytique complexe ainsi que l'application réciproque. Ainsi, on peut dire que G est une sous-variété analytique complexe au voisinage de $x \in G$ si, dans un voisinage convenable Ω de x, G est

la même chose (à un isomorphisme analytique près) qu'un sous-espace vectoriel complexe au voisinage de l'origine.

Définition 2. Soit U un ouvert de E, et $G \subset U$; on dit que G est une sous-variété analytique complexe de U si :

1º/ G est fermé dans U,

2º/ pour chaque point $x \in G$, G est une "sous-variété analytique complexe au voisinage de x" (au sens de la définition 1).

On définit de même une sous-variété analytique réelle, en remplaçant partout le mot "complexe" par "réel" dans les définitions précédentes.

Démonstration du théorème. On va d'abord prouver :

Proposition. Chacun des groupes G envisagés de (1) à (7) est, au voisinage de l'élément neutre $1 \in G$, une sous-variété analytique (analytique complexe si le sous espace vectoriel V_G est complexe, analytique réelle si V_G est un sous-espace vectoriel réel).

En effet, on sait que l'application $A \longmapsto \log A$ est un isomorphisme analytique complexe (et aussi analytique réel) d'un voisinage Ω de 1 dans $GL(n, \mathbb{C})$ sur un voisinage Ω' de 0 dans $M_n(\mathbb{C})$; il résulte de l'étude faite plus haut que si Ω a été pris assez petit, l'application $A \longmapsto \log A$ applique bijectivement $G \cap \Omega$ sur $V_G \cap \Omega'$; donc G est bien une sous-variété au voisinage de $1 \in G$, d'après la définition 1. Ceci prouve la proposition .

Pour prouver le théorème, il reste à prouver que chacun des groupes G est une sous-variété analytique au voisinage de chacun de ses points (on le sait déjà pour le point $1 \in G$) ; cela suffira, car on sait que chaque G est fermé dans l'ouvert $GL(n, \mathbb{C})$.

Soit donc $A \in G$; la translation à gauche $B \longmapsto AB$ de $GL(n, \mathbb{C})$ dans $GL(n, \mathbb{C})$ est évidemment une transformation analytique complexe, ainsi que l'application réciproque $B \longmapsto A^{-1}B$.

Elle induit une bijection de G sur G, puisque $A \in G$ et que G est un sous-groupe de $GL(n, \mathbb{C})$.

Soit Ω un voisinage ouvert de 1 dans $GL(n, \mathbb{C})$, tel que $G \cap \Omega$ soit

variété analytique (cf. proposition précédente) ; la translation $B \longmapsto A\,B$ induit un isomorphisme analytique de Ω sur un ouvert (noté $A\,\Omega$) qui contient A, qui applique bijectivement $G \cap \Omega$ sur $G \cap (A\,\Omega)$. Il s'ensuit que G est une sous-variété analytique au voisinage de $A \in G$; et comme A est un point arbitraire de G, le théorème est démontré.

Remarque : on définit la dimension d'une sous-variété, comme égale à la dimension de l'espace vectoriel qui s'introduit dans la définition 1 ; naturellement, il y a une "dimension complexe" pour une variété analytique complexe, et une "dimension réelle" pour une variété analytique réelle. D'ailleurs toute variété analytique complexe peut être considérée comme une variété analytique réelle ; sa dimension réelle est alors le double de sa dimension complexe.

Si nous passons en revue les groupes G de (1) à (7), nous avons donc les résultats suivants :

$$\begin{cases} \dim_{\mathbb{R}} GL(n, \mathbb{R}) = n^2, \\ \dim_{\mathbb{C}} SL(n, \mathbb{C}) = n^2 - 1, \\ \dim_{\mathbb{R}} SL(n, \mathbb{R}) = n^2 - 1, \\ \dim_{\mathbb{R}} O(n) = \dfrac{n(n-1)}{2}, \\ \dim_{\mathbb{R}} U(n) = n^2, \\ \dim_{\mathbb{C}} Sp(n, \mathbb{C}) = n(2n+1) \\ \dim_{\mathbb{R}} Sp(n) = n(2n+1) \end{cases}$$

Matrices hermitiennes.

Soit $H(n)$ l'espace vectoriel réel des matrices $A \in M_n(\mathbb{C})$ qui sont hermitiennes :

$$A \in H(n) \Longleftrightarrow A \in M_n(\mathbb{C}) \quad \text{et} \quad A^* = A.$$

Associons à A la fonction $x \longmapsto (Ax \mid x)$ de $\mathbb{C}^n$ dans $\mathbb{R}$. Alors par définition

$$\boxed{A \geq 0 \Longleftrightarrow \forall\, x \in \mathbb{C}^n, \quad (Ax \mid x) \geq 0}$$

$$\boxed{A \gg 0 \Longleftrightarrow \forall\, x \in \mathbb{C}^n,\ x \neq 0, \quad (Ax \mid x) > 0}$$

Remarque : $A \geq 0$ et $A \neq 0$ n'implique pas $A \gg 0$.

Proposition 1.

Soit $A \in H(n)$ donnée. Il existe une base (e_i) de $\mathbb{C}^n$, orthonormée (au sens hermitien = au sens euclidien dans $\mathbb{R}^{2n}$) telle que

$$\forall i \quad (1 \leq i \leq n), \quad A(e_i) = \lambda_i e_i, \text{ avec } \lambda_i \in \mathbb{R}.$$

Démonstration.

1. Lemme. $A \in H(n) \Longrightarrow$ les valeurs propres de A sont réelles.

Démonstration. Soit λ une valeur propre, et x un vecteur propre associé à λ.

$Ax = \lambda x \Longrightarrow (Ax \mid x) = (\lambda x \mid x) = \lambda(x, x) \in \mathbb{R}$. Or $x \neq 0$, donc

$(x, x) \neq 0 \Longrightarrow \lambda \in \mathbb{R}$.

Conséquence. $\det(A - \lambda 1)$ possède n racines réelles (distinctes ou non).

2. Il reste à chercher une base orthonormée formée de vecteurs propres.

Soit λ_1 une valeur propre, et soit x_1 un vecteur propre associé à λ_1 : $Ax_1 = \lambda_1 x_1$. On prend alors le vecteur unitaire $e_1 = \frac{x_1}{\|x_1\|}$, qui est aussi un vecteur propre associé à λ_1.

Si x est orthogonal à e_1, alors Ax est orthogonal à e_1, car :

$$(x \mid e_1) = 0 \Longrightarrow (Ax \mid e_1) = (x \mid Ae_1) = (x \mid \lambda_1 e_1)$$
$$= \lambda_1 (x \mid e_1) = 0.$$

Les x orthogonaux à e_1 forment un hyperplan complexe de dimension $n-1$, qui est stable par A. La restriction de A à cet hyperplan V est encore hermitienne, et on peut appliquer l'hypothèse de récurrence à $A \mid V$: il existe une base orthonormée de V formée par des vecteurs $e_2, \ldots, e_n$ vérifiant $Ae_i = \lambda_i e_i$, $\lambda_i \in \mathbb{R}$, $2 \leq i \leq n$. Et par conséquent $\{e_1, e_2, \ldots, e_n\}$ est une base de $\mathbb{C}^n$ répondant à la question.

Remarque.

Les valeurs propres de la matrice A ne sont pas obligatoirement distinctes ; mais alors on peut les ranger par paquets, en mettant dans un même paquet toutes les valeurs propres égales à un nombre donné. Si $\lambda_1 = \ldots = \lambda_k$ sont les valeurs propres d'un tel paquet, le sous-espace engendré par $e_1, \ldots, e_k$ est tel que la restriction de A à ce sous-espace est une homothétie de rapport réel égal à $\lambda_1 = \ldots = \lambda_k$.

Alors $\mathbb{C}^n$ est somme directe de sous-espaces de ce type ; ces sous-espaces sont uniquement déterminés : chacun d'eux est formé de tous les vecteurs propres relatifs à une valeur propre donnée. Ces sous-espaces sont deux à deux orthogonaux. On a ainsi prouvé :

Proposition 2. Le sous-espace relatif à une racine λ de l'équation caractéristique a une dimension complexe égale à l'ordre de multiplicité de cette racine λ. Les sous-espaces relatifs aux valeurs propres distinctes sont deux à deux orthogonaux (au sens hermitien), et l'espace total $\mathbb{C}^n$ en est la somme directe.

Faire un changement de base qui envoie la base canonique de $\mathbb{C}^n$ sur une base orthonormée de $\mathbb{C}^n$ (au sens hermitien) c'est faire une transformation unitaire.

La proposition 1 s'énonce donc aussi de la manière suivante : $\exists\ U \in U(n)$, tel que $U A U^{-1} = D$, où D est une matrice diagonale réelle.

Remarque : Si B est hermitienne, alors $\forall\ U \in U(n)$, $U B U^{-1}$ est hermitienne.

Démonstration : $(U B U^{-1})^* = (U^{-1})^* B^* U^* = U B U^{-1}$.

Soit $A \in H(n)$. Alors $A \geq 0 \iff U A U^{-1} \geq 0$.

Démonstration.

$$A \geq 0 \iff \forall\ x \in \mathbb{C}^n,\quad (Ax \mid x) \geq 0 \quad ;\quad \text{or}$$

$(U A U^{-1} x \mid x) = (A U^{-1} x \mid U^{-1} x) \geq 0, \forall\ x \in \mathbb{C}^n$, d'où $U A U^{-1} \geq 0$. Ceci montre que $A \geq 0 \Longrightarrow U A U^{-1} \geq 0$; la réciproque est évidente car $A = U^{-1} (U A U^{-1}) U$.

Proposition. Pour que A hermitienne soit ≥ 0, il faut et il suffit que toutes les valeurs propres λ_i de A soient ≥ 0 ; pour que $A \gg 0$, il faut et il suffit que tous les λ_i soient > 0.

Démonstration : d'après ce qui précède, on peut supposer que A est une matrice diagonale D, dont les éléments diagonaux sont les λ_i ; on a

$$A \geq 0 \Longleftrightarrow (Dx \mid x) \geq 0 \Longleftrightarrow \sum_i \lambda_i x_i \overline{x_i} \geq 0,\ \forall\ x \in \mathbb{C}^n$$

$$\Updownarrow$$

$$\lambda_i \geq 0 \text{ pour tout } i.$$

Remarque : $\forall i : \lambda_i > 0 \iff \lambda_i \geq 0$ et D inversible ; autrement dit : pour une A hermitienne, on a les équivalences suivantes :

$$A \gg 0 \iff A \geq 0 \text{ et } A \text{ inversible.}$$
$$\Updownarrow$$
$$A \geq 0 \text{ et } A \in GL(n, \mathbb{C}).$$

Soit $A \in H(n)$ (espace vectoriel réel), et considérons l'ensemble $\{A \in H(n) \mid A \gg 0\}$; c'est un ouvert de $H(n)$.

Démonstration.

Supposons $A_0 \gg 0$ et soit A hermitienne vérifiant $\| A - A_0 \| \leq \varepsilon$. Alors $(Ax \mid x) = (A_0 x \mid x) + ((A-A_0)x \mid x)$. Mais $(A_0 x \mid x) \geq \lambda_1 (x \mid x)$, où λ_1 est la plus petite valeur propre de la matrice A_0 ; c'est évident en considérant la forme diagonale D_0 de A ; on a donc

$$(Ax \mid x) \geq \lambda_1 (x|x) - \varepsilon \| x \| . \| x \| , \text{ soit}$$
$$(Ax \mid x) \geq \lambda_1 (x|x) - \varepsilon (x|x) = (\lambda_1 - \varepsilon)(x|x) .$$

Donc si on prend $\varepsilon < \lambda_1$, on est sûr que $(Ax \mid x) > 0$ dès que $x \neq 0$; donc A est $\gg 0$.

Cas où $n = 1$.

$H(1) = \{$ matrices réduites à un élément λ réel $\} = \mathbb{R}$.

$\{A \in H(1) : A \gg 0\} = \mathbb{R}^+ =]0, +\infty[$ qui est bien un ouvert de $\mathbb{R}$. Dans ce cas, l'exponentielle $\lambda \longmapsto e^{\lambda}$ est une bijection de $\mathbb{R}$ sur $\mathbb{R}^+$. Nous allons voir qu'on a un résultat analogue pour n quelconque.

Lemme. Si $M \in H(n)$, alors $\exp M \in H(n)$ et $\exp M \gg 0$.

Démonstration. Si M est hermitienne, alors $M = M^* \Longrightarrow (\exp M)^* = \exp M^* = \exp M$; donc $\exp M$ est hermitienne. De plus, comme $\frac{M}{2}$ commute avec elle-même, on a

$$\exp M = (\exp \tfrac{M}{2})^2 .$$

Il en résulte que $\exp M \geq 0$; en effet, si A est hermitienne, A^2 est hermitienne ≥ 0, car

$$(A^2 x \mid x) = (Ax \mid Ax) \geq 0, \qquad \forall x \in \mathbb{C}^n.$$

Ainsi, on a donc $\exp M \geq 0$; or $\exp M \in GL(n, \mathbb{C})$; donc $\exp M \gg 0$.

emarque : $\forall i : \lambda_i > 0 \iff \lambda_i \geq 0$ et D inversible ; autrement dit :

our une A hermitienne, on a les équivalences suivantes :

$$A \gg 0 \iff A \geq 0 \quad \text{et} \quad A \text{ inversible.}$$
$$\Updownarrow$$
$$A \geq 0 \quad \text{et} \quad A \in GL(n, \mathbb{C}).$$

oit $A \in H(n)$ (espace vectoriel réel), et considérons l'ensemble $\{A \in H(n) \mid A \gg 0\}$;

'est un ouvert de $H(n)$.

émonstration.

upposons $A_0 \gg 0$ et soit A hermitienne vérifiant $\| A - A_0 \| \leq \varepsilon$. Alors

$(Ax \mid x) = (A_0 x \mid x) + ((A-A_0)\, x \mid x)$. Mais $(A_0\, x \mid x) \geq \lambda_1 (x \mid x)$, où λ_1 est la

lus petite valeur propre de la matrice A_0 ; c'est évident en considérant la forme

iagonale D_0 de A ; on a donc

$$(Ax \mid x) \geq \lambda_1 (x|x) - \varepsilon \| x \| \cdot \| x \|, \text{ soit}$$
$$(Ax \mid x) \geq \lambda_1 (x|x) - \varepsilon (x|x) = (\lambda_1 - \varepsilon)(x|x).$$

onc si on prend $\varepsilon < \lambda_1$, on est sûr que $(Ax \mid x) > 0$ dès que $x \neq 0$; donc A

est $\gg 0$.

s où $n = 1$.

$H(1) = \{$ matrices réduites à un élément λ réel $\} = \mathbb{R}$.

$\{A \in H(1) : A \gg 0\} = \mathbb{R}^+ =]0, +\infty[$ qui est bien un ouvert de $\mathbb{R}$. Dans ce cas,

exponentielle $\lambda \longmapsto e^\lambda$ est une bijection de $\mathbb{R}$ sur $\mathbb{R}^+$. Nous allons voir

'on a un résultat analogue pour n quelconque.

mme. Si $M \in H(n)$, alors $\exp M \in H(n)$ et $\exp M \gg 0$.

monstration. Si M est hermitienne, alors $M = M^* \Longrightarrow (\exp M)^* = \exp M^* = \exp M$;

nc $\exp M$ est hermitienne. De plus, comme $\frac{M}{2}$ commute avec elle-même, on a

$$\exp M = (\exp \tfrac{M}{2})^2 .$$

en résulte que $\exp M \geq 0$; en effet, si A est hermitienne, A^2 est hermitienne

0, car

$$(A^2 x \mid x) = (Ax \mid Ax) \geq 0, \qquad \forall x \in \mathbb{C}^n.$$

i, on a donc $\exp M \geq 0$; or $\exp M \in GL(n, \mathbb{C})$; donc $\exp M \gg 0$.

Théorème :

L'application exponentielle est un isomorphisme analytique réel de $H(n)$ sur $H^+(n)$, où $H^+(n)$ désigne l'ouvert de $H(n)$ formé des matrices hermitiennes $\gg 0$.

Démonstration. Si $n = 1$, on sait qu'il est bien ainsi. Pour n quelconque, on sait déjà que si $M \in H(n)$, alors $\exp M \in H^+(n)$; d'ailleurs l'application $M \longmapsto \exp M$ est analytique. Il reste à montrer que cette application est bijective et que l'application réciproque est aussi analytique.

a) $M \longmapsto \exp M$ est bijective de $H(n)$ sur $H^+(n)$. Autrement dit :

Lemme. Soit A une matrice hermitienne $\gg 0$. Il existe une matrice hermitienne M et une seule telle que $\exp M = A$.

Démonstration du lemme.

Supposons le problème résolu et soit M une matrice hermitienne telle que $\exp M = A$. Soient λ_i les valeurs propres distinctes de M. M étant hermitienne, ces valeurs propres sont réelles et ont chacune un ordre de multiplicité α_i. Alors l'espace $\mathbb{C}^n$ est somme directe de sous-espaces E_i deux à deux orthogonaux, où E_i est l'espace propre de dimension α_i associé à la valeur propre λ_i :

$$\mathbb{C}^n = \bigoplus_i E_i .$$

L'application $A = \exp M$ laisse stable chaque E_i ; et si $x \in E_i$, $A(x) = e^{\lambda_i} x$. Si $\lambda_i \neq \lambda_j$, alors $e^{\lambda_i} \neq e^{\lambda_j}$ [car $x \longmapsto e^x$ est une application bijective de $\mathbb{R}$ dans $\mathbb{R}^+$]. Donc E_i, qui est stable par A, est le sous-espace relatif à la valeur propre e^{λ_i}.

Les sous-espaces propres E_i sont donc les mêmes pour M et pour A.

Conséquence.

Si M existe on n'a pas le choix : les E_i de M sont ceux de A. Si les valeurs propres de A sont $\mu_i > 0$, les valeurs propres λ_i de M sont nécessairement :

$$\lambda_i = \log \mu_i .$$

On trouve ainsi l'unique M hermitienne telle que $\exp M = A$.

Définition.

Soit A une matrice hermitienne $\gg 0$; on note $\log A$ l'unique matrice hermitienne M telle que $\exp M = A$.

On a donc :

(1) $\forall\ A \in H^*(n)$, $\exp(\operatorname{Log} A) = A$.

(2) $\forall\ M \in H(n)$, $\log(\exp M) = M$; en effet, pour vérifier l'égalité, il suffit de vérifier que les exponentielles des deux membres sont égales. Or

$$\exp(\log(\exp M)) = \exp M \qquad \text{d'après (1).}$$

L'application logarithmeest donc l'application réciproque de l'application exponentielle. Pour achever la démonstration du théorème, il reste à prouver que l'application $A \longmapsto \log A$ est analytique.

Observons d'abord ceci :

(3) $\forall\ k \in \mathbb{Z}$, $\log(A^k) = k \log A$;

en effet, les deux membres ont même exponentielle, (car $\exp(k M) = (\exp M)^k$).

b) Soit $A_0 \in H^+(n)$. On veut montrer que pour A suffisamment voisine de A_0 ($\| A - A_0 \| \leq \varepsilon$), l'application log est une fonction analytique de A. Or on peut trouver $\lambda > 0$ tel que la matrice λA_0 ait ses valeurs propres dans l'intervalle ouvert $]0, 1[$; alors la matrice $1_n - \lambda A_0$ aura ses valeurs propres strictement positives et < 1, donc $1_n - \lambda A_0 \in H^+(n)$, et on a $0 \ll \lambda A_0 \ll 1_n$.

Supposons qu'on ait montré que $\log A$ est analytique au voisinage de λA_0 ; alors par homothétie, $\log A$ sera analytique au voisinage de A_0, car

$$\log(\lambda A) = (\log \lambda)\, 1_n + \log A$$

$$\log A_0 = (\log \tfrac{1}{\lambda})\, 1_n + \log \lambda A_0$$

$$\log A = (\log \tfrac{1}{\lambda})\, 1_n + \log \lambda A.$$

Pour A voisin de A_0, λA est voisin de λA_0. Or l'application $A \longmapsto \lambda A$ est analytique. On a le schéma

$$A \xmapsto{p} \lambda A \xmapsto{i} \log \lambda A \xmapsto{p'} \log A.$$

Pour montrer que $A \longmapsto \log A$ est analytique, il suffit de montrer que i est analytique, car p l'est ainsi que p' qui consiste à ajouter une constante.

Désormais on suppose donc que $0 \ll A_0 \ll 1_n$, et on va montrer qu'au voisinage d'une telle matrice A_0, le logarithme d'une matrice hermitienne A est une fonction analytique de A.

Si, $\| A - A_0 \| \leq \varepsilon$ convenable, on a encore $0 \ll A \ll A_n$ (cf. valeurs propres).

Donc $\| 1 - A \| < 1$.

Posons $U = 1_n - A$; U est hermitienne et voisine de $U_0 = 1_n - A_0$. Montrons que $\log A = \log(1-U) = -\left(U + \frac{U^2}{2} + \ldots + \frac{U^n}{n} + \ldots\right)$, série convergente pour $|U| < 1$; ceci prouvera que $\log A$ est une fonction analytique de A au voisinage de A_0.

Il reste à démontrer que le logarithme défini précédemment admet bien ce développement en série entière pour $U \in H(n)$ et $|U| < 1$.

Pour cela il suffit de vérifier :

(1) que le deuxième membre définit une matrice hermitienne ;

(2) que son exponentielle est égale à $1 - U$.

(1) $\quad U \in H(n), \quad U^2 \in H(n), \ldots, U^n \in H(n), \ldots$

On réduit U à la forme diagonale : $U = \begin{pmatrix} \lambda_1 & & \\ & \ddots & \\ & & \lambda_n \end{pmatrix}$

Alors $\quad \frac{U^n}{n} = \begin{pmatrix} \frac{\lambda_1^n}{n} & & \\ & \ddots & \\ & & \frac{\lambda_n^n}{n} \end{pmatrix}$

$$-\left(U + \frac{U^2}{2} + \ldots + \frac{U^n}{n} + \ldots\right) = -\begin{pmatrix} \lambda_1 + \frac{\lambda_1^2}{2} + \ldots + \frac{\lambda_1^n}{n} + \ldots & & \\ & \ddots & \\ & & \lambda_n + \frac{\lambda_n^2}{2} + \ldots + \frac{\lambda_n^n}{n} + \ldots \end{pmatrix} = \begin{pmatrix} \operatorname{Log}(1-\lambda_1) & & \\ & \ddots & \\ & & \operatorname{Log}(1-\lambda_n) \end{pmatrix}$$

qui est bien une matrice hermitienne.

(2) deux méthodes de démonstration, :

a) son exponentielle est égale à $1-U$, car c'est un calcul de série formelle que nous savons être vrai.

b) Si les valeurs propres de U sont les λ_i, alors les valeurs propres du second membre sont les $\log(1 - \lambda_i) \Rightarrow$ les valeurs propres de l'exponentielle du

second membre sont les $1 - \lambda_i$, c'est-à-dire les valeurs propres de $1 - U$; donc l'exponentielle du second membre est $1 - U$.

La démonstration du théorème est ainsi achevée.

Corollaire. Soit A une matrice hermitienne $\gg 0$; alors il existe une matrice hermitienne $B \gg 0$ et une seule qui vérifie $B^2 = A$; on la note $\sqrt{A}$, ou $A^{\frac{1}{2}}$.

Démonstration. Supposons le problème résolu : $B^2 = A$. Alors $\log B^2 = 2 \log B = \log A \Longrightarrow \log B = \frac{1}{2} \log A$ et $B = \exp(\frac{1}{2} \log A)$ est la solution unique.

Etude des matrices réelles symétriques.

Ce sont les matrices hermitiennes qui en outre sont réelles. On sait que M définit une forme quadratique

$$\begin{cases} \forall x \in \mathbb{R}^n, \langle Mx, x \rangle \geq 0 \Longleftrightarrow M \geq 0 \\ \forall x \in \mathbb{R}^n - \{0\}, \langle Mx, x \rangle > 0 \Longleftrightarrow M \gg 0 \end{cases}$$

On peut recopier la théorie des matrices hermitiennes.

Proposition. Etant donnée M symétrique réelle, il existe une base orthonormée (e_i) de $\mathbb{R}^n$ telle que $M(e_i) = \lambda_i e_i$, où λ_i sont les valeurs propres (réelles) de M.

Démonstration. A priori il n'est pas évident que le polynôme caractéristique $\det(M - \lambda 1_n)$ ait toutes ses racines réelles. Mais comme nous avons démontré qu'il en est ainsi lorsque $M \in H(n)$, c'est vrai lorsque $M \in H(n)$ est réelle. Soit λ_1 une valeur propre, et e_1 un vecteur propre associé tel que $\|e_1\| = 1$ $M(e_1) = \lambda_1 e_1$.

L'hyperplan réel orthogonal à e_1, de dimension n-1, est stable par M ; on peut alors appliquer l'hypothèse de récurrence : $\{e_2, \ldots, e_n\}$ est une base orthonormée de cet hyperplan vérifiant la proposition, et $\{e_1, \ldots, e_n\}$ est une base orthonormée de $\mathbb{R}^n$ qui répond à la question. Donc $\mathbb{R}^n$ est somme directe d'espaces E_i deux à deux orthogonaux, où E_i est l'espace propre associé à la valeur propre λ_i, de dimension égale à l'ordre de multiplicité de λ_i.

On a les assertions suivantes : M symétrique $\Longrightarrow \exists\, O \in O(n)$ telle que $O\,M\,O^{-1} = D$ soit diagonale. Pour une M symétrique :

$\begin{cases} M \geq 0 \iff \text{ses valeurs propres } \lambda_i \text{ sont } \geq 0 \\ M \gg 0 \iff \text{ses valeurs propres } \lambda_i \text{ sont } > 0 \\ M \gg 0 \iff M \geq 0 \text{ et } M \text{ inversible.} \end{cases}$

Notations.

$S(n)$ désigne l'espace vectoriel réel des matrices symétriques de $M_n(\mathbb{R})$.

$S^+(n)$ désigne l'ouvert des matrices de $S(n)$ qui sont $\gg 0$.

On a $S(n) \subset H(n)$, $S^+(n) \subset H^+(n)$.

Théorème. L'application expoentielle $M \longmapsto \exp M$ est un isomorphisme analytique réel de l'espace $S(n)$ sur l'ouvert $S^+(n)$. [On recopie la démonstration donnée dans le cas des matrices hermitiennes].

Décomposition canonique de $GL(n, \mathbb{C})$.

Théorème. Toute matrice $A \in GL(n, \mathbb{C})$ s'écrit d'une seule manière comme un produit $A = UH$, où $U \in U(n)$ et $H \in H^+(n)$. De plus U et H sont des fonctions analytiques de A.

Démonstration.

1. Lemme préliminaire : $\forall\, A \in GL(n, \mathbb{C})$, $A^* A \in H^+(n)$. En effet :

a) $\forall\, A \in M_n(\mathbb{C})$, $A^* A$ est hermitienne ≥ 0, car $\forall\, x \in \mathbb{C}^n$, $(A^* Ax \mid x) = (Ax \mid Ax)$ qui est bien ≥ 0.

b) Si A est inversible, alors $A^* A$ est inversible, donc $A^* A \gg 0$.

2. Supposons le problème résolu :

$A = UH$. Alors $A^* = H^* U^*$ avec $\begin{cases} H^* = H \text{ puisque } H \in H^+(n) \\ U^* = U^{-1} \text{ puisque } U \in U(n). \end{cases}$

On a $A^* = HU^{-1}$, d'où $A^* A = H^2$, avec $H \in H^+(n)$. Si A est donnée, alors H^2 est connue, et on a nécessairement $H = \sqrt{A^* A}$.

Il en résulte que U est parfaitement déterminée : $U = AH^{-1}$. Ceci prouve l'unicité. Pour l'existence, posons $H = \sqrt{A^* A}$; il reste à vérifier que

$$A\,H^{-1} \in U(n).$$

Or $(A H^{-1})^* = (H^{-1})^* A^* = H^{-1} A^*$, car $H^{-1} \in H(n)$. Donc

$U^* U = H^{-1} A^* A H^{-1} = H^{-1} H^2 H^{-1} = 1 \Longrightarrow U \in U(n)$.

Montrons maintenant que U et H sont des <u>fonctions analytiques</u> de A :

(1) $H = \sqrt{A^* A}$ est une fonction analytique de $A \in GL(n, \mathbb{C})$; en effet,

$A \longmapsto A^*$ est une fonction analytique réelle de A, car $x + iy \longmapsto x - iy$ est une fonction analytique réelle de $x + iy$.

$A \longmapsto A^* A$ est une fonction analytique de A, car la loi de multiplicité des matrices est analytique.

$A \longmapsto \sqrt{A^* A}$ est une fonction analytique de A, car la racine carrée d'une $M \gg 0$ est une fonction analytique de M.

(2) $U = A H^{-1}$ est une fonction analytique de A ; en effet :

$A \longmapsto (\sqrt{A^* A})^{-1} = H^{-1}$ étant une fonction analytique de A,

$A \longmapsto A H^{-1}$ est aussi une fonction analytique de A.

<u>Théorème.</u> On a un <u>isomorphisme de variétés analytiques réelles entre</u> $GL(n, \mathbb{C})$ <u>et</u> $U(n) \times H^+(n)$.

<u>Démonstration</u>. $U : GL(n, \mathbb{C}) \longrightarrow U(n)$ et $H : GL(n, \mathbb{C}) \longrightarrow H^+(n)$

$A \longmapsto A(\sqrt{A^* A})^{-1}$ $\qquad$ $A \longmapsto \sqrt{A^* A}$

sont des fonctions analytiques ; d'où une application analytique (réelle)

$$GL(n, \mathbb{C}) \longrightarrow U(n) \times H^*(n).$$

L'application réciproque $(U, H) \longmapsto U H$ étant évidemment analytique, ces deux applications sont des isomorphismes analytiques réels.

C.Q.F.D.

Remarque ; On a vu que la fonction exponentielle est un isomorphisme analytique de $H(n)$ sur $H^+(n)$. Il existe donc un isomorphisme analytique de $GL(n, \mathbb{C})$ sur $U(n) \times H(n)$; l'isomorphisme réciproque étant défini par $(U, M) \longrightarrow U.(\exp M)$.

On a $\dim_{\mathbb{R}} U(n) = n^2$, $\dim_{\mathbb{R}} H(n) = n^2$; d'ailleurs :

$$\dim_{\mathbb{C}} GL(n, \mathbb{C}) = n^2 \Longleftrightarrow \dim_{\mathbb{R}} GL(n, \mathbb{C}) = 2n^2.$$

$U(n)$ est un compact ; $H(n)$ est un espace vectoriel.

Cas particulier.

On a $GL(1, \mathbb{C}) = \mathbb{C}^* \xrightarrow{\simeq} U(1) \times H^+(1)$ où

$$\begin{cases} U(1) = \{\text{complexes de module } 1\} = \text{cercle unité} \\ H^+(1) = \mathbb{R}^+ \quad (\text{nombres réels} > 0). \end{cases}$$

L'isomorphisme est défini par $z \longmapsto (a, r)$, où $a = \frac{z}{|z|}$, $r = |z|$.

On peut également définir un isomorphisme de $\mathbb{C}^*$ sur $U(1) \times H(1)$, où $H(1) = \mathbb{R}$: $z \longmapsto (u, \lambda)$, avec $z = u e^{\lambda}$, où $u \in U(1)$ et $\lambda \in \mathbb{R}$.

PROBLÈME

Soit G un sous-groupe de $GL(n, \mathbb{C})$. Si $A \in G$, que peut-on dire de $H = \sqrt{A^* A}$ et $U = AH^{-1}$? On va étudier successivement le cas de quatre sous-groupes de $GL(n, \mathbb{C})$.

(1)- $\boxed{G = GL(n, \mathbb{R})}$.

Alors $H = \sqrt{{}^t A A}$; ${}^t AA$ est une matrice symétrique > 0 ; donc H est réelle, H^{-1} est donc réelle et $U = AH^{-1}$ est réelle.

Conséquence.

$$A \in GL(n, \mathbb{R}) \Longleftrightarrow U \text{ et } H \in GL(n, \mathbb{R}).$$

On trouve ainsi deux isomorphismes analytiques :

a] $GL(n, \mathbb{R}) \xrightarrow{\simeq} O(n) \times S^+(n)$

b] $GL(n, \mathbb{R}) \xrightarrow{\simeq} O(n) \times S(n)$, en prenant le logarithme.

On a $\dim_{\mathbb{R}} GL(n, \mathbb{R}) = n^2$, $\dim_{\mathbb{R}} O(n) = \frac{n(n-1)}{2}$, $\dim_{\mathbb{R}} S(n) = \frac{n(n+1)}{2}$; $O(n)$ est un compact, $S(n)$ un espace vectoriel.

On en déduit les deux isomorphismes de variétés analytiques réelles :

a] $GL^+(n, \mathbb{R}) \xrightarrow{\simeq} SO(n) \times S^+(n)$,

b] $GL^+(n, \mathbb{R}) \xrightarrow{\simeq} SO(n) \times S(n)$.

Remarque.

Si on sait que $SO(n)$ est connexe, comme on sait que $S(n)$ l'est, on conclut que $GL^+(n, \mathbb{R})$ est connexe (si on ne le sait pas encore).

Cas particulier.

$$GL(1, \mathbb{R}) = \mathbb{R}^* \xrightarrow{\sim} \{-1, +1\} \times \mathbb{R}^+.$$

(2). $\boxed{G = O(n, \mathbb{C})}$

$A \in G \iff {}^tAA = 1$.

$H = \sqrt{A^* A}$. Montrons que $A^* A$ est une transformation orthogonale, i.e. que ${}^t(A^* A)\,(A^* A) = 1$; en fait :

$${}^tA\ {}^tA^*\ A^*\ A = {}^tA\ \overline{A}\ {}^t\overline{A}\ A = {}^tA \cdot 1 \cdot A = {}^tA\,A = 1.$$

Montrons maintenant que $H \in G$. Il suffit de prouver :

Lemme. Si $H > 0$ et si $H^2 \in O(n, \mathbb{C})$, alors $H \in O(n, \mathbb{C})$.

Démonstration : soit M hermitienne telle que $\exp M = H^2$; alors $H = \exp \frac{M}{2}$.

Cherchons à quelle condition doit satisfaire une matrice hermitienne M pour que $\exp M$ soit orthogonale : ${}^t(\exp M) = (\exp M)^{-1}$, soit $\exp({}^tM) = \exp(-M)$.

Comme ${}^tM$ et $-M$ sont hermitiennes, et que $\exp$ est bijectif de $H(n)$ sur $H^+(n)$, on conclut que ${}^tM = -M$ (nécessaire et suffisant).

Ces M forment un sous-espace vectoriel de $H(n)$; si M y appartient, $\frac{M}{2}$ aussi donc $H \in O(n, \mathbb{C})$, et le lemme est démontré.

Remarque : posons $M = iM'$; les conditions $M^* = M$ et ${}^tM = -M$ se traduisent par ${}^t\overline{M'} + M' = 0$ et ${}^tM' + M' = 0$, c'est-à-dire : M' réelle et "symétrique gauche". L'espace vectoriel des M' réelles et symétriques-gauches est évidemment de dimension (réelle) $\frac{n(n-1)}{2}$; Si on le note $E(n)$, on a un isomorphisme de variétés analytiques réelles

$$O(n, \mathbb{C}) \xrightarrow{\sim} (U(n) \cap O(n, \mathbb{C})) \times E(n).$$

Etudions le groupe $U(n) \cap O(n, \mathbb{C})$:

$$\left.\begin{array}{l} A \in O(n, \mathbb{C}) \iff {}^tA = A^{-1} \\ A \in U(n) \iff {}^t\overline{A} = A^{-1} \end{array}\right\} \iff A \text{ est réelle et } {}^tA = A^{-1}.$$

Donc $U(n) \cap O(n, \mathbb{C}) = O(n)$.

On a donc les deux isomorphismes analytiques suivants :

a] $O(n, \mathbb{C}) \xrightarrow{\approx} O(n) \times E(n)$,

b] $SO(n, \mathbb{C}) \xrightarrow{\approx} SO(n) \times E(n)$,

avec $\dim_{\mathbb{C}} O(n, \mathbb{C}) = \frac{n(n-1)}{2}$, $\dim_{\mathbb{R}} O(n) = \dim_{\mathbb{R}} E(n) = \frac{n(n-1)}{2}$.

(3). $\boxed{G = SL(n, \mathbb{C})}$

Si $\det A = 1$, alors $\det A^* = 1$, donc $\det H = 1$.

On trouve donc un isomorphisme analytique de $SL(n, \mathbb{C})$ sur $SU(n) \times E'(n)$, où $E'(n)$ désigne le sous-espace vectoriel de $H(n)$ formé des $M \in H(n)$ telles que $Tr(M) = 0$.

On a $\dim_{\mathbb{C}} SL(n, \mathbb{C}) = n^2 - 1$, $\dim_{\mathbb{R}} SU(n) = n^2 - 1$, $\dim_{\mathbb{R}} E'(n) = n^2 - 1$.

(4)- $\boxed{G = Sp(n, \mathbb{C})}$

Montrons que si $A \in G$, alors $H = \sqrt{A^* A} \in G$.

Remarque préliminaire :

Soit G un des groupes classiques étudiés ; alors :

$$A \in G \Longrightarrow {}^tA \in G \quad \text{et} \quad \overline{A} \in G, \quad \text{d'où} \quad A^* \in G.$$

Faisons la démonstration dans le cas qui nous occupe:

$$A \in G \iff {}^tA\, J\, A = J, \quad \text{où} \quad J = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}.$$

Comme ${}^tJ = J^{-1}$, on a, en transposant, ${}^tA\, J^{-1}\, A = J^{-1}$, ou encore $J\,{}^tA\, J^{-1}\, A = 1$.

Donc $A(J\,{}^tA\, J^{-1}\, A)\, A^{-1} = AA^{-1} = 1$, soit $AJ\,{}^tA\, J^{-1} = 1$, ou encore $A\, J\,{}^tA = J$, ce qui exprime que ${}^tA \in G$.

Il est clair que $A \in G \Longrightarrow \overline{A} \in G$, donc $A \in G \Longrightarrow A^* \in G$.

Ainsi, $A \in G \Longrightarrow A^* A \in G$. On a $A^* A = H^2$, $H \gg 0$.

Cherchons à quelle condition doit satisfaire une matrice $M \in H(2n)$ pour que

$$\exp M \in Sp(n, \mathbb{C}).$$

La condition s'écrit ${}^t(\exp M)\, J(\exp M) = J$, ce qui équivaut à ${}^t(\exp M) = J(\exp -M)\, J^{-1}$. Or ${}^t(\exp M) = \exp({}^tM)$,

$$J(\exp -M)\, J^{-1} = \exp(-J\, M\, J^{-1}).$$

M étant hermitienne, ${}^tM$ et $J(-M)\, J^{-1}$ le sont aussi. La relation $\exp({}^tM) = \exp(-J\, M\, J^{-1})$ équivaut donc à ${}^tM = -J\, M\, J^{-1}$, ou encore $\boxed{{}^tM\, J + JM = 0}$

Telle est la condition cherchée.

Or si cette condition est vraie pour M, elle l'est pour $\frac{M}{2}$. Donc si $H^2 = \exp M \in Sp(n, \mathbb{C})$, il en est de même de $H = \exp \frac{M}{2}$.

Ainsi lorsque $A = U H \in Sp(n, \mathbb{C})$, on a $U \in Sp(n, \mathbb{C})$ et $H \in Sp(n, \mathbb{C})$.

On en déduit l'isomorphisme analytique suivant

$$Sp(n, \mathbb{C}) \xrightarrow{\approx} \left[U(2n) \cap Sp(n, \mathbb{C})\right] \times E''(2n),$$

où $E''(2n)$ est l'espace vectoriel des matrices hermitiennes M telles que ${}^tM J + JM = 0$. D'ailleurs on sait que $U(2n) \cap Sp(n, \mathbb{C}) = Sp(n)$. D'où

$$\boxed{Sp(n, \mathbb{C}) \xrightarrow{\approx} Sp(n) \times E''(2n)}$$

Calculons la dimension de l'espace vectoriel $E''(2n)$. Soit $M = \begin{pmatrix} A & B \\ C & D \end{pmatrix}$, où $A, B, C, D \in M_n(\mathbb{C})$. Pour que ${}^tM J + JM = 0$, il faut et il suffit que :

$$A \in H(n), \quad B \text{ symétrique (complexe)}, \quad C = \overline{B}, \quad D = -\overline{A}.$$

La dimension de l'espace des A est n^2 ; les B forment un espace vectoriel de dimension complexe $\frac{n(n+1)}{2}$, donc de dimension réelle $n(n+1)$.

D'où : $\dim E''(2n) = n^2 + n(n+1) = n(2n+1)$.

On sait que $n(2n+1)$ est aussi la dimension réelle de la variété $Sp(n)$, tandis que $Sp(n, C)$ est une variété analytique complexe de dimension (complexe) $n(2n+1)$.

LE GROUPE HOMOGRAPHIQUE à une VARIABLE : APPLICATIONS.

Etude particulière de $GL(2, \mathbb{C})$.

$GL(2, \mathbb{C})$ se compose des transformations

(1) $\quad x \longmapsto ax + by, \quad y \longmapsto cx + dy$

(a, b, c, d complexes, $ad - bc \neq 0$) portant sur les variables complexes x et y. Donc $GL(2, \mathbb{C})$ opère dans $\mathbb{C}^2 - \{0\}$; en fait, une transformation telle que (1) induit une transformation sur $z = \frac{x}{y}$, à savoir

(2) $\quad z \longmapsto \frac{az + b}{cz + d} \qquad (ad - bc \neq 0)$;

mais il faut considérer que z peut prendre la valeur ∞ (pour $y = 0, x \neq 0$), et de même $\frac{az + b}{cz + d}$ peut prendre la valeur ∞ pour $z = -\frac{d}{c}$ (si $c \neq 0$).

Donnons plus de détails : on va définir pour cela avec précision la droite projective complexe $P_1(\mathbb{C})$. Considérons l'espace $\mathbb{C} \times \mathbb{C} - \{0\} = \mathbb{C}^2 - \{0\}$; un point de cet espace est défini par un couple (x, y) de nombres complexes non nuls tous deux. Définissons la relation d'équivalence $\mathcal{R}$ que voici

$(x, y) \underset{\mathcal{R}}{\sim} (x', y')$ si et seulement s'il existe un $\lambda \in \mathbb{C}$, $\lambda \neq 0$, tel que

$$x' = \lambda x, \quad y' = \lambda y.$$

L'ensemble quotient $(\mathbb{C}^2 - \{0\})/\mathcal{R}$ peut être muni d'une topologie, la "topologie-quotient". D'une manière générale, si X est un espace topologique et $\mathcal{R}$ une relation d'équivalence, dans X, on a une application canonique $p : X \longrightarrow X/\mathcal{R}$ (qui à chaque point $x \in X$ associe sa classe d'équivalence); et on définit sur $X/\mathcal{R}$ la topologie que voici : un sous-ensemble $U \subset X/\mathcal{R}$ est dit ouvert si et seulement si $p^{-1}(U)$ est un ouvert de X. Alors l'application $p : X \longrightarrow X/\mathcal{R}$ est continue, et possède la propriété (qui caractérise la topologie de $X/\mathcal{R}$) : pour qu'une application $f : X/\mathcal{R} \longrightarrow Y$ (où Y est un espace topologique quelconque) soit continue, il faut et il suffit que $f \circ p : X \longrightarrow Y$ soit continue. Ou encore : toute application continue $g : X \longrightarrow Y$, constante

sur les classes d'équivalence de $\mathcal{R}$, définit, par passage au quotient, une application continue $f : X/\mathcal{R} \longrightarrow Y$.

Par définition, la droite projective complexe, notée $P_1(\mathbb{C})$, est l'espace topologique quotient $(\mathbb{C}^2 - \{0\})/\mathcal{R}$. Si $z \in P_1(\mathbb{C})$, tout point (x, y) de $p^{-1}(z)$ s'appelle un système de coordonnées homogènes du point z ; on passe d'un système à un autre par une homothétie de rapport complexe $\lambda \neq 0$.

Lorsque $y = 0$, tous les points $(x, 0)$ (où $x \neq 0$) de $\mathbb{C}^2 - \{0\}$ forment une classe d'équivalence ; on notera ∞ le point correspondant de $P_1(\mathbb{C})$. Lorsque $y \neq 0$, la classe d'équivalence d'un point (x, y) de $\mathbb{C}^2 - \{0\}$ est caractérisée par le quotient $\frac{x}{y}$, qui est un nombre complexe z ; donc le complémentaire U du point ∞ dans $P_1(\mathbb{C})$ est en correspondance bijective avec $\mathbb{C}$ (corps des nombres complexes).

On va montrer que cette correspondance bijective $U \longleftrightarrow \mathbb{C}$ est un homéomorphisme. Elle est en effet définie par deux applications $f : \mathbb{C} \longrightarrow U$ et $g : U \longrightarrow \mathbb{C}$, réciproques l'une de l'autre, à savoir :

- f associe à $z \in \mathbb{C}$ la classe d'équivalence de $(z, 1) \in \mathbb{C}^2 - \{0\}$;
- g associe à la classe de (x, y) (où $y \neq 0$) le nombre $\frac{x}{y} \in \mathbb{C}$.

Il est clair que $g \circ f$ est l'application identique de $\mathbb{C}$, et $f \circ g$ l'application identique de U ; et tout revient donc à vérifier que f et g sont continues. Observons que $p^{-1}(U) = \mathbb{C} \times \{\mathbb{C} - \{0\}\}$.

a) f est continue, parce qu'elle est composée des deux applications continues

$$\mathbb{C} \xrightarrow{\alpha} p^{-1}(U) \xrightarrow{p} U,$$

avec $\alpha(z) = (z, 1)$.

b) g est continue, car la composée

$$p^{-1}(U) \xrightarrow{p} U \xrightarrow{g} \mathbb{C}$$

est l'application $(x, y) \longmapsto \frac{x}{y}$, qui est continue sur

$$p^{-1}(U) = \mathbb{C} \times \{\mathbb{C} - \{0\}\} ;$$

il s'ensuit que g est continue, d'après la définition de la topologie-quotient

[un sous-ensemble $V \subset U$ est ouvert si et seulement si $p^{-1}(V)$ est ouvert dans $p^{-1}(U)$].

Ainsi f et g sont deux homéomorphismes, réciproques l'un de l'autre, qui permettent d'identifier $\mathbb{C}$ au sous-espace U de $P_1(\mathbb{C})$; rappelons que U est le complémentaire du point ∞.

La définition de la topologie quotient sur $P_1(\mathbb{C})$ permet de montrer facilement (exercice 1) : pour qu'une suite de points $z_n \in \mathbb{C}$ ait pour limite le point $\infty \in P_1(\mathbb{C})$, il faut et il suffit que $|z_n|$ tende vers l'infini. [Ceci signifie que l'espace $P_1(\mathbb{C})$ s'identifie à l'espace "compactifié d'Alexandroff" de l'espace $\mathbb{C}$, par "adjonction d'un point à l'infini"].

Revenons alors aux transformations (1) et (2). Soit S la transformation de $\mathbb{C}^2$ définie par (1) ; S induit un homéomorphisme $\mathbb{C}^2 - \{0\} \xrightarrow{\sim} \mathbb{C}^2 - \{0\}$, puisque $ad - bc \neq$ cet homéomorphisme passe au quotient : il existe une unique application S' qui rend commutatif le diagramme :

$$\begin{array}{ccc} \mathbb{C}^2 - \{0\} & \xrightarrow{S} & \mathbb{C}^2 - \{0\} \\ \downarrow p & & \downarrow p \\ P_1(\mathbb{C}) & \xrightarrow{S'} & P_1(\mathbb{C}) \end{array},$$

et cette application est <u>continue</u> d'après la définition de la topologie quotient [il suffit de vérifier que $S' \circ p$ est continue ; or

$$S' \circ p = p \circ S,$$

et $p \circ S$ est continue]. Comme le même raisonnement marche pour S^{-1}, on voit de même que S'^{-1} est continue. Donc S' <u>est un homéomorphisme de</u> $P_1(\mathbb{C})$.

De plus, il est évident que si $S = S_2 \circ S_1$ (composé de deux homéomorphismes S_1 et S_2 de $\mathbb{C}^2 - \{0\}$ sur lui-même), alors $S' = S'_2 \circ S'_1$.

La transformation S' associée à la transformation S définie par (1) transforme $z \in \mathbb{C} \subset P_1(\mathbb{C})$ en $\frac{az + b}{cz + d}$, qui est un point de $\mathbb{C}$ si $cz + d \neq 0$; si $cz + d = 0$, on vérifie facilement que le point $S'(z)$ est le point $\infty \in P_1(\mathbb{C})$.- De même, le transformé $S'(\infty)$ est $\frac{a}{c} \in \mathbb{C}$ si $c \neq 0$; si $c = 0$ (ce qui implique $a \neq 0$ puisque $ad - bc \neq 0$), c'est le point $\infty \in P_1(\mathbb{C})$.

C'est avec ces conventions qu'on peut dire que la "transformation homographique" (2) définit un homéomorphisme $P_1(\mathbb{C}) \longrightarrow P_1(\mathbb{C})$. Nous ferons toujours ces conventions.

L'application $S \longmapsto S'$, qui à chaque transformation (1) de $GL(2, \mathbb{C})$, associe la transformation (2) (définie par les mêmes valeurs de a, b, c, d) est un homomorphisme du groupe $GL(2, \mathbb{C})$ dans le groupe de tous les homéomorphismes de $P_1(\mathbb{C})$. L'image de cet homomorphisme s'appelle le groupe homographique, ou groupe projectif complexe à une variable ; on le notera $GLP(1, \mathbb{C})$. Insistons bien sur les deux faits suivants :

1º/ $GLP(1, \mathbb{C})$ est un sous-groupe du groupe de tous les homéomorphismes de $P_1(\mathbb{C})$ dans lui-même ;

2º/ On a un homomorphisme surjectif :

$$GL(2, \mathbb{C}) \longrightarrow GLP(1, \mathbb{C}) .$$

Cherchons maintenant le noyau de cet homomorphisme : c'est le sous-groupe de $GL(2, \mathbb{C})$ formé des transformations (1) telles que la transformation homographique (2) associée soit l'application identique. On doit donc, en particulier, avoir $\frac{az + b}{cz + d} = z$ quel que soit $z \in \mathbb{C}$ tel que $cz + d \neq 0$, d'où

$$az + b = z(cz + d), \quad \forall\, z \in \mathbb{C}$$

(même si $cz + d = 0$, par passage à la limite). Cette identité exige

$$c = 0, \quad b = 0, \quad d = a \neq 0.$$

Ces conditions nécessaires sont évidemment suffisantes pour que (2) soit l'identité. Elles expriment que la transformation (1) est une homothétie (de rapport complexe $\neq 0$). Ainsi le noyau de

$$GL(2, \mathbb{C}) \longrightarrow GLP(1, \mathbb{C})$$

est le sous-groupe des homothéties, groupe qui est isomorphe au groupe multiplicatif $\mathbb{C}^* = \mathbb{C} - \{0\}$. On a donc une suite exacte :

$$\boxed{(1) \longrightarrow \mathbb{C}^* \longrightarrow GL(2, \mathbb{C}) \longrightarrow GLP(1, \mathbb{C}) \longrightarrow (1).}$$

Remarque 1. Le sous-groupe des homothéties est contenu dans le centre de $GL(2, \mathbb{C})$; on montre facilement (exercice !) que c'est le centre.

Remarque 2. Deux transformations (1), définies respectivement par (a, b, c, d) et (a', b', c', d'), définissent la même transformation (2) si et seulement s'il existe un $\lambda \in \mathbb{C}^*$ tel que

$$a' = \lambda a, \quad b' = \lambda b, \quad c' = \lambda c, \quad d' = \lambda d$$

(c'est-à-dire si les deux systèmes (a, b, c, d) et (a', b', c', d') sont proportionnels).

L'isomorphisme $GLP(1, \mathbb{C}) \approx SL(2, \mathbb{C})/\{\pm 1\}$.

La surjection $GL(2, \mathbb{C}) \longrightarrow GLP(1, \mathbb{C})$ induit un homomorphisme

$$\varphi : SL(2, \mathbb{C}) \longrightarrow GLP(1, \mathbb{C}).$$

Rappelons que $SL(2, \mathbb{C})$ désigne le sous-groupe de $GL(2, \mathbb{C})$ formé des transformations dont le déterminant $ad - bc$ est égal à 1.

Je dis que φ est surjectif ; autrement dit, toute transformation homographique peut être définie par des constantes (complexes) a, b, c, d telles que $ad - bc = 1$. En effet, on peut multiplier a, b, c, d par un même nombre complexe $\lambda \neq 0$; alors $ad - bc$ est multiplié par λ^2. On peut choisir λ de façon que

$$\lambda^2(ad - bc) = 1,$$

car tout nombre complexe $\neq 0$ possède une racine carrée (et même deux).

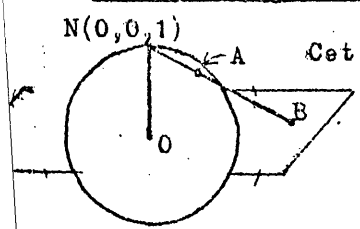
Quel est le noyau de l'homomorphisme surjectif φ ? Il se compose des $\lambda \in \mathbb{C}^*$ tels que $\lambda^2 = 1$, c'est-à-dire du sous-groupe $\{\pm 1\}$ de $\mathbb{C}^*$. D'où l'isomorphisme annoncé :

$$\boxed{GLP(1, \mathbb{C}) \approx SL(2, \mathbb{C})/\{\pm 1\}} \quad ;$$

il est entendu que $+1$ désigne l'homothétie de rapport $+1$, et -1 l'homothétie de rapport -1.

Exercice : Calculer l'inverse de $z \longmapsto \dfrac{az + b}{cz + d}$, lorsque $ad - bc = 1$ (on cherchera l'inverse de la matrice $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$).

Homéomorphisme de la droite projective complexe $P_1(\mathbb{C})$ et de la sphère S^2.



Cet homéomorphisme va être déduit de la "projection stéréographique". Celle-ci établit une correspondance bijective et bicontinue entre :

- le plan $\mathbb{C}$ de la variable complexe z ;

- et la sphère S^2 privée d'un point.

'une façon précise, soit S^2 la sphère-unité dans l'espace $\mathbb{R}^3$, dont nous appe-
ons les coordonnées x, y, u. Soit N le point $(0, 0, 1) \in S^2$ (pôle nord).
dentifions $\mathbb{C}$ au plan $u = 0$ de l'espace $\mathbb{R}^3$, en posant $x + iy = z$.

A chaque point $A \in S^2 - \{N\}$ associons l'unique point B du plan $u = 0$
ligné avec N et A ; réciproquement, à chaque point B du plan associons l'uni-
ue point $A \in S^2$ aligné avec N et B. La correspondance ainsi définie (projec-
ion stéréographique) est évidemment continue dans les deux sens : elle définit un
oméomorphisme de $\mathbb{C}$ sur $S^2 - \{N\}$. Un calcul élémentaire montre que le point B
ssocié à A (de coordonnées x, y, u telles que $x^2 + y^2 + u^2 = 1$, $u \neq 1$) est
éfini par

$$z = \frac{x + iy}{1 - u} = \frac{1 + u}{x - iy} \quad . \tag{3}$$

Inversement, le point A qui correspond au point B défini par $z \in \mathbb{C}$ est le point
(x, y, u) donné par les formules :

$$x + iy = \frac{2z}{z\bar{z} + 1} \quad , \quad u = \frac{z\bar{z} - 1}{z\bar{z} + 1} \quad . \tag{4}$$

Maintenant, si z tend vers ∞ (au sens de la topologie de $P_1(\mathbb{C})$), le point
$x, y, u)$ tend vers $(0, 0, 1)$, c'est-à-dire vers le point N ; et réciproquement
i A tend vers N, le point B tend vers l'infini. Donc <u>la correspondance se
rolonge en un homéomorphisme</u> θ <u>de</u> $P_1(\mathbb{C})$ <u>sur la sphère</u> S^2 <u>tout entière</u>.

Noter que S^2 est un espace compact et que cet homéomorphisme θ met donc en
vidence le fait que <u>la droite projective complexe</u> $P_1(\mathbb{C})$ <u>est un espace compact</u>.
a sphère S^2, munie de l'homéomorphisme θ de $P_1(\mathbb{C})$ sur S^2, s'appelle souvent
<u>sphère de Riemann</u> dans la théorie des fonctions holomorphes d'une variable complexe.

On sait que les sections planes de la sphère S^2 sont des cercles (pourvu que
plan rencontre S^2 et ne lui soit pas tangent). Demandons-nous quelles sont les
urbes de $P_1(\mathbb{C})$ qui, par l'homéomorphisme θ, correspondent aux cercles tracés
r S^2. La théorie classique de l'<u>inversion</u> dans l'espace $\mathbb{R}^3$ montre qu'on obtient
nsi :

- d'une part les droites (réelles) du plan $\mathbb{C}$ [droites dont chacune doit être complétée par le point $\infty \in P_1(\mathbb{C})$] ;

- d'autre part les cercles contenus dans $\mathbb{C}$.

C'est pourquoi nous appellerons, par abus de langage, cercles de $P_1(\mathbb{C})$ les courbes qui sont soient des cercles contenus dans $\mathbb{C}$, soient des droites de $\mathbb{C}$ complétées par le point à l'infini de $P_1(\mathbb{C})$. En somme, une droite est un cercle qui passe par le point ∞.

Avec cette convention, l'homéomorphisme θ établit une correspondance bijective entre les cercles de S^2 et les cercles de $P_1(\mathbb{C})$; aux cercles de S^2 passant par le pôle nord N correspondent les cercles de $P_1(\mathbb{C})$ passant par le point à l'infini.

Proposition. Le groupe projectif $GLP(1, \mathbb{C})$ (qui opère dans $P_1(\mathbb{C})$) transforme les cercles en cercles.

Démonstration. On veut montrer que la transformation

$$z \longmapsto \frac{az + b}{cz + d} \qquad (ad - bc \neq 0) \tag{2}$$

transforme tout cercle de $P_1(\mathbb{C})$ en un cercle. Regardons d'abord le cas où elle transforme ∞ dans ∞ ; on a déjà vu qu'il en est ainsi si et seulement si $c = 0$; alors (2) n'est autre qu'une translation

$$z \longmapsto z + h \qquad (h \in \mathbb{C}),$$

et il est clair que tout cercle est transformé en un cercle (une droite, c'est-à-dire un cercle passant par ∞, est transformée en une droite).

Supposons maintenant $c \neq 0$. On a

$$\frac{az + b}{cz + d} = \frac{a}{c} + \frac{bc - ad}{c^2} \cdot \frac{1}{z + \frac{d}{c}} \quad ;$$

donc la transformation (2) est composée des transformations suivantes :

$$\begin{cases} z \longmapsto z + \dfrac{d}{c} & \text{(translation)} \\ z \longmapsto \dfrac{k}{z} & \\ z \longmapsto z + \dfrac{a}{c} & \text{(translation)} \end{cases}$$

Il suffit donc de montrer que la transformation $z \longmapsto \frac{k}{z}$ $(k \neq 0)$ transforme tout cercle de $P_1(\mathbb{C})$ en un cercle. Or c'est la composée de

$$z \longmapsto \frac{k}{z} \quad \text{et} \quad z \longmapsto \bar{z} \ ;$$

la première est une inversion (plane) de pôle 0 et de puissance k, et la seconde une symétrie par rapport à l'axe réel. Il est clair que toutes ces transformations transforment cercles en cercles (avec la convention de langage faite sur le mot "cercle" dans $P_1(\mathbb{C})$). C.Q.F.D.

Exercice : montrer que le groupe $GLP(1, \mathbb{C})$ se compose de tous les produits d'un nombre pair de transformations, dont chacune est une inversion plane (de pôle quelconque) ou une symétrie par rapport à une droite quelconque. Les produits d'un nombre quelconque d'inversions ou de symétries forment un groupe G', qui contient comme sous-groupe G d'indice 2 le groupe $GLP(1, \mathbb{C})$. Les éléments de $G' - G$ sont les transformations

$$z \longmapsto \frac{a\bar{z} + b}{c\bar{z} + d} \qquad (ad - bc \neq 0) \ .$$

Définition. On appelle repère dans $P_1(\mathbb{C})$ un triplet (M_1, M_2, M_3) formé de points distincts (dont l'un peut être ∞).

Théorème. Etant donnés deux repères (M_1, M_2, M_3) et (M'_1, M'_2, M'_3), il existe une transformation $\sigma \in GLP(1, \mathbb{C})$ et une seule, telle que

$$\sigma(M_i) = M'_i \qquad \text{pour} \quad i = 1, 2, 3.$$

Démonstration. Il suffit de la faire lorsque (M'_1, M'_2, M'_3) est un repère particulier, par exemple $(0, \infty, 1)$. Si $M_2 \neq \infty$, on peut déjà trouver $\tau \in GLP(1, \mathbb{C})$ tel que $\tau(M_2) = \infty$; car si $z_2 \in \mathbb{C}$ représente M_2, on n'a qu'à prendre

$$\tau(z) = \frac{1}{z - z_2} \ .$$

Posons $\sigma_1 = \sigma \circ \tau^{-1}$; la recherche de σ équivaut à celle de σ_1 qui transforme $\tau(M_1), \tau(M_2), \tau(M_3))$ en $(0, \infty, 1)$. On est donc ramené au cas où $M_2 = \infty$. Changeant les notations, nous avons un triplet (z_1, ∞, z_3), et nous cherchons σ tel que

$$\sigma(\infty) = \infty, \qquad \sigma(z_1) = 0, \qquad \sigma(z_3) = 1.$$

La condition $\sigma(\infty) = \infty$ exprime que σ est de la forme

$$\sigma(z) = uz + v, \quad u \in \mathbb{C}, \quad v \in \mathbb{C}, \quad u \neq 0.$$

Les conditions $\sigma(z_1) = 0$, $\sigma(z_3) = 1$ équivalent alors à

$$uz_1 + v = 0, \qquad uz_3 + v = 1,$$

c'est-à-dire $u = \dfrac{1}{z_3 - z_1}$, $v = \dfrac{-z_1}{z_3 - z_1}$. Donc σ satisfaisant à (*) existe et est unique, ce qui prouve le théorème.

Remarque. Ayant choisi le repère initial $(0, \infty, 1)$, on voit que $GLP(1, \mathbb{C})$ est en correspondance bijective avec l'ensemble des repères (M_1, M_2, M_3). Or cet ensemble est doué d'une topologie, car c'est un ouvert de l'espace produit

$$P_1(\mathbb{C}) \times P_1(\mathbb{C}) \times P_1(\mathbb{C}).$$

Si on identifie $P_1(\mathbb{C})$ à la sphère S^2 comme plus haut, on voit que l'espace topologique $GLP(1, \mathbb{C})$ s'identifie à

$$S^2 \times S^2 \times S^2 - \Delta ,$$

où Δ désigne le sous-espace de $S^2 \times S^2 \times S^2$ formé des triplets de points non tous distincts. C'est une variété de dimension 6.

Revenons aux repères. Il est facile d'expliciter l'unique $\sigma \in GLP(1, \mathbb{C})$ qui transforme le repère (z_1, z_2, z_3) dans le repère $(0, \infty, 1)$, au moins lorsque z_1, z_2 et z_3 sont $\neq \infty$: c'est

$$\sigma(z) = \frac{z - z_1}{z - z_2} : \frac{z_3 - z_1}{z_3 - z_2} = \frac{z - z_1}{z - z_2} \cdot \frac{z_3 - z_2}{z_3 - z_1} .$$

On peut d'ailleurs donner un sens au second membre lorsque z_1, z_2 ou z_3 est ∞, en passant à la limite : pour $z_1 = \infty$ c'est $\dfrac{z_3 - z_2}{z - z_2}$, pour $z_2 = \infty$ c'est $\dfrac{z - z_1}{z_3 - z_1}$, pour $z_3 = \infty$ c'est $\dfrac{z - z_1}{z - z_2}$. Cela étant :

Théorème. Pour qu'il existe un $\tau \in GLP(1, \mathbb{C})$ tel que

$$\tau(z_i) = z'_i \qquad (i = 1, 2, 3, 4),$$

où (z_1, z_2, z_3, z_4) sont distincts (l'un d'eux pouvant être ∞), de même que (z'_1, z'_2, z'_3, z'_4), il faut et il suffit que :

(4) $$\boxed{\frac{z_4-z_1}{z_4-z_2} : \frac{z_3-z_1}{z_3-z_2} = \frac{z'_4-z'_1}{z'_4-z'_2} : \frac{z'_3-z'_1}{z'_3-z'_2}}$$

Démonstration. une condition nécessaire et suffisante est que l'unique τ tel que $\tau(z_i) = z'_i$ $(i = 1, 2, 3)$ transforme z_4 dans z'_4. Ou encore : si σ est défini par

$$\sigma(z_1, z_2, z_3) = (0, \infty, 1),$$

et σ' par $\sigma'(z'_1, z'_2, z'_3) = (0, \infty, 1)$, il faut et il suffit que $\sigma(z_4) = \sigma'(z'_4)$. Or $\sigma(z_4)$ et $\sigma'(z'_4)$ sont respectivement les deux membres de (4). D'où le théorème.

Définition. Etant donnés quatre points distincts z_1, z_2, z_3, z_4 de $P_1(\mathbb{C})$, on appelle birapport de ces quatre points le nombre complexe (fini)

$$\frac{z_4-z_1}{z_4-z_2} : \frac{z_3-z_1}{z_3-z_2}.$$

On le notera $(z_1 ; z_2 ; z_3 ; z_4)$. Le théorème 4 nous dit que toute transformation homographique conserve le birapport de 4 points distincts, et que réciproquement si deux quadruples de points distincts ont même birapport, il existe une transformation homographique (unique) qui transforme l'un dans l'autre.

Remarque. Le birapport $(z_1 ; z_2 ; z_3 ; z_4)$ dépend de l'ordre des 4 points. A titre d'exercice, on montrera que si $(z_1 ; z_2 ; z_3 ; z_4) = \rho$, et si l'on effectue sur z_1, z_2, z_3, z_4 les 24 permutations possibles, le birapport prend les 6 valeurs

$$\rho, \frac{1}{\rho}, 1-\rho, 1-\frac{1}{\rho}, \frac{1}{1-\rho}, \frac{\rho}{\rho-1},$$

qui sont en général distinctes. Etudier pour quelles valeurs de ρ elles ne sont pas distinctes. Dans le cas où elles sont distinctes, expliciter le groupe des 4 permutations sur z_1, z_2, z_3, z_4 qui ne changent pas le birapport.

Problème. A quelle condition doivent satisfaire les points z_1, z_2, z_3, z_4 pour que le birapport $(z_1 ; z_2 ; z_3 ; z_4)$ soit réel ? Il est facile de résoudre le problème : soit σ l'unique transformation homographique qui transforme (z_1, z_2, z_3) en $(0, \infty, 1)$; on a vu que

$$\sigma(z_4) = (z_1 ; z_2 ; z_3 ; z_4).$$

Posons $\sigma(z_4) = u$; la condition cherchée est donc que u soit réel. Or ceci exprime que u est sur le "cercle" de $P_1(\mathbb{C})$ qui passe par les points 0, 1 et ∞. La condition cherchée est donc : 0, ∞, 1 et u sont sur un même cercle. Mais comme σ transforme les cercles en cercles, on obtient :

Proposition. Pour que $(z_1 ; z_2 ; z_3 ; z_4)$ soit réel, il faut et il suffit que les points z_1, z_2, z_3, z_4 (supposés distincts) soient sur un même cercle de $P_1(\mathbb{C})$.

Applications holomorphes $P_1(\mathbb{C}) \longrightarrow P_1(\mathbb{C})$.

Définition. Une application $f : P_1(\mathbb{C}) \longrightarrow P_1(\mathbb{C})$ est dite holomorphe si :

1º/ elle est continue ;

2º/ f est holomorphe au voisinage de chaque point de $P_1(\mathbb{C})$.

Pour que cette définition soit satisfaisante, il reste à dire ce qu'on appelle application "holomorphe au voisinage d'un point" de $P_1(\mathbb{C})$. Pour cela, nous distinguerons plusieurs cas :

(1) soit z_o un point $\neq \infty$, donc $z_o \in \mathbb{C}$; et supposons de plus que $f(z_o) \neq \infty$. comme f est continue, il existe un voisinage U de z_o, tel que $f(z) \neq \infty$ pour tout $z \in U$. En restreignant f à U, on est donc ramené à dire quand une application continue $g : U \longrightarrow \mathbb{C}$ est holomorphe au voisinage d'un point $z \in U$. Mais ceci est une notion classique, supposée connue. On sait même ce que c'est qu'une g holomorphe $U \longrightarrow \mathbb{C}$ (c'est une g qui est holomorphe au voisinage de chaque point de U).

(2) soit toujours $z_o \neq \infty$, mais supposons $f(z_o) = \infty$. Posons $h(z) = \frac{1}{f(z)}$; h est une application continue $P_1(\mathbb{C}) \longrightarrow P_1(\mathbb{C})$, telle que $h(z_o) = 0$. Par définition, on dit que f est holomorphe au voisinage de z_o si h est holomorphe (au sens de (1)) au voisinage de z_o.

(3) supposons maintenant $z_o = \infty$, et posons $k(z) = f(\frac{1}{z})$; k est composée de $z \longmapsto \frac{1}{z}$ (transformation homographique $P_1(\mathbb{C}) \longrightarrow P_1(\mathbb{C})$ qui transforme 0 en ∞), et de f. Par définition, f est holomorphe au voisinage de $z_o = \infty$ si k est holomorphe au voisinage de 0 (au sens de (1) si $k(0) = f(z_o) \neq \infty$, au sens de (2) si $k(0) = f(z_o) = \infty$).

Tous les cas ayant été examinés, la définition est complète. On laisse au lecteur le soin de vérifier :

(a) si f est holomorphe au voisinage de z_0, alors il existe un ouvert $U \ni z_0$ tel que f soit holomorphe au voisinage de chaque point de U ;

(b) toute transformation homographique

$$\sigma(z) = \frac{az + b}{cz + d} \qquad (ad - bc \neq 0)$$

est holomorphe de $P_1(\mathbb{C})$ dans $P_1(\mathbb{C})$.

Définition. On appelle automorphisme holomorphe de $P_1(\mathbb{C})$ tout homéomorphisme $P_1(\mathbb{C}) \longrightarrow P_1(\mathbb{C})$ qui est holomorphe ainsi que l'homéomorphisme réciproque.

Ainsi : $GLP(1, \mathbb{C})$ est un groupe d'automorphismes holomorphes de $P_1(C)$.

Théorème. $GLP(1, \mathbb{C})$ est le groupe de tous les automorphismes holomorphes de $P_1(\mathbb{C})$

En d'autres termes : tout automorphisme holomorphe de $P_1(\mathbb{C})$ est homographique.

Démonstration.

1- Cas particulier :

Soit f un automorphisme holomorphe tel que $f(\infty) = \infty$. Alors $f(z) \neq \infty$ si $z \neq \infty$, puisque f est bijectif. f est donc une fonction holomorphe de $\mathbb{C}$ dans $\mathbb{C}$ si on retire le point ∞ ; f est donc développable en série entière dans tout le plan :

$$f(z) = \sum_{n \geq 0} a_n z^n$$

(le rayon de convergence étant infini).

Deux cas se présentent :

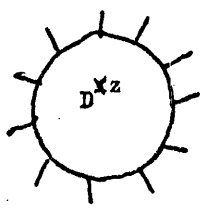
- ou bien il y a une infinité de $a_n \neq 0$; (1)
- ou bien il n'y a qu'un nombre fini de $a_n \neq 0$. (2)

(1) $\Longleftrightarrow$ ∞ est un "point singulier essentiel" ;

(2) $\Longleftrightarrow$ f est un polynôme.

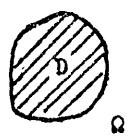
Nous admettons le :

Théorème de Weierstrass. Quand on a un point singulier essentiel et qu'on regarde les valeurs que prend la fonction dans un voisinage de ce point, alors l'image est un ensemble qui est dense dans tout le plan :



$$\overline{f(D - \{z\})} = \mathbb{C}.$$

Ici $z = \infty$, un voisinage de z est donc l'extérieur d'un cercle de rang aussi grand que l'on veut : voisinage de $\infty = D^c$, dont le complémentaire contient un ouvert non vide Ω.



Mais, f étant un isomorphisme, $f(D^c)$ ne rencontre pas l'ouvert non vide $f(\Omega)$, donc la propriété de Weierstrass ne peut pas arriver.

Conclusion : Le cas (1) (point singulier essentiel) ne se présente pas, donc $f(z)$ est un polynôme (évidemment non constant). D'après le théorème de d'Alembert, si $f(z)$ est un polynôme de degré n, f prend n fois chaque valeur a autre que les valeurs de f aux points où la dérivée $f'(z)$ s'annule. Comme f est bijective, ceci implique $n = 1$.

Conclusion. f est un polynôme de degré un : $f(z) = \alpha z + \beta$, $\alpha \neq 0$. Effectivement, un tel polynôme définit bien une application holomorphe $\mathbb{C} \longrightarrow \mathbb{C}$, dont l'application réciproque $z \longmapsto \frac{1}{\alpha} z - \frac{\beta}{\alpha}$ est holomorphe. Une telle transformation n'est autre qu'une transformation homographique qui laisse fixe le point ∞.

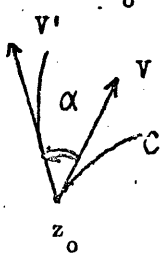
2- Cas général.

Supposons $f(\infty) = z_0 \neq \infty$. Considérons alors une transformation homographique g telle que $g(z_0) = \infty$ (par exemple $g(z) = \frac{1}{z - z_0}$). Alors $g \circ f(\infty) = \infty$, et on se trouve dans le cas particulier précédent : $h = g \circ f$ est linéaire, donc homographique. On a alors $f = g^{-1} \circ h$, où g^{-1} et h sont homographiques, donc f est bien une transformation homographique.

Ceci achève la démonstration du théorème.

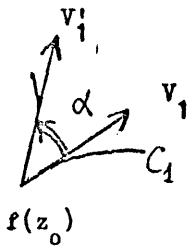
Propriété conforme des transformations holomorphes.

Soit z_o un point de $\mathbb{C}$; nous voulons étudier, au voisinage de z_o, la transformation définie par une fonction f holomorphe au voisinage de z_o, dans le cas où la dérivée $f'(z_o)$ est $\neq 0$. Par définition de la dérivée, on a



$$f(z_o + h) - f(z_o) = h(f'(z_o) + \varepsilon(h)),$$

avec $\lim_{h \to 0} \varepsilon(h) = 0$.



Si un point variable $z(t)$, fonction dérivable d'un paramètre réel t, décrit une courbe C passant au point z_o pour $t = t_o$, le vecteur tangent à cette courbe, en z_o, est défini par le nombre complexe $V = z'(t_o)$; la transformation f transforme la courbe C en une courbe C_1 définie par

$$t \longmapsto f(z(t)),$$

et le vecteur tangent V_1 à cette courbe au point $f(z_o)$ est $V_1 = f'(z_o).z'(t_o)$. On passe donc de V à V_1 par la multiplication par le nombre complexe non nul $f'(z_o)$. Donc V_1 se déduit de V par une multiplication par le scalaire $|f'(z_o)|$ et une rotation d'angle égal à $\arg f'(z_o)$.

Donc si on a deux courbes passant par z_o, dont les vecteurs tangents V et V' en z_o font entre eux un angle α, les vecteurs tangents V_1 et V'_1, au point $f(z_o)$, font entre eux le même angle α. On exprime ce fait en disant que la transforme f conserve les angles, ou est conforme. Il y a d'ailleurs plus : l'angle (V_1, V'_1) a la même orientation que l'angle (V, V') ; autrement dit, f est conforme et conserve l'orientation.

On a examiné le cas d'un point $z_o \in \mathbb{C}$, avec $f(z_o) \neq \infty$; le cas où $z_o = \infty$, ou celui où $f(z_o) = \infty$ se traiterait de même.

En conclusion, puisque la transformation $z \longmapsto \frac{az + b}{cz + d}$ est une transformation holomorphe, elle conserve les angles et l'orientation de $P_1(\mathbb{C})$. Grâce à l'homéomorphisme θ de $P_1(\mathbb{C})$ sur la sphère S^2 (qui lui aussi conserve les angles), on voit

que le groupe homographique $GLP(1, \mathbb{C})$ se traduit par des transformations conformes de la sphère de Riemann. En particulier, si deux cercles de S^2 se coupent suivant un angle, les cercles transformés se coupent suivant le même angle.

GROUPE $GL(2, \mathbb{R})$.

Supposons qu'on prenne seulement $GL(2, \mathbb{R})$ au lieu de $GL(2, \mathbb{C})$, et qu'on le fasse opérer par

$$\begin{cases} x \longrightarrow ax + by \quad , \quad a, b, c, d \in \mathbb{R}, \\ y \longrightarrow cx + dy \qquad ad - bc \neq 0. \end{cases}$$

On en déduit $z \longmapsto \frac{az + b}{cz + d}$, pour $z = \frac{x}{y}$. Ces dernières transformations forment un groupe noté $GLP(1, \mathbb{R})$, et on a une suite exacte :

$$(1) \longrightarrow \mathbb{R}^* \xrightarrow{\varphi} GL(2, \mathbb{R}) \longrightarrow GLP(1, \mathbb{R}) \longrightarrow (1)$$

$\varphi(a)$ = homothétie de rapport a; \\ quotient.

$GL(2, \mathbb{R})$ n'est pas connexe : $GL^+(2, \mathbb{R})$ est la composante connexe de l'identité. On notera $GLP^+(1, \mathbb{R})$ son image dans $GLP(1, \mathbb{R})$. Les transformations de $GLP^+(1, \mathbb{R})$ sont celles définies par a, b, c, d réels tels que $ad - bc > 0$. On a la suite exacte

$$(1) \longrightarrow \mathbb{R}^* \longrightarrow GL^+(2, \mathbb{R}) \longrightarrow GLP^+(1, \mathbb{R}) \longrightarrow (1).$$

$GLP^+(1, \mathbb{R})$ est le quotient d'un groupe connexe, il est donc connexe : c'est un sous-groupe d'indice 2 de $GLP(1, \mathbb{R})$.

Toute classe d'éléments de $GL^+(2, \mathbb{R})$ modulo le sous-groupe $\mathbb{R}^*$ des homothéties contient un élément tel que $ad - bc = 1$, c'est-à-dire un élément de $SL(2, \mathbb{R})$: car on peut toujours choisir u réel tel que $u^2(ad - bc) = 1$ lorsque $ad - bc > 0$. Il y a deux tels u.

L'application qui envoie $SL(2, \mathbb{R})$ sur $GLP^+(1, \mathbb{R})$ est donc encore surjective et on a la suite exacte

$$(1) \longrightarrow \{-1, +1\} \longrightarrow SL(2, \mathbb{R}) \longrightarrow GLP^+(1, \mathbb{R}) \longrightarrow (1).$$

$GLP^+(1, \mathbb{R})$ est donc isomorphe au quotient de $SL(2, \mathbb{R})$ par $\{-1, +1\}$: homothétie de rapport -1 et homothétie de rapport $+1$.

Ainsi toute transformation homographique du groupe $GLP^+(1, \mathbb{R})$ peut-être définie

par a, b, c, d réels tels que $ad - bc = 1$ (on peut alors remplacer a, b, c, d par -a, -b, -c, -d sans changer la transformation).

Nous noterons $P_1(\mathbb{R})$ la droite projective réelle, obtenue en adjoignant à $\mathbb{R}$ un point à l'infini ; on peut transposer à $P_1(\mathbb{R})$ ce qui a été dit pour $P_1(\mathbb{C})$. Mais ici la projection stéréographique définit un homéomorphisme de la droite projective $P_1(\mathbb{R})$ sur le cercle S^1. $P_1(\mathbb{R})$ est en correspondance bijective avec les droites du plan $\mathbb{R}^2$ qui passent par 0. En résumé, le groupe $GLP(1, \mathbb{R})$ est un groupe d'automorphismes de la droite projective $P_1(\mathbb{R})$.

Opérations de $GLP(1, \mathbb{R})$ dans $P_1(\mathbb{C})$.

$z \longmapsto \frac{az + b}{cz + d}$ opère aussi sur la variable complexe z (prenant éventuellement la valeur ∞). Le groupe $GLP(1, \mathbb{R})$ apparaît alors comme un sous-groupe du groupe $GLP(1, \mathbb{C})$ des automorphismes homographiques de $P_1(\mathbb{C})$. C'est le sous-groupe des homographies qui transforment $P_1(\mathbb{R})$ en lui-même [$P_1(\mathbb{R})$ étant identifié à un sous-espace de $P_1(\mathbb{C})$]. Si on interprète $P_1(\mathbb{R})$ comme un grand cercle de la sphère de Riemann, on voit qu'une transformation de $P_1(\mathbb{R})$ peut soit échanger les deux hémisphères, soit les conserver. Par la correspondance entre S^2 et $P_1(\mathbb{C})$ les deux hémisphères ouverts viennent respectivement sur demi-plan $\operatorname{Im} z > 0$ et sur le demi-plan $\operatorname{Im} z < 0$ du plan $\mathbb{C}$ de la variable complexe z. On a $\frac{ai+b}{ci+d} = \frac{(ai+b)\,(d-ci)}{c^2+d^2} = i\,\frac{ad - bc}{c^2+d^2} + \frac{ac + bd}{c^2+d^2}$.

Donc le transformé de i a pour partie imaginaire $i\,\frac{ad - bc}{c^2+d^2}$; ceci montre que lorsque $ad - bc > 0$, les deux demi-plans sont conservés ; lorsque $ad - bc < 0$, ils s'échangent. Ainsi :

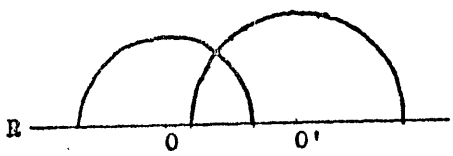
$GLP^+(1, \mathbb{R}) = \{$transformations qui conservent chaque demi-plan$\}$;

$GLP^-(1, \mathbb{R}) = \{$transformations qui échangent les deux demi-plans$\}$.

Posons $G = GLP^+(1, \mathbb{R})$, $G' = GLP(1, \mathbb{R})$, $GLP^-(1, \mathbb{R}) = G' - G$. Un élément de G transforme le $\frac{1}{2}$ plan inférieur en lui-même, le $\frac{1}{2}$ plan supérieur en lui-même. Si $z \in \mathbb{R}$, la dérivée de la transformation est $\frac{ad - bc}{(cz+d)^2} = \frac{1}{(cz+d)^2} > 0 \Longrightarrow$ la transformation conserve l'orientation de l'axe réel.

Si $ad - bc = -1$, alors la transformation homographique change le sens de parcours de l'axe réel, et échange le demi-plan supérieur avec le demi-plan inférieur.

Le demi-plan $\{\text{Im } z > 0\}$ est aussi appelé demi-plan de Poincaré. G transforme les cercles en cercles (ou droites). En particulier, si on prend un cercle centré sur $\mathbb{R}$, sa partie supérieure sera transformée en un demi-cercle supérieur centré sur $\mathbb{R}$, ou en une demi-droite orthogonale à l'axe réel (i.e. demi-cercle passant par l'infini) De même un cercle orthogonal à $\mathbb{R}$ qui passe par le point à l'infini se transforme en "cercle" orthogonal à $\mathbb{R}$.



Toutes ces transformations sont holomorphes et tous les points du demi-plan supérieur sont toujours transformés en points $\neq \infty$. (seuls les points réels peuvent se transformer dans le point ∞).

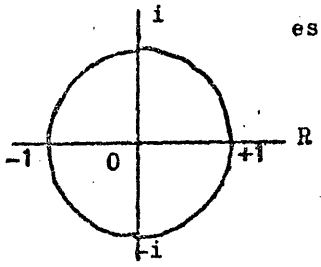
Théorème. Tout isomorphisme holomorphe f du demi-plan supérieur ouvert dans lui-même est une transformation homographique du type précédent : $a, b, c, d \in \mathbb{R}$, $ad - bc = 1$.

Démonstration : Soit f tel que $f(i) = i$. Supposons qu'on ait démontré (cf. lemme ci-dessous) que dans ce cas f est homographique. On va alors le prouver dans le cas général, comme suit. Le groupe homographique G est transitif dans le demi-plan supérieur, car on peut donc transformer i en n'importe quel point $u + vi$, $v > 0$. En effet il suffit de prendre $f(z) = u + vz$.

Ainsi, il existe $\sigma \in G$ tel que $\sigma(i) = f(i)$. Alors l'application $\tau = \sigma^{-1} \circ f$ laisse fixe i : $\tau(i) = i$. Mais τ est un automorphisme holomorphe donc, d'après ce qu'on a provisoirement admis, τ est une transformation homographique ; par conséquent $f = \sigma \circ \tau$, composée de deux transformations homographiques, est homographique. C.Q.F.D.

Lemme 1. Tout isomorphisme holomorphe f du demi-plan de Poincaré, tel que $f(i) = i$ est de la forme : $\frac{z - i}{z + i} \longmapsto e^{i\theta} \frac{z - i}{z + i}$. Posons $Z = \frac{z - i}{z + i}$; donc Z transforme les cercles en cercles. On veut savoir en quoi Z transforme le demi-plan supérieu

a) Cherchons le transformé de l'axe réel : nous savons que c'est un cercle ; il est donc déterminé par 3 points :



$$z = 0 \Longrightarrow Z = -1$$

$$z = \infty \Longrightarrow Z = +1$$

$$z = 1 \Longrightarrow Z = \frac{(1-i)^2}{2} = -i$$

$z \longmapsto Z$ transforme donc l'axe réel en le cercle unité.

b) Si $z = i$, alors $Z = 0$; donc le demi-plan supérieur est transformé par $z \longmapsto Z$ en l'intérieur du disque unité. Soit σ un automorphisme holomorphe du demi-plan supérieur. Alors si on pose $\tau(z) = \frac{z - i}{z + i}$, le composé $\tau \circ \sigma \circ \tau^{-1}$ est un automorphisme holomorphe du disque unité (le transformé de σ par τ).

De plus, les σ qui laissent fixe i sont ceux qui sont tels que $\tau \sigma \tau^{-1}$ laissent fixe 0. On est ainsi ramené à cherché les automorphismes holomorphes du disque unité (ouvert) qui laissent fixe 0. Alors le lemme 1 va évidemment être une conséquence du :

Lemme 2. Soit D le disque-unité ouvert. Si $g : D \longrightarrow D$ est un automorphisme holomorphe et si $g(0) = 0$, alors $g(Z) = e^{i\theta} Z$; autrement dit, g est une rotation autour du centre .

Démonstration du lemme 2.

1-Lemme de Schwarz : Soit $g : D \longrightarrow D$ une fonction holomorphe telle que $g(0) = 0$; alors $|g(z)| \leq |z|$ pour tout z tel que $|z| < 1$.

Démonstration : le développement de g en série entière montre que $g(z) = z\, h(z)$, où h est holomorphe dans D. Il suffira de montrer que $|h(z)| \leq 1$ pour $|z| < 1$. Supposons que $|z| = r < 1$. Alors $h(z) = \frac{g(z)}{z}$ est tel que $|h(z)| = \frac{|g(z)|}{r} \leq \frac{1}{r}$. Ceci reste vrai pour $|z| \leq r < 1$ car une fonction holomorphe au voisinage d'un disque compact atteint son maximum dans le disque sur le bord du disque. Donc pour $|z| \leq r < 1$ on a $|h(z)| \leq \frac{1}{r}$. Soit z_o tel que $|z_o| < 1$; prenons r tel que $|z_o| \leq r < 1$; on a $|h(z_o)| \leq \frac{1}{r}$. Donc à la limite $|h(z_o)| \leq 1$. C.Q.F.D.

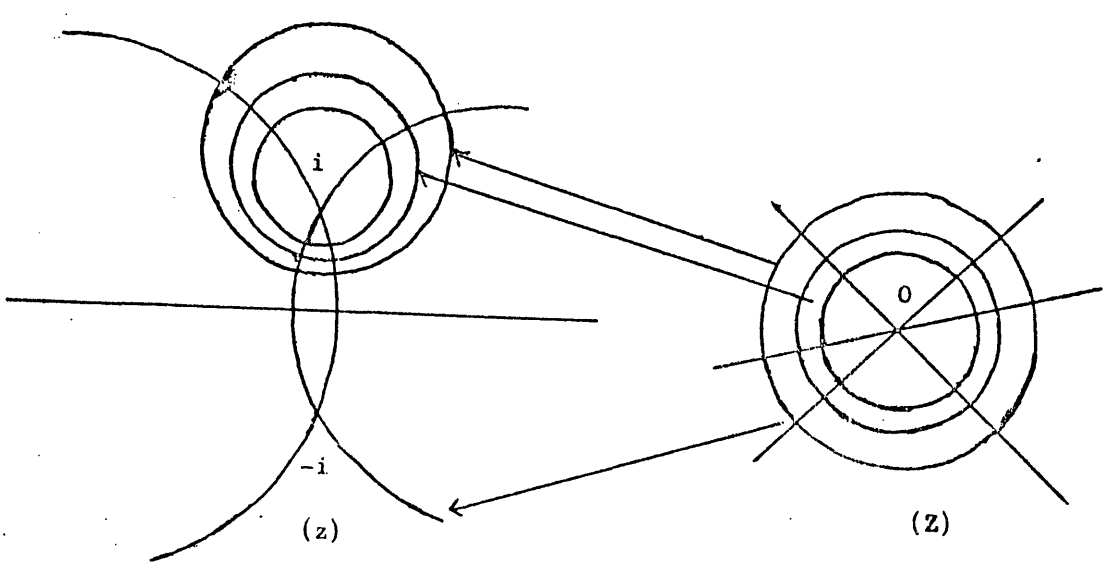
Remarque : la propriété $|g(z)| \leq |z|$ exprime que g transforme chaque disque centré en 0 dans lui-même.

2.- Appliquons le lemme de Schwarz à l'automorphisme $g : D \longrightarrow D$ tel que $g(0) = 0$. On a $|g(z)| \leq |z|$. Appliquons aussi le lemme de Schwarz à l'automorphis réciproque ; on trouve $|z| \leq |g(z)|$.

Conclusion : on a $|g(z)| = |z|$. Donc $\frac{g(z)}{z}$ est une fonction holomorphe ayant un module constant ; ceci implique que $\frac{g(z)}{z}$ est une constante de module 1, i.e: $g(z) = e^{i\theta} z$,

Résumé :

En géométrie euclidienne : les cercles concentriques de centre 0 sont ceux qui sont orthogonaux aux droites passant par 0, i.e. aux cercles passant par 0 et le point à l'infini. Transformons ceci à l'aide de $(z \longmapsto Z)^{-1}$, soit $Z \longmapsto i\,\frac{1+Z}{1-Z} = z$. Un cercle passant par 0 et l'infini se transforme en cercle passant par i et -i ; les cercles de centre 0 se transforment donc en les cercles du faisceau de Porcelet de points +i et -i (cercles orthogonaux aux cercles passant par i et -i)



Exercice : Le même raisonnement que précédemment montrerait que tout automorphisme holomorphe du disque est homographique :

$$z \longmapsto e^{i\theta} \frac{z - a}{1 - \bar{a} z} \quad , \quad \text{où} \quad a \in \mathbb{C}, \quad |a| < 1;$$

(ceci) est l'automorphisme holomorphe le plus général du disque unité.

CLASSIFICATION des TRANSFORMATIONS HOMOGRAPHIQUES à COEFFICIENTS REELS.

Soit $\tau(z) = \frac{az + b}{cz + d}$, où a, b, c, d $\in \mathbb{R}$, ad - bc = 1 (ou, plus généralement, ad - bc > 0). On cherche à déterminer comment opère τ dans le demi-plan de Poincaré Im z > 0.

Les "points doubles, ou points fixes de la transformation τ sont les points z tels que z' = z, soit z(cz + d) = az + b, ou encore

(1) $$cz^2 + (d-a) z - b = 0.$$

Les points fixes sont donc les solutions d'une équation du second degré à coefficients réels. Il a donc trois cas possibles :

1- deux points fixes z_0 et $\bar{z}_0$ imaginaires conjugués (par ex., $\mathrm{Im}(z_0) > 0$) : on peut supposer que c'est i et -i, car sinon il existe une transformation $\sigma \in \mathrm{GLP}^+(1, \mathbb{R})$ telle que $\sigma(i) = z_0$, $\sigma(-i) = \bar{z}_0$, et alors $\sigma^{-1} \circ \tau \circ \sigma$ a pour points fixes i et -i. On a vu que dans ce cas $\sigma^{-1} \circ \tau \circ \sigma$ est de la forme $\frac{z-i}{z+i} \longmapsto e^{i\theta} \frac{z-i}{z+i}$. On dit alors que τ est elliptique.

2- deux points fixes réels et confondus : on peut choisir σ de façon que les deux points fixes confondus de $\sigma^{-1} \circ \tau \circ \sigma$ soient le point ∞. Alors $\sigma^{-1} \circ \tau \circ \sigma$ est $z \longmapsto z + h$, $h \in \mathbb{R}$ (translation réelle). On dit alors que τ est parabolique.

3- deux points fixes réels et distincts ; on peut supposer que c'est 0 et ∞, en remplaçant τ par $\sigma^{-1} \circ \tau \circ \sigma$ pour un σ convenable. Pour que les racines de (1) soient 0 et ∞, il faut et il suffit que b = 0, c = 0 ; donc $\sigma^{-1} \circ \tau \circ \sigma$ est de la forme $z \longmapsto kz$ $(k > 0, k \neq 1)$: c'est une homothétie. On dit alors que τ est hyperbolique.

Recherche d'un invariant différentiel :

Soit $Z = \frac{az + b}{cz + d}$, $a, b, c, d \in \mathbb{R}$ $\quad ad - bc = 1$. On a $\frac{dZ}{dz} = \frac{1}{(cz + d)^2}$,

$$\operatorname{Im} Z = \operatorname{Im} \frac{(az + b)(\bar{cz} + d)}{|cz + d|^2} = \frac{\operatorname{Im} z\,(ad - bc)}{|cz + d|^2} = \frac{\operatorname{Im} z}{|cz + d|^2} .$$

Donc :

$$\boxed{\frac{|dZ|}{\operatorname{Im} Z} = \frac{|dz|}{\operatorname{Im} z}} \qquad (1)$$

On a trouvé quelque chose qui ne change pas quand on effectue sur z une transformation du groupe $GLP^+(1, \mathbb{R})$: c'est $\frac{|dz|}{\operatorname{Im} z}$. D'une façon plus explicite, supposons que z décrive une courbe de classe C^1 : $z = f(t)$, $t \in \mathbb{R}$. On a alors $Z = F(t) = \frac{a f(t) + b}{c f(t) + d}$, et (1) devient $\frac{|f'(t)|}{\operatorname{Im} f(t)} = \frac{|F'(t)|}{\operatorname{Im} F(t)}$. $|f'(t)|$ n'est autre que $\frac{ds}{dt}$, où ds désigne l'élément d'arc de la courbe décrite par $f(t)$; $\operatorname{Im} f(t) = y$ si $f(t) = z = x + iy$. Donc $\frac{ds}{y}$ est un invariant différentiel des courbes du demi-plan de Poincaré ; c'est un invariant vis-à-vis du groupe homographique $G = GLP^+(1, \mathbb{R})$. ds est l'élément de longueur euclidien, $d\sigma = \frac{ds}{y}$ est le nouvel élément de longueur. Lorsqu'on multiplie les longueurs par $\frac{1}{y}$, les aires sont multipliées par $\frac{1}{y^2}$; donc $\frac{dx \wedge dy}{y^2}$ sera le nouvel élément d'aire : il est invariant par G. [$dx \wedge dy$ est l'élément d'aire euclidien].

On va donc avoir une nouvelle géométrie : géométrie (non euclidienne) du demi-plan de Poincaré.

Considérons un arc de courbe $z(t) = f(t) + ig(t)$ de classe C^1 $(t \in [0, 1])$, avec $g(t) > 0$. La nouvelle "longueur" de cet arc de courbe sera

$$\int_0^1 \frac{\sqrt{f'^2 + g'^2}}{g(t)}\, dt,$$ alors que sa longueur euclidienne est $$\int_0^1 \sqrt{f'^2 + g'^2}\, dt.$$

La longueur non-euclidienne est invariante par toute transformation de $G = GLP^+(1, \mathbb{R})$.

"Plus court chemin" d'un point à un autre.

Appelons droite non euclidienne, ou simplement "droite" (entre guillemets) toute demi-droite verticale (orthogonale à l'axe réel) du demi-plan de Poincaré, ou tout demi-cercle orthogonal à l'axe réel. Autrement dit, une "droite" est l'intersection

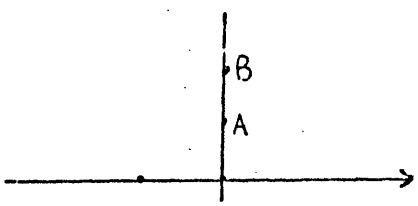
orthogonal à $P_1(\mathbb{R})$

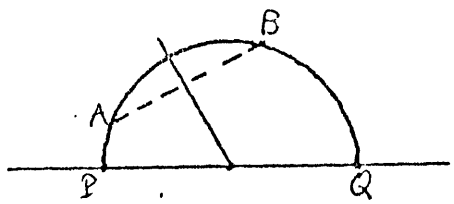
du demi-plan de Poincaré avec un cercle de $P_1(\mathbb{C})$ (passant ou non par le point ω).

Il est clair que le groupe $G = PLG^+(1, \mathbb{R})$ transforme toute "droite" en "droite".

Soient A et B deux points distincts du demi-plan de Poincaré. Par A et B il passe une "droite" et une seule, à savoir :

- la demi-droite verticale joignant A et B si A et B ont même abscisse ;
- l'unique cercle euclidien centré sur l'axe réel, et passant par A et B dans le cas contraire.





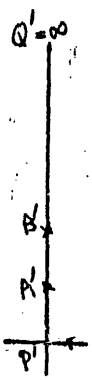
Définition. On appelle distance non euclidienne de A et B, et on notera $d(A, B)$, la "longueur" non euclidienne du "segment de droite" joignant A et B. On sait d'avance que cette distance est invariante par le groupe G : si $\sigma \in G$, on a

$$d(\sigma(A), \sigma(B)) = d(A, B).$$

On se propose de calculer effectivement $d(A, B)$ à l'aide des données euclidiennes de la situation.

1er cas A et B ont même abscisse x. Alors, en posant $y(A) = a$, $y(B) = b$, et supposant par exemple $a < b$, on a

$$d(A, B) = \int_a^b \frac{dy}{y} = \log \frac{b}{a} .$$



2eme Cas. (Cas général). Soient P et Q les points où le cercle orthogonal à l'axe réel et passant par A et B coupe l'axe réel (voir figure). Nous fixons le choix de P et Q en convenant que si l'on parcourt continûment le demi-cercle en partant de P et allant vers Q, on rencontre d'abord A et ensuite B. Par une transformation de G, on se ramène au cas où A et B sont sur une même verticale [par exemple, faire une transformation elliptique convenable σ ayant A pour point fixe, et transformant le cercle de diamètre PQ en la verticale du point A].

Si l'ordonnée de $B' = \sigma(B)$ est plus grande que celle de $A' = \sigma(A)$, P vient en $P' = \sigma(P)$ d'ordonnée nulle, Q vient en $Q' = \sigma(Q)$ à l'infini. On a, d'après le 1er cas, $$d(A', B') = \log \frac{b'}{a'} = \log (0 ; \infty ; a' ; b').$$

Ceci est le log du rapport anharmonique $(P' ; Q' ; A' ; B')$ des quatre points P', Q', A', B'. Mais comme σ conserve le rapport anharmonique, c'est aussi égal à

$$\log(P ; Q ; A ; B).$$

En résumé, on a dans tous les cas

$$\boxed{d(A, B) = \log(P ; Q ; A ; B)} ,$$

où P et Q sont les points de rencontre avec l'axe réel de la "droite" joignant A et B (avec la convention que P et Q ont été choisis de façon qu'il existe un sens de parcours sur la "droite" dans lequel on rencontre successivement P, A, B, Q).

Théorème. Pour tout arc de courbe de classe C^1, contenu dans le demi-plan de Poincaré, d'origine A et d'extrémité B, la "longueur" non euclidienne $\widehat{AB}$ de cet arc de courbe est $\geq d(A, B)$; elle ne lui est égale que si l'arc de courbe est le "segment de droite" d'origine A et d'extrémité B.

On exprime cette propriété en disant brièvement que "le segment de droite est le plus court chemin d'un point à un autre".

Démonstration. On peut supposer A et B sur une même verticale (sinon, faire une transformation $\sigma \in G$ convenable). Alors, si l'arc de courbe est

$$t \longmapsto f(t) + ig(t), \quad f \text{ et } g \text{ de classe } C^1$$

pour $t \in [0, 1]$, $g(t) > 0$ pour tout t, et si l'ordonnée b de B est plus grande que l'ordonnée a de A, on a

$$\widehat{AB} = \int_0^1 \frac{\sqrt{f'^2 + g'^2}}{g(t)}\, dt \geq \int_0^1 \frac{|g'(t)|}{g(t)}\, dt \geq \int_0^1 \frac{g'(t)}{g(t)}\, dt =$$

$$= \log \frac{g(1)}{g(0)} = \log \frac{b}{a} = d(A, B).$$

L'égalité ne peut avoir lieu que si, pour tout t, on a

$$\sqrt{(f'(t))^2 + (g'(t))^2} = g'(t).$$

ce qui exige $f'(t) = 0$ et $g'(t) \geq 0$; ceci exprime que $f(t)$ est constant, et que $g(t)$ croît de a à b.

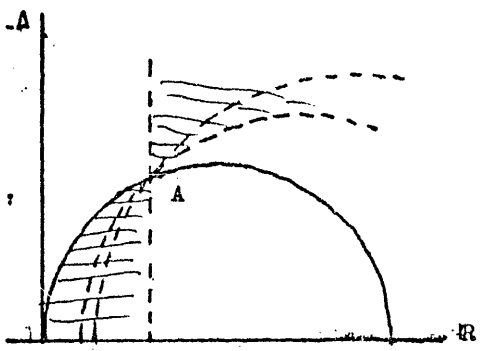
Remarque : le théorème reste valable pour un arc de courbe qui est de classe C^1 par morceaux, par exemple, pour une "ligne brisée" formée de "segments de droite". On en déduit aussitôt :

Corollaire. Soient A et B deux points distincts. Si un point C n'est pas sur le "segment de droite" joignant A et B, on a l'inégalité stricte :

$$d(A, B) < d(A, C) + d(C, B).$$

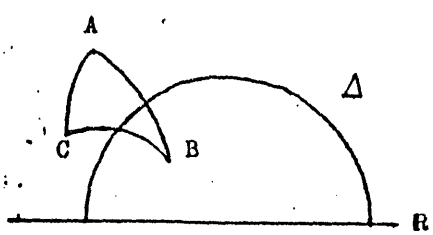
Remarque importante.

Dans notre nouvelle géométrie, la notion de parallélisme n'est plus une relation d'équivalence :



Soit A un point donné et Δ une demi-droite verticale ne passant pas par A. Regardons toutes les "droites" qui passent par A et qui ne rencontrent pas Δ ; le cercle qui passe par A et qui est tangent à Δ ne coupe pas Δ (dans le demi-plan de Poincaré) ; on voit que toutes les "droites" qui passent par A et qui sont dans l'angle hachuré ne rencontrent pas Δ : il y a donc une infinité de "droites" parallèles de Δ passant par A.

Signification de : Une "droite" Δ partage le plan en deux régions.



Soient deux points A et B et une "droite" Δ ne contenant ni A ni B. Il y a alors deux possibilité :

a) le "segment" $[A, B]$ coupe Δ ;

b) le "segment" $[A, B]$ ne coupe pas Δ .

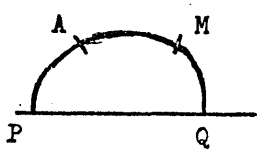
On constate que si $[A, B]$ et $[B, C]$ coupent Δ (C étant un troisième point $\notin \Delta$) alors $[A, C]$ ne coupe pas Δ (faire par exemple la figure en supposant que Δ est une demi-droite verticale).

Ceci prouve que la relation, pour un couple de points A, B hors de Δ : "le segment $[A, B]$ ne coupe pas Δ " est une relation d'équivalence dans le complémentaire de Δ. Il y a deux classes d'équivalence : les deux composantes connexes du complémentaire de Δ.

"Demi-droites".

Si on prend un point A sur une "droite" Δ, il partage cette "droite" en deux régions, à savoir les deux composantes connexes de $\Delta - \{A\}$. Deux points M et M' de $\Delta - \{A\}$ sont dans la même région si et seulement si A $\notin$ segment [M,M'] .

Ces deux régions s'appellent les deux "demi-droites" d'origine A. Etant donné une demi-droite AQ issue de A , on peut porter sur cette demi-droite une "longueur" égale à un nombre $d > 0$ arbitraire ; cela signifie qu'il existe, sur la demi-droite, un point M et un seul tel que $d(A, M) = d$, c'est-à-dire

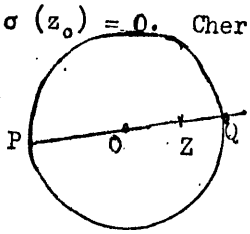


$$\log (P ; Q ; A ; M) = d$$

En effet, lorsque M décrit l'arc AQ, la distance d (A,M) croît strictement de 0 à $+\infty$, et prend donc une fois et une seule toute valeur > 0 .

"Cercles".

Considérons maintenant l'ensemble Γ des points du demi-plan de Poincaré qui à une "distance" donnée d d'un point donné z_0 ($\operatorname{Im} z_0 > 0$). On l'appelle, par définition, le "cercle" de "centre" z_0 et de "rayon" d . On sait qu'il existe une transformation homographique σ du demi-plan sur le disque $|Z| < 1$, telle que $\sigma(z_0) = 0$. Cherchons $\sigma(\Gamma)$: c'est l'ensemble des points Z tels que



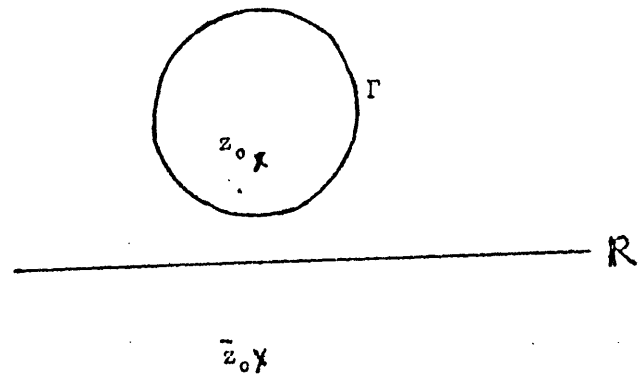
$$d(O, Z) = d$$

avec $d(O, Z) = \log (P ; Q ; O ; Z) = \log \frac{1+x}{1-x}$,

x désignant la distance euclidienne de O à Z. Donc

$$x = \frac{e^{d}-1}{e^{d}+1} ,$$

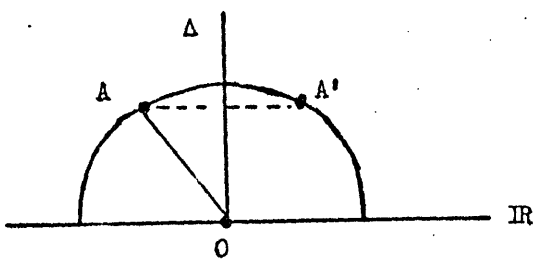
et $\sigma(\Gamma)$ est donc le cercle euclidien de centre 0 et de rayon $\frac{e^d - 1}{e^d + 1}$. Par σ^{-1}, ce cercle est transformé en un cercle (contenu dans le demi-plan de Poincaré Im $z > 0$) du faisceau dont les points de Poncelet sont z_o et $\bar{z}_o$.



Un problème de construction.

Soient donnés une "droite" Δ et un point $A \notin \Delta$. On va montrer qu'il passe par A une "droite" Δ' et une seule qui coupe Δ suivant un angle droit (i.e : qui est orthogonale à Δ au point de rencontre de Δ et Δ').

Par un automorphisme $\sigma \in GLP^+(1, \mathbb{R})$, on se ramène au cas où Δ est une demi-droite euclidienne verticale. Une "droite" orthogonale à Δ n'est autre chose qu'un demi-cercle euclidien centré au point de rencontre 0 de Δ avec l'axe réel. On cherche un tel cercle, assujetti en outre à la condition de passer par A. Il est clair qu'il y a une solution unique.



Angles de demi-droites.

Soit A un point du demi-plan de Poincaré. Notons G_A le groupe d'isotropie du point A, c'est-à-dire le sous-groupe de G formé des homographies σ telles que $\sigma(A) = A$. Ce groupe est isomorphe à SO (2). Pour le voir, nous transformons la situation, au moyen d'une homographie τ qui transforme le demi-plan Im $z > 0$ en le disque ouvert $|Z| < 1$, et le point A dans le centre $Z = 0$. Le groupe transformé $\tau\, G_A\, \tau^{-1}$ est le groupe des automorphismes holomorphes du disque-unité qui laissent fixe le centre, i.e : $Z \mapsto e^{i\theta} Z$.

Ce groupe est bien isomorphe à $U(1) = SO(2)$. C.Q.F.D.

Le groupe G_A opère d'une façon simplement transitive dans l'ensemble des "demi-droites" d'origine A : c'est évident si on regarde le groupe $\tau\, G_A\, \tau^{-1}$. Soient donnés deux couples (D,D') et (D_1, D_1') de demi-droites d'origine A ; pour que les "angles orientés" (D,D') et (D_1,D_1') soient "égaux", c'est-à-dire pour qu'il existe un $\sigma \in G_A$ tel que

$$\sigma(D) = D_1, \quad \sigma(D') = D_1',$$

il faut et il suffit que l'unique $\alpha \in G_A$ tel que $\alpha(D) = D'$ soit égal à l'unique $\alpha_1 \in G_A$ tel que $\alpha_1(D_1) = D_1'$ [Exercice : (le) démontrer, en utilisant le fait que le groupe G_A est commutatif]. Ainsi, lorsqu'on associe à chaque couple (D,D') l'élément $\alpha \in G_A$ tel que $\alpha(D) = D'$, on voit que α caractérise une classe d'angles "égaux" entre eux. C'est pourquoi le groupe $G_A \simeq SO(2)$ s'appelle aussi le groupe des angles (orientés) de demi-droites d'origine A.

On ne doit pas confondre l'élément de $SO(2) \simeq U(1)$ associé ainsi à un angle, avec ce qu'on appelle improprement la mesure de cet angle. Le problème de la mesure des angles est un autre problème (aussi bien en géométrie euclidienne que dans la géométrie du demi-plan de Poincaré). On démontre que l'application $t \mapsto e^{it}$ est un homomorphisme (me) surjectif $\varphi : \mathbb{R} \longrightarrow U(1)$, dont le noyau se compose du groupe additif des multiples entiers de 2π. Etant donné un élément $\alpha \in U(1)$, $\varphi^{-1}(\alpha)$ se compose d'une classe de nombres réels définis module 2π ; c'est cette classe qu'on appelle la mesure de l'angle associé à α. On aurait d'ailleurs d'autres mesures en considérant l'homomorphisme

$$t \mapsto e^{ikt},$$

où $k \in \mathbb{R} - \{0\}$ est arbitraire. Parmi toutes ces "mesures", la première

$$t \mapsto e^{it} = \cos t + i \sin t$$

présente cette particularité que c'est une fonction $\mathbb{R} \to \mathbb{C}$ dont la dérivée est égale à

$$i\, e^{it} = \sin t + i \cos t$$

Autrement dit :

$$\frac{d}{dt}(\cos t) = -\sin t, \quad \frac{d}{dt}(\sin t) = \cos t$$

Il faut bien insister sur le fait que cos t et sin t sont des fonctions d'une variable réelle t.

Le radian est l'angle de mesure 1, c'est-à-dire l'angle associé à l'élément $e^i \in U(1)$.

Elément d'aire.

On a déjà défini l'élément d'aire (non euclidienne)

$$\iint \frac{dx \wedge dy}{y^2} .$$

Etant donné un ensemble fermé F du demi-plan de Poincaré H, la valeur de l'intégrale

$$\iint_F \frac{dx \wedge dy}{y^2}$$

(supposée convergente) s'appellera l'"aire" de F.

On se propose de calculer l'"aire" d'un "triangle". Qu'entend-on par "triangle" ? Soient A, B, C trois points distincts non alignés (c'est-à-dire non situés sur une même "droite"). On leur associe les "segments" [A,B] [B,C] [C,A] dont la réunion partage le demi-plan H en deux régions ; l'une d'elles est bornée, autrement dit son adhérence F est compacte. Par définition l'"aire" de F s'appelle l'"aire du triangle" ; nous la noterons S (A B C).

On notera $\hat{A}$, $\hat{B}$, $\hat{C}$ les mesures des angles du triangle :

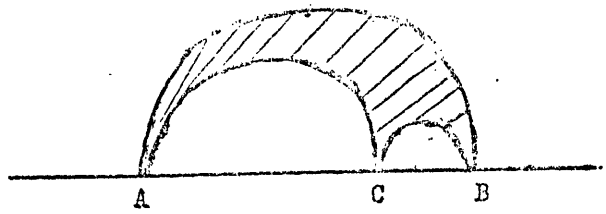
$$0 < \hat{A} < \pi, \quad 0 < \hat{B} < \pi, \quad 0 < \hat{C} < \pi.$$

Théorème. On a

(1) $$\boxed{\hat{A} + \hat{B} + \hat{C} = \pi - S(A\ B\ C)}$$

(donc la somme des mesures des angles d'un "triangle" est toujours $< \pi$, et l'"aire" d'un "triangle" est toujours $< \pi$).

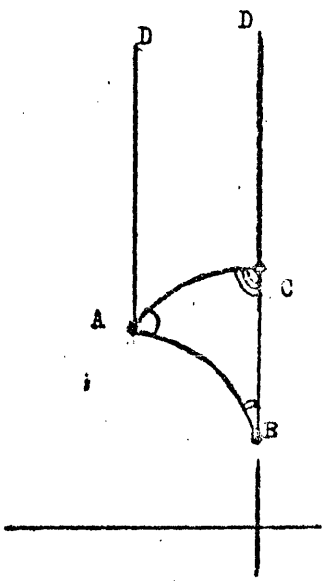
On va même prouver une proposition un peu plus générale, en n'excluant pas le cas où l'un des sommets du "triangle", A par exemple, serait sur l' axe réel ; alors on a évidemment $\hat{A} = 0$; on peut même envisager des "triangles" ayant deux ou trois sommets sur l'axe réel (figure).



On montrera que la formule (1) est encore valable dans ce cas.

Démonstration de (1) : on peut supposer que la "droite" joignant B et C est une demi-droite euclidienne orthogonale à l'axe réel, puisque l'"aire" et les angles sont invariants par toute transformation homographique

$$z \mapsto \frac{az + b}{cz + d} \quad , \ a, b, c, d \text{ réels}, \ ad - bc = 1.$$



Supposons par exemple que l'ordonnée de C soit plus grande que celle de B [On n'exclut pas le cas où l'ordonnée de B est 0, ni celui où l'ordonnée de C est infinie]. Menons par A la verticale ascendante A D (D étant à l'infini) ; D est aussi le point à l'infini sur la verticale ascendante du point C.

Considérons les "triangles" ABD et ACD ; on a

$$S(ABC) = S(ABD) - S(ACD).$$

Supposons que la formule (1) soit déjà démontrée pour les triangles ABD et ACD ayant un sommet D à l'infini, c'est-à-dire

$$(2) \qquad \widehat{DAB} + \widehat{ABD} = \pi - S(ABD)$$

$$(3) \qquad \widehat{DAC} + \widehat{ACD} = \pi - S(ACD)$$

Retranchons membre à membre la relation (2) de (3); il vient

$$(4) \qquad \widehat{DAC} - \widehat{DAB} + \widehat{ACD} - \widehat{ABD} = S(ABC).$$

Or

$$\widehat{DAC} - \widehat{DAB} = - \widehat{CAB} = - \hat{A},$$

$$\widehat{ACD} = \pi - \widehat{ACB} = \pi - \hat{C},$$

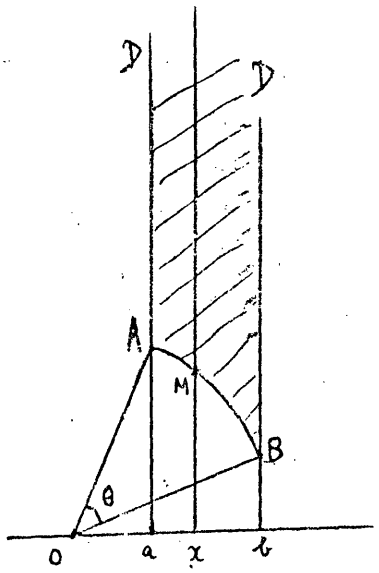
$$\widehat{ABD} = \widehat{ABC} = \hat{B},$$

donc (4) s'écrit

$$\pi - \hat{A} - \hat{B} - \hat{C} = S(ABC),$$

ce qui donne la relation (1) à démontrer.

En résumé, il suffit de démontrer (2) et (3) ; la démonstration est la même (dans les deux cas il s'agit d'un "triangle" ayant un sommet à l'infini). Faisons par exemple la démonstration de (2).



$$\mathcal{S}(ABD) = \iint_{ABD} \frac{dx \wedge dy}{y^2}$$

Soient a et b les abscisses de A et B, en supposant par exemple $a < b$. On a

$$S(ABD) = \int_a^b dx \int_{y(M)}^{+\infty} \frac{dy}{y^2} ,$$

en notant M le point de l'arc $\overset{\frown}{AB}$ d'abscisse x, et y(M) l'ordonnée de ce point. Or

$$\int_{y(M)}^{+\infty} \frac{dy}{y^2} = \left[-\frac{1}{y}\right]_{y(M)}^{+\infty} = \frac{1}{y(M)} , \text{ d'où}$$

$$S(ABD) = \int_a^b \frac{dx}{y(M)} .$$

Prenons une représentation paramétrique de l'arc de cercle :

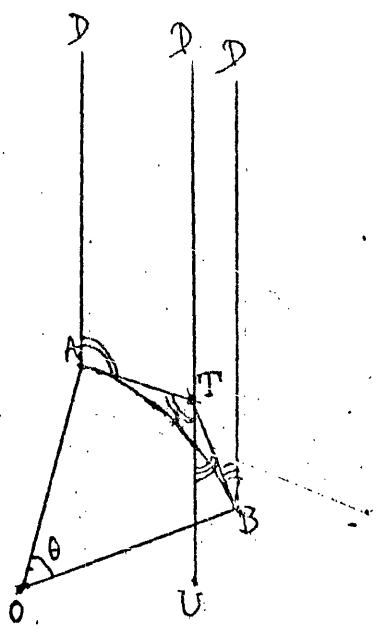
$x = r \cos t$, $y = \sin t$,

t décroissant de t_1 à t_0 , $\cos t_1 = a$, $\cos t_0 = b$.

Alors

$$S(ABD) = -\int_{t_0}^{t_1} \frac{-r \sin t \, dt}{r \sin t} = \int_{t_0}^{t_1} dt = \theta,$$

θ étant la mesure de l'angle $\widehat{AOB}$.



Or soit T l'intersection des tangentes en A et B ; la mesure de $\widehat{ATB}$ est $\pi - \theta$. Soit TU la verticale descendante ; on a

$$\widehat{DAB} = \widehat{DAT} , \quad \widehat{ABD} = \widehat{TBD},$$

$$\pi - \theta = \widehat{ATU} + \widehat{UTB} = \widehat{DAT} + \widehat{TBD},$$

d'où finalement la relation (2) à démontrer.

Ceci achève la démonstration du théorème.

Le groupe des isométries du demi-plan de Poincaré.

Notons H le demi-plan de Poincaré, muni de la "distance" $d(A,B)$.

Définition : on appelle isométrie de H une application $f : H \to H$ qui conserve la distance, c'est-à-dire satisfait à

$$d(f(A), f(B)) = d(A, B), \forall A, B \in H .$$

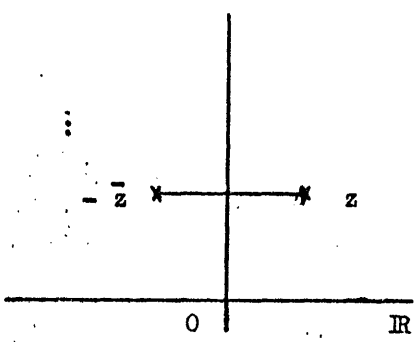
Une telle application est évidemment injective, car

$$f(A) \neq f(B) \Rightarrow d(f(A), f(B)) > 0 \Rightarrow d(A,B) > 0 \Rightarrow A \neq B.$$

Elle est continue, car la "distance" définit évidemment la topologie de H (engendrée par les "cercles" de centre donné).

Exemple d'isométries : le groupe G des transformations

$$z \mapsto \frac{az + b}{cz + d} \quad , a, b, c, d \text{ réels, } ad-bc>0$$



se compose d'isométries, puisque la "distance" $d(A, B)$ a été définie de façon à être invariante par G. De plus, $z \mapsto -\bar{z}$ (transformation de H dans H) est évidemment une isométrie. Comme la composée de deux isométries est une isométrie, le groupe G' engendré par G et $z \mapsto \bar{z}$ est un groupe d'isométries. On voit que G' - G se compose des transformations

$$z \mapsto \frac{a\bar{z} + b}{c\bar{z} + d} \quad , a, b, c, d \text{ réels, } ad - bc < 0.$$

Remarque : les transformations de G conservent l'orientation, celles de G' - G la changent.

On démontrera plus loin que toute isométrie appartient à G'. Cela résultera d'une étude plus approfondie du groupe G' et de son sous-groupe G d'indice 2.

Proposition 1. Un $\sigma \in G$ qui laisse fixes deux points distincts A et B est l'identité.

Démonstration : Le groupe d'isotropie G_A opère d'une façon simplement transitive dans l'ensemble des demi-droites d'origine A. Donc si $\sigma \in G_A$ et si σ laisse fixe $B \neq A$, on a $\sigma = id$.

Proposition 2. Etant donnés deux points distincts A et B, il existe un unique $\tau \in G' = G$ tel que

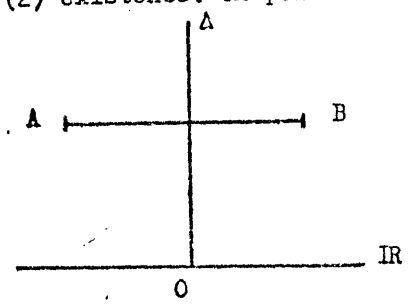
$$\tau(A) = B, \quad \tau(B) = A ;$$

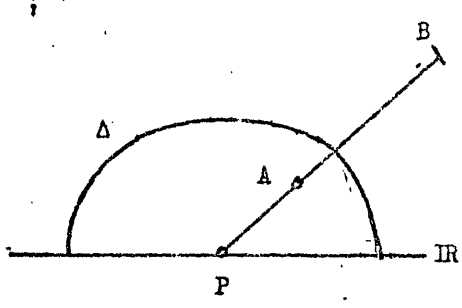
on a de plus $\tau^2 = id$.

Démonstration : (1) unicité. Si on a aussi $\tau_1 \in G' - G$, $\tau_1(A) = B$, $\tau_1(B) = A$, alors $\tau_1 \circ \tau \in G$; $\tau_1 \circ \tau$ laisse fixes A et B, donc (prop. 1) $\tau_1 \circ \tau = id$. Ceci vaut en particulier si $\tau_1 = \tau$, d'où $\tau^2 = id$, c'est-à-dire $\tau = \tau^{-1}$. Donc

$$\tau_1 \circ \tau^{-1} = id. \Rightarrow \tau_1 = \tau$$

(2) existence. On peut se ramener au cas où A et B sont sur une même horizontale. Le segment AB possède alors une médiatrice euclidienne Δ, et par translation on se ramene cas où Δ passe par O. Alors la transformation τ définie par $\tau(z) = -\bar{z}$ (symétrie par rapport à Δ) répond à la question. Dans le cas général, le τ cherché est l'inversion de pôle P qui échange A et B, i.e. dont la puissance est $\overline{PA}.\overline{PB}$; une telle inversion est bien un élément de G' (le vérifier). Les points fixes de τ forment une "droite" Δ qui est le cercle d'inversion, i.e. le cercle de centre P et de rayon $k = \sqrt{\overline{PA}.\overline{PB}}$.

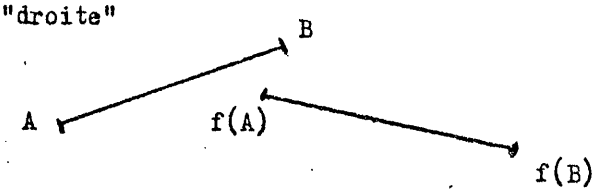




On vérifie à nouveau que τ est bien involutif ($\tau^2 = 1$). Δ est l'ensemble des points "équidistants" de A et B.

Remarque : Faisons une autre démonstration qui prouve que si un $\tau \in G' - G$ laisse fixes deux points distincts A et B les points fixes de τ forment une "droite".

Lemme. Soit $f : H \to H$ une isométrie. Alors f transforme bijectivement toute "droite" en "droite"



En effet, supposons que M soit sur le "segment" [A, B] ; alors f (M) est sur le "segment" [f(A), f (B)], car

d (A,B) = d (A,M) + d (M,B) ; or

$$\left.\begin{array}{l} d\,(A,B) = d\,[f(A),\ f(B)] \\ d\,(A,M) = d\,[f(A),\ f(M)] \\ d\,(M,B) = d\,[f(M),\ f(B)] \end{array}\right\} \Rightarrow$$

$d\,[f(A),\ f(B)] = d\,[f(A),\ f(M)] + d\,[f(M),\ f(B)] \iff f(M) \in [f(A),\ f(B)]$.

Si M' n'est pas sur le "segment" [A,B] mais sur la "droite" AB, alors ou bien B est sur le "segment" [A,M'], ou bien A est sur le segment [B,M']; on constate donc que f (A), f (B) et f (M') sont "alignés".

D'autre part, la correspondance entre les deux "droites" est bijective, car nous savons que sur une "demi-droite" il existe un point et un seul qui est à une distance donnée de l'origine de cette "demi-droite".

Proposition . Si $\tau \in G' - G$ échange deux points distincts A et B de H, l'ensemble des points fixes de τ est une "droite" Δ ; c'est l'ensemble des points "équidistants" de A et B.

Démonstration : soit M le "milieu" du "segment" [A, B], à savoir l'unique point M de la "droite" A B tel que $d\,(M,A) = d\,(M,B)$.

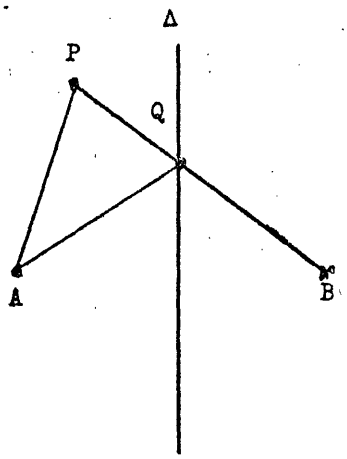
τ transforme la "droite" AB en elle-même, et M en l'unique point de cette droite tel que $d\,(\tau(M),B) = d\,(\tau(M),A)$. Ainsi $\tau\,(M) = M$: M est fixe par τ. Montrons qu'il y a d'autres points fixes par τ ; pour cela, raisonnons par l'absurde, en supposant que M soit le seul point fixe. Soit P un point $\neq M$; alors $P \neq \tau\,(P)$, et τ échange P et $\tau\,(P)$, puisque τ^2 = identité. Donc τ laisse fixe le "milieu" du "segment" $[P, \tau\,(P)]$, et par suite ce milieu est l'unique point fixe M. Il s'ensuit que τ transforme tout point P en son "symétrique" par rapport à M; donc τ est la "rotation" de l'angle π autour de M. Or cette rotation appartient à G, et puisque $\tau \in G' - G$, on arrive à une contradiction.

τ étant une isométrie et laissant fixe au moins deux points distincts, τ laisse fixes les points de la "droite" Δ qui les joint. Si τ avait un point fixe $\notin \Delta$, alors tous les points de H seraient fixes, ce qui est absurde, puisque $\tau \neq$ identité.

On a donc prouvé que l'ensemble des points fixes de τ est une "droite" Δ. Si $P \in \Delta$, on a (1) $d\,(P,A) = d\,(P,B)$, puisque τ est une isométrie, $\tau\,(P) = P$, $\tau\,(A) = B$. Il reste enfin à montrer que réciproquement la relation (1) implique que P

est sur Δ.

Or soit P ∉ Δ ; puisque Δ partage le plan en deux régions, et que A et B sont dans des régions distinctes (car [A,B] coupe Δ au point M), P est (par exemple) dans la même région que A ; alors [P,B] coupe Δ en un point Q, avec d (Q,A) = d (Q,B). On a



(2) $\quad d(A,P) < d(A,Q) + d(Q,P)$

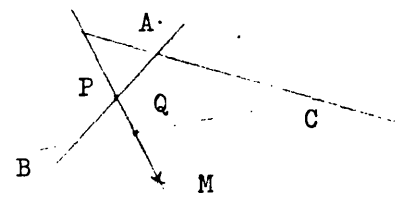
car on ne peut avoir égalité que si Q appartient au segment [A,P], ce qui n'est pas le cas puisque [A,P] ne rencontre pas Δ. Dans (2), remplaçons d (A,Q) par d (B,Q) qui lui est égal, et tenons compte de d (B,Q) + d (Q,P) = d (B,P) ; on obtient d (A,P) < d (B,P), donc P n'est pas "équidistant" de A et B. En résumé, les seuls points "équidistants" de A et B sont les points de Δ, ce qui achève la démonstration.

Théorème :

Il n'y a pas d'autre isométrie H → H que les transformations de G'. Pour cela on a besoin d'un lemme.

Lemme : Si une isométrie laisse fixes trois points A, B, C non "alignés", alors f est l'identité.

Démonstration du Lemme : Considérons le "triangle" de sommets A, B, C. Soit f une isométrie qui laisse fixes A, B et C ; alors f laisse fixe chaque point de chacune des "droites" AB, BC et CA. Soit maintenant M un point du plan qui n'appartient à aucune de ces droites ; choisissons un point P sur le segment [A, B] et distinct de A et B ; la droite MP partage le plan en deux régions, et A et B sont dans deux régions distinctes ; supposons par exemple que C soit dans la même région que A. Alors la droite MP coupe le segment [C, B] en un point Q ; les points P, et Q sont distincts. Donc f laisse fixes deux points distincts de la droite MP, et puisque f est une isométrie, f laisse fixes tous les points de cette droite, et en particulier le point M. C.Q.F.D.



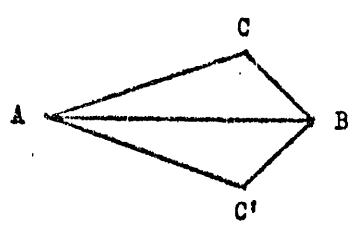
Démonstration du théorème :

Soit f une isométrie ; prenons trois points de H non "alignés" A, B, C. Considérons f (A), f (B) et f (C) ; ils ne sont pas "alignés", puisque f applique bijectivement la "droite" AB sur la "droite" joignant f (A) et f (B) ; or C n'est pas sur cette droite. Puisque d (A, B) = d [f(A), f (B)], il existe une transformation σ une seule de G, telle que τ (A) = f (A) et τ (B) = f (B). Considérons alors l'isométrie $g = \sigma^{-1} \circ f$. On a :

$$g(A) = A, \quad g(B) = B, \quad g(C) = C',$$

1) Si C' = C, alors, d'après le lemme, (g = id) donc f = σ ∈ G, ρ.q.f.d.

2) Si C' ≠ C, alors A est "équidistant" de C et C', B est "équidistant" de C et C'. Soit alors τ l'unique élément de G' - G qui échange C et C' ; puisque l'ensemble des points fixes de τ est l'ensemble des points "équidistants" de C et C', on voit que A et B sont fixes par τ.



On a donc $\tau \circ g(A) = A$, $\tau \circ g(B) = B$, $\tau \circ g(C) = C$. Mais τ∘g est une isométrie. D'après lemme, on en déduit que τ∘g = id. D'où $g = \tau^{-1} = \tau$, $f = \sigma\tau$, et par suite f ∈ G'. Le théorème est démontré.

Une axiomatique de la géométrie plane

Cette axiomatique recouvre aussi bien la géométrie plane euclidienne que la géométrie plane non euclidienne que nous avons étudiée précédemment dans le demi-plan de Poincaré.

Par définition, le "plan" est un espace métrique, non vide, non réduit à un point ; c'est un ensemble de points muni d'une distance qui satisfait à :

$$d(A, B) \geqslant 0$$

$$d(A, B) = d(B, A),$$

$$d(A, B) = 0 \iff A = B$$

$$d(A, B) \leqslant d(A, C) + d(C, B).$$

On pose une série d'axiomes.

Axiome 1.

On se donne certains sous-ensembles du plan, baptisés droites et on suppose :

- quels que soient les points distincts A et B, il existe une droite Δ et une seule telle que $A \in \Delta$ et $B \in \Delta$.
- Le plan n'est pas réduit à une droite ; ou encore : il existe trois points non alignés.

Remarques.

- Cet unique axiome ne caractérise pas les espaces métriques à deux dimensions ; par exemple il est vérifié par l'espace euclidien $\mathbb{R}^n$ pour $n \geqslant 2$.
- Une droite, qui est un sous-espace du plan, est un espace métrique.
- On va supposer que les nombres réels sont connus ; ou tout au moins nous allons supposer que $\mathbb{R}$est un groupe abélien muni d'une relation d'ordre total invariante par translation.

Axiome 2.

Si Δ est une droite du plan, Δ est isométrique à $\mathbb{R}$

Commentaires :

Par définition, une isométrie est une application bijective qui respecte la distance donnée sur Δ et sur $\mathbb{R}$; sur $\mathbb{R}$, on prend la distance habituelle

$$d(a, b) = |a-b|.$$

Quand on a une isométrie $f : \Delta \to \mathbb{R}$, on trouve toutes les isométries $\Delta \to \mathbb{R}$ en prenant les $\sigma \circ f$, où σ est une isométrie arbitraire de $\mathbb{R}$ sur $\mathbb{R}$. Or on connaît les σ ; ce sont les transformations $x \mapsto x + h$ et $x \mapsto -x + h$.

Une isométrie $f : \Delta \to \mathbb{R}$ permet de transporter la relation d'ordre de $\mathbb{R}$ sur Δ ; alors $\sigma \circ f$ définit sur Δ la même relation d'ordre ou la relation opposée, suivant que σ est $x \mapsto x + h$ (qui conserve l'ordre) ou $x \mapsto -x + h$ (qui le renverse).

On a donc la notion de "segment" sur Δ : c'est ce qui se transporte par une isométrie sur un segment de $\mathbb{R}$. On a de même la notion de demi-droite ; un point $A \in \Delta$ définit deux demi-droites d'origine A.

On a la caractérisation d'un segment $[A,B]$ de Δ :

$$C \in [A,B] \iff d(A,B) = d(A,C) + d(C,B)$$

(En effet, ceci est vrai sur $\mathbb{R}$). Ceci n'implique pas a priori que si trois points A,B,C du plan vérifient $d(A,B) = d(A,C) + d(C,B)$, ils sont alignés.

Toutefois nous poserons un nouvel axiome :

Axiome 2 bis .

$\forall$ A, B, C $\in$ plan, $C \in [A,B] \iff d(A,B) = d(A,C) + d(C,B)$

Autrement dit, lorsque $C \notin [A,B]$, alors $d(A,B) < d(A,C) + d(C,B)$.

Conséquence de l'axiome 2 bis : toute isométrie du plan dans lui-même transforme les droites en droites.

Axiome 3 :

Toute droite Δ partage le plan en deux régions.

Commentaires : l'axiome 3 veut dire que, dans le complémentaire de Δ, la relation

$$[A,B] \cap \Delta = \emptyset$$

est une relation d'équivalence, et qu'il y a deux classes d'équivalence.

L'axiome 3 est équivalent à :

Si une droite Δ ne passe par aucun des points A,B,C non alignés, alors le nombre des segments $[A,B]$, $[B,C]$, $[A,C]$ coupés par Δ est égal à 0 ou 2. (Exercice facile : le démontrer).

Axiome 4.

On postule la donnée d'un groupe G d'isométries du plan possédant les propriétés suivantes :

a) G est transitif ;

b) Si A est un point du plan, le groupe d'isotropie G_A, ensemble des éléments de G qui laissent A fixe, est simplement transitif dans l'ensemble des demi-droites issues de A (ou encore dans chaque cercle de centre A) [en appelant cercle de centre A et de rayon $r > 0$ le lieu des points M tels que $d(A, M) = r$].

Corollaire. Si on a deux couples de points du plan (A, B) et (A', B') tels que $d(A, B) = d(A', B') \neq 0$, alors il existe un $\sigma \in G$ et un seul tel que $\sigma(A) = A'$ et $\sigma(B) = B'$.

Conséquence. Si une isométrie $\sigma \in G$ laisse fixes deux points distincts A et B, alors σ est l'identité.

Symétrie par rapport à un point O. C'est, par définition, la transformation σ qui laisse fixe O et qui, à chaque point $M \neq O$ associe l'unique point M' de la droite MO tel que $d(O, M') = d(O, M)$, $M' \neq M$.

Proposition. La symétrie σ par rapport à O appartient au groupe G.

Démonstration. Choisissons un point $A \neq O$, et soit A' son symétrique $\sigma(A)$. Soit $\tau \in G$ tel que

$$\tau(O) = O, \quad \tau(A) = A'$$

[τ existe, puisque $d(O, A) = d(O, A')$] ; τ n'est pas l'identité, donc n'a pas d'autre point fixe que O, puisque $\tau \in G$.

Evidemment τ transforme la droite OA dans la droite OA', c'est-à-dire transforme la droite AA' en elle-même. Le point $\tau(A')$ est sur cette droite, sa distance à O est égale à $d(O, A') = d(O, A)$, donc $\tau(A') = A$ (puisque $\tau(A') \neq A'$). Il s'ensuit que τ^2 laisse fixes A et A', donc $\tau^2 = \text{identité}$. Soit maintenant M un point quelconque $\neq O$; soit $M' = \tau(M)$. On a $\tau(M') = M$ puisque

τ^2 = identité ; donc τ laisse fixe le milieu du segment $[M, M']$, et par suite ce milieu est O (unique point fixe de τ). Donc M' est le symétrique $\sigma(M)$, et donc $\tau = \sigma$. Puisque $\tau \in G$ par hypothèse, il s'ensuit que $\sigma \in G$. C.Q.F.D.

Axiome 5.

On suppose donné un groupe G' d'isométries, contenant G, et tel que G soit d'indice 2 dans G'. On suppose en outre : quels que soient les points distincts A et B, il existe une transformation $\tau \in G' - G$ qui échange A et B.

Proposition. La transformation τ de l'axiome 5 est unique ; elle est involutive (i.e. : $\tau^2 = id.$)

Démonstration. Supposons qu'on ait τ et τ_1 : $\begin{cases} \tau(A) = \tau_1(A) = B, \\ \tau(B) = \tau_1(B) = A. \end{cases}$

Alors $\tau\tau_1(A) = A$ et $\tau\tau_1(B) = B$; puisque τ et τ_1 sont dans $G' - G$, on a $\tau \circ \tau_1 \in G$, donc $\tau\tau_1 = id$.

Ceci est vrai en particulier pour $\tau_1 = \tau \Rightarrow \tau^2 = id$, c'est-à-dire $\tau = \tau^{-1}$.

Alors $\tau \circ \tau_1 = id$ donne $\tau^{-1} \circ \tau_1 = id$, c'est-à-dire $\tau = \tau_1$.

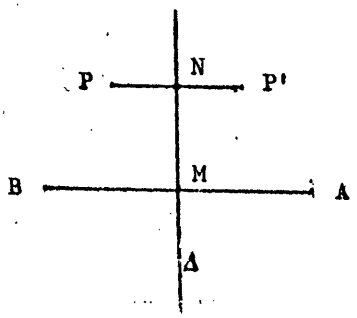
Proposition. L'ensemble des points fixes de τ est une droite Δ ; c'est l'ensemble des points équidistants de A et de B. On l'appelle la médiatrice du segment $[A, B]$.

Démonstration. (elle est calquée sur une démonstration déjà faite pour le demi-plan de Poincaré).

τ possède au moins un point fixe : le milieu M du segment $[A, B]$. Si τ possède un autre point fixe, alors tous les points de la droite qui les joint sont fixes (à cause de l'isomorphisme avec $\mathbb{R}$) ; τ ne peut pas en posséder davantage sinon tous les points du plan seraient fixes, ce qui est absurde, car $\tau \in G' - G$ n'est pas l'identité.

Il suffit donc de montrer que M n'est pas le seul point fixe de τ.

Supposons que M soit l'unique point fixe de τ. Soit P un point du plan,



$P \neq M$. Alors $\tau(P) = P' \neq P$, et $\tau(P') = \tau^2(P) = P$.

Donc τ échange P et P' $\Longrightarrow$ τ laisse fixe le milieu N de PP' $\Longrightarrow (N = M) \Longrightarrow$ τ est la symétrie par rapport à M ; or on a vu que cette symétrie appartient à G. On arrive à une

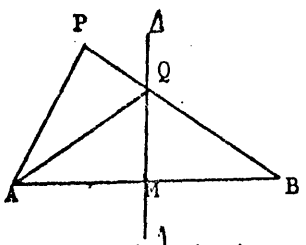
absurdité, puisque $\tau \in G' - G$ par hypothèse. On a donc bien démontré que l'ensemble des points fixes de τ est une droite Δ.

Montrons maintenant que Δ est l'ensemble des points équidistants de A et B.

Soit $P \in \Delta$; alors $\tau(P) = P$, d'où

$$d(P, A) = d[\tau(P), \tau(A)] = d(P, B)$$ puisque τ est une isométrie.

Soit $P \notin \Delta$. Montrons que $d(P, A) \neq d(P, B)$.



Nous savons que Δ partage le plan en deux régions et que A et B ne sont pas dans la même région, car le milieu M de $[A, B] \in \Delta$. Supposons que P soit dans la région de A ; alors le segment $[P, B]$ coupe Δ en Q, et on a $d(Q, A) = d(Q, B)$ d'après ce qu'on vient de voir.

D'après l'axiome 2^{bis}, on a

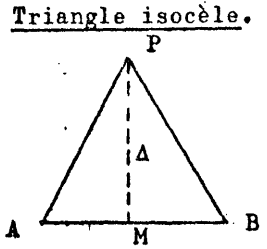
$$d(A, P) < d(A, Q) + d(Q, P)$$, car Q n'est pas sur le segment $[A, P]$ puisque $[A, P]$ ne rencontre pas Δ. Or $d(A, Q) = d(B, Q)$; d'où

$$d(A, P) < d(B, Q) + d(Q, P).$$

Mais $d(B, Q) + d(Q, P) = d(B, P)$ puisque $Q \in [P, B]$. On a donc $d(A, P) < d(B, P)$

C.Q.F.D.

Triangle isocèle. Un triangle isocèle est un triangle APB tel que $d(P, A) = d(P, B)$.



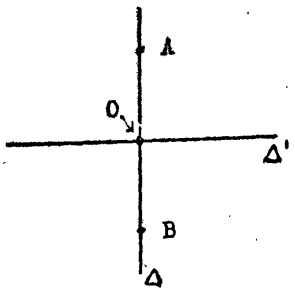
Il existe donc un unique $\tau \in G' - G$ tel que $\tau(P) = P$, $\tau(A) = B$, $\tau(B) = A$. C'est le τ de l'axiome 5, qui laisse fixe P puisque P est équidistant de A et B.

Proposition. Quelle que soit la droite Δ, il existe un unique $\tau \in G' - G$ qui laisse fixes les points de Δ. En outre, $\tau^2 = id$. Cet unique τ sera appelé la symétrie par rapport à la droite Δ.

Démonstration.

Unicité : supposons que τ et τ_1 répondent à la question ; alors $\tau \circ \tau_1 \in G$ et laisse fixes les points de $\Delta \Rightarrow \tau \circ \tau_1 = id$. En particulier $\tau^2 = id$, et on en déduit que $\tau_1 = \tau$.

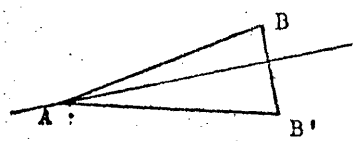
Existence : soit $O \in \Delta$, et soient $A, B \in \Delta$ distincts tels que O soit le milieu du segment $[A, B]$. Soit $\rho \in G' - G$ l'unique élément qui échange A et B ; ρ laisse fixes les points de Δ', médiatrice de $[A, B]$. Soit σ la symétrie par rapport au point O ; on a $\sigma \in G$. Alors $\sigma \circ \rho \in G' - G$ et laisse fixes A et $B \Longrightarrow \sigma \circ \rho$ laisse fixes tous les points de Δ C.Q.F.D.



Remarque : la symétrie par rapport à la droite Δ est le produit d'une symétrie par rapport à la droite Δ' (médiatrice de $[A, B]$) et de la symétrie par rapport à O.

Proposition. Soit $\sigma \in G' - G$; si A est fixe par σ ($\sigma(A) = A$), alors σ est la symétrie par rapport à une certaine droite passant par A.

Démonstration. Choisissons un point B tel que $\sigma(B) = B' \neq B$, ce qui est possible puisque $\sigma \neq$ identité. On a $d(A, B) = d(A, B')$. Soit τ la symétrie par rapport à la médiatrice de BB' : $\tau \in G' - G$, $\tau(B) = B'$ et $\tau(B') = B$. On a alors $\tau(A) = A$, puisque A est équidistant de B et B'. De plus : $\tau \circ \sigma \in G$, $\tau \circ \sigma(A) = A$, $\tau \circ \sigma(B) = B \Longrightarrow \tau \circ \sigma = id$. Mais comme $\tau = \tau^{-1}$, on trouve que $\sigma = \tau$, donc σ est la symétrie par rapport à la médiatrice de $[B, B']$.



Théorème : Toute isométrie appartient à G'.

Démonstration. La démonstration est identique à celle déjà faite dans le cas du demi-plan de Poincaré : on commence par montrer que si une isométrie laisse fixes trois points A, B, C non alignés, alors cette isométrie est l'identité. Ensuite on démontre facilement le théorème.

Définition. Soit G_A le groupe d'isotropie du point A (sous-groupe formé des $\sigma \in G$ tels que $\sigma(A) = A$). Un élément de G_A s'appelle aussi une rotation autour de A.

Théorème. Le groupe G_A est commutatif.

Démonstration : Soit τ la symétrie par rapport à une droite passant par A : $\tau \in G' - G \Longrightarrow \tau \notin G_A$. Soit $\sigma \in G_A$. Alors $\sigma \circ \tau \in G' - G$ et $\sigma \circ \tau(A) = A$. D'après une proposition antérieure, $\sigma \circ \tau$ est la symétrie par rapport à une certaine

droite passant par A. En particulier, $(\sigma \circ \tau)^2 = id$, ou encore $\sigma \tau \sigma \tau = id$, $\tau \sigma \tau = \sigma^{-1}$. Or $\tau = \tau^{-1}$. Donc σ^{-1} est le transformé de σ par l'automorphisme intérieur défini par τ.

Soient alors $\sigma_1 \in G_A$ et $\sigma_2 \in G_A$. On a

$$\left.\begin{array}{l} \tau \sigma_1^{-1} \tau = \sigma_1 \\ \tau \sigma_2^{-1} \tau = \sigma_2 \end{array}\right\} \Rightarrow \sigma_1 \sigma_2 = \tau \sigma_1^{-1} \tau \tau \sigma_2^{-1} \tau = \tau (\sigma_2 \sigma_1)^{-1} \tau = \sigma_2 \sigma_1 .$$

C.Q.F.D.

Problème.

Comment peut-on comparer les rotations autour de A et les rotations autour de B ?

Soit $\alpha \in G$ tel que $\alpha(A) = B$: nous savons que α existe puisque G est transitif. A tout $\sigma \in G_A$, on associe $\alpha \sigma \alpha^{-1} \in G_B$; on obtient ainsi un isomorphisme du groupe G_A sur le groupe G_B.

Montrons que cet isomorphisme ne dépend pas du choix de α : remplaçons α par la transformation la plus générale de G qui envoie A sur B ; c'est une transformation de la forme $\alpha \sigma'$, où σ' est une rotation autour de A.

L'isomorphisme devient alors $\sigma \longmapsto (\alpha \sigma') \sigma (\alpha \sigma')^{-1} = \alpha (\sigma' \sigma \sigma'^{-1}) \alpha^{-1} = \alpha \sigma \alpha^{-1}$

car $\sigma' \sigma \sigma'^{-1} = \sigma$ puisque G_A est commutatif.

On retrouve donc bien le même isomorphisme.

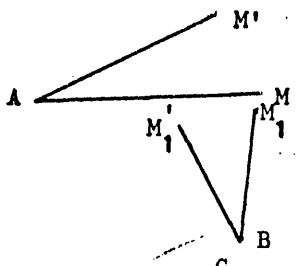
EGALITE de DEUX FIGURES

Nous ne définirons pas la notion de "figure", car il y a plusieurs conceptions possibles de ce que c'est qu'une figure. Nous verrons des exemples. D'autre part, il y a deux sortes d'égalité des "figures" :

- égalité suivant G, s'il existe une transformation de G qui transforme la première figure dans la seconde ;
- égalité suivant G', s'il existe une transformation de G' qui transforme la première figure dans la seconde.

Voyons d'abord l'exemple des "angles".

Angle orienté de deux demi-droites de même origine.



On considère la "figure" (AM, AM') ; une "figure" étant ici la donnée d'une première demi-droite AM et d'une deuxième demi-droite AM'. Soient (AM, AM') et (BM_1, BM'_1) deux telles "figures". Par définition,

$$(AM, AM') \overset{G}{=} (BM_1, BM'_1) \Longleftrightarrow \exists\, \sigma \in G : \quad \sigma(A) = B \ ; \ \sigma(AM) = BM_1 \ ; \ \sigma(AM') = BM'_1 \ .$$

Il est clair que σ est unique puisque G_A est simplement transitif dans l'ensemble des demi-droites issues de A.

Conséquence.

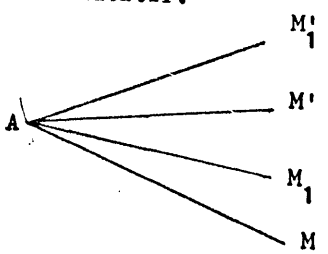
Si on se donne trois demi-droites AM, AM', BP , alors il existe une demi-droite BP' et une seule d'origine B, telle que

$$(BP, BP') \overset{G}{=} (AM, AM').$$

Considérons des angles de même sommet A :

$$(AM, AM') \overset{G}{=} (AM_1, AM'_1) \Longleftrightarrow \begin{cases} \text{le } \sigma \in G_A \text{ qui envoie AM sur } AM_1, \text{ envoie AM' sur } AM'_1 \\ \Updownarrow \\ \text{le } \sigma' \in G_A \text{ qui envoie AM sur AM', envoie } AM_1 \text{ sur } AM'_1 \end{cases}$$

En effet, l'équivalence des deux assertions de droite va résulter du fait que le groupe G_A est commutatif.



Désignons par $\sigma_{P',P}$ le $\sigma \in G_A$ qui envoie AP sur AP'. On a alors

$$\sigma_{M',M} = \sigma_{M',M_1} \circ \sigma_{M_1,M}$$

$$\sigma_{M'_1,M_1} = \sigma_{M'_1,M'} \circ \sigma_{M',M_1} = \sigma_{M',M_1} \circ \sigma_{M'_1,M'}$$

Or par hypothèse $\sigma_{M_1,M} = \sigma_{M'_1,M'}$. On en déduit $\sigma_{M',M} = \sigma_{M'_1,M_1}$. La réciproque se prouve de même.

Si à chaque angle (AM, AM') on associe l'unique rotation $\sigma_{M',M}$ qui transforme AM en AM', on a donc l'équivalence :

$$(AM, AM') \overset{G}{=} (AM_1, AM'_1) \Longleftrightarrow \sigma_{M',M} = \sigma_{M'_1,M_1} \ .$$

Conclusion : Les classes d'angles égaux sont mis ainsi en correspondance bijective avec les éléments de G_A. Si on choisit une fois pour toutes un côté origine, alors un repère pour le groupe G_A sera défini par la donnée d'une demi-droite AM' issue de A. La composition des éléments de G_A se transporte dans l'addition des classes d'angles, et on a la relation de Chasles définie sur ces classes d'angles :

$$(AM, AM'') = (AM, AM') + (AM', AM'').$$

On a défini plus haut un isomorphisme canonique entre G_A et G_B ; si $(AM, AM') \overset{G}{=} (BM_1', BM_1')$, l'unique $\sigma \in G_A$ qui envoie AM sur AM' correspond par cet isomorphisme à l'unique $\sigma_1 \in G_B$ qui envoie BM_1 sur BM_1'.

Remarque : Etant donnée une demi-droite AM d'origine A, il existe une unique demi-droite AM', d'origine A, telle que l'angle (AM, AM') soit G-égal à un angle donné.

Egalité selon G'. Nous considérons toujours des angles orientés de demi-droites. On dit que les angles (AM, AM') et (BM_1, BM_1') sont égaux selon G', ou G'-égaux, s'il existe un $\sigma \in G'$ qui transforme A en B, la demi-droite AM en la demi-droite BM_1, la demi-droite AM' en la demi-droite BM_1'. On observera que l'on a

$$(*) \qquad (AM, AM') \overset{G'}{=} (AM', AM)$$

(échange des deux côtés d'un angle) ; car si on choisit les points M et M' (sur les demi-droites respectives) de façon que

$$d(A, M) = d(A, M'),$$

l'unique $\tau \in G' - G$ qui échange M et M' laisse fixe A : d'où la relation (*).

Angle non orienté de deux demi-droites de même origine.

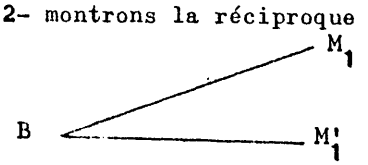
Une "figure" est ici un ensemble de deux demi-droites (et non plus un couple).

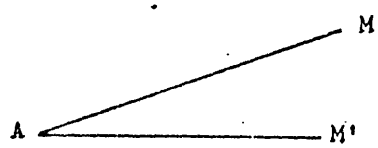
Proposition. L'égalité de deux angles (non orientés) suivant G est équivalente à l'égalité de ces angles suivant G'.

Démonstration.

1- l'égalité suivant G $\Longrightarrow$ l'égalité suivant G', car $G \subset G'$;

2- montrons la réciproque : supposons qu'on ait fait coïncider les deux angles par une transformation σ de G' ; supposons $\sigma \in G' - G$.





Nous savons qu'il existe une transformation τ de $G' - G$ qui transforme AM' dans AM et AM dans AM' ; alors $\sigma \circ \tau \in G$, et $\sigma \circ \tau$ transforme $\{AM, AM'\} = \{AM', AM\}$ dans $\{BM_1, BM_1'\}$.

Donc les deux angles sont égaux suivant G. C.Q.F.D.

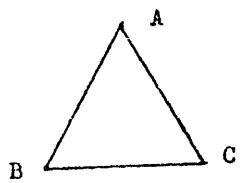
Notations.

On note $\widehat{MAM'} = \widehat{M'AM}$ la classe d'équivalence de l'angle non orienté $\{AM, AM'\}$.

On note $(\widehat{AM, AM'})$ la classe, suivant G, de l'angle orienté (AM, AM').

Exemple :

Dans un triangle isocèle ABC, où $d(A, B) = d(A, C)$, si on considère la transformation $\tau \in G' - G$ qui change B et C (et laisse fixe A), on voit que



$\widehat{CBA} = \widehat{BCA}$

$(\widehat{BC, BA}) \overset{G}{=} -(\widehat{CB, CA})$

$(\widehat{BC, BA}) \overset{G'}{=} (\widehat{CB, CA})$

Cas d'égalité des triangles.

Un triangle est un triplet (A, B, C) (A est le premier "sommet", B le second, C le troisième). On suppose A, B, C non alignés.

Nous considérerons l'égalité des triangles suivant G'. Donc deux triangles (A, B, C) et (A', B', C') sont ~~dans~~ égaux s'il existe $\sigma \in G'$ tel que $\sigma(A') = A$, $\sigma(B') = B$, $\sigma(C') = C$.

Premier cas d'égalité. Un angle et deux côtés adjacents. Autrement dit

$$\hat{A} = \hat{A}' \; ; \; d(A, B) = d(A', B') \; ; \; d(A, C) = d(A', C')$$

entraînent l'égalité du triangle (A, B, C) et du triangle (A', B', C').

Démonstration. Si $\hat{A} = \hat{A}'$, alors il existe $\sigma \in G'$ tel que $\begin{cases} \sigma(A) = A' \\ \sigma(AB) = A'B' \\ \sigma(AC) = A'C' \end{cases}$

On vérifie alors aisément que $\sigma(B) = B'$ et $\sigma(C) = C'$, à cause de la conservation des distances par σ.

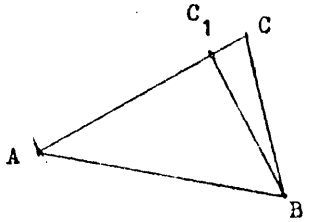
Deuxième cas d'égalité. Un côté et deux angles adjacents. Autrement dit :

$d(A, B) = d(A', B')$; $\widehat{CAB} = \widehat{C'A'B'}$; $\widehat{CBA} = \widehat{C'B'A'}$

entraînent l'égalité du triangle (A, B, C) et du triangle (A', B', C').

Démonstration. Il existe $\sigma \in G'$ tel que $\sigma(A') = A$, $\sigma(B') = B$; alors σ transforme la demi- droite A'C' en la demi-droite AC ou en sa symétrique par rapport à AB. Quitte à multiplier σ par la symétrie par rapport à AB, on peut donc supposer que $\sigma(A'C') = AC$.

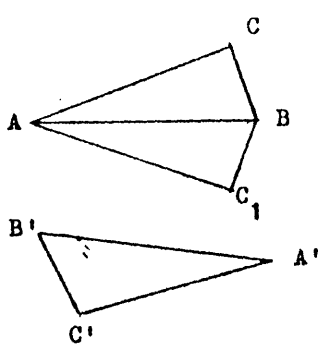
On va montrer que $\sigma(C') = C$.



Soit $C_1 = \sigma(C')$; C_1 est sur la demi-droite AC, et on a $\widehat{ABC_1} = \widehat{ABC}$. Il faut donc démontrer que si deux demi-droites font le même angle avec une demi-droite donnée BA, et si elles sont d'un même côté de BA, alors elles coïncident.

Nous savons que $\widehat{ABC_1} = \widehat{ABC} \Longrightarrow$ BC et BC_1 sont soit confondues soient symétriques par rapport à la demi-droite AB. Comme C et C_1 sont du même côté de AB, on en déduit que les demi-droites BC_1 et BC coïncident, et par suite que $C = C_1$. C.Q.F.D.

Troisième cas d'égalité. Trois côtés égaux. D'une façon précise :



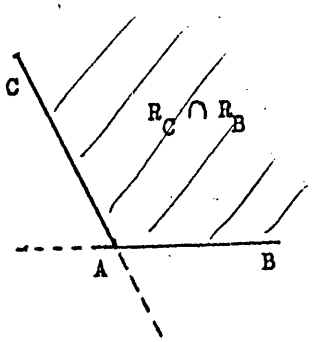
$d(A,B) = d(A',B')$; $d(A,C) = d(A',C')$; $d(B,C) = d(B',C')$ entraîne que les (ai) angles (A, B, C) et (A', B', C') sont égaux. En effet, il existe une unique transformation $\sigma \in G$ telle que $\sigma(A') = A$, $\sigma(B') = B$; posons $\sigma(C') = C_1$.

Si $C = C_1$, la démonstration est terminée.

Si $C \neq C_1$, alors la symétrie τ par rapport à AB échange C et C_1, donc $\tau \circ \sigma$ transforme A' en A, B' en B et C' en C. Donc les triangles sont égaux.

Relation d'ordre dans les angles non-orientés de demi-droites.

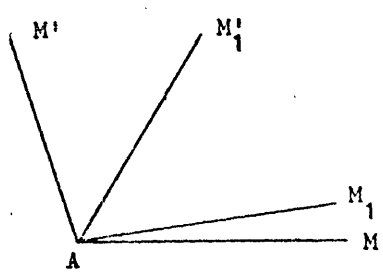
Nous avons vu que l'égalité suivant G est équivalente à l'égalité suivant G'. Soit un angle $\widehat{BAC}$ tel que les demi-droites AB et AC soient distinctes et non



symétriques par rapport à A ; ce qui signifie que les trois points A, B, C ne sont pas alignés. La droite définie par les points A et B partage le plan en deux régions et la demi-droite AC est contenue dans l'une de ces régions : soit R_c. De même la demi-droite AB est contenue dans l'une des régions définies par la droite AC, soit R_B.

$R_C \cap R_B$ est, par définition, l'angle solide défini par l'angle non orienté de demi-droite $\widehat{BAC}$. On obtient ainsi une correspondance bijective entre : angles solides de sommet A, et angles non-orientés de demi-droites d'origine A, non opposées ni confondues.

Soient alors $M_1 \widehat{A M'_1}$ et $\widehat{MAM'}$ deux angles non orientés de demi-droites. Si l'angle solide associé à $\widehat{M_1AM'_1}$ est contenu dans l'angle solide associé à $\widehat{MAM'}$, alors on a, par définition, $\widehat{M_1AM'_1} \leq \widehat{MAM'}$. Montrons que la relation : "il existe deux représentants dont les angles solides soient tels que l'un soit contenu dans l'autre", est une relation d'ordre dans l'ensemble des classes d'équivalence d'angles non orientés.



1) c'est réflexif : évident ;

2) c'est transitif : évident ;

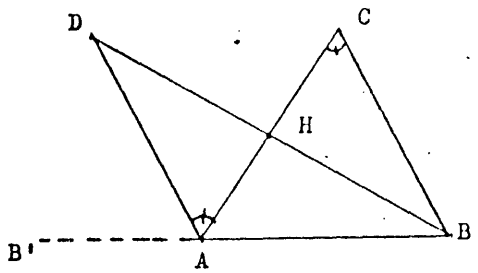
3) si l'angle solide $M_2AM'_2$ est contenu dans l'angle solide $M_1AM'_1$, et celui-ci contenu dans MAM', et si $\widehat{M_2AM'_2} = \widehat{MAM'}$, alors $\widehat{M_1AM'_1} = \widehat{MAM'}$; car si les angles solides $M_2 A M'_2$ et MAM', dont le premier est contenu dans le second, sont égaux (comme angles), ils sont confondus.

On a ainsi défini, dans l'ensemble des classes d'équivalence d'angles non orientés, une relation d'ordre indépendante de toute notion de "mesure des angles".

Proposition. Dans un triangle, un angle extérieur est strictement supérieur à chacun des angles intérieurs non adjacent (i.e. non relatifs au même sommet).

Démonstration. Soit (A, B, C) un triangle. Soit AB' la demi-droite opposée à la demi-droite AB ; montrons que

(1) $\widehat{ACB} < \widehat{B'AC}$.



Soit H le milieu de AC, et soit D le symétrique de B par rapport à H. On a alors $\widehat{CAD} = \widehat{ACB}$, car la symétrie par rapport à H est un élément de G.

AD est du même côté que H par rapport à la droite BB', donc du même côté que C. Donc l'angle solide associé à $\widehat{DAC}$ est strictement contenu dans l'angle solide associé à $\widehat{B'AC}$. On a donc $\widehat{DAC} < \widehat{B'AC}$, et comme $\widehat{DAC} = \widehat{BCA}$, on obtient (1).

Proposition. Dans un triangle (A, B, C) tel que d(A, B) = d(A, C), on a

$$\widehat{ABC} = \widehat{ACB}.$$

Démonstration. l'unique $\tau \in G' - G$ qui échange B et C laisse fixe A, donc transforme l'angle $\{BA, BC\}$ dans l'angle $\{CA, CB\}$.

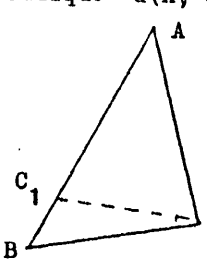
Proposition. Si un angle (A, B, C) est tel que d(A, B) > d(A, C), alors on a

$$\widehat{ACB} > \widehat{ABC}.$$

Démonstration. Soit C_1 l'unique point de la demi-droite AB qui vérifie

$$d(A, C_1) = d(A, C).$$

Puisque d(A, C) < d(A, B), C_1 appartient au segment $[A, B]$ et est $\neq B$.



Le triangle ACC_1 est isocèle, donc $\widehat{AC_1C} = \widehat{ACC_1}$. On a $\widehat{ACB} > \widehat{C_1CA}$ (regarder les angles solides associés). Dans le triangle (B, C, C_1), l'angle extérieur $\widehat{CC_1A}$ est strictement plus grand que l'angle intérieur $\widehat{CBA}$. Finalement :

$\widehat{ACB} > \widehat{C_1CA} = \widehat{CC_1A} > \widehat{CBA}$, d'où la relation annoncée

$$\boxed{\widehat{ACB} > \widehat{ABC}}$$

Maintenant, si on suppose $\widehat{ACB} > \widehat{ABC}$, alors d(A, B) et d(A, C) sont différents ; or on ne peut pas avoir d(A, B) < d(A, C) d'après la proposition précédente.

Conclusion. Les cas s'excluant mutuellement, les réciproques sont vraies ; autrement dit :

$$\widehat{ACB} > \widehat{ABC} \iff d(A, B) > d(A, C)$$

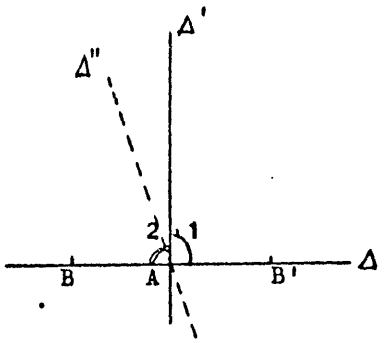
$$\widehat{ACB} = \widehat{ABC} \iff d(A, B) = d(A, C)$$

Orthogonalité.

Définition. On dit que deux droites sont perpendiculaires (ou orthogonales) en un point commun si les quatre angles (non orientés) de demi-droites qu'elles définissent sont égaux.

Théorème. Etant donnés une droite Δ et un point A sur cette droite, il existe une droite Δ' et une seule passant par A et orthogonale à Δ.

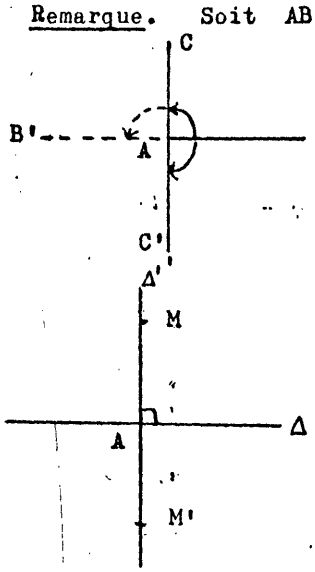
Démonstration. Soient B et B' deux points de Δ symétriques par rapport à A.



Nous savons que la médiatrice de BB' est l'ensemble des points fixes de l'unique $\tau \in G' - G$ qui échange B et B'. Soit Δ' cette médiatrice ; τ laisse fixes les points de Δ' et échange les angles 1 et 2. Ces deux angles sont donc égaux, et par conséquent Δ' répond à la question.

Montrons que Δ' est unique : supposons qu'on ait deux solutions Δ' et Δ''. Si $\Delta' \neq \Delta''$, on a nécessairement une inclusion stricte des angles solides associés à B'A Δ' et B' A Δ''. Il s'ensuit une inégalité stricte des angles correspondants, et par conséquent Δ'' ne peut pas être orthogonale à Δ et distincte de Δ'.

Remarque. Soit AB une demi-droite. La droite perpendiculaire en A à la demi-droite AB est formée de deux demi-droites AC et AC'. Les deux angles orientés $(\widehat{AB, AC})$ et $(\widehat{AB, AC'})$ sont les deux angles dont le double est égal à l'angle plat $(\widehat{AB, AB'})$.



Problème. Etant donnés une droite Δ et un point M non sur Δ, montrer qu'il existe une droite et une seule orthogonale à Δ et qui passe par M.

Solution. Supposons le problème résolu ; soit Δ' une solution ; Δ' coupe Δ en A et est orthogonale à Δ en A. Soit M' le symétrique de M par rapport à A. L'unique $\tau \in G' - G$

qui échange M et M' laisse fixes les points de Δ : donc Δ' doit passer par le symétrique M' de M par rapport à Δ.

Réciproquement, la droite qui joint M à M' est bien orthogonale à Δ : c'est la solution du problème.

Corollaire. Si on considère deux droites Δ' et Δ'' perpendiculaires à une même droite Δ, alors Δ' et Δ'' sont parallèles.

Démonstration. Supposons Δ' et Δ'' non confondues, et montrons qu'elles ne se rencontrent pas. Raisonnons par l'absurde : si Δ' et Δ'' ont un point commun M, M n'est pas sur Δ (sinon Δ' et Δ'' seraient confondus) ; donc M est distinct de son symétrique M' par rapport à Δ ; M' est aussi un point commun à Δ' et Δ'', et par conséquent Δ' et Δ'' ont deux points distincts en commun : c'est absurde.

C.Q.F.D.

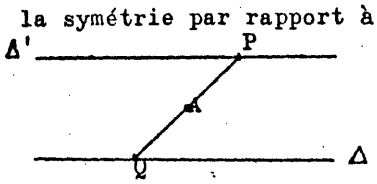
Proposition. Soit A un point, et soit σ la symétrie par rapport à A. Alors σ transforme toute droite Δ en une droite Δ' parallèle à Δ.

Démonstration. On va montrer que si Δ et Δ' se rencontrent, elles sont confondues. Supposons que Δ et $\Delta' = \sigma(\Delta)$ aient un point commun M. Si $M = A$, alors Δ et Δ' coïncident. Si $M \neq A$, alors $M' = \sigma(M)$ est distinct de M et est commun à Δ et Δ' ; Δ et Δ' ont donc deux points distincts communs, et donc $\Delta = \Delta'$.

C.Q.F.D.

Proposition. Soit Δ une droite, et soit P un point non sur Δ ; alors il existe au moins une parallèle à Δ passant par P.

Démonstration. Soit Q un point de Δ et soit A le milieu du segment PQ. Soit σ la symétrie par rapport à A ; on a $\sigma(Q) = P$, posons $\sigma(\Delta) = \Delta'$; Δ' passe par P. D'après la proposition précédente, Δ' est parallèle à Δ, ce qui prouve bien la proposition.



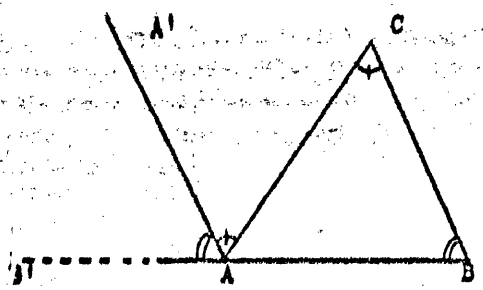
Remarque. La proposition ne parle pas de l'unicité d'une telle parallèle.

Postulat d'Euclide. Unicité de la parallèle à Δ menée par un point P $\Longleftrightarrow$ la relation de parallélisme entre droites est une relation d'équivalence.

Si nous ajoutons cet axiome aux précédents, on va pouvoir montrer que notre plan est alors isométrique au plan euclidien. Auparavant, tirons quelques premières conséquences du postulat d'Euclide.

1) Notion de direction de droite dans le plan : une direction est, par définition, une classe d'équivalence de droites suivant la relation de parallélisme.

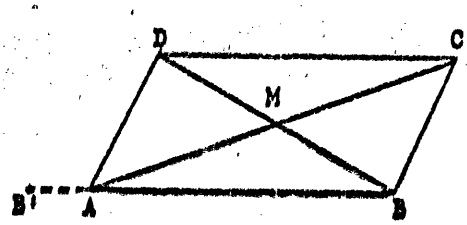
2) La somme des angles d'un triangle est un angle plat :



Soit (A, B, C) un triangle, et soit AA' la parallèle à BC menée par A. On a $\hat{B} + \hat{C} + \hat{A} = \widehat{B'AA'} + \widehat{A'AC} + \widehat{CAB}$ = angle plat.

En effet : $\hat{C} = \widehat{A'AC}$ (cf. symétrie par rapport au milieu de [A, C]) ; et $\widehat{B'AA'} = \hat{B}$ parce que l'unique demi-droite d'origine A, qui fait avec AB' un angle égal à B et est du même côté de AB que C, est parallèle à BC (sinon contradiction : regarder angle extérieur d'un triangle).

3) Si on a quatre points A, B, C, D non alignés et tels que les côtés AB et CD soient parallèles, ainsi que AD et BC, alors les diagonales AC et BD se coupent en leur milieu ; car soit σ la symétrie par rapport au milieu M de [A, C]. $\sigma(A) = C$, σ transforme AB en une parallèle à AB (donc en CD), et transforme AD en une parallèle à AD (donc en BC), donc σ transforme B en D, et par suite M est le milieu de [B, D]. C.Q.F.D.



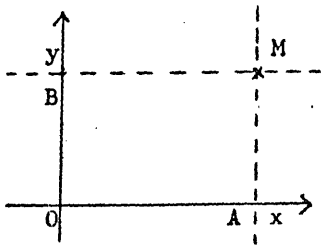
On en déduit : $d(A, B) = d(C, D)$ $d(A, D) = d(B, C)$

$\widehat{DAB} = \widehat{BCD}$, $\widehat{ADC} = \widehat{ABC}$.

(Propriétés du parallélogramme).

Conséquence. Si dans un parallélogramme, un angle est droit, alors tous les autres sont droits ⟹ on a un rectangle.

Conséquence. On va définir une correspondance bijective entre les points M du plan et les couples $(x, y) \in \mathbb{R} \times \mathbb{R}$:



On prend deux droites perpendiculaires en un point O pris comme origine des coordonnées ; par un point M du plan on mène les parallèles à ces deux droites qui les coupent en x et y ; la figure Ox My est un rectangle.

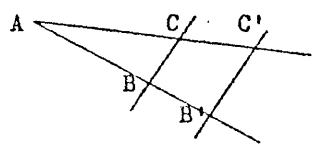
Théorème fondamental (toujours modulo le postulat d'Euclide).

Le plan est isométrique à $\mathbb{R}^2$ muni de la distance euclidienne.

Démonstration. Tout revient à montrer que $(d(O, M))^2 = x^2 + y^2$. On doit donc établir la relation de Pythagore entre les côtés d'un triangle rectangle.

Indications pour la démonstration :

- Théorème de Thalès : si BC et B'C' sont parallèles, on a

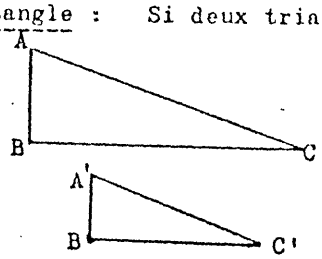


$$\frac{d(A, B)}{d(A,B')} = \frac{d(A, C)}{d(A,C')} = \frac{d(B, C)}{d(B',C)}$$

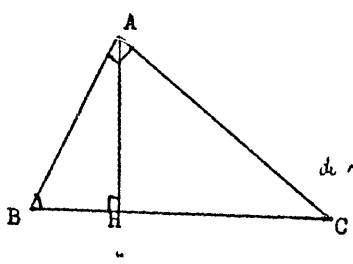
- Théorie des triangles semblables. Soit (A, B, C) et (A', B', C') deux triangles ;

$$\hat{A} = \hat{A}', \quad \hat{B} = \hat{B}', \quad \hat{C} = \hat{C}' \Longrightarrow \frac{d(A,B)}{d(A',B')} = \frac{d(A,C)}{d(A',C')} = \frac{d(B,C)}{d(B',C')}.$$

- Théorie du triangle rectangle : Si deux triangles rectangles ont un angle aigu égal, ils sont semblables .



- Conséquence : Soit (A, B, C) un triangle rectangle en A, et soit AH la perpendiculaire à BC. Alors AHB et CAB sont semblables ; on a donc



$$\frac{d(A, B)}{d(B,H)} = \frac{d(B,C)}{d(A,B)} \Longrightarrow$$

$$\left.\begin{array}{l} d(A, B)^2 = d(B, H).d(B, C) \\ \text{de même : } d(A, C)^2 = d(C, H).d(B, C) \end{array}\right\} \text{ ; on ajoute}$$

membre à membre et il vient :

$$d(A, B)^2 + d(A, C)^2 = d(B, C).\left[d(B, H) + d(H, C)\right] = d(B, C)^2$$

C.Q.F.D.

GEOMETRIE AFFINE EN DIMENSION n

On se place dans l'espace $\mathbb{R}^n$ que l'on munit du groupe linéaire-affine : c'est le groupe $G\,L\,A(n, \mathbb{R})$ formé des transformations $x \to A\,x + b$, où $A \in G\,L(n, \mathbb{R})$ et $b \in \mathbb{R}^n$.

Il contient comme sous-groupe le groupe $G\,L(n, \mathbb{R})$.

Par définition même, toute transformation $S \in G\,L\,A(n, \mathbb{R})$ s'écrit sous la forme $S = T \circ A$, où $A \in G\,L(n, \mathbb{R})$, et où T est une translation $x \to x + b$. Une telle écriture est unique, car $T \circ A = T' \circ A' \Longrightarrow T'^{-1} \circ T = A' \circ A^{-1}$, d'où on déduit $T'^{-1}\,T$ = identité (translation laissant fixe 0) .

Soit $b \in \mathbb{R}^n$, on notera T_b la translation définie par $T_b(x) = x + b$.

Ces translations, lorsque b parcourt $\mathbb{R}^n$, forment un groupe abélien. Montrons qu'il est distingué dans $G\,L\,A(n, \mathbb{R})$: soit $S \in G\,L\,A(n, \mathbb{R})$ et soit T_a une translation. Supposons S définie par $S(x) = A\,x + b$, et étudions $S \circ T_a \circ S^{-1}$:

$$x' = A\,x + b \Longrightarrow x = A^{-1}\,x' - A^{-1}\,b \text{ , donc}$$

$$S^{-1}(x) = A^{-1}\,x - A^{-1}\,b \quad , \quad T_a \circ S^{-1}(x) = A^{-1}\,x - A^{-1}\,b + a \ ,$$

$$S \circ T_a \circ S^{-1}(x) = x - b + Aa + b = x + Aa = x + a' = T_{a'}(x);$$

On a donc

$$\boxed{S\,T_a\,S^{-1} = T_{A(a)}}$$

ce qui prouve que le sous-groupe des translations est distingué.

Calculons $(T_a \circ A) \circ (T_b \circ B) = T_c \circ C$.

On sait que $A \circ T_b \circ A^{-1} = T_{A(b)} \Longrightarrow A \circ T_b = T_{A(b)} \circ A$.

On en déduit

$$(T_a \circ A) \circ (T_b \circ B) = T_a \circ (A \circ T_b) \circ B = T_a \circ T_{A(b)} \circ A \circ B$$

$$= T_{a+A(b)} \circ (A \circ B) \ .$$

Donc si on considère $G\,L\,A(n, \mathbb{R})$ comme l'ensemble des couples de la forme (T_a, A) on a la loi de composition :

$$(T_a, A) \circ (T_b, B) = (T_{a+A(b)}\ , A \circ B) \ ;$$

on dit que $G\,L\,A(n, \mathbb{R})$ est un produit croisé du groupe linéaire homogène $G\,L(n, \mathbb{R})$ par le groupe des translations, dans lequel $G\,L(n, \mathbb{R})$ opère par $T_b \to T_{A(b)}$.

Notions intrinsèques de la géométrie affine. - L'origine $0 \in \mathbb{R}^n$ est un point de l'espace qui ne joue aucun rôle particulier, puisque le groupe $GLA(n, \mathbb{R})$ est transitif.

1 - Barycentre d'un système fini de points : Soit un nombre fini de points $x_i \in \mathbb{R}^n$; pour chaque i on se donne un scalaire $\lambda_i \in \mathbb{R}$, et on suppose que

$$\boxed{\sum_i \lambda_i = 1}$$

On appelle barycentre des points x_i affectés des masses λ_i, le point $\sum_i \lambda_i x_i$ qui est bien défini si l'on considère les x_i comme vecteurs.

Montrons que la notion de barycentre est une notion affine, i.e. :

$$(1) \qquad \boxed{S\left(\sum_i \lambda_i x_i\right) = \sum_i \lambda_i S(x_i)} \quad \begin{cases} \text{pour } S \in GLA(n, \mathbb{R}) \\ \text{et } \sum_i \lambda_i = 1 \end{cases}$$

Il suffit de le vérifier quand S est une translation, et quand $S \in GL(n, \mathbb{R})$.

- Cas où S est une translation T_b :

$$S\left(\sum_i \lambda_i x_i\right) = \sum_i \lambda_i x_i + b, \quad \sum_i \lambda_i S(x_i) = \sum_i \lambda_i (x_i + b) = \sum_i \lambda_i x_i + \left(\sum_i \lambda_i\right) b,$$

d'où l'égalité puisque $\sum_i \lambda_i = 1$.

- Cas où S est une transformation linéaire homogène : la relation à démontrer est évidente : elle exprime que S est linéaire (homogène).

Etant donnés deux points A et B, l'ensemble des barycentres à masses $\geqslant 0$ de ces deux points forme le segment $[A, B]$. L'ensemble de tous les barycentres à coefficients réels forme la droite affine définie par A et B (lorsque A et B sont distincts).

Définition

Soit E un sous-ensemble de $\mathbb{R}^n$; alors

E convexe $\Longleftrightarrow$ $\{x \in E, y \in E \Longrightarrow \lambda x + \mu y \in E$ dès que $\lambda \geqslant 0$ $\mu \geqslant 0$ et $\lambda + \mu = 1\}$

Ceci exprime que le segment joignant deux points de E est contenu dans E.

.../...

Conséquence :

Le plus petit ensemble convexe qui contient les points $x_1, \ldots, x_p$ de $\mathbb{R}^n$ (appelé enveloppe convexe de ces points) est l'ensemble :

$$E = \left\{ \sum_{i=1}^{p} \lambda_i x_i \ , \quad \lambda_i \geqslant 0 \ , \ \sum_{i=1}^{p} \lambda_i = 1 \right\}$$

La démonstration est laissée à titre d'exercice.

Ainsi l'enveloppe convexe est l'ensemble des barycentres des points x_i à masses $\geqslant 0$.

2 - Lorsque $\sum_i \lambda_i \neq 1$, la relation (1) n'a plus lieu.

Toutefois, lorsque $\sum_i \lambda_i = 0$, le vecteur $\sum_i \lambda_i x_i$ ne change pas si on effectue sur les x_i une même translation T :

(2) $$\boxed{\sum_i \lambda_i \ T(x_i) = \sum_i \lambda_i x_i \quad \text{pour} \quad \sum_i \lambda_i = 0}$$

La vérification est immédiate :

$$\sum_i \lambda_i (x_i + b) = \sum_i \lambda_i x_i + \left(\sum_i \lambda_i \right) b$$

$$= \sum_i \lambda_i x_i \ .$$

Ainsi, étant donnés des points x_i en nombre fini, et des scalaires λ_i dont la somme est nulle, on définit $\sum_i \lambda_i x_i$ comme un vecteur de $\mathbb{R}^n$, ou, ce qui revient au même, comme un élément du groupe des translations de $\mathbb{R}^n$.

Cas particulier : deux points x et y définissent un vecteur $x - y$: c'est le vecteur qui définit la translation qui transforme y en x , car

$$x - y = b \iff x = y + b \ .$$

Définition : des points x_i , en nombre fini, sont dits linéairement indépendants (au sens affine) si la relation $\sum_i \lambda_i x_i = 0$ (avec $\sum_i \lambda_i = 0$) , entraîne que tous les λ_i sont nuls.

Dans le cas contraire, les points x_i sont dits linéairement dépendants ; si on a alors $\sum_{i=1}^{p} \lambda_i x_i = 0$ $\left(\sum_i \lambda_i = 0 \right)$,

et, par exemple, $\lambda_1 \neq 0$, on a

$$x_1 = - \sum_{i=2}^{p} \frac{\lambda_i}{\lambda_i} x_i \ ,$$

donc x_1 est un barycentre de $x_2, \ldots, x_p$, avec des masses $\mu_i = -\frac{\lambda_i}{\lambda_1}$ dont la somme est bien égale à 1. Réciproquement, si un point x_1 est un barycentre de $x_2, \ldots x_p$, alors les points $x_1, x_2, \ldots, x_p$ sont linéairement dépendants.

Définition - Un sous-ensemble $V \subset \mathbb{R}^n$ est une variété linéaire-affine si et seulement si $(x_i \in V \Longrightarrow \sum_i \lambda_i x_i \in V$ chaque fois que $\sum_i \lambda_i = 1)$;

ou encore : V est une variété linéaire-affine si et seulement si tout barycentre de points de V est un point de V. Il suffit d'exprimer cette condition pour les barycentres de deux points.

Remarque

Si V est une variété linéaire-affine, alors V est convexe (mais la réciproque est fausse ; par exemple, un segment de droite n'est pas une variété linéaire-affine).

Proposition - Pour que $V \subset \mathbb{R}^n$ soit une variété linéaire-affine, il faut et il suffit que $V = \emptyset$, ou que V soit le translaté d'un sous-espace vectoriel.

Démonstration : $\emptyset$ est trivialement une variété linéaire-affine. Si une variété linéaire-affine V n'est pas vide, soit $a \in V$, et soit V' l'ensemble des $x - a$, où $x \in V$; alors si $x'_1 \in V'$ et $x'_2 \in V'$, on a $x'_1 + a \in V$, $x'_2 + a \in V$, donc $t(x'_1 + a) + (1 - t)(x'_2 + a) \in V$, c'est-à-dire $t x'_1 + (1 - t) x'_2 \in V'$ quel que soit $t \in \mathbb{R}$; on en déduit que V' est un sous-espace vectoriel. Réciproquement, tout translaté d'un sous-espace vectoriel est bien une variété linéaire-affine.

Exemples : un point est une variété linéaire-affine (translaté du sous-espace vectoriel de dimension zéro) ; le translaté d'un sous-espace vectoriel de codimension un s'appelle un hyperplan affine.

.../...

Proposition. L'intersection d'une famille quelconque de variétés linéaires-affines est une variété linéaire-affine.

C'est évident d'après la définition (condition du barycentre).

Remarque. Si $\bigcap_{i \in I} V_i \neq \emptyset$, et si $a \in \bigcap_{i \in I} V_i$, soit $V_i' = V_i - a$ le sous-espace vectoriel associé à V_i ; alors $\bigcap_{i \in I} V_i$ est translatée du sous-espace vectoriel $\bigcap_{i \in I} V_i'$ par la translation $T_a : x \longmapsto x + a$.

Variété linéaire-affine engendrée : soit $E \subset \mathbb{R}^n$ un ensemble de points ; l'intersection de toutes les variétés linéaires-affines contenant E est une variété linéaire-affine (la "plus petite" de celles qui contiennent E) ; on l'appelle la variété linéaire-affine engendrée par E, et on la note $V(E)$.

Proposition. $V(E)$ se compose de tous les barycentres de systèmes finis de points de E.

(Démonstration laissée au lecteur).

En particulier, si $x_0, x_1, \ldots, x_p$ sont $(p+1)$ points linéairement indépendants (au sens affine), tout point de la variété linéaire-affine qu'ils engendrent s'écrit d'une seule manière sous la forme

$$\sum_{i=0}^{p} \lambda_i x_i \qquad \left(\sum_i \lambda_i = 1\right).$$

Notion de repère.

Définition : On appelle repère affine (dans $\mathbb{R}^n$) toute suite de $n+1$ points linéairement indépendants (au sens affine).

Si $(x_0, \ldots, x_n)$ est un tel repère, la variété linéaire-affine engendrée par ces points est l'espace $\mathbb{R}^n$ tout entier ; tout point $x \in \mathbb{R}^n$ est caractérisé par le système des λ_i réels $\left(0 \leq i \leq n, \ \sum_i \lambda_i = 1\right)$ tels que

$$x = \sum_{i=0}^{n} \lambda_i x_i.$$

On les appelle les coordonnées affines du point x par rapport au repère $(x_0, x_1, \ldots, x_n)$.

A un repère $(x_0, x_1, \ldots, x_n)$ on peut associer la suite $(x_0, x_1 - x_0, \ldots, x_n - x_0)$ formée du point x_0 (appelé origine du repère) et des vecteurs $x_1 - x_0, \ldots, x_n - x_0$. Ces n vecteurs sont linéairement indépendants (au sens vectoriel).

Réciproquement, la donnée d'un point x_0 et d'une base $(e_1, \ldots, e_n)$ de l'espace vecto-

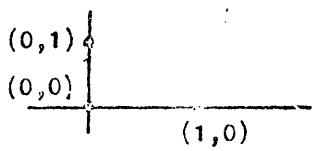
riel $\mathbb{R}^n$ définit un repère affine:

$$(x_o,\ x_o+e_1,\ldots,\ x_o+e_n).$$

Repère canonique : c'est celui qui correspond au point $x_o = 0$ et à la base canonique de $\mathbb{R}^n$:

$$e_1 = (1, 0,\ldots, 0),\ e_2 = (0, 1, 0,\ldots, 0),\ldots,\ e_n = (0,\ldots, 0, 1).$$

Par exemple, pour $n = 2$ (plan affine), le repère canonique est formé des trois points $(0, 0)$, $(1, 0)$, $(0, 1)$.



Proposition. Le groupe $GLA(n, \mathbb{R})$ opère de façon simplement transitive dans l'ensemble des repères affines.

Démonstration. Il suffit de vérifier qu'il existe un unique $S \in GLA(n, \mathbb{R})$ qui transforme le repère canonique en un repère $(x_o, x_1,\ldots, x_n)$ arbitrairement donné.

Or, si on pose $S(x) = Ax + b$, on voit que l'on doit avoir $b = x_o$, et que A doit transformer la base canonique de $\mathbb{R}^n$ dans la base

$$e_1 = x_1 - x_o,\ldots,\ e_n = x_n - x_o. \qquad \text{C.Q.F.D.}$$

Définition. Deux "figures" sont égales (au sens affine) s'il existe un $S \in GLA(n, \mathbb{R})$ qui transforme l'une des figures dans l'autre.

Exemple : pour $n \geq 2$, deux triangles sont toujours égaux (il suffit de compléter chaque triangle en un repère affine).

GEOMETRIE EUCLIDIENNE en DIMENSION n

On considère à nouveau l'espace $\mathbb{R}^n$, mais on fait opérer cette fois le groupe des transformations : $x \longmapsto Ax + b$, où $b \in \mathbb{R}^n$ et $A \in O(n)$ (groupe orthogonal). Ces transformations forment un groupe G' que l'on appelle le groupe de la géométrie euclidienne. G' est un sous-groupe du groupe linéaire affine $GLA(n, \mathbb{R})$; G' possède un sous-groupe G d'indice 2, à savoir $G = \{x \longmapsto Ax+b,\ b \in \mathbb{R}^n,\ A \in SO(n)\}$; c'est l'une des deux composantes connexes de G'.

Les transformations de G' s'appellent déplacements, celles de G s'appellent déplacements directs.

Notions de géométrie euclidienne.

1- Un repère euclidien est un couple formé d'un point de $\mathbb{R}^n$ et d'une base orthonormée de $\mathbb{R}^n$.

On a encore le repère canonique $(0, e_1, \cdots, e_n)$, où $(e_1, \cdots, e_n)$ est la base canonique de $\mathbb{R}^n$. Le groupe G' opère d'une manière simplement transitive dans l'ensemble des repères euclidiens.

Un repère euclidien direct est un couple formé d'un point de $\mathbb{R}^n$ et d'une base orthonormée directe de $\mathbb{R}^n$. Le groupe G opère d'une manière simplement transitive dans l'ensemble des repères euclidiens directs.

2- Les notions de la géométrie affine sont encore valables ici, notamment celles de barycentre, variété linéaire-affine, ensemble convexe.

3- On a la notion de produit scalaire : un vecteur étant défini par un couple (x, y) de points [un tel couple définit le vecteur x-y], on associe à deux vecteurs (x, y) et (x', y') le scalaire

$$\sum_{i=1}^{n} (x_i - y_i)(x'_i - y'_i) \quad , \text{ noté } \langle x-y \, , \, x'-y' \rangle .$$

En particulier, on a le carré scalaire $\langle x-y \, , \, x-y \rangle$ d'un vecteur ; la racine carrée $\sqrt{\langle x-y, \, x-y \rangle}$ s'appelle la distance euclidienne des deux points x et y, et se note d(x, y). Elle est invariante par le groupe G' : si $S \in G'$, on a

$$d(S(x) \, , \, S(y)) = d(x, y).$$

Deux vecteurs (x, y) et (x', y') sont dits orthogonaux si le produit scalaire $\langle x-y, \, x'-y' \rangle$ est nul.

Définition. Une isométrie est une transformation de l'espace dans lui-même qui conserve les distances.

Conséquence : tout élément de G' est une isométrie.

Théorème. Toute isométrie est un élément de G'.

Démonstration. Soit $f : \mathbb{R}^n \longrightarrow \mathbb{R}^n$ une transformation qui conserve les distances, i.e. une isométrie; posons f(0) = b. L'application $g : x \longmapsto f(x) - b$ est encore une isométrie, et on a g(0) = 0 : si on montre que $g \in G'$, il s'ensuivra que $f \in G'$.

On est donc ramené à prouver le théorème pour une isométrie f telle que $f(0) = 0$. Il suffit de prouver :

Proposition. Toute isométrie f qui laisse fixe l'origine est un élément de $O(n)$.

L'origine étant fixe, nous identifions points de l'espace et vecteurs de $\mathbb{R}^n$. Toute la question est de démontrer que f est linéaire, car toute transformation linéaire qui conserve la distance appartient à $O(n)$, par définition.

1) Soient A, B deux points, et $A' = f(A)$, $B' = f(B)$ leurs transformés. On a

$$(1) \qquad \langle OA', OB' \rangle = \langle OA, OB \rangle ,$$

car

$$2 \langle OA, OB \rangle = d(O, A)^2 + d(O, B)^2 - d(A, B)^2 ,$$

et le membre de droite est égal à

$$d(O, A')^2 + d(O, B')^2 - d(A', B')^2 = 2 \langle OA', OB' \rangle$$

puisque f conserve les distances et transforme O en O, A en A' et B en B'. Ce qui prouve la relation (1).

2) En particulier, f transforme les vecteurs d'une base orthonormée de R^n en vecteurs d'une base orthonormée. Donc l'image de $\mathbb{R}^n$ par f contient les vecteurs d'une base orthonormée. Il s'ensuit que si un vecteur x est orthogonal à tous les vecteurs de l'image de f, il est nul.

3) Soient x et y deux vecteurs quelconques. Pour montrer que $f(x+y)$ est égal à $f(x) + f(y)$, il suffit (d'après ce qui précéde) de montrer que

$$\langle f(x+y) , f(z) \rangle = \langle f(x) + f(y), f(z) \rangle$$

quel que soit le vecteur z. Or le premier membre est égal à $\langle x+y, z \rangle = \langle x, z \rangle + \langle y, z \rangle$ puisque f conserve le produit scalaire ; le second membre est égal à

$$\langle f(x), f(z) \rangle + \langle f(y), f(z) \rangle = \langle x, z \rangle + \langle y, z \rangle$$

C.Q.F.D.

4) On montre enfin que $f(\lambda x) = \lambda f(x)$ pour tout $\lambda \in \mathbb{R}$, en prouvant que

$$\langle f(\lambda x), f(z) \rangle = \langle \lambda f(x), f(z) \rangle .$$

quel que soit le vecteur z. Le lecteur achèvera la démonstration.

Notion d'angle en géométrie euclidienne.

Cas de la dimension 2.

1- Angle orienté de deux demi-droites.

Soient D et D' deux demi-droites d'origine O. Soit $\theta(D, D')$ l'unique $\theta \in SO(2)$ qui transforme D en D'. Et soit $\widehat{(D, D')}$ la classe d'équivalence du couple (D, D') modulo la relation d'équivalence définie par SO(2). On sait que

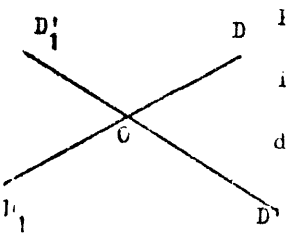
$$(\widehat{(D, D')} = \widehat{(D_1, D_1')}) \Longleftrightarrow \theta(D, D') = \theta(D_1, D_1')$$

[cf. axiomatique de la géométrie plane ; cela résulte du fait que le groupe SO(2) est commutatif]. Si on écrit additivement le groupe abélien SO(2), on a

$$\theta(D, D'') = \theta(D, D') + \theta(D', D'').$$

2- Angle orienté de deux droites.

Considérons un couple de droites Δ, Δ' passant par O. La droite Δ définit deux demi-droites D et D_1 ; la droite Δ' définit deux demi-droites D' et D_1'.



Pour qu'une rotation $\alpha \in SO(2)$ transforme Δ sur Δ', il faut et il suffit que α transforme D en D' ou D_1'. Le couple (Δ, Δ') définit donc deux angles orientés de demi-droites, à savoir

$$\theta(D, D') = \theta(D_1, D_1')$$

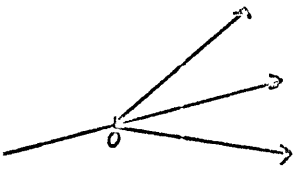
et $$\theta(D, D_1') = \theta(D_1, D').$$

Chacun d'eux est la "somme" de l'autre et de l'angle plat (unique élément $\omega \neq SO(2)$ tel que $2\omega = 0$, $\omega \neq 0$; ω est la symétrie par rapport à O). Donc le couple (Δ, Δ') définit un élément bien déterminé du groupe quotient $SO(2)/\mathbb{Z}_2$, en notant $\mathbb{Z}_2$ le groupe à deux éléments formé de l'identité et de la symétrie par rapport à O. Ce groupe quotient s'appelle le groupe des angles orientés de droites.

On va voir que ce groupe est lui-même isomorphe à SO(2). En effet, définissons un homomorphisme

$$\varphi \quad SO(2) \longrightarrow SO(2)$$

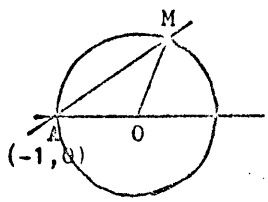
par $\varphi(\alpha) = 2\alpha$ (φ associe à chaque angle son double, en notation additive). Cet homomorphisme est surjectif, car tout angle orienté de demi-droites peut être divisé par



2 (il y a deux <u>bissectrices</u> d'un angle de demi-droites : ce sont deux demi-droites opposées). Le <u>noyau</u> de cet homomorphisme est évidemment le sous-groupe $\mathbb{Z}_2$ (formé des ω tels que $2\omega = 0$). Donc φ induit un <u>isomorphisme</u>

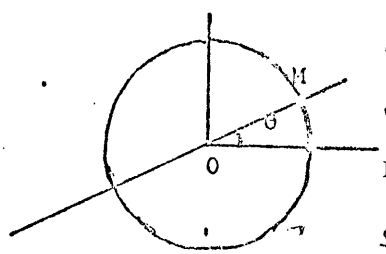
$$\Psi : SO(2) / \mathbb{Z}_2 \xrightarrow{\sim} SO(2).$$

<u>Interprétation géométrique de cet isomorphisme</u> (voir figure) : à toute <u>droite</u> AM passant par A on associe la <u>demi-droite</u> OM passant par O ; d'où une correspondance bijective entre les angles de droites et les angles de demi-droites. C'est la classique correspondance entre "angle inscrit" et "angle au centre".



3- <u>Angles non orientés de demi-droites.</u>

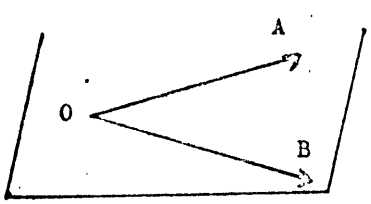
Considérons le cercle unité. Alors (cos θ, sin θ) caractérise un angle orienté de deux demi-droites (Ox, OM). Si on échange les rôles des demi-droites, (cos θ, sin θ) est remplacé par (cos θ, -sin θ).



Donc un angle non-orienté de demi-droites est caractérisé par son <u>cosinus</u> (nombre réel ≤ 1 et ≥ -1).

<u>Cas de la dimension</u> $n \geq 3$.

Soient OA et OB deux demi-droites dans l'espace $\mathbb{R}^n$ ($n \geq 3$). L'angle (OA, OB) est égal à (OB, OA), même au sens des déplacements directs de l'espace ambiant. Soit $A = (a_1, \ldots, a_n)$, $B = (b_1, \ldots, b_n)$. Alors



$$\cos\theta = \frac{\sum_{i=1}^{n} a_i b_i}{\sqrt{(\sum a_i^2)(\sum b_i^2)}} = \frac{\vec{a}.\vec{b}}{|\vec{a}| \times |\vec{b}|}$$

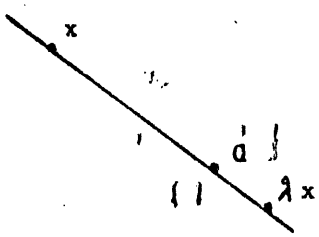
caractérise la classe d'équivalence de (OA, OB) modulo le groupe des déplacements directs.

GEOMETRIE PROJECTIVE REELLE

Définition de l'espace projectif $P_n(\mathbb{R}) = P_n$.

1- Du point de vue ensembliste :

On considère l'espace numérique $\mathbb{R}^{n+1}$ privé de l'origine $\{0\}$. Un point de cet espace est caractérisé par un $(n+1)$-uple $(x_0, x_1, \ldots, x_n)$, où les x_i ne sont pas tous nuls. On identifie deux points homothétiques x et λx, si $\lambda \in \mathbb{R}^*$, ou encore deux points alignés avec 0. Deux points sont donc équivalents s'ils définissent le même sous-espace vectoriel de dimension 1 : les classes d'équivalence sont en correspondance bijective avec les sous-espaces vectoriels de dimension 1 de l'espace $\mathbb{R}^{n+1}$.



Notons $\mathcal{R}$ cette relation d'équivalence dans $\mathbb{R}^{n+1} - \{0\}$; on pose $P_n(\mathbb{R}) = \mathbb{R}^{n+1} - \{0\}/\mathcal{R} \longleftrightarrow$ droites de $\mathbb{R}^{n+1}$ passant par 0. Soit $p : \mathbb{R}^{n+1} - \{0\} \longrightarrow P_n(\mathbb{R})$ l'application canonique de $\mathbb{R}^{n+1} - \{0\}$ sur son quotient. Si $u \in P_n(\mathbb{R})$, tout point $x = (x_0, x_1, \ldots, x_n)$ de $p^{-1}(u)$ définit ce qu'on appelle un système de coordonnées homogènes du point $u \in P_n(\mathbb{R})$.

Remarque. La relation d'équivalence $\mathcal{R}$ est celle définie, dans $\mathbb{R}^{n+1} - \{0\}$, par groupe des homothéties de rapport $\neq 0$; ce groupe opère dans $\mathbb{R}^{n+1} - \{0\}$ et est isomorphe au groupe multiplicatif $\mathbb{R}^* = \mathbb{R} - \{0\}$.

2- Du point de vue topologique.

L'espace numérique $\mathbb{R}^{n+1} - \{0\}$ est muni de la topologie habituelle. Puisque $P_n(\mathbb{R}) = \mathbb{R}^{n+1} - \{0\}/\mathcal{R}$, on va munir $P_n = P_n(\mathbb{R})$ de la topologie quotient : par définition un ensemble $U \subset P_n$ est ouvert si $p^{-1}(U) \subset \mathbb{R}^{n+1} - \{0\}$ est un ouvert de $\mathbb{R}^{n+1} - \{0\}$. Rappelons la propriété caractéristique de la topologie quotient : pour qu'une application $f : P_n \longrightarrow X$ (où X est un espace topologique quelconque) soit continue, il faut et il suffit que $f \circ p : \mathbb{R}^{n+1} - \{0\} \longrightarrow X$ soit continue.

Proposition. Soit A un ouvert de $\mathbb{R}^{n+1} - \{0\}$. Soit V le saturé de A, c'est-à-dire la réunion des classes d'équivalence qui rencontrent A. Alors V est ouvert.

[Conséquence : p(A) est un ouvert de $P_n(\mathbb{R})$; autrement dit, l'application p une application ouverte].

Démonstration. On sature un ensemble en prenant avec chaque point tous les homothétiques. Le saturé de A est donc $V = \bigcup_{\lambda \in \mathbb{R}^*} \lambda A$. Or si A est ouvert, λA est ouvert, car c'est le transformé d'un ouvert par un homéomorphisme ; par conséquent V est une réunion d'ouverts : c'est bien un ouvert.

Exemples d'espaces projectifs : P_0 est un point ;

P_1 est homéomorphe au cercle S^1 (on le verra plus loin).

Remarque. Soit U un ouvert de P_n. Alors $V = p^{-1}(U)$ est un ouvert de $\mathbb{R}^{n+1} - \{0\}$. On peut considérer le quotient $V/\mathcal{R}_V$, où $\mathcal{R}_V$ est la relation d'équivalence induite par $\mathcal{R}$ sur V ; $V/\mathcal{R}_V$ s'identifie, du point de vue ensembliste, à U.

Sur U il y a donc deux topologies :

(1) la topologie induite par celle de P_n ;

(2) la topologie quotient de $V/\mathcal{R}_V$.

En fait, ces topologies sont les mêmes ; en effet, soit $U' \subset U$; dire que U' est ouvert signifie :

- dans le cas (1), que $p^{-1}(U')$ est ouvert dans $\mathbb{R}^{n+1} - \{0\}$;
- dans le cas (2), que $p^{-1}(U')$ est un ouvert de V ; mais V étant un ouvert de $\mathbb{R}^{n+1} - \{0\}$, cela équivaut à dire que $p^{-1}(U')$ est ouvert dans $\mathbb{R}^{n+1} - \{0\}$. C.Q.F.D.

Définition. Soit $V_i \subset \mathbb{R}^{n+1} - \{0\}$ l'ensemble défini par : $(x_0, x_1, \ldots, x_n) \in V_i \Leftrightarrow$ $\Leftrightarrow x_i \neq 0$. C'est un ouvert, puisque x_i est une fonction continue. On a n+1 tels ouverts. De plus les V_i sont saturés, car si $x \in V_i$ et $\lambda \neq 0$, alors $\lambda x \in V_i$. On note $U_i = p(V_i)$: c'est un ouvert car $p^{-1}(U_i) = V_i$ est ouvert. U_i est l'ensemble des points tels que la i-ième coordonnée d'un système de coordonnées homogènes soit $\neq 0$.

Proposition. P_n est réunion des U_i ; ou encore : $\mathbb{R}^{n+1} - \{0\}$ est réunion des V_i.

C'est évident, car si $(x_0, \ldots, x_n) \in \mathbb{R}^{n+1} - \{0\}$, l'un au moins des x_i est $\neq 0$.

Proposition. Pour chaque i $(0 \leq i \leq n)$, il existe un homéomorphisme de U_i sur $\mathbb{R}^n$.

Définition. Les U_i forment ainsi un recouvrement ouvert de P_n ; on l'appelle le recouvrement ouvert canonique de P_n.

Démonstration. Supposons, pour fixer les idées, $i = 0$ et définissons un homéomorphisme de U_0 sur $\mathbb{R}^n$. On sait que $U_0 = V_0 / \mathcal{R}$. On définit deux applications continues

$$\begin{cases} f : \mathbb{R}^n \longrightarrow U_0 \\ g : U_0 \longrightarrow \mathbb{R}^n \end{cases}$$ comme suit :

1) f est la composée $\mathbb{R}^n \xrightarrow{i} V_0 \xrightarrow{p} U_0$, ou $i(x_1, \ldots, x_n) = (1, x_1, \ldots, x_n)$. L'application f est donc l'application qui à tout point $(x_1, \ldots, x_n) \in \mathbb{R}^n$ associe la classe d'équivalence de $(1, x_1, \ldots, x_n)$; f est composée de deux applications continues, donc est continue.

2) g est définie par passage au quotient : considérons l'application $h : V_0 \longrightarrow \mathbb{R}^n$ définie par $h(x_0, x_1, \ldots, x_n) = (\frac{x_1}{x_0}, \ldots, \frac{x_n}{x_0})$ (c'est possible puisque $x_0 \neq 0$).

h est continue, et est constante sur les classes d'équivalence, car

$$h(\lambda x_0, \lambda x_1, \ldots, \lambda x_n) = (\frac{x_1}{x_0}, \ldots, \frac{x_n}{x_0}) \quad \text{si} \quad \lambda \neq 0.$$

Par passage au quotient, on obtient $g : U_0 \longrightarrow \mathbb{R}^n$ qui est continue, puisque U_0 (avec sa topologie) est l'espace quotient de V_0 par la relation d'équivalence induite par $\mathcal{R}$ sur V_0.

Il reste à vérifier que $g \circ f = id$, et $f \circ g = id$.

$$g \circ f(x_1, \ldots, x_n) = g \circ p \circ i(x_1, \ldots, x_n) = h \circ i(x_1, \ldots, x_n) = h(1, x_1, \ldots, x_n) =$$

$$= (x_1, x_2, \ldots, x_n).$$

$$f \circ g(p(x_0, x_1, \ldots, x_n)) = f \circ h(x_0, x_1, \ldots, x_n) = f(\frac{x_1}{x_0}, \ldots, \frac{x_n}{x_0}) =$$

$$= p \circ i(\frac{x_1}{x_0}, \ldots, \frac{x_n}{x_0}) = p(1, \frac{x_1}{x_0}, \ldots, \frac{x_n}{x_0}) = p(x_0, x_1, \ldots, x_n).$$

Ainsi g est un homéomorphisme de U_0 sur $\mathbb{R}^n$, et f en est l'homéomorphisme réciproque. On ferait de même pour chaque U_i.

Corollaire. P_n est une variété topologique de dimension n, i.e. un espace topologique dont chaque point possède un voisinage ouvert homéomorphe à $\mathbb{R}^n$.

Sous-variétés linéaires projectives

On appelle sous-variété linéaire projective (ou simplement sous-variété projective) de P_n un sous-ensemble X de P_n qui vérifie la condition :

$$\boxed{p^{-1}(X) \cup \{0\} \text{ est un sous-espace vectoriel de } \mathbb{R}^{n+1}}$$

Ceci signifie que $p^{-1}(X)$ est un sous-espace vectoriel de $\mathbb{R}^{n+1}$ privé de $\{0\}$.

On a donc une correspondance bijective entre les sous-variétés projectives de P_n et les sous-espaces vectoriels de $\mathbb{R}^{n+1}$.

Exemples : $\emptyset$ est la variété linéaire projective qui correspond au sous-espace vectoriel réduit à 0.

Un point de P_n est une variété linéaire projective définie par un sous-espace vectoriel de dimension 1 de $\mathbb{R}^{n+1}$.

Définition. Une sous-variété projective $X \subset P_n$ est dite de dimension p si $p^{-1}(X) \cup \{0\}$ est un sous-espace vectoriel (de $\mathbb{R}^{n+1}$) de dimension $p+1$. Donc $\emptyset$ est de dimension -1, un point est de dimension 0. On appelle hyperplan projectif une variété projective de dimension $n-1$.

Remarque. $P_n - U_0$ est un ensemble fermé ; $p^{-1}(P_n - U_0) \cup \{0\}$ est l'ensemble des points de $\mathbb{R}^{n+1}$ dont la coordonnée x_0 est nulle ; donc $P_n - U_0$ est un hyperplan projectif ; on l'appelle l'hyperplan des "points à l'infini" de P_n (son complémentaire, homéomorphe à $\mathbb{R}^n$, s'identifie à l'ouvert des points "à distance finie").

la condition pour que $u^0, \ldots, u^k$ soient linéairement indépendants (au sens ... tif est que $x^0, \ldots, x^k$ soient linéairement indépendants (au sens vectoriel). Alors $x^0, \ldots, x^k$ engendrent un sous-espace vectoriel de dimension $k+1$; par suite la sous-variété projective engendrée par $u^0, \ldots, u^k$ est de dimension k.

Exercice : toute sous-variété projective de P_n, de dimension p, est homéomorphe à P_p.

Théorème.- L'espace projectif P_n est un espace compact ; il s'identifie au quotient de la sphère S^n par la relation d'équivalence antipodique.

[La relation antipodique, sur S^n, est celle dont les classes d'équivalence sont les ensembles de deux points diamétralement opposés].

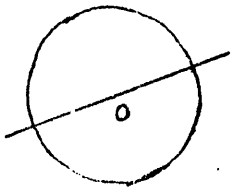
Démonstration.

a) Montrons d'abord que la topologie de P_n satisfait à l'axiome de Hausdorff, i.e. deux points distincts ont des voisinages ouverts disjoints. Soient x et y deux points distincts de P_n. Il existe un hyperplan projectif H tel que x et y ne soient pas dans H : en effet, x et y proviennent de deux vecteurs ξ et η de $\mathbb{R}^{n+1} - \{0\}$ non proportionnels ; il existe un hyperplan (vectoriel) de $\mathbb{R}^{n+1}$ ne contenant aucun de ces deux vecteurs. En effet, par une transformation linéaire on se ramène au cas où $\xi = (1, 0, \ldots, 0)$ et $\eta = (0, 1, 0, \ldots, 0)$. On cherche un hyperplan $a_0 \xi_0 + \ldots + a_n \xi_n = 0$ qui ne contienne ni $(1, 0, \ldots, 0)$ ni $(0, 1, 0, \ldots, 0)$; pour cela, il faut et il suffit que $a_0 \neq 0$ et $a_1 \neq 0$.

Soit donc H un tel hyperplan projectif, alors $U = P_n - H$ est un ouvert homéomorphe à $\mathbb{R}^n$, et on a $x, y \in U$; $\mathbb{R}^n$ étant séparé, la topologie de U est séparée, et on peut donc trouver deux ouverts U' et U'' de U disjoints qui contiennent respectivement x et y. U étant un ouvert de P_n, U' et U'' sont des ouverts de P_n.

C.Q.F.D.

b) Considérons l'inclusion $S^n \subset \mathbb{R}^{n+1} - \{0\}$, où $S^n = \{x \in \mathbb{R}^{n+1} : d(0, x) = 1\}$.

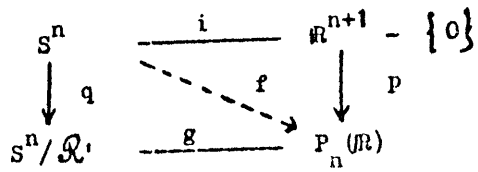


Soit $\mathcal{R}$ la relation d'équivalence définie par les homothéties sur $\mathbb{R}^{n+1} - \{0\}$, et soit $\mathcal{R}'$ la relation induite sur S^n ; il est clair que $\mathcal{R}'$ est la relation antipodique. Alors

l'injection $i : S^n \longrightarrow \mathbb{R}^{n+1} - \{0\}$ induit, par passage aux quotients, une injection

$$g : S^n/\mathcal{R}' \longrightarrow (\mathbb{R}^{n+1} - \{0\})/\mathcal{R} = P_n.$$

Le diagramme suivant est commutatif :



Soit $f = p \circ i = g \circ q$; p et i étant continues, f est continue, donc g est continue (d'après la caractérisation de la topologie quotient). Or on a :

Lemme 1. Soit $g : X \longrightarrow Y$ une application continue injective ; si Y est séparé, alors X est séparé. [Démonstration : exercice laissé au lecteur].

Démonstration. Ici, on sait que P_n est séparé (cf. a)) ; on en conclut que $\mathcal{R}$ est un espace topologique séparé . Or :

Lemme 2. Si un espace X a la propriété de Borel-Lebesgue, alors le quotient $X/\mathcal{R}$ de X par une relation d'équivalence $\mathcal{R}$ a aussi la propriété de Borel-Lebesgue. [Démonstration laissée au lecteur à titre d'exercice].

Ici, S^n est un espace compact, donc a la propriété de Borel-Lebesgue . D'après le lemme 2, $S^n/\mathcal{R}'$ a aussi cette propriété. Comme $S^n/\mathcal{R}'$ est séparé, on conclut que $S^n/\mathcal{R}'$ est compact.

c) On a l'application continue $g : S^n/\mathcal{R}' \longrightarrow P_n$; elle est injective ; elle est aussi surjective (car toute classe d'équivalence de $\mathbb{R}^{n+1} - \{0\}$ rencontre la sphère S^n) donc g est bijective. Or on sait qu'une application continue et bijective d'un espace compact dans un espace séparé est un homéomorphisme [car l'image directe d'un fermé est un fermé, puisque c'est un compact].

On conclut donc ici que P_n est compact, et que $g : S^n/\mathcal{R}' \longrightarrow P_n$ est un homéomorphisme , ce qui démontre le théorème.

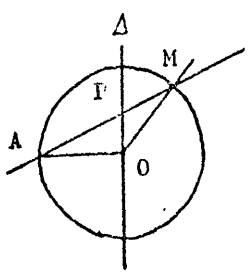
Cas particulier : P_1 est homéomorphe à $S^1/\mathbb{Z}_2$, où $S^1 = \{z \in \mathbb{C} : |z| = 1\}$, $\mathbb{Z}_2 = \{+1, -1\}$. C'est le groupe des angles de droites qui, lui-même, est homéomorphe à S^1 ; donc $P_1(\mathbb{R})$ est homéomorphe au cercle S^1.

Toute droite projective dans P_n est homéomorphe à P_1, donc à S^1.

Explicitons un homéomorphisme $S^1 \longrightarrow P_1$. Il suffit de composer l'homéomorphisme $S^1 \longrightarrow S^1/\mathbb{Z}_2$ qui, à chaque point M de S^1, associe la droite AM, avec l'homéomorphisme

$$S^1/\mathbb{Z}_2 \longrightarrow P_1$$

qu'on vient de trouver, et qui est finalement celui qui, à chaque droite du plan passant par A (où A est maintenant pris pour origine), associe le point correspondant de l'espace projectif P_1. Finalement l'homéomorphisme cherché $S^1 \longrightarrow P_1$ associe à chaque point M du cercle-unité de centre O la direction de droite AM (éventuellement : la direction tangente en A si M est confondu avec A). On encore, par projection stéréographique : soit Δ la droite de $\mathbb{R}^2$ passant par O et perpendiculaire à AO ; à chaque M du cercle-unité on associe le point $P \in \Delta$ situé sur la droite AM (du moins lorsque $M \neq A$), et le "point à l'infini" de Δ si $M = A$. On trouve ainsi, un homéomorphisme du cercle sur la droite Δ complétée par un point à l'infini.



Revenons au cas général de l'espace projectif P_n : par identification de $\mathbb{R}^n$ avec l'ouvert $U_o \subset P_n$, on voit que P_n est une "compactification" de $\mathbb{R}^n$ obtenue en adjoignant à $\mathbb{R}^n$ les points de l'"hyperplan à l'infini" $P_n - U_o$.

Etude du groupe linéaire-projectif $GLP(n, \mathbb{R})$.

Considérons le groupe $GL(n+1, \mathbb{R})$, qui opère dans $\mathbb{R}^{n+1}$, et aussi dans $\mathbb{R}^{n+1} - \{0\}$. Si $f \in GL(n+1, \mathbb{R})$, f transforme tout sous-espace vectoriel de dimension 1 en un sous-espace vectoriel de dimension 1 ; donc, par passage au quotient, f induit une application $\overline{f} : P_n \longrightarrow P_n$ qui est continue. D'ailleurs $\overline{f}$ est un homéomorphisme de P_n ; car si $g = f^{-1}$, on a $\overline{g} \circ \overline{f} = \overline{g \circ f} =$ identité de P_n, et $\overline{f} \circ \overline{g} = \overline{f \circ g} =$ identité de P_n. C.Q.F.D.

Les $\overline{f}$ ainsi associées aux $f \in GL(n+1, \mathbb{R})$ forment un groupe d'automorphismes de l'espace projectif P_n ; on l'appelle le groupe linéaire projectif, noté $GLP(n, \mathbb{R})$.

L'application qui associe $\overline{f}$ à f est un homomorphisme de groupes, car $\overline{g \circ f} = \overline{g} \circ \overline{f}$.

On a ainsi un homomorphisme surjectif : $GL(n+1, \mathbb{R}) \longrightarrow GLP(n, \mathbb{R})$. Cherchons son noyau : il se compose des $f \in GL(n+1, \mathbb{R})$ telles que $\overline{f}$ = identité. Cela signifie que f transforme chaque sous-espace vectoriel de dimension 1 de $\mathbb{R}^{n+1}$ en lui-même. Montrons que f est nécessairement une homothétie : soit $(e_1, \ldots, e_n)$ une base de $\mathbb{R}^{n+1}$; on veut que $f(e_i) = \lambda_i e_i$; de plus $f(e_1 + \ldots + e_n) = \lambda_1 e_1 + \ldots + \lambda_n e_n$ doit être de la forme $\mu(e_1 + \ldots + e_n)$; donc $\mu = \lambda_1 = \ldots = \lambda_n$, ce qui prouve que les λ_i sont égaux, et que f est une homothétie de rapport μ.

Le noyau cherché est donc le groupe des homothéties qui a servi à définir la relation d'équivalence ; il est isomorphe à $\mathbb{R}^*$ (groupe multiplicatif). On a ainsi une suite exacte :

$$(1) \longrightarrow \mathbb{R}^* \longrightarrow GL(n+1, \mathbb{R}) \longrightarrow GLP(n, \mathbb{R}) \longrightarrow (1).$$

On en déduit que le nombre de paramètres dont dépend une application $\sigma \in GLP(n, \mathbb{R})$ est $(n+1)^2 - 1 = n(n+2)$; ceci sera précisé plus loin.

Repères projectifs.

Définition. On appelle repère projectif dans P_n (ou simplement : repère) une suite $(a_0, a_1, \ldots, a_{n+1})$ de $n+2$ points tels que $n+1$ quelconques d'entre eux engendrent P_n, c'est-à-dire tels que $n+1$ quelconques d'entre eux ne soient pas contenus dans un hyperplan.

Notation : On désigne par $(a_0, \ldots, \widehat{a_i}, \ldots, a_{n+1})$ la suite privée du point a_i.

Exemples : $n = 1$; un repère de P_1 est une suite (a_0, a_1, a_2) de trois points tels que deux quelconques d'entre eux ne soient pas confondus. Un repère de P_1 est donc une suite de trois points distincts.

$n = 2$: un repère de P_2 est une suite $(a_0, \ldots, a_3)$ de quatre points tels que trois quelconque d'entre eux ne soient pas alignés (i.e. : sur une même droite projective).

Repère canonique. Il est formé de la suite des classes d'équivalence des vecteurs $e_0, \ldots, e_n$ et $e_0 + e_1 + \ldots + e_n$ [où $(e_0, \ldots, e_n)$ désigne la base canonique de $\mathbb{R}^{n+1}$].

Ce sont donc les $n+2$ points admettant les systèmes de coordonnées homogènes suivants :

$(1, 0, \ldots, 0)$, $(0, 1, 0, \ldots, 0)$, $\ldots$, $(0, \ldots, 0, 1)$, $(1, 1, \ldots, 1)$.

Par exemple, pour $n = 1$, on trouve

$$(1, 0)\ ,\ (0, 1),\ (1, 1).$$

qui sont des systèmes de coordonnées homogènes pour les points 0, ∞, 1 de la droite projective $P_1(\mathbb{R})$ (i.e. : $\mathbb{R}$ complétée par un point ∞).

Théorème. Le groupe projectif $GLP(n, \mathbb{R})$ opère d'une façon simplement transitive dans l'ensemble des repères projectifs de P_n.

Démonstration. Il suffit de montrer : si $(a_0, \ldots, a_{n+1})$ est un repère, il existe une $\overline{f} \in GLP(n, \mathbb{R})$ et une seule, telle que $\overline{f}$ transforme le repère canonique dans le repère $(a_0, \ldots, a_{n+1})$.

Pour cela, choisissons $x_i \in \mathbb{R}^{n+1} - \{0\}$ dans la classe d'équivalence de a_i (pour $0 \leq i \leq n+1$). On cherche une $f \in GL(n+1, \mathbb{R})$ telle qu'il existe des scalaires $\lambda_i \neq 0$ satisfaisant à

$$(1) \qquad \begin{cases} f(e_i) = \lambda_i x_i & \text{pour} \quad 0 \leq i \leq n, \\ f(e_0 + \ldots + e_n) = \lambda_{n+1} x_{n+1}, \end{cases}$$

en notant $(e_0, \ldots, e_n)$ la base canonique de $\mathbb{R}^{n+1}$. La deuxième relation (1) s'écrit (puisque f est linéaire)

$$\sum_{i=0}^{n} f(e_i) = \lambda_{n+1} x_{n+1},$$

c'est-à-dire, compte tenu de la première relation (1) :

$$(2) \qquad \sum_{i=0}^{n} \lambda_i x_i = \lambda_{n+1} x_{n+1}.$$

Puisque $(a_0, \ldots, a_{n+1})$ est un repère, $x_0, x_1, \ldots, x_n$ forment une base de $\mathbb{R}^{n+1}$, on a donc a priori

$$x_{n+1} = \sum_{i=0}^{n} \mu_i x_i,$$

et de plus les μ_i sont tous $\neq 0$, sinon il y aurait n parmi les x_i qui seraient linéairement dépendants, et $(a_0, \ldots, a_{n+1})$ ne serait pas un repère.

On voit maintenant qu'il est facile de choisir $\lambda_0, \ldots, \lambda_{n+1}$ de façon à satisfaire à (2) : le système $(\lambda_0, \ldots, \lambda_n, \lambda_{n+1})$ est nécessairement proportionnel à

$$(\mu_0, \ldots, \mu_n, 1).$$

Ceci montre que f existe, et est <u>déterminée à une homothétie près</u>. Donc $\bar{f}$ existe et est unique. C.Q.F.D.

<u>Remarque</u> : le choix du repère canonique met donc en correspondance (bijective) <u>l'ensemble des repères projectifs</u> et l'<u>ensemble sous-jacent au groupe</u> $GLP(n, \mathbb{R})$. Or l'ensemble des repères projectifs a une topologie naturelle, car il s'identifie à un sous-ensemble de

$$(P_n(\mathbb{R}))^{n+2}$$

(espace des suites <u>quelconques</u> de $n+2$ points de $P_n(\mathbb{R})$).

[<u>Exercice</u> : montrer que l'espace des repères projectifs est un <u>ouvert</u> de $(P_n)^{n+2}$ c'est donc une <u>variété de dimension</u> $n(n+2)$. Ainsi $GLP(n, \mathbb{R})$ se trouve muni d'une structure de variété topologique de dimension $n(n+2)$].

<u>Exercice</u> : (1) La topologie ainsi définie sur $GLP(n, \mathbb{R})$ est la <u>topologie quotient</u> de

$$GL(n+1, \mathbb{R})/\mathbb{R}^* .$$

(2) Note. $Rep(P_n)$ l'espace des repères projectifs de P_n, et $Rep(\mathbb{R}^{n+1})$ l'espace des reperes vectoriels de $\mathbb{R}^{n+1}$ (i.e. : des <u>bases</u> de $\mathbb{R}^{n+1}$). A chaque base $(x_0, \ldots, x_n)$ de $\mathbb{R}^{n+1}$ associons le repère de P_n formée des classes d'équivalence

$$p(x_0), \ldots, p(x_n), \quad p(x_0 + x_1 + \ldots + x_n).$$

On obtient ainsi une application <u>continue surjective</u>

$$\varphi : Rep(\mathbb{R}^{n+1}) \longrightarrow Rep(P_n).$$

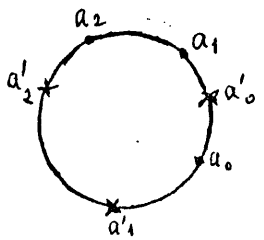
Montrer que le diagramme suivant est commutatif :

$$\begin{array}{ccc} Rep(\mathbb{R}^{n+1}) & \xrightarrow{\varphi} & Rep(P_n) \\ \downarrow \approx & & \downarrow \approx \\ GL(n+1, \mathbb{R}) & \xrightarrow{\psi} & GLP(n, \mathbb{R}) \end{array}$$

où les flèches verticales désignent les bijections canoniques, et où ψ est l'application $f \longmapsto \bar{f}$.

Proposition. GLP(n, $\mathbb{R}$) est connexe pour n pair, et a deux composantes connexes lorsque n est impair.

Démonstration. Regardons d'abord le cas où $n = 1$. On peut se rendre compte du fait que GLP(1, $\mathbb{R}$) n'est pas connexe : un repère est une suite de trois points distincts sur le cercle ; peut-on faire varier (a'_0, a'_1, a'_2) de façon continue et le faire coïncider avec (a_0, a_1, a_2) sans que les trois points cessent d'être distincts à chaque instant ? Il est intuitif (ceci n'est pas encore une démonstration) que ce n'est pas possible si les points des deux repères ne sont pas rencontrés "dans le même ordre circulaire" lorsqu'on parcourt le cercle.



On va maintenant traiter le problème en général. Rappelons que GLP(n, $\mathbb{R}$) $\approx$ GL(n+1, $\mathbb{R}$)/$\mathbb{R}^*$; dans GL(n+1, $\mathbb{R}$), on a le groupe spécial SL(n+1, $\mathbb{R}$). On se pose alors le problème suivant : y-a-t-il un représentant de chaque classe dans SL(n+1, $\mathbb{R}$) ?

Soit $\sigma \in$ GL(n+1, $\mathbb{R}$) ; par une homothétie de rapport $\lambda \neq 0$ on obtient σ', et on se demande si on peut choisir λ de façon que det $\sigma' = +1$. Or si on compose σ avec une homothétie de rapport λ, le déterminant est multiplié par λ^{n+1}. D'où deux cas à distinguer :

1er cas. n est pair. Alors n+1 est impair, et λ^{n+1} peut prendre toute valeur réelle $\neq 0$. Donc toute classe de GL(n+1, $\mathbb{R}$) modulo le groupe des homothéties rencontre SL(n+1, $\mathbb{R}$), et l'application naturelle

$$SL(n+1, \mathbb{R}) \longrightarrow GL(n+1, \mathbb{R})/\mathbb{R}^* \approx GLP(n, \mathbb{R})$$

est surjective ; comme SL(n+1, $\mathbb{R}$) ne rencontre le sous-groupe $\mathbb{R}^*$ des homothéties que pour $\lambda = 1$, on trouve un isomorphisme

$$SL(n+1, \mathbb{R}) \approx GLP(n, \mathbb{R}).$$

Alors, SL(n+1, $\mathbb{R}$) étant connexe, GLP(n, $\mathbb{R}$) est connexe.

2ème cas. n est impair. Alors n+1 est pair, donc $\lambda^{n+1} > 0$ pour tout

$\lambda \neq 0$; on peut donc seulement ramener le déterminant de σ à être $+1$ ou -1. Toute classe d'équivalence ne rencontre donc plus $SL(n+1, \mathbb{R})$ celles qui le rencontre sont les classes des éléments de $GL^+(n+1, \mathbb{R})$ et elles rencontrent $SL(n+1, \mathbb{R})$ pour deux valeurs opposées de λ. Posons $GLP^+(n, \mathbb{R}) = GL^+(n+1, \mathbb{R})/\mathbb{R}^*$, où $\mathbb{R}^*$ est le groupe des homothéties de rapport non nul. On a alors

$$GLP^+(n, \mathbb{R}) \approx SL(n+1, \mathbb{R})/\{+1, -1\}$$

[Observons qu'une homothétie de rapport -1 a un déterminant $= +1$] Ainsi $GLP(n, \mathbb{R})$ a deux composantes connexes : celle qui contient l'élément neutre est $GLP^+(n, \mathbb{R}) \approx SL(n+1, \mathbb{R})/\{\pm 1\}$

[Nota : nous avions déjà fait cette observation pour $n = 1$, lorsque nous avons étudié le groupe homographique réel].

Questions d'orientabilité.

Soit V un espace vectoriel réel de dimension $n \geq 1$, que signifie "orienter cet "espace" ?

Soit $(e_1, \ldots, e_n)$ une base de V ; on dit que deux bases définissent la même orientation si et seulement si la transformation linéaire $\sigma \in GL(V)$ qui transforme l'une dans l'autre a un déterminant > 0. Les bases se répartissent en deux familles : deux bases quelconques de la même famille définissent une même orientation de V, deux bases de deux familles distinctes définissent des orientations différentes. On a ainsi deux orientations possibles pour un espace vectoriel V de dimension ≥ 1.

Si on considère $V = \mathbb{R}^n$, alors on peut se contenter de regarder les bases orthonormées. Pour orienter $\mathbb{R}^n$, il suffit de se donner une base orthonormée de $\mathbb{R}^n$. Une autre base de $\mathbb{R}^n$ définit la même orientation si et seulement si la matrice qui fait passer de l'une à l'autre appartient à $SO(n)$, c'est-à-dire si son déterminant est $+1$.

Considérons maintenant le cas de la sphère S^n c'est une sous-variété de $\mathbb{R}^{n+1}$ $S^n \subset \mathbb{R}^{n+1} - \{0\}$. Soit $M \in S^n$, et soit H l'hyperplan tangent en M à S^n. On a alors l'espace vectoriel V correspondant, qui est le translaté de H passant par 0. Orienter la sphère au point M, c'est orienter l'hyperplan tangent en M, ou

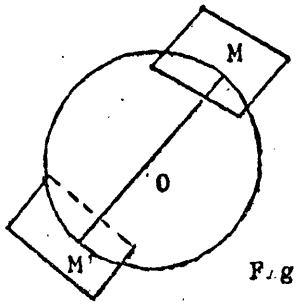
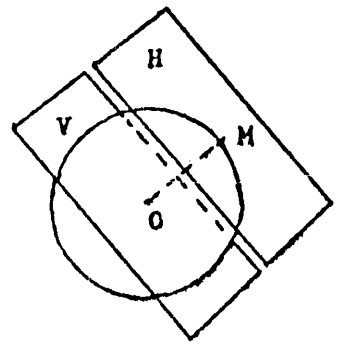


Fig.2



encore orienter l'hyperplan passant par O et orthogonal à OM. Pour cela, on se donne une base orthonormée $(e_1, \ldots, e_n)$ de V. Soit $e_o = \overrightarrow{OM}$. Alors $(e_o, e_1, \ldots, e_n)$ est une base orthonormée de l'espace $\mathbb{R}^{n+1}$. Deux bases $(e_1, \ldots, e_n)$ et $(e'_1, \ldots, e'_n)$ de V définissent la même orientation au point M si et seulement si on passe de la base $(e_o, e_1, \ldots, e_n)$ à la base (e_o, e'_1, e'_n) par une transformation de déterminant +1.

Si maintenant on a une orientation en $M \in S^n$, définie par une base orthonormée $(\overrightarrow{OM}, e_1, \ldots, e_n)$, et une orientation en $M' \in S^n$, définie par une base orthonormée $(\overrightarrow{OM'}, e'_1, \ldots, e'_n)$, elles (sont "en accord" si les deux bases de $\mathbb{R}^{n+1}$:

$$(\overrightarrow{OM}, e_1, \ldots, e_n) \quad \text{et} \quad (\overrightarrow{OM'}, e'_1, \ldots, e'_n)$$

définissent la même orientation de l'espace vectoriel $\mathbb{R}^{n+1}$.

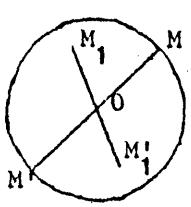
Considérons enfin l'espace projectif P_n comme quotient de la sphère S^n par la relation antipodique. Par définition, si $M \in S^n$, une orientation de S^n au point M définit une orientation de P_n au point de la classe de M ; mais on convient qu'une orientation de S^n au point M' diamétralement opposé à M définit la même orientation de P_n (au même point de P_n) si la symétrie par rapport à O. transforme l'orientation de S^n en M dans l'orientation de S^n en M' (Fig.2); cela signifie que l'orientation de S^n en M, définie par une base orthonormée

$$(e_o = \overrightarrow{OM}, e_1, \ldots, e_n)$$

de $\mathbb{R}^{n+1}$, et l'orientation de S^n en M', définie par la base orthonormée

$$(-e_o = \overrightarrow{OM'}, -e_1, \ldots, -e_n)$$

définissent la même orientation de P_n au point défini par la classe d'équivalence antipodique formée de M et M'.



Si (M, M') et (M_1, M'_1) sont deux points distincts de P_n, on dira qu'une orientation de P_n au point (M, M') est en accord avec une orientation au point

(M_1, M_1') si les orientations correspondantes de S^n aux points M et M' d'une part, aux points M_1 et M_1' d'autre part, sont toutes en accord. Ceci suppose déjà que les orientations en M et en M' sont en accord, c'est-à-dire que les deux bases

$$(e_o, e_1, \ldots, e_n) \quad \text{et} \quad (-e_o, -e_1, \ldots, -e_n)$$

définissent la même orientation de $\mathbb{R}^{n+1}$. Or le déterminant de la transformation qui fait passer de l'une à l'autre est $(-1)^{n+1}$; donc n doit être impair. S'il en est ainsi, on pourra, pour chaque point de P_n, choisir une orientation de façon que toutes ces orientations soient "en accord" : on dira qu'on a orienté P_n (et ceci est possible de deux façons). En revanche, pour n pair, on ne peut pas orienter P_n : on dit que P_n est non-orientable.

On voit que ces phénomènes sont en relation avec le fait que $GLP(n, \mathbb{R})$ est non-connexe pour n impair (P_n orientable), et connexe pour n pair (P_n non-orientable).

Caractérisations diverses des transformations linéaires-projectives.

Soit $\sigma \in GLP(n, \mathbb{R})$; si V_k est une sous-variété projective de dimension k, il est clair que $\sigma(V_k)$ est aussi une sous-variété projective de dimension k. En effet, σ provient par passage au quotient d'une $f \in GL(n+1, \mathbb{R})$, et f transforme tout sous-espace vectoriel de dimension k+1 en un espace vectoriel de dimension k+1. Il est naturel de se poser la question suivante : si un automorphisme σ de P_n transforme toute sous-variété projective en une sous-variété de même dimension, peut-on conclure que $\sigma \in GLP(n, \mathbb{R})$? On va voir maintenant des réponses à cette question.

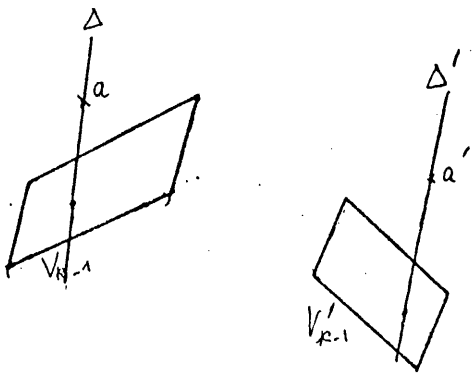
Lemme 1. Soit f une application de P_n dans lui-même. On suppose que f applique bijectivement toute droite projective Δ sur une droite projective Δ'. Alors, pour tout entier k $(1 \leq k \leq n)$ et pour toute variété linéaire projective V_k de dimension k, f applique bijectivement V_k sur une variété linéaire projective V_k' de même dimension k. En particulier (pour $k = n$), f applique bijectivement P_n sur lui-même.

Démonstration.

1) f est injective. En effet, deux points distincts définissent une droite (projective) et une seule Δ ; puisque f applique bijectivement Δ sur une droite Δ'

par hypothèse, les transformés des deux points sont distincts.

2) Faisons une récurrence sur k. Pour $k = 1$, la propriété à démontrer est vraie par hypothèse. Supposons-la vraie pour $k-1$ $(k \geq 2)$, et montrons-la pour k. Soit V_k une sous-variété de dimension k, et soit V_{k-1} une sous-variété de dimension $k-1$ contenue dans V_k. Soit $a \in V_k$, $a \notin V_{k-1}$. Nous savons que deux sous-variétés de dimensions complémentaires dans V_k se coupent toujours.



Donc toute droite de V_k qui passe par a coupe V_{k-1} en un point et un seul.

V_k est donc réunion des droites passant par a et qui rencontrent V_{k-1}. Par l'hypothèse de récurrence, on sait que V_{k-1} est transformée bijectivement par f en une sous-variété V'_{k-1} de dimension $k-1$. Soit $f(a) = a'$; on a $a' \notin V'_{k-1}$ puisque f est injective. Si Δ est une droite de V_k qui passe par a, alors $\Delta' = f(\Delta)$ est une droite qui passe par a' et rencontre V'_{k-1}. Réciproquement toute droite qui passe par a' et qui rencontre V'_{k-1} provient d'une droite passant par a et qui rencontre V_{k-1}, car f applique bijectivement V_{k-1} sur V'_{k-1}. On en déduit que $f(V_k)$ est la réunion des droites Δ' passant par a' et qui rencontrent V'_{k-1} ; c'est donc la variété linéaire projective V'_k engendrée par a' et V'_{k-1}, qui est de dimension k puisque $a' \notin V'_{k-1}$. Et f, qui est injective, induit donc une bijection de V_k sur V'_k.

C.Q.F.D.

Birapport.

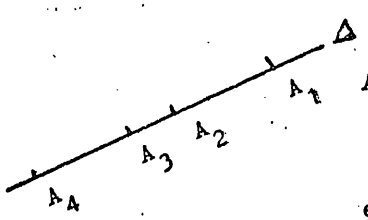
On a déjà défini (p. 250) le birapport de 4 points distincts de $P_1(\mathbb{R})$,

$$(z_1 ; z_2 ; z_3 ; z_4) = \frac{z_4 - z_1}{z_4 - z_2} : \frac{z_3 - z_1}{z_3 - z_2},$$

qui a un sens même si l'un des z_i est ∞.

Nous savons qu'une transformation homographique σ conserve le birapport

$$(\sigma(z_1) ; \sigma(z_2) ; \sigma(z_3) ; \sigma(z_4)) = (z_1 ; z_2 ; z_3 ; z_4)$$



Soit maintenant Δ une droite de P_n, et soient A_1, A_2, A_3, A_4 quatre points distincts de Δ ; on veut définir le birapport de ces quatre points. Nous avons défini une bijection entre les droites projectives Δ et les sous-espaces vectoriels de dimension 2 de $\mathbb{R}^{n+1}$; à Δ on associe $p^{-1}(\Delta) \cup \{0\}$. Une base de $p^{-1}(\Delta) \cup \{0\}$ définit un isomorphisme vectoriel de $p^{-1}(\Delta) \cup \{0\}$ sur $\mathbb{R}^2$, d'où, par passage au quotient, une bijection ω de Δ sur $P_1(\mathbb{R})$. Si on change de base, la bijection ω est remplacée par $\alpha \circ \omega$, où $\alpha : P_1 \longrightarrow P_1$ est une transformation homographique (déduite d'un automorphisme linéaire de $\mathbb{R}^2$ par passage au quotient).

Par définition, le rapport anharmonique $(A_1 , A_2 , A_3 ; A_4)$ des quatre points de Δ est égal au birapport

$$(\omega(A_1) ; \omega(A_2) ; \omega(A_3) \quad \omega(A_4))$$

des points de P_1 qui leur correspondent par ω. Cette définition est justifiée par le fait que si on remplace ω par $\alpha \circ \omega$, ce birapport n'est pas changé (puisque le birapport de quatre points de P_1 est invariant par toute transformation homographique α).

Ayant ainsi défini le birapport de quatre points alignés de P_n, nous pouvons énoncer :

Proposition. - Soit $\sigma \in GLP(n, \mathbb{R})$. Si A_1, A_2, A_3, A_4 sont quatre points alignés et distincts de P_n, on a

$$(\sigma(A_1) ; \sigma(A_2) ; \sigma(A_3) ; \sigma(A_4)) \quad (A_1 ; A_2 ; A_3 ; A_4)$$

[En bref : les transformations linéaires-projectives conservent le birapport de quatre points alignés].

Démonstration. Soit Δ la droite projective contenant A_1, A_2, A_3 et A_4, et soit $\Delta' = \sigma(\Delta)$. Soient $V = p^{-1}(\Delta) \cup \{0\}$, $V' = p^{-1}(\Delta') \cup \{0\}$; σ provient, par passage aux quotients, d'un automorphisme linéaire f de $\mathbb{R}^{n+1}$, tel que $f(V) = V'$. Choisissons comme plus haut un isomorphisme vectoriel $\varphi : V' \xrightarrow{\sim} \mathbb{R}^2$, qui induit $\omega' : \Delta' \longrightarrow P_1$. Alors $\varphi \circ f$ est un isomorphisme vectoriel

$V \longrightarrow \mathbb{R}^2$, qui induit $\omega : \Delta \longrightarrow P_1$. On a $\omega = \omega' \circ \sigma$. Par définition, on a

$$(A_1 ; A_2 ; A_3 ; A_4) = (\omega(A_1) ; \omega(A_2) ; \omega(A_3) ; \omega(A_4)) ;$$

si $A'_i = \sigma(A_i)$ $(i = 1, 2, 3, 4)$, on a

$$(A'_1 ; A'_2 ; A'_3 ; A'_4) = (\omega'(A'_1) ; \omega'(A'_2) ; \omega'(A'_3) ; \omega'(A'_4)).$$

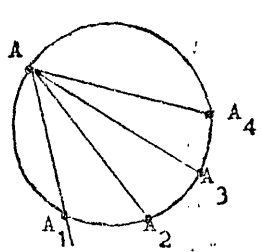
Puisque $\omega = \omega' \circ \sigma$, on a $\omega(A_i) = \omega'(A'_i)$, d'où l'égalité annoncée :

$$(A_1 ; A_2 ; A_3 ; A_4) = (A'_1 ; A'_2 ; A'_3 ; A'_4).$$

Exercice 1. Dans le plan projectif, coupons quatre droites concourantes distinctes Δ_1, Δ_2, Δ_3, Δ_4 par une sécante Δ les coupant en des points distincts A_1, A_2, A_3, A_4. Montrer que $(A_1 ; A_2 ; A_3 ; A_4)$ ne dépend pas du choix de la sécante Δ ; on l'appelle le birapport des quatre droites concourantes Δ_1, Δ_2, Δ_3, Δ_4 (dans cet ordre).

Exercice 2. Soient D_1, D_2, D_3, D_4 quatre droites distinctes passant par l'origine de $\mathbb{R}^2$; elles définissent des droites projectives Δ_1, Δ_2, Δ_3, Δ_4 dans $P_2(\mathbb{R})$ ($\mathbb{R}^2$ étant identifié au complémentaire de la droite de l'infini dans P_2). Montrer que $(\Delta_1 ; \Delta_2 ; \Delta_3 ; \Delta_4)$ [cf. exercice 1] est égal au birapport des quatre points de $P_1(\mathbb{R})$ définis respectivement par les sous-espaces vectoriels D_1, D_2, D_3, D_4 de $\mathbb{R}^2$.

Exercice 3. On a plus haut identifié S^1 à $P_1(\mathbb{R})$. Par cette identification, on définit le birapport de quatre points distincts A_1, A_2, A_3, A_4 du cercle S^1 ; montrer qu'il est égal au birapport des quatre droites AA_1, AA_2, AA_3, AA_4 joignant un point $A \in S^1$ aux points A_1, A_2, A_3, A_4.



Théorème 1.- Soit $f : P_1 \longrightarrow P_1$ une application injective qui conserve le birapport de quatre points. Alors $f \in GLP(1, \mathbb{R})$.

Démonstration. $(f(0), f(\infty), f(1))$ est un repère projectif. Il existe donc $\sigma \in GLP(1, \mathbb{R})$ tel que : $\sigma(0) = f(0)$, $\sigma(\infty) = f(\infty)$, $\sigma(1) = f(1)$.

Alors $g = \sigma^{-1} \circ f$ laisse fixes 0, ∞ et 1. On sait que $(0 ; \infty ; 1 ; x) = x$; d'autre part g conserve le birapport donc

$x = (0 ; \infty ; 1 ; x) = (g(0) ; g(\infty) ; g(1) ; g(x)) = (0 ; \infty ; 1 ; g(x)) = g(x)$. C.Q.F.D

Théorème 2.- Soit f une application injective de P_n dans P_n qui transforme des points alignés en points alignés et qui conserve le birapport de quatre points distincts alignés. Alors $f \in GLP(n, \mathbb{R})$.

Démonstration. Puisque f conserve le birapport de quatre points alignés, f applique toute droite Δ de P_n bijectivement sur une droite Δ' de P_n. Nous savons alors (cf. lemme 1 ci-dessus) que f est bijective, et que f et f^{-1} transforment toute variété linéaire projective en une variété linéaire projective de même dimension.

En particulier, f transforme tout repère projectif en un repère projectif. Rappelons qu'un repère projectif est une suite de $n+2$ points $a_0, a_1, \ldots, a_{n+1}$ tels que $n+1$ quelconques d'entre eux ne soient pas dans un hyperplan. On en déduit que $f(a_0), f(a_1), \ldots, f(a_{n+1})$ vérifient aussi la même propriété, et par conséquent forment un repère projectif de P_n.

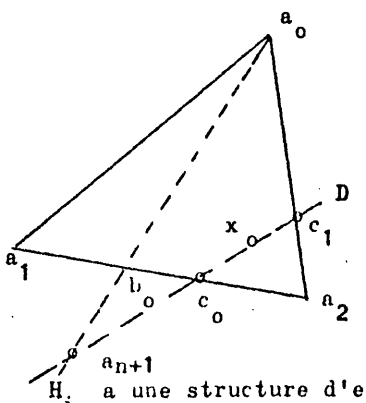
Soit σ la transformation de $GLP(n, \mathbb{R})$ qui envoie le repère $(a_0, a_1, \ldots, a_{n+1})$ sur le repère $(f(a_0), f(a_1), \ldots, f(a_{n+1}))$. On a donc $\sigma(a_i) = f(a_i)$ pour tout i $(0 \leq i \leq n+1)$. L'automorphisme $g = \sigma^{-1} \circ f$ laisse fixes les points $a_0, a_1, \ldots, a_{n+1}$ et transforme des points alignés en points alignés, chaque variété linéaire projective en une variété linéaire projective de même dimension. De plus, g conserve le rapport anharmonique de quatre points alignés. On est donc ramené à prouver le théorème dans le cas particulier où f laisse fixes les points d'un repère projectif. Il suffit alors de démontrer :

Proposition. Si $f : P_n \longrightarrow P_n$ est un automorphisme qui laisse fixes les points d'un repère projectif, transforme des points alignés en points alignés, et conserve le birapport de quatre points alignés distincts, alors f est l'identité.

Démonstration. Elle se fait par récurrence sur n : c'est vrai pour n = 1, en vertu du théorème 1. Supposons que la proposition soit vraie pour n-1 ($n \geq 2$), et montrons la pour n.

Notation : Soit, pour $0 \leq i \leq n$, (H_i) l'hyperplan projectif engendré par les n+1 premiers points du repère sauf a_i :

$$H_i = \{a_0, a_1, \ldots, \hat{a_j}, \ldots, a_n\}$$



Exemple (n = 2) :

H_0 = droite $a_1 a_2$

H_1 = droite $a_0 a_2$

H_2 = droite $a_0 a_1$

H_i a une structure d'espace projectif de dimension n-1 ; $f(H_i)$ est donc un hyperplan $H_i' = \{f(a_0), \ldots, \widehat{f(a_i)}, \ldots, f(a_n)\}$. On a $H_i' = H_i$ puisque f laisse les points du repère projectif. Montrons que la restriction de f à H_i est l'identité ; pour cela il suffit de montrer que f laisse fixes les points d'un repère projectif dans H_i, et d'appliquer l'hypothèse de récurrence. Etudions par exemple le cas de H_0, ce qui n'enlève rien à la généralité ; dans H_0, les points $a_1, a_2, \ldots, a_n$ sont fixes par f ; soit b_0 le point de rencontre de H_0 avec la droite $a_0 a_{n+1}$, qui est transformée par f en elle-même. Alors $f(b_0) = b_0$ nécessairement, car $f(b_0)$ appartient à $f(H_0) = H_0$ et à la droite $a_0 a_{n+1}$.

Alors $(b_0, a_1, \ldots, a_n)$ est un repère de H_0, et f laisse fixes les points de ce repère. Par l'hypothèse de récurrence, f laisse fixes tous les points de

$H_0 \Longrightarrow f|H_0 = \text{identité}$.

De même, pour tout i tel que $0 \leq i \leq n$, on a $f \mid H_i = \text{identité}$. Montrons maintenant que les points qui n'appartiennent à aucun des H_i sont fixes par f. C'est bien le cas du point a_{n+1}, par hypothèse. Soit alors $x \neq a_{n+1}$, $x \notin H_i$ pour $0 \leq i \leq n$.

La droite D joignant x et a_{n+1} coupe chaque H_i en un point c_i et un seul, sinon elle serait contenue dans H_i, ce qui est absurde puisque $a_{n+1} \notin H_i$. On a $f(c_i) = c_i$ puisque $c_i \in H_i$; $c_i \neq a_{n+1}$ car $a_{n+1} \notin H_i$,

$c_i \neq x$ car $x \notin H_i$.

De plus, c_i et a_{n+1} étant fixes par f, la droite D se transforme en elle-même. Nous savons que si trois points distincts d'une droite D sont fixes par f qui conserve le birapport alors tous les points de D sont fixes. Il reste à montrer que les points $c_0, c_1, \ldots, c_n$ ne sont pas tous confondus ; il en résultera que tous les points de D sont fixes, donc que $f(x) = x$. Or $c_0 \in H_0$, $c_1 \in H_1, \ldots, c_n \in H_n$; il suffit donc de montrer que $H_0 \cap H_1 \cap \ldots \cap H_n = \emptyset$. Raisonnons par l'absurde : soient $x_0, \ldots, x_n \in \mathbb{R}^{n+1}$ dans les classes d'équivalence de $a_0, \ldots, a_n$ respectivement. Alors $(x_0, \ldots, \widehat{x_i}, \ldots, x_n)$ est la base d'un hyperplan $V_i \subset \mathbb{R}^{n+1}$ tel que $V_i = p^{-1}(H_i) \cup \{0\}$. L'intersection des V_i est réduite à $\{0\}$, car si $\sum_{i=0}^{n} \lambda_i x_i \in V_i$ on a $\lambda_i = 0$. Donc $\bigcap_i H_i = \emptyset$. C.Q.F.D.

Théorème 3. On suppose $n \geq 2$. Soit f une application injective de P_n dans P_n qui transforme des points alignés en points alignés et des points non alignés en points non alignés ; alors f est un automorphisme linéaire projectif.

Démonstration. Observons d'abord que le théorème 3 est faux pour $n = 1$; en effet, dans ce cas, le théorème devient :

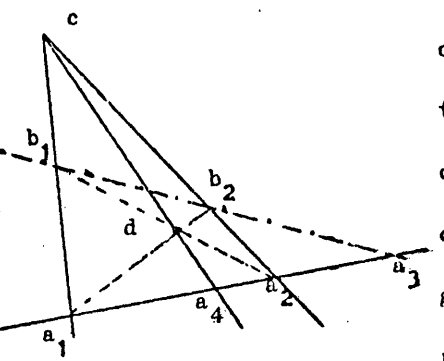
"toute application injective de P_1 dans P_1 est homographique", ce qui est absurde.

Nous supposons donc $n \geq 2$. D'après le théorème 2, il nous suffit de montrer que f conserve le birapport de quatre points distincts alignés.

Définition. On dit que quatre points distincts x_1, x_2, x_3, x_4 sur une droite Δ forment une division harmonique si et seulement si $(x_1 ; x_2 ; x_3 ; x_4) = -1$. On vérifie alors que $(x_3 ; x_4 ; x_1 ; x_2) = -1$, $(x_2 ; x_1 ; x_4 ; x_3) = 1$, $(x_4 ; x_3 ; x_2 ; x_1) = -1$. On dit alors que x_3 et x_4 sont conjugués harmoniques par rapport à x_1 et x_2 (et réciproquement).

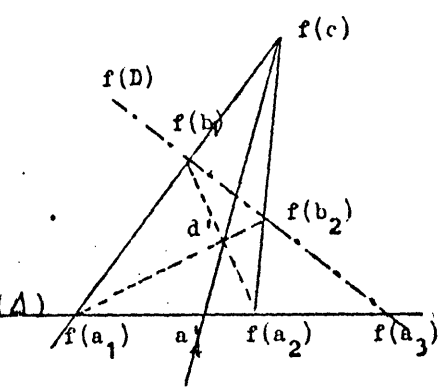
a) Montrons que, sous les hypothèses de l'énoncé, f transforme toute division harmonique en une division harmonique : si on a trois points (distincts alignés) a_1, a_2, a_3 alors on a une construction géométrique du point a_4, conjugué harmonique de a_3 par rapport à a_1 et a_2. Soit Δ la droite $a_1 a_2 a_3$, et soit $c \notin \Delta$, ce qui est possible

puisque $n \geq 2$. Soit $D \neq \Delta$ une droite quelconque issue de a_3, mais distincte de Δ et ne passant pas par c ; elle coupe ca_1 en b_1, ca_2 en b_2. On obtient un "quadrilatère complet" dont les "diagonales" b_1a_2 et a_1b_2 se coupent en d. La droite cd coupe Δ en le point a_4 cherché. Les transformés $f(a_1)$, $f(a_2)$, $f(a_3)$ sont alignés et distincts, car f est injective ; $f(c)$ n'est pas aligné avec $f(a_1)$, $f(a_2)$ puisque f transforme des points non alignés en points non alignés.



On fait alors la même construction que précédemment pour construire $f(a_4)$. La droite $f(D)$ coupe $f(c)f(a_1)$ en $b_1' = f(b_1)$ et $f(c)f(a_2)$ en $b_2' = f(b_2)$. On en déduit facilement que $d' = f(d)$ et par suite que $a_4' = f(a_4)$. On a donc

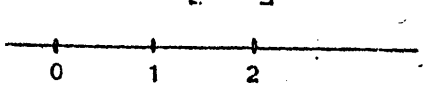
$$(a_1;a_2;a_3;a_4) = (f(a_1); f(a_2); f(a_3); f(a_4)) = -1$$



b) Montrons maintenant que f conserve le birapport.

Soit Δ une droite. Quitte à composer f avec une transformation $\sigma \in GLP(n, \mathbb{R})$, on peut supposer que f transforme Δ en elle-même. Il reste donc à montrer que si une transformation injective $f : \Delta \longrightarrow \Delta$ transforme toute division harmonique en division harmonique, alors f conserve le birapport de quatre points distincts de Δ. Par un isomorphisme de Δ avec $P_1(\mathbb{R})$, il suffit de faire la démonstration pour P_1, identifié à $\mathbb{R}$ complété par un point ∞.

Quitte à composer f avec une homographie, on peut supposer que f laisse fixes les trois points distincts 0, ∞ et 1. Il s'agit de montrer que f est alors l'identité, sachant que f transforme toute division harmonique en division harmonique. Montrons d'abord que $f(2) = 2$. Le conjugué harmonique de ∞ par rapport à 0 et 2 est le milieu de $[0, 2]$ soit 1. Donc le conjugué harmonique de $f(\infty)$ par rapport à $f(0)$, et $f(2)$ est $f(1)$, qui est le milieu de



$[f(0), f(2)]$. Or $f(1) = 1$, $f(0) = 0 \Longrightarrow 1$ est le milieu de $[f(0), f(2)] \Rightarrow f(2) =$?

On démontre de la même manière que tous les points à cordonnées entières sont fixes par f. Le conjugué harmonique de ∞ par rapport à 0 et 1 est $\frac{1}{2}$. On en d[illegible] $\frac{1}{2}$ est fixe par f, ainsi que $\frac{3}{2}$, $\frac{5}{2}$,.... On trouve ensuite que tous les points $\frac{p}{2^k}$, où $p \in \mathbb{Z}$, sont fixes : ce sont les nombres dyadiques. Pour achever la démonstration, il nous suffit de montrer que f conserve l'ordre (i.e. que f est continue) : en effet dans ce cas tout point d'un segment dont les extrémités sont fixes par f est transformé par f en un point de ce même segment, et par conséquent on voit à la limite que f laisse fixes tous les points de P_1.

Soient donc a et b tels que $f(a) = a$, $f(b) = b$, et soit c tel que $a < c < b$; on veut montrer que $a < f(c) < b$.

(1) Montrons qu'il existe un couple (x, y) et un seul (à l'ordre près) qui soit à la fois conjugué du couple (a, c) et du couple (b, ∞) ; la relation de conjugaison de (x, y) avec (b, ∞) exprime en effet que b est le milieu du segment $[x, y]$, et la relation de conjugaison de (x, y) avec (a, c) exprime alors que $\overline{bx}^2 = \overline{ba}.\overline{bc}$. Le second membre est positif, puisque b-a et c-a ont le même signe ; donc les points cherchés x et y sont les deux points dont la distance à b est égal à $\sqrt{\overline{ba}.\overline{bc}}$. Puisque f transforme toute division harmonique en division harmonique et laisse fixes a et b, le couple $(f(x), f(y))$ est conjugué du couple $(a, f(c))$ et du couple (b, ∞) ; d'après ce qu'on vient de voir, ceci implique que b-a et f(c) -a ont le même signe.

(2) Echangeons les rôles de a et b dans le raisonnement précédent. On conclut que a-b et f(c) - b ont le même signe.

De tout cela on conclut

$$f(c) - a > 0 \quad \text{et} \quad f(c) - b < 0,$$

c'est-à-dire $a < f(c) < b$.

C.Q.F.D.

Ceci achève la démonstration.

GEOMETRIE ELLIPTIQUE

On a déjà vu la suite exacte :

$$(1) \longrightarrow \mathbb{R}^* \longrightarrow GL(n+1, \mathbb{R}) \xrightarrow{\varphi} GLP(n, \mathbb{R}) \longrightarrow (1).$$

Nous savons que $O(n+1)$ est un sous-groupe de $GL(n+1, \mathbb{R})$. Nous appellerons $\underline{OP(n)}$ l'image par φ de $O(n+1)$; donc $OP(n) \subset GLP(n, \mathbb{R})$. Le noyau de la restriction de à $O(n+1)$ est $\mathbb{R}^* \cap O(n+1) = \{+1, -1\}$. Nous avons donc la suite exacte :

$$(1) \longrightarrow \{+1, -1\} \longrightarrow O(n+1) \longrightarrow OP(n) \longrightarrow (1),$$

et par suite $OP(n) \simeq O(n+1) / \{-1, -1\}$.

Le groupe $O(n+1)$ opère dans S^n. Si $\sigma \in O(n+1)$, le diagramme suivant est commutatif :

$$\begin{array}{ccc} S^n & \xrightarrow{\sigma} & S^n \\ \downarrow & & \downarrow \\ P_n & \xrightarrow{\sigma'} & P_n \end{array}$$

$\{-1, +1\}$ opère identiquement dans P_n (un point de S^n est transformé en lui-même ou son antipodique : il définit le même point de P_n).

D'où une interprétation de l'action de $OP(n)$ dans P_n, considéré comme quotient de S^n.

Remarques :

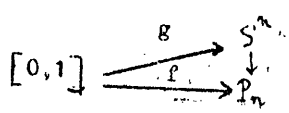
Supposons n $\underline{\text{pair}}$; soit h une homothétie de rapport -1 ; $\det h = (-1)^{n+1} = -1$. Donc

$$SO(n+1) \simeq O(n+1) / \{-1, +1\}.$$

$OP(n)$ et $SO(n+1)$ sont isomorphes, et l'action de $OP(n)$ sur P_n s'identifie à celle de $SO(n+1)$.

$\underline{\text{Supposons}}$ n $\underline{\text{impair}}$; soit h la même homothétie ; alors $\det h = (-1)^{n+1} = +1$. $OP(n)$ a alors deux composantes connexes ; celle qui contient l'élément neutre est le groupe $SO(n+1) / \{-1, +1\}$; on la notera $SOP(n)$; c'est un sous-groupe d'indice 2 de $OP(n)$.

$\underline{\text{Définition.}}$ On appelle arc de courbe continue une application continue $f : [0,1] \to P_n$



On peut "relever" f en g continue de deux façons différentes, suivant que l'on part d'un point de S^n ou de son antipodique. Les deux relèvements g se déduisent l'un de l'autre par la transformation antipodique de S^n

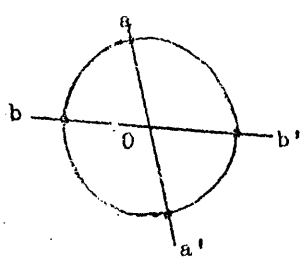
Si f est de classe C^1 (ou seulement de classe C^1 par morceaux), il en est de même de chacun des deux relèvements g. On appelle alors <u>longueur</u> de la courbe f la <u>longueur</u> de l'une quelconque des deux courbes g (elles ont la même longueur) ; il s'agit de la longueur d'un arc de courbe tracé sur la sphère S^n, qui est donc un arc de courbe dans l'espace euclidien $\mathbb{R}^{n+1}$. Cette longueur est

$$\int_0^1 |g'(t)|\, dt ,$$

où g' désigne la dérivée de la fonction $g : I \longrightarrow \mathbb{R}^{n+1}$, et $|g'(t)|$ est la longueur euclidienne du vecteur $g'(t)$.

Cette longueur d'un arc de courbe sur S^n est évidemment invariante par les transformations de $O(n+1)$. Il s'ensuit que la longueur d'un arc de courbe sur P_n est <u>invariante par le groupe</u> $OP(n)$.

Les segments de droite de P_n se relèvent en arcs de <u>grands cercles</u> de S^n (un "grand cercle" est l'intersection de S^n avec un plan 2-dimensionnel passant par l'origine de $\mathbb{R}^{n+1}$). Si A et B sont deux points <u>distincts</u> de P_n, soient a et a' les relèvements de A dans S^n, b et b' les relèvements de B dans S^n, a et b sont distincts et ne sont pas antipodiques, donc ils déterminent un arc de grand cercle $\overset{\frown}{ab}$ de longueur $< \pi$; son image dans P_n est un segment de droite joignant A et B, donc la longueur est la longueur ℓ de l'arc $\overset{\frown}{ab}$. De même, a et b' ne sont pas antipodiques, et déterminent un arc de grand cercle $\overset{\frown}{ab'}$ de longueur $\pi - \ell$, dont l'image dans P_n est l'<u>autre</u> segment de droite joignant A et B.



On voit que la longueur totale de la droite qui passe par A et B est égale à π, somme des longueurs des deux segments déterminés par a et b.

<u>Définition</u>. Etant donnés deux points distincts A et B de P_n, on appelle <u>distance</u> de ces deux points, et on note $d(A, B)$, la plus petite des longueurs des deux segments de droite joignant A et B. On pose en outre $d(A, A) = 0$. On a toujours

$$d(A, B) \leq \frac{\pi}{2} ,$$

l'égalité n'étant atteinte que si b est sur la $(n-1)$-sphère, intersection de S^n

avec l'hyperplan orthogonal à Oa. L'image de cette (n-1)-sphère dans P_n est un hyperplan, qu'on appellera l'hyperplan polaire du point A ; c'est le lieu des points $M \in P_n$ tels que $d(A, M) = \frac{\pi}{2}$.

La distance d(A, B), sur P_n, satisfait à l'inégalité du triangle :

$$d(A, B) \leq d(A, C) + d(C, B).$$

Cela va résulter immédiatement du

Théorème 1. d(A, B) est la borne inférieure des longueurs des arcs de courbe (de classe C^1 par morceaux) tracés sur P_n, d'origine A et d'extrémité B ; cette borne inférieure n'est atteinte que pour l'unique segment de droite joignant A et B et de longueur d(A, B) (si $d(A, B) < \frac{\pi}{2}$), resp. que pour chacun des deux segments de droite joignant A et B (si $d(A, B) = \frac{\pi}{2}$).

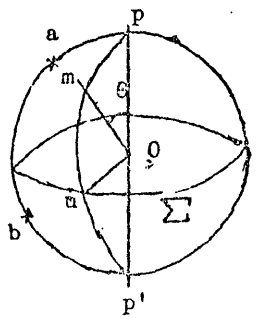
Le théorème 1 résulte à son tour d'un théorème relatif à la sphère S^n dont P_n est le quotient. Pour $a \in S^n$ et $b \in S^n$, non confondus et non antipodiques, soit d(a, b) la longueur de l'arc de grand cercle $\overset{\frown}{ab}$.

Théorème 2. Sous les hypothèses précédentes, d(a, b) est la borne inférieure des longueurs des arcs de courbe (de classe C^1 par morceaux) tracés sur S^n, d'origine a et d'extrémité b ; cette borne inférieure n'est atteinte que pour l'arc de grand cercle $\overset{\frown}{ab}$.

Démonstration du théorème 2. Soit $t \longrightarrow f(t)$ un arc de courbe de classe C^1 par morceaux ($0 \leq t \leq 1$, $f(0) = a$, $f(1) = b$). Supposons d'abord qu'il soit possible de choisir, sur le grand cercle passant par a et b, un point p tel que ni p ni p' (antipode de p) ne soient sur l'arc $\overset{\frown}{ab}$, et tel en outre que, le chemin $t \longrightarrow f(t)$ ne passe pas par le point p ni par le point p'. Tout point $m \in S^n$, distinct de p et p', définit un grand cercle passant par p (et p') ; soit u le point de l'"équateur" $\sum$ (sphère de dimension n-1, intersection de S^n avec l'hyperplan orthogonal à pp' et passant par O) où le demi grand cercle de diamètre pp' qui contient m coupe $\sum$; et soit θ la mesure en radians ($0 < \theta < \pi$) de l'angle (Om, Op). Tout point m distinct de p et p' étant ainsi repéré par u et θ, on a évidemment :

$$\overrightarrow{Om} = \overrightarrow{Op} \cos\theta + \vec{u} \sin\theta .$$

Donc la fonction $t \longmapsto f(t)$ définit deux fonctions $\theta(t)$ et $u(t)$, de classe C^1 par morceaux, telles que



$$\overrightarrow{f(t)} = \overrightarrow{Op} \cos\theta(t) + \overrightarrow{u(t)} \sin\theta(t).$$

La dérivée f' est donnée par

$$\overrightarrow{f'(t)} = (-\overrightarrow{Op} \sin\theta(t) + \overrightarrow{u(t)} \cos\theta(t))\,\theta'(t) + \overrightarrow{u'(t)} \sin\theta(t) ;$$

les trois vecteurs $\overrightarrow{Op}$, $\overrightarrow{u(t)}$ et $\overrightarrow{u'(t)}$ sont deux à deux orthogonaux [car la dérivée $\overrightarrow{u'(t)}$ d'un vecteur unitaire $\overrightarrow{u(t)}$ lui est orthogonale ; et comme $\overrightarrow{u(t)}$ est constamment orthogonal à $\overrightarrow{Op}$, sa dérivée est aussi orthogonale à $\overrightarrow{Op}$] ; d'où

$$|\overrightarrow{f'(t)}|^2 = (\sin^2\theta + \cos^2\theta)\,\theta'^2 + |\overrightarrow{u'}|^2 \sin^2\theta$$

$$= \theta'^2 + |\overrightarrow{u'}|^2 \sin^2\theta .$$

Par suite la longueur de l'arc de courbe est

$$\int_0^1 \sqrt{\theta'^2 + |u'|^2 \sin^2\theta}\, dt \geq \int_0^1 |\theta'(t)|\, dt \geq \int_0^1 \theta'(t)\, dt ;$$

observons que $\sin\theta(t) \neq 0$ pour $0 \leq t \leq 1$, donc l'égalité des membres extrêmes ne peut avoir lieu que si $u'(t) = 0$ constamment, et $\theta'(t) \geq 0$ constamment. Nous supposons, pour fixer les idées, que l'angle θ du point a est plus petit que l'angle θ du point b, de sorte que la longueur de l'arc $\overset{\frown}{ab}$ n'est autre que

$$\int_0^1 \theta'(t)\, dt.$$

On a ainsi prouvé que la longueur de l'arc de courbe $t \longrightarrow f(t)$ est $\geq$ longueur de $\overset{\frown}{ab}$, l'égalité ne pouvant avoir lieu qu'à deux conditions :

1º/ $u(t)$ est constant, c'est-à-dire le point $f(t)$ se déplace sur le grand cercle passant par a et b ;

2º/ $\theta'(t) \geq 0$ pour tout t, c'est-à-dire l'angle $\theta(t)$ croît constamment (au sens large) depuis la valeur de θ au point a jusqu'à la valeur de θ au point b.

Ceci exprime que le chemin de a vers b doit être (au paramétrage près) l'arc du grand cercle d'origine a et d'extrémité b.

Mais, pour faire cette démonstration, on a dû supposer qu'on pouvait choisir p de la façon dite. Il s'agit maintenant de lever cette restriction. Or c'est certainement possible si le "diamètre" du chemin f est $< \pi$ (le "diamètre" étant la borne supérieure de $d(f(t_1), f(t_2))$ quand t_1 et t_2 varient indépendamment de 0 à 1). Cela étant, le chemin f étant donné, on peut évidemment le subdiviser en un nombre fini de chemins dont chacun a un diamètre $< \pi$; soient :

$$a_o = a, a_1, \ldots, a_{p-1}, a_p = b$$

les valeurs de $f(t)$ aux points de subdivision

$$t_o = 0, t_1, \ldots, t_{p-1}, t_p = 1.$$

D'après ce qui précède, la longueur totale du chemin f, quand t varie de 0 à 1, est au moins égale à

$$d(a_o, a_1) + d(a_1, a_2) + \ldots + d(a_{p-1}, a_p),$$

l'égalité ne pouvant avoir lieu que si le chemin est obtenu en parcourant successivement les arcs de cercle $\overset{\frown}{a_o a_1}$, $\overset{\frown}{a_1 a_2}, \ldots, \overset{\frown}{a_{p-1} a_p}$. Il reste alors à montrer que la somme des longueurs de ces arcs de grands cercles est $\geq d(a, b)$, l'égalité n'ayant lieu que si les points $a_1, \ldots, a_{p-1}$ sont situés sur $\overset{\frown}{ab}$ et s'y trouvent dans cet ordre. Autrement dit on est ramené à démontrer encore le théorème, mais dans le cas simple où l'arc de courbe étudié est une "ligne brisée" formée d'arcs de grands cercles successifs. Par récurrence, il suffit d'étudier le cas de deux arcs de grands cercles $\overset{\frown}{ac}$ et $\overset{\frown}{cb}$. Dans ce cas, il est évident que l'on peut choisir le point p de la façon désirée, et par suite la démonstration du théorème est achevée.

ETUDE plus PARTICULIERE de la DIMENSION 2 ($n = 2$).

On étudie donc la géométrie du plan projectif P_2, muni du groupe d'opérateurs

$$OP(2) \approx SO(3) ;$$

$SO(3)$ opère sur la sphère S^2 et, par passage au quotient par la relation antipodique, sur P_2.

Dans ce cas, l'hyperplan polaire d'un point $A \in P_2$ est une droite ("droite polaire"). Inversement, toute droite Δ possède un pôle : l'unique point dont elle est

la polaire ; c'est le point de P_2 dont la distance à chaque point de Δ est égale à $\frac{\pi}{2}$.

Symétrie par rapport à une droite Δ : la droite $\Delta \subset P_2$ est l'image, par $p : S^2 \longrightarrow P^2$, d'un grand cercle $\sum$ de S^2 ; soit H le plan de ce grand cercle. Dans $\mathbb{R}^3$, la symétrie par rapport à H est un élément α de $O(3)$ opérant dans S^2 α induit, par passage au quotient, un automorphisme σ de P_2, tel que $\sigma^2 = \text{identité}$. Chaque point de Δ est fixe par σ, qu'on appelle la symétrie par rapport à Δ. Cherchons s'il y a un point $A \in P_2$, $A \notin \Delta$, fixe par σ ; soit $a \in S^2$ tel que $A = p(a)$; il faut et il suffit que $\alpha(a)$ soit a ou le point antipodique a' ; $\alpha(a) = a$ implique que α est sur le grand cercle $\sum$, donc $A \in \Delta$; par suite, si $A \notin \Delta$, la seule possibilité est que $\alpha(a) = a'$, ce qui exige que a soit sur le diamètre orthogonal au plan H. On voit que A n'est autre que le pole de la droite Δ. En résumé : la symétrie par rapport à Δ laisse fixe, outre les points de Δ, le pôle de la droite Δ.

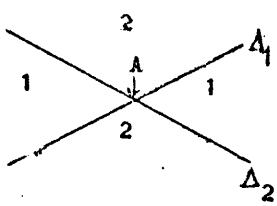
Remarque. Si on compose α et la symétrie par rapport à O, on obtient $\beta \in SO(3)$, qui n'est autre que la symétrie par rapport au diamètre aa' orthogonal au plan H. Donc σ est aussi obtenu par passage au quotient à partir de β.

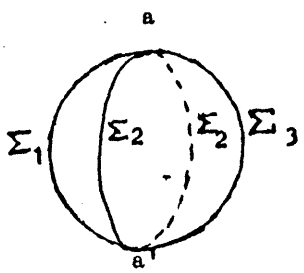
Exercices. 1) le lieu des points de P_2 équidistants de deux points distincts A et B se compose de deux droites qui se coupent orthogonalement au pôle de la droite joignant A et B.

2) le groupe d'isotropie d'un point $A \in P_2$ (sous-groupe formé des $\sigma \in OP(2)$ tels que $\sigma(A) = A$) est isomorphe à $O(2)$, donc n'est pas connexe. Préciser l'isomorphie.

Rappelons qu'une droite ne partage pas le plan P_2 en deux régions.

Angles. Soient Δ_1 et Δ_2 deux droites distinctes passant par A ; elles déterminent deux angles solides de sommet A : on s'en rend compte en regardant ce qui se passe sur la sphère S^2 : A provient de deux points a et a' antipodiques, Δ_1 et Δ_2 proviennent de deux grands cercles $\sum_1$ et $\sum_2$ se coupant en a et a' ; ils déterminent sur

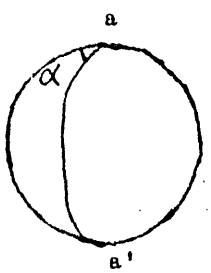




S^2 quatre fuseaux, qui se déduisent 2 à 2 par symétrie par rapport à O. Leurs images dans P_2 sont les deux angles solides en question.

Deux angles solides (dans P_2) sont égaux s'il existe une transformation de $OP(2) \approx SO(3)$ qui amène le premier sur le second. Un angle solide est caractérisé (à "égalité" près) par son cosinus, ou encore par sa mesure (> 0 et $< \pi$). La somme des mesures des deux angles solides définis par deux droites sécantes Δ_1 et Δ_2 est évidemment égale à π.

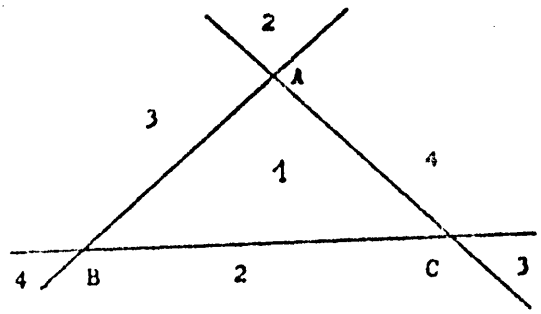
Aires. Sur la sphère S^2, on sait mesurer l'aire d'un ouvert, ou d'un fermé. En particulier, l'aire d'un fuseau est égal au double de la mesure (en radians) de l'angle α que font ses côtés [puisque l'aire de l'hémisphère est 2π]. Si un ensemble ouvert ou fermé $u \subset S^2$ est appliqué injectivement sur un ensemble $U \subset P_2$ par $p : S^2 \longrightarrow P_2$, on définit l'aire de U (dans P_2) comme égale à l'aire de u (dans S^2). Par exemple, l'aire d'un angle solide est égale au double de la mesure de l'angle.



Triangles dans le plan projectif.

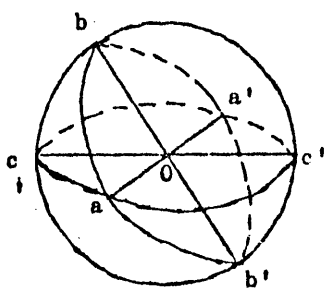
Soient A, B, C trois points non alignés. Ils définissent quatre triangles (régions du plan) : par exemple, choisissons l'un des deux angles solides de sommet A (définis par les droites AB et AC), et l'un des deux angles solides de sommet B (définis par les droites BA et BC) ; leur intersection est l'un des quatre triangles en question, elle est contenue automatiquement dans l'un des deux angles solides de sommet C. Lorsqu'on a choisi l'un des quatre triangles, on a du même coup, pour chaque couple de "sommets" (B et C par exemple), choisi l'un des deux segments de droite d'extrémités B et C [à savoir : celui qui est dans l'angle solide de sommet A contenant le triangle]. Inversement, le choix de trois segments joignant respectivement A et B, A et C, B et C détermine un triangle, mais ces trois choix ne sont pas arbitraires ; deux d'entre eux déterminent le triangle.

Si on se représente P_2 comme $\mathbb{R}^2$ complété par la "droite de l'infini", il est facile de représenter les quatre triangles :



on les a numérotés 1, 2, 3, 4 sur la figure.

On peut aussi se représenter les choses en regardant la situation sur la sphère S^2. On a trois grands cercles distincts dont les plans se coupent deux à deux suivant aa', bb', cc' ; ils découpent sur la sphère huit triangles sphériques, deux à deux symétriques par rapport à O :



a b c, a b c' ; a b' c, a b' c',

a' b' c', a' b' c, a' b c', a' b c.

Il est clair que la réunion des quatre premiers triangles est l'hémisphère situé sur le devant de la figure, et limité par le grand cercle passant par b, c, b' et c'.

Ayant choisi l'un des quatre triangles de sommets A, B, C, nous noterons S(A B C) l'aire de ce triangle, et $\hat{A}$, $\hat{B}$, $\hat{C}$ les mesures de ses angles (en radians). Cette notation est ambiguë. En revanche, sur la sphère, les notations S(a b c), $\hat{a}$, $\hat{b}$, $\hat{c}$ ne le sont pas, car le choix des sommets a, b, c détermine le triangle sphérique (et, du même coup, le triangle correspondant dans P_2).

Théorème. Pour tout triangle dans le plan projectif, on a

$$\boxed{S(A\ B\ C) = \hat{A} + \hat{B} + \hat{C} - \pi}.$$

(En d'autres termes : l'aire du triangle est égale à l'excès sur π de la somme des angles du triangle).

Démonstration: Cela revient à démontrer, sur la sphère, et sans ambiguïté de notation :

$$S(a\ b\ c) = \hat{a} + \hat{b} + \hat{c} - \pi. \tag{1}$$

Or la somme des aires de quatre triangles dont la réunion est un hémisphère est évidemment égale à 2π :

$$S(a\ b\ c) + S(a\ b\ c') + S(a\ b'\ c) + S(a\ b'\ c') = 2\pi ,$$

ou encore, puisque $S(a\ b'\ c') = S(a'\ b\ c)$ [triangles symétriques par rapport à O] :

(2) $$S(a\ b\ c) + S(a\ b\ c') + S(a\ b'\ c) + S(a'\ b\ c) = 2\pi .$$

D'autre part, le fuseau déterminé par les demi-grands cercles a c a' et a b a' donne la relation :

$$S(a\ b\ c) + S(a'\ b\ c) = 2\hat{a} .$$

On a de même

$$S(a\ b\ c) + S(a\ b'\ c) = 2\hat{b},$$

$$S(a\ b\ c) + S(a\ b\ c') = 2\hat{c}.$$

En ajoutant ces trois relations membre à membre, on trouve

(3) $$2S(a\ b\ c) + S(a\ b\ c) + S(a'b\ c) + S(a\ b'c) + S(a\ b\ c') = 2(\hat{a} + \hat{b} + \hat{c}),$$

ce qui, compte tenu de (2), donne la relation (1) à démontrer. C.Q.F.D.

ELEMENTS de GEOMETRIE ALGEBRIQUE.

1- L'espace affine.

Soit k un corps commutatif quelconque (fini ou infini). On pose $k^n = k \times \dots \times k$ (n facteurs) ; un point $x \in k^n$ est donc défini par une suite $(x_1, \dots, x_n)$, avec $x_i \in k$ pour $1 \leq i \leq n$.

On munit k^n de la structure d'espace vectoriel sur k évidente :

$$\begin{cases} (x_1, \dots, x_n) + (y_1, \dots, y_n) = (x_1+y_1, \dots, x_n+y_n) , \\ \lambda (x_1, \dots, x_n) = (\lambda x_1, \dots, \lambda x_n) \quad \text{pour } \lambda \in k. \end{cases}$$

La base canonique de k^n est

$$e_1 = (1, 0, \dots, 0),\ e_2 = (0, 1, 0, \dots, 0), \dots, e_n = (0, \dots, 0, 1).$$

Les automorphismes de l'espace vectoriel k^n forment un groupe, noté GL(n, k) ; un élément de GL(n, k) est défini par une matrice $(a_{ij})_{\substack{1 \leq i \leq n \\ 1 \leq j \leq n}}$ avec les $a_{ij} \in k$, telle que son déterminant $\det(a_{ij})$ soit $\neq 0$.

Le groupe linéaire-affine est le groupe des transformations $x \longmapsto Ax + b$, où $A \in GL(n, k)$, $b \in k^n$.

On peut encore parler de <u>barycentres</u> (mais plus de barycentres de masses positives !). Une <u>variété linéaire-affine</u> est un ensemble V tel que tout barycentre de points de V soit dans V ; une telle variété peut être vide, et si elle n'est pas vide, c'est la translatée d'un sous-espace vectoriel.

Une <u>forme linéaire-affine</u> est une application $k^n \longrightarrow k$ du type suivant :

$$x = (x_1, \ldots, x_n) \longmapsto \sum_{i=1}^{n} \lambda_i x_i + \mu,$$

avec $\lambda_i \in k$, $\mu \in k$.

<u>Proposition 1.</u> Toute variété linéaire-affine est l'ensemble des zéros communs à une famille finie de formes linéaires-affines. [Démonstration laissée au lecteur].

<u>Remarque</u> : Une forme linéaire-affine f n'est autre qu'un <u>polynôme du premier degré</u> en les coordonnées $x_1, \ldots, x_n$ du point x ; plus exactement, sa valeur $f(x)$ en un point x n'est autre que la valeur que prend un polynôme

$$\sum_{i=1}^{n} \lambda_i X_i + \mu_i$$

lorsqu'on substitue aux "indéterminées" X_i les valeurs x_i des coordonnées du point x.

2- En géométrie algébrique, on considère l'ensemble des zéros communs à une famille finie de <u>polynômes de degrés quelconques</u> (et plus nécessairement de polynômes du premier degré).

D'une façon plus précise, on va supposer donnés deux corps commutatifs k et Ω, $k \subset \Omega$. Considérons l'algèbre des polynômes

$$k[X_1, \ldots, X_n]$$

(polynômes à n indéterminées X_i, à coefficients dans k).

L'entier n est supposé donné. Soit $\Omega^n = \Omega \times \ldots \times \Omega$ (n facteurs), considéré comme espace vectoriel sur le corps Ω. Nous considérons l'application

(1) $$k[X_1, \ldots, X_n] \times \Omega^n \longrightarrow \Omega$$

qui, à un polynôme $P(X_1, \ldots, X_n)$ et à un point $x = (x_1, \ldots, x_n) \in \Omega^n$, associe

$$P(x_1, \ldots, x_n) \in \Omega,$$

<u>valeur du polynôme</u> au point x. Si on fixe P, (1) définit l'application partielle

$$\Omega^n \longrightarrow \Omega, \quad (x_1, \ldots, x_n) \longmapsto P(x_1, \ldots, x_n) ;$$

c'est la fonction-polynôme définie par P.

Proposition 2: Si le corps Ω est infini, la fonction-polynôme définie par P ne peut être zéro (i.e. : sa valeur est nulle en tout point de Ω^n) qui si le polynôme P est identiquement nul (i.e. tous ses coefficients sont nuls).

Démonstration: par récurrence sur le nombre n des variables. Pour $n = 1$, on sait qu'un polynôme $P \neq 0$, de degré p, ne peut pas prendre la valeur zéro pour $p+1$ valeurs distinctes de la variable ; donc si Ω est infini et si $P(x) = 0$, $\forall\, x \in \Omega$, P est identiquement nul.

Si la proposition est vraie pour $n - 1$ $(n \geq 2)$, soit

$$P(X_1, \ldots, X_n) = a_o(X_n)^d + a_1(X_n)^{d-1} + \ldots + a_d,$$

où $a_1, \ldots, a_d$ sont des éléments de $k[X_1, \ldots, X_{n-1}]$. Fixons $x_1, \ldots, x_{n-1} \in \Omega$; alors

$$P(x_1, \ldots, x_{n-1}, X)$$

est un polynôme en X qui s'annule pour toute valeur donnée à X dans Ω ; donc il est identiquement nul, i.e. :

$$a_i(x_1, \ldots, x_{n-1}) = 0 \quad \text{pour} \quad 0 \leq i \leq d.$$

Ceci étant vrai quels que soient $x_1, \ldots, x_{n-1}$ dans Ω, l'hypothèse de récurrence permet de conclure que $a_o, \ldots, a_d$ sont des polynômes identiquement nuls. Donc P est identiquement nul. C.Q.F.D.

Remarque : On se rappelle que la proposition 2 est un défaut lorsque Ω est un corps fini. Par exemple, si $\Omega = \mathbb{F}_q$ (corps à $q = p^2$ éléments), le polynôme $X^q - X$ prend la valeur zéro pour chaque $x \in \mathbb{F}_q$, et pourtant n'est pas identiquement nul.

Revenons à l'application (1). Si on fixe maintenant le point $x = (x_1, \ldots, x_n) \in \Omega^n$ et qu'on fait varier P, on obtient l'autre application partielle

$$\varphi : k[X_1, \ldots, X_n] \longrightarrow \Omega, \quad P(X_1, \ldots, X_n) \longmapsto P(x_1, \ldots, x_n).$$

Utilisant la définition des opérations (addition et multiplication) dans $k[X_1, \ldots, X_n]$, on voit que cette application φ est un homomorphisme d'anneaux ; de plus, si on identifie k à un sous-anneau de $k[X_1, \ldots, X_n]$ (le sous-anneau des polynômes de degré zéro), φ prolonge l'application d'injection $k \longrightarrow \Omega$.

Proposition 3. Réciproquement, si $\varphi : k[X_1, \ldots, X_n] \longrightarrow \Omega$ est un homomorphisme d'anneaux qui prolonge l'injection de k dans Ω, il existe un point $(x_1, \ldots, x_n) \in \Omega^n$ et un seul, tel que $\forall\, P \in k[X_1, \ldots, X_n]$, on ait

$$\varphi(P) = P(x_1, \ldots, x_n),$$

valeur du polynôme P au point $(x_1, \ldots, x_n)$.

Démonstration. Considérons en particulier les polynômes $X_1, X_2, \ldots, X_n$; soit $x_i = \varphi(X_i) \in \Omega_i$. On a alors $\varphi(P) = P(x_1, \ldots, x_n)$ quel que soit P. Le point $(x_1, \ldots, x_n)$ répond donc à la question, et c'est le seul.

Ainsi on a établi une correspondance bijective entre Ω^n et l'ensemble des k-homomorphismes $k[X_1, \ldots, X_n] \longrightarrow \Omega$ [par k-homomorphisme on entend un homomorphisme d'anneaux qui prolonge l'injection de k dans Ω].

3- Zéros d'un polynôme.

A chaque $P \in k[X_1, \ldots, X_n]$ nous associons l'ensemble

$$\mathcal{V}_\Omega(P) = \left\{ (x_1, \ldots, x_n) \in \Omega^n \mid P(x_1, \ldots, x_n) = 0 \right\},$$

appelé la variété du polynôme P, et aussi $\mathcal{V}(P)$ si aucune ambiguïté n'existe au sujet de Ω. D'après la proposition 2, on a $\mathcal{V}_\Omega(P) \neq \Omega^n$ si P n'est pas identiquement nul. [On supposera toujours que le corps k est infini].

Exemple. Pour $n = 1$, si P est de degré ≥ 1, et si Ω est algébriquement clos, la variété $\mathcal{V}_\Omega(P)$ n'est pas vide et se compose d'un nombre fini de points.

Définition. Une k-variété algébrique dans Ω^n, ou variété algébrique définie sur k, est une intersection

$$V = \bigcap_{i \in I} \mathcal{V}_\Omega(P_i), \quad \text{où} \quad P_i \in k[X_1, \ldots, X_n],$$

I étant un ensemble fini d'indices. Autrement dit, V est l'ensemble des zéros communs à une famille finie de polynômes $P_i \in k[X_1, \ldots, X_n]$.

Par exemple, toute variété linéaire-affine de Ω^n est une variété algébrique définie sur Ω ; elle n'est pas toujours définie sur k [ainsi, pour $n = 2$, le sous-espace vectoriel formé des $(x, y) \in \Omega^2$ tels que $x - y\sqrt{2} = 0$ n'est pas défini sur $\mathbb{Q}$].

Autre exemple : pour $n = 1$, une k-variété algébrique est formée d'un nombre fini de points, sauf si c'est Ω tout entier.

Proposition 4. $\emptyset$ et Ω^n sont des k-variétés algébriques. L'intersection de deux k-variétés algébriques est une k-variété algébrique ; de même pour la réunion.

Démonstration : $\emptyset$ est l'ensemble des zéros du polynôme constant égal à 1 ; Ω^n est l'ensemble des zéros du polynômes identiquement nul. Soient V_1 et V_2 deux variétés algébriques :

$$V_1 = \bigcap_{i \in I} \mathcal{V}_\Omega(P_i) \quad , \quad V_2 = \bigcap_{j \in J} \mathcal{V}_\Omega(Q_j) .$$

Alors $V_1 \cap V_2$ est l'ensemble des zéros communs aux polynômes P_i et Q_j, donc est une variété algébrique. D'autre part, on a

$$V_1 \cup V_2 = \bigcap_{(i,j) \in I \times J} \mathcal{V}_\Omega(P_i\, Q_j), \qquad \text{car si}$$

$x \in \cap \mathcal{V}_\Omega(P_i Q_i)$ est tel que $P_i(x) \neq 0$ pour tout $i \in 1$, on a $Q_j(x) = 0$ pour tout $j \in J$. Donc $V_1 \cup V_2$ est bien une variété algébrique.

Remarque. On verra plus loin que l'intersection d'une famille quelconque (même infinie) de k-variétés algébriques est une k-variété algébrique. Il en résulte que les k-variétés algébriques sont les ensembles fermés d'une certaine topologie sur Ω^n, appelée la topologie de Zariski. Un ouvert de cette topologie est un ensemble dont le complémentaire est une k-variété algébrique. L'adhérence d'un sous-ensemble X est la plus petite k-variété algébrique contenant X, à savoir l'intersection de toutes les k-variétés algébriques contenant X.

4- Idéal associé à une k-variété.

Soit V une k-variété algébrique dans Ω^n. On lui associe l'ensemble $\mathfrak{J}(V)$ de tous les $P \in k[X_1, \ldots, X_n]$ qui s'annulent sur V, c'est-à-dire satisfont à

$$P(x_1, \ldots, x_n) = 0 \text{ pour tout } (x_1, \ldots, x_n) \in V.$$

Il est immédiat que $\mathfrak{J}(V)$ est un idéal de l'anneau $k[X_1, \ldots, X_n]$.

Proposition 5. Si V est une k-variété algébrique, l'ensemble des zéros communs à tous les $P \in \mathfrak{J}(V)$ n'est autre que V.

Démonstration. Puisque V est une k-variété algébrique, il existe des P_i en nombre fini tels que

$$V = \bigcap_{i \in I} \mathcal{V}_\Omega(P_i) ;$$

les P_i sont dans l'idéal $\mathfrak{J}(V)$; $\bigcap_{P \in \mathfrak{J}(V)} \mathcal{V}_\Omega(P) \subset V$, et comme l'inclusion inverse résulte de la définition de $\mathfrak{J}(V)$, on a bien

$$V = \bigcap_{P \in \mathfrak{J}(V)} \mathcal{V}_\Omega(P).$$

Exemple : si $n = 1$, et si $V \neq \Omega$, on a vu que V est un ensemble fini E ; alors $\mathfrak{J}(V)$ se compose de tous les polynômes qui s'annulent aux points de E ; c'est l'idéal engendré par le polynôme unitaire P ayant pour zéros simples les points de E.

[Remarque : on savait déjà que, dans $k[X]$, tout idéal est principal].

Propriétés évidentes :

$$(2) \quad \begin{cases} V \subset V' \iff \mathfrak{J}(V) \supset \mathfrak{J}(V') \\ V = V' \iff \mathfrak{J}(V) = \mathfrak{J}(V') \\ \mathfrak{J}(V_1 \cup V_2) \iff \mathfrak{J}(V_1) \cap \mathfrak{J}(V_2) \end{cases}$$

(démonstration laissée au lecteur).

5- Structure des idéaux de $k[X_1, \ldots, X_n]$.

Théorème 1. (Hilbert)- Tout idéal I de $k[X_1, \ldots, X_n]$ est de type fini, i.e. est engendré par un nombre fini d'éléments. Cela signifie donc qu'il existe des $P_i \in I$ en nombre fini, tels que tout $P \in I$ soit de la forme

$$P = \sum_i Q_i P_i \quad , \quad Q_i \in k[X_1, \ldots, X_n] .$$

[Un anneau commutatif A tel que tout idéal de A soit de type fini s'appelle un anneau noethérien. Le théorème de Hilbert dit donc que l'anneau des polynômes à n indéterminées à coefficients dans un corps commutatif est noethérien].

On va prouver le théorème 1, en démontrant le :

Théorème 2. Si A est un anneau commutatif noethérien, l'anneau des polynômes $A[X]$ est noethérien.

En effet, si le théorème 2 est démontré, on prouve le théorème 1 par récurrence

sur n : il est vrai pour $n = 1$, car un corps k est un anneau noethérien ; s'il est vrai pour $n = 1$, il est vrai pour n, car $k[X_1, \ldots, X_{n-1}, X_n]$ s'identifie à $A[X_n]$, avec $A = k[X_1, \ldots, X_{n-1}]$.

Avant de faire la démonstration du théorème 2, nous aurons besoin d'une remarque : soit A un anneau noethérien, et soit $\{a_\gamma\}$ $(\gamma \in \Gamma)$ une famille quelconque d'éléments de A. Soit I l'idéal engendré par les a_γ (i.e. l'ensemble des combinaisons linéaires finies des a_γ à coefficients dans A). Alors I est déjà engendré par une sous famille finie de $\{a_\gamma\}$.

Démonstration. I est engendré par une famille finie d'éléments b_I, dont chacun est combinaison linéaire d'un nombre fini d'éléments a_γ ; il existe donc Γ' fini $\subset \Gamma$, tels que les b_I soient des combinaisons linéaires des a_γ pour $\gamma \in \Gamma'$. Alors tout élément de I est combinaison linéaire des a_γ pour $\gamma \in \Gamma'$.

Démonstration du théorème 2. Tout $P \in A[X]$ non identiquement nul s'écrit

$$P(X) = a X^n + Q(X),$$

$\deg Q < n$, $a \neq 0$. L'élément $a \in A$ s'appelle le coefficient dominant du polynôme $P \neq 0$.

Soit alors I un idéal de $A[X]$; on peut supposer $I = \{0\}$, sinon le théorème est démontré : I est alors engendré par le seul élément 0. Considérons l'idéal j de A engendré par les coefficients dominants des polynômes non nuls $P \in I$. Puisque A est noethérien par hypothèse, j est un idéal de type fini ; d'après la remarque précédente j est engendré par les coefficients dominants d'une famille finie de polynômes $P_\ell \in I$; soit a_ℓ le coefficient dominant de P_ℓ. Soit J l'idéal de $A[X]$ engendré par les P_ℓ ; on a $J \subset I$. Soit n_ℓ le degré de P_ℓ, et soit n le plus grand des entiers n_ℓ.

Lemme 1. Tout $Q \in I$ est congru (mod. J) à un polynôme de degré $< n$ (éventuellement nul).

Autrement dit, il existe $R \in A[X]$ tel que

$$\deg R < n, \qquad Q - R \in J ;$$

et naturellement, un tel R appartient à I, puisque $J \subset I$.

Il suffit de prouver ceci : si $Q \in I$ et $\deg Q \geq n$, il existe un polynôme R tel que

$$\deg R < \deg Q, \qquad Q - R \in J.$$

Or soit : $Q = a X^q + Q_1$, $q \geq n$, $\deg Q_1 < q$; on a $a = \sum_\ell \lambda_\ell a_\ell$, puisque a est dans l'idéal j. Alors

$$R(X) = Q(X) - \sum_\ell \lambda_\ell X^{q-n} P_\ell(X)$$

est un polynôme de degré $< q$, et $Q(X) - R(X)$ appartient bien à l'idéal J engendré par les P_ℓ. C.Q.F.D.

Notons, pour chaque entier p, N_p l'ensemble des polynômes de I dont le degré est $< p$; c'est évidemment un A-module. Le lemme 1 nous dit que tout $Q \in I$ est congru (modulo J) à un élément de N_n. Pour prouver le théorème 2, il suffit maintenant de montrer que N_n est un A-module de type fini.

Plus généralement, montrons que, pour tout p, N_p est un A-module de type fini, c'est-à-dire :

Lemme 2. Il existe un nombre fini d'éléments de N_p tels que tout élément de N_p soit une combinaison linéaire de ces éléments à coefficients dans A.

Le lemme 2 se démontre par récurrence sur p. La récurrence démarre avec $N_0 = \{0\}$. Il suffit de prouver :

Lemme 3. $p \geq 1$ étant donné, il existe des $R_h \in N_p$ en nombre fini, tels que tout élément de N_p soit somme d'un élément de N_{p-1} et d'une combinaison linéaire des R_h (à coefficients dans A).

Démonstration du lemme 3 : soit $\mathfrak{a}$ l'idéal engendré par les coefficients de X^{p-1} dans les polynômes $\in N_p$; $\mathfrak{a}$ est de type fini ; soient

$$R_h(X) = a_h X^{p-1} + \ldots$$

des éléments de N_p, en nombre fini, tels que les a_h engendrent $\mathfrak{a}$. Pour tout $R(X) \in N_p$, $R(X) = a X^{p-1} + \ldots$,

on a $a = \sum_h \lambda_h a_h$ ($\lambda_h \in A$), donc $R(X) - \sum_h \lambda_h R_h(X)$ appartient à N_{p-1}. C.Q.F.D.

Nous avons ainsi achevé la démonstration du théorème 2, et du même coup celle du théorème 1.

Conséquences du théorème de Hilbert. Soit I une famille infinie de polynômes $P_i \in k[X_1, \ldots, X_n]$; alors il existe un sous-ensemble fini J de I, tel que tout P_i (pour $i \in I$) soit combinaison linéaire des P_j ($j \in J$) à coefficients dans $k[X_1, \ldots, X_n]$. Il s'ensuit que

$$\bigcap_{i \in I} \mathcal{V}_\Omega(P_i) = \bigcap_{j \in J} \mathcal{V}_\Omega(P_j).$$

Autrement dit : l'intersection de toutes les variétés $\mathcal{V}_\Omega(P_i)$ est déjà l'intersection d'un nombre fini d'entre elles ; c'est donc une k-variété algébrique.

Plus généralement, l'intersection $\bigcap_{i \in I} V_i$ d'une famille infinie de k-variétés algébriques est déjà l'intersection $\bigcap_{j \in J} V_j$ d'une sous-famille finie d'entre elles (regarder les équations polynomiales définissant les V_i). C'est donc une k-variété algébrique.

Corollaire. Toute suite décroissante (au sens large) de k-variétés algébriques est stationnaire.

Cela veut dire que si on a $V_1 \supset V_2 \supset V_3 \supset \ldots \supset V_p \supset \ldots$ les V_p étant des k-variétés algébriques, toutes ces variétés sont égales à partir d'un certain rang.

6- Variété associée à un idéal de $k[X_1, \ldots, X_n]$.

Soit I un idéal. On lui associe la k-variété algébrique

$$\mathcal{V}_\Omega(I) = \bigcap_{P \in I} \mathcal{V}_\Omega(P) ;$$

c'est l'ensemble des zéros communs à tous les $P \in I$. En fait, c'est déjà l'ensemble des zéros communs à un système fini de générateurs de l'idéal I. On écrira souvent $\mathcal{V}(I)$ au lieu de $\mathcal{V}_\Omega(I)$, pour alléger l'écriture.

Propriétés.

$$(3) \qquad \begin{cases} I \subset J \implies \mathcal{V}(I) \supset \mathcal{V}(J), \\ \mathcal{V}(I + J) = \mathcal{V}(I) \cap \mathcal{V}(J), \\ \mathcal{V}(I \cap J) = \mathcal{V}(I) \cup \mathcal{V}(J). \end{cases}$$

La première des relations (3) est évidente. Pour la seconde, on a noté $I + J$ la somme des idéaux I et J : c'est l'idéal formé des sommes $P + Q$, où $P \in I$ et $Q \in J$;

c'est le plus petit idéal contenant I et J. Si I est engendré par des P_i en nombre fini, et J par des Q_j en nombre fini, $I + J$ est engendré par les P_i et les Q_j, et $\mathcal{V}(I + J)$ est la variété définie par les équations

$$P_i(x_1, \ldots, x_n) = 0, \qquad Q_j(x_1, \ldots, x_n) = 0 \ ;$$

ce qui prouve la deuxième relation (3).

Pour prouver la troisième relation (3), introduisons l'idéal IJ (appelé produit des idéaux I et J) engendré par les produits PQ, où $P \in I$ et $Q \in J$.

Il est clair que

$$\mathcal{V}(I\,J) = \mathcal{V}(I) \cup \mathcal{V}(J).$$

Or $IJ \subset I \cap J$, d'où

$$\mathcal{V}(I\,J) \supset \mathcal{V}(I \cap J) \supset \mathcal{V}(I) \cup \mathcal{V}(J),$$

et comme les extrêmes sont égaux, on a

$$\mathcal{V}(I\,J) = \mathcal{V}(I \cap J) = \mathcal{V}(I) \cup \mathcal{V}(J).$$

Autres propriétés.

Soit V une k-variété algébrique. On sait déjà (proposition 5) que

$$\mathcal{V}(\mathfrak{J}(V)) = V. \tag{4}$$

D'autre part, si I est un idéal de $k[X_1, \ldots, X_n]$, il est trivial que

$$\mathfrak{J}(\mathcal{V}(I)) \supset I. \tag{5}$$

Montrons sur un exemple que l'inclusion (5) ne peut pas être remplacée par une égalité : prenons $n = 1$, et soit I l'idéal de $k[X]$ engendré par le polynôme X^2 ; alors $\mathcal{V}(I)$ se compose du point $0 \in \Omega$, et $\mathfrak{J}(\mathcal{V}(I))$ est l'idéal des $P(X)$ tels que $P(0) = 0$, autrement dit c'est l'idéal engendré par X. On voit qu'il est distinct de l'idéal engendré par X^2.

On reviendra plus loin sur l'importante question de savoir quelle relation exacte il y a entre l'idéal I et l'idéal $\mathfrak{J}(\mathcal{V}(I))$ formé de tous les polynômes qui s'annulent sur la variété de I.

Voici au contraire un exemple où $\mathfrak{J}(\mathcal{V}(I)) = \mathfrak{J}$: c'est celui où I est engendré par des polynômes du premier degré, le corps Ω étant supposé infini ; dans ce cas,

on peut montrer que tout polynôme qui s'annule sur une k-variété linéaire affine définie par des équations $P_i(X_1, \ldots, X_n) = 0$ (P_i du premier degré) appartient à l'idéal engendré par les P_i. [Exercice : faire cette démonstration ; distinguer le cas où la variété est vide, et celui où elle ne l'est pas ; dans ce second cas, on se ramène à un k-sous-espace vectoriel de Ω^n].

Remarque. Nous verrons plus loin, comme conséquence d'un "théorème fondamental", que si Ω est algébriquement clos, et si $I \neq k[X_1, \ldots, X_n]$ (c'est-à-dire si $1 \in I$), alors la variété $\mathcal{V}_\Omega(I)$ n'est pas vide. Nous savons déjà qu'il en est ainsi pour $n = 1$: tout polynôme non constant possède au moins un zéro dans Ω ; en fait, il se décompose en produit de polynômes de degré 1 à coefficients dans Ω.

7- Variétés irréductibles ; composantes irréductibles d'une variété algébrique quelconque.

Les corps k et $\Omega \supset k$ étant toujours donnés, soit V une k-variété algébrique dans Ω^n.

Définition. On dit que V est irréductible (ou, plus précisément, k-irréductible) si :

(i) V n'est pas vide ;

(ii) la relation $V = V_1 \cup V_2$ (où V_1 et V_2 sont des k-variétés algébriques) entraîne $V = V_1$ ou $V = V_2$.

Une k-variété $V \neq \emptyset$ sera donc dite réductible s'il existe des k-variétés V_1 et V_2 telles que

$$V = V_1 \cup V_2 , \quad V \neq V_1 , \quad V \neq V_2.$$

Proposition 6. Pour que V soit k-irréductible, il faut et il suffit que l'idéal $\mathfrak{J}(V)$ soit premier.

Démonstration. Rappelons qu'un idéal I (dans un anneau commutatif A à élément unité) est premier si :

(i) $1 \notin I$;

(ii) ($a \in A$, $b \in A$ et $ab \in I$) $\Longrightarrow$ $a \in I$ ou $b \in I$.

Il revient au même de dire que l'anneau-quotient A/I est intègre, c'est-à-dire que

1°/ son élément unité est $\neq 0$;

2°/ le produit de deux éléments $\neq 0$ de A/I est $\neq 0$.

Montrons d'abord : V irréductible $\Longrightarrow$ $\mathfrak{J}(V)$ premier. D'abord, 1 ne s'annule pas sur V, puisque V n'est pas vide ; de plus, si P et Q sont des polynômes tels que $PQ \in \mathfrak{J}(V)$, soit

$$V_1 = \{(x_1, \ldots, x_n) \in V \mid P(x_1, \ldots, x_n) = 0\},$$
$$V_2 = \{(x_1, \ldots, x_n) \in V \mid Q(x_1, \ldots, x_n) = 0\};$$

on a $V = V_1 \cup V_2$, donc $V = V_1$ ou $V = V_2$; si $V = V_1$, on a $P \in \mathfrak{J}(V)$, si $V = V_2$, on a $Q \in \mathfrak{J}(V)$. Donc $\mathfrak{J}(V)$ est premier.

Montrons ensuite : V réductible $\Longrightarrow$ $\mathfrak{J}(V)$ non premier. C'est évident si $V = \emptyset$, car alors $1 \in \mathfrak{J}(V)$; si $V \neq \emptyset$, soit $V = V_1 \cup V_2$, $V_1 \neq V$, $V_2 \neq V$. Puisque $V_1 \neq V$, il existe $P \in \mathfrak{J}(V_1)$ tel que $P \notin \mathfrak{J}(V)$; puisque $V_2 \neq V$, il existe $Q \in \mathfrak{J}(V_2)$ tel que $Q \notin \mathfrak{J}(V)$. Alors le produit PQ s'annule sur V, c'est-à-dire $PQ \in \mathfrak{J}(V)$. Il s'ensuit que $\mathfrak{J}(V)$ n'est pas premier.

Remarque. La proposition 6 n'est pas un résultat profond. C'est une conséquence des définitions.

Lemme. Soit V une k-variété irréductible. Si $V = \bigcup_{i \in I} V_i$, réunion finie de k-variétés V_i, alors V est égale à l'une des V_i.

Démonstration: par récurrence sur le cardinal de I. C'est trivial si Card I = 1. Supposons la propriété vraie si Card I = p-1 ($p \geq 2$), et montrons-la pour p ; soit donc

$$V = V_1 \cup V_2 \cup \ldots \cup V_p$$
$$= W \cup V_p,$$

avec $W = V_1 \cup V_2 \cup \ldots \cup V_{p-1}$. Puisque V est irréductible, on a $V = W$ ou $V = V_p$; dans le second cas, le lemme est démontré. Dans le premier, l'hypothèse de récurrence nous dit que V est égal à l'un des V_i pour $1 \leq i \leq p-1$. C.Q.F.D.

Corollaire. Si V est irréductible et $V \subset V_1 \cup V_2 \cup \ldots \cup V_p$, alors il existe i tel que $V \subset V_i$.

[En effet, $V = W_1 \cup W_2 \cup \ldots \cup W_p$, en posant $W_i = V \cap V_i$ pour $1 \leq i \leq p$; d'où $V = W_i$ pour un i].

Théorème 3.- Pour toute k-variété algébrique V, il existe une famille finie de k-variétés algébriques irréductibles V_i ($i \in I$, I ensemble fini) telles que

(i) $V = \bigcup_{i \in I} V_i$;

(ii) $i \neq j \Longrightarrow V_i \not\subset V_j$.

Une telle famille est unique (à une bijection près de l'ensemble d'indices). Les V_i s'appellent les composantes irréductibles de V (plus précisément : composantes k-irréductibles).

Démonstration: si $V = \emptyset$, le théorème est évident : on prend la famille vide de variétés irréductibles. Supposons donc $V \neq \emptyset$. Si V est irréductible, le théorème est évident. Supposons donc $V \neq \emptyset$ et réductible.

Lemme.- Il existe des k-variétés V' et W' telles que :

$$V = V' \cup W' \quad V \text{ irréductible}, \quad V' \neq V, \quad W' \neq V$$

En effet, puisque V est réductible, on a

$$V = V_1 \cup W_1 \ , \quad V_1 \neq V, \quad W_1 \neq V \ ;$$

si V_1 est irréductible, le lemme est démontré ; sinon il suffit de prouver le :

Sous-lemme: si $V = V_1 \cup W_1$, $V_1 \neq V$, $W_1 \neq V$, V_1 réductible, il existe V_2 et W_2 telles que

$$V = V_2 \cup W_2 \ , \quad W_2 \neq V \ ; \quad V_2 \subset V_1 \ , \quad V_2 \neq V_1 \ .$$

[Démonstration du sous-lemme : puisque $V_1 \neq \emptyset$ est réductible, on a $V_1 = V_1' \cup V_1''$, $V_1' \neq V_1$. On a $V = V_1' \cup V_1'' \cup W_1$; de deux choses l'une : ou bien

$V_1'' \cup W_1 \neq V$, et alors on prend $V_2 = V_1'$, $W_2 = V_1'' \cup W_1$;

ou bien $V_1'' \cup W_1 = V$, et alors on prend $V_2 = V_1''$, $W_2 = W_1$].

Le sous-lemme entraîne le lemme, sinon on définirait par récurrence V_p et W_p telles que

$$V = V_p \cup W_p, \quad W_p \neq V, \quad V_p \subset V_{p-1}, \quad V_p \neq V_{p-1},$$

et la suite décroissante $V_1 \supset V_2 \supset \dots \supset V_p \supset \dots$ ne serait pas stationnaire : ceci contredit un corollaire antérieur. Donc, pour un p convenable, V_p est irréductible, et il suffit de prendre $V' = V_p$, $W' = W_p$ pour obtenir le lemme.

Achevons maintenant la démonstration du théorème 3.

Si $V \neq \emptyset$ est réductible, on a, d'après le lemme :

$$V = V_1 \cup W_1 \ , \ V_1 \neq V \ , \ W_1 \neq V, \ V_1 \text{ irréductible.}$$

Pour la même raison, si W_1 est réductible, on a

$$W_1 = V_2 \cup W_2 \ , \ V_2 \neq W_1 \ , \ W_2 \neq W_1, \ V_2 \text{ irréductible.}$$

Et ainsi de suite. Ces opérations ont une fin, sinon on aurait une suite infinie strictement décroissante

$$W_1 \supset W_2 \supset W_3 \supset \cdots,$$

ce qui est impossible. Donc V est une réunion finie $\bigcup_{i \in I} V_i$ de variétés irréductibles V_i.

Si maintenant il existe un couple (i, j), $i \neq j$ tel que $V_i \subset V_j$, on peut supprimer la variété V_i de la famille. Au moyen de telles suppressions successives, on obtiendra une famille $(V_i)_{i \in I}$ telle que $i \neq j \Longrightarrow V_i \not\subset V_j$, ce qui est la condition (ii) de l'énoncé du théorème 3. Donc l'existence est prouvée.

Reste à prouver l'unicité. Supposons donc

$$\bigcup_{i \in I} V_i = \bigcup_{\alpha \in A} W_\alpha \ ,$$

les ensembles I et A étant finis, les variétés V_i et W_α étant irréductibles.

Donnons-nous i ; on a

$$V_i \subset \bigcup_{\alpha \in A} W_\alpha \ ,$$

donc (cf. un corollaire antérieur) il existe un α tel que $V_i \subset W_\alpha$.

Pour la même raison, il existe un $j \in I$ tel que $W_\alpha \subset V_j$.

On a donc $V_i \subset V_j$, ce qui entraîne $j = i$, et $V_i = W_\alpha$. Ainsi à chaque $i \in I$ correspond un unique $\alpha \in A$ tel que $V_i = W_\alpha$; d'où une application $\varphi : I \to A$ telle que $V_i = W_{\varphi(i)}$ pour tout i. Il est immédiat que φ est une bijection, et l'unicité est démontrée.

Corollaire du théorème 3. Soit V une k-variété algébrique. On a

$$\mathfrak{J}(V) = \bigcap_{i \in I} \mathfrak{J}(V_i),$$

où les $\mathfrak{J}(V_i)$ sont les idéaux premiers qui correspondent aux composantes irréductibles

V_i de V. Ainsi $\mathfrak{J}(V)$ est une intersection finie d'idéaux premiers. On reviendra plus loin sur cette question.

8- Agrandissement du corps Ω.

La théorie précédente a été faite avec deux corps k et Ω, tels que [illegible]. Voyons ce qui arrive quand on remplace Ω par un corps plus grand $\Omega' \supset \Omega$.

A chaque k-variété algébrique $V \subset \Omega^n$ nous associons une k-variété $V' \subset \Omega'^n$ de la manière suivante : V' est l'ensemble des zéros communs (dans Ω'^n) à tous les $P \in k[X_1, \ldots, X_n]$ qui s'annulent sur V. En formule :

$$V' = \mathcal{V}_{\Omega'}(\mathfrak{J}(V)).$$

Proposition 7. On a $\boxed{V' \cap \Omega^n = V \quad \text{et} \quad \mathfrak{J}(V') = \mathfrak{J}(V)}$.

Démonstration.

$$V' \cap \Omega^n = \mathcal{V}_{\Omega'}(\mathfrak{J}(V)) \cap \Omega^n = \mathcal{V}_{\Omega}(\mathfrak{J}(V)) = V.$$

De plus, puisque les éléments de $\mathfrak{J}(V)$ s'annulent sur V', on a $\mathfrak{J}(V') \supset \mathfrak{J}(V)$; et puisque $V \subset V'$, on a $\mathfrak{J}(V) \supset \mathfrak{J}(V')$; d'où l'égalité $\mathfrak{J}(V') = \mathfrak{J}(V)$.

Remarque. V' n'est autre que l'adhérence de V dans Ω'^n, muni de la k-topologie de Zariski.

Corollaire. Pour que V' soit k-irréductible, il faut et il suffit que V soit k-irréductible.

[En effet, le k-irréductibilité de V' (resp. de V) s'exprime par le fait que l'idéal $\mathfrak{J}(V')$ (resp. $\mathfrak{J}(V)$) est premier. Or ces deux idéaux sont égaux].

Exercice. Soient V_i les composantes irréductibles de V ; alors les V'_i associées aux V_i sont les composantes irréductibles de V'.

9- Rapetissement du corps k.

Laissons maintenant le corps Ω fixe, et remplaçons k par un sous-corps $k' \subset k$.

Soit $V \subset \Omega^n$ une k-variété algébrique, il n'est pas certain que V soit une k'-variété algébrique, c'est-à-dire l'annulation de polynômes à coefficients dans k'. Par exemple (n = 2) la variété d'équation $x - y\sqrt{2} = 0$ n'est pas une variété définie sur le corps $\mathbb{Q}$.

Supposons que V soit aussi une k'-variété. Alors l'idéal I' des

$P \in k'[X_1, \ldots, X_n]$ qui s'annulent sur V n'est autre que l'intersection de l'idéal $I = \mathfrak{J}(V) \subset k[X_1, \ldots, X_n]$ avec le sous-anneau $k'[X_1, \ldots, X_n]$ de $k[X_1, \ldots, X_n]$. Si I est premier, I' est donc premier ; autrement dit, si V est k-irréductible, est aussi k'-irréductible. Mais <u>la réciproque est fausse</u> : par exemple, prenons $n = 2$, $k' = \mathbb{Q}$, $k = \mathbb{R}$, $\Omega = \mathbb{C}$; la variété d'équation $x^2 - 2y^2 = 0$ est irréductible sur $\mathbb{Q}$, mais sur $\mathbb{R}$ elle a deux composantes irréductibles, à savoir les deux droites $x - \sqrt{2}\, y = 0$ et $x + \sqrt{2}\, y = 0$.

10- <u>Cas où le corps Ω est algébriquement clos</u>

On supposera dans ce numéro que Ω est <u>algébriquement clos</u> (et on ne répétera pas tout le temps cette hypothèse, faite une fois pour toute).

<u>Théorème 4.</u> (<u>Théorème fondamental</u>). Si I est un idéal <u>premier</u> de $k[X_1, \ldots, X_n]$, on a

$$\boxed{\mathfrak{J}(\mathcal{V}_\Omega(I)) = I} \quad ;$$

autrement dit, tout polynôme P qui s'annule sur la variété $\mathcal{V}_\Omega(I)$ appartient nécessairement à I (lorsque Ω est <u>algébriquement clos</u> !)

<u>Corollaire</u>. Si I est premier, la variété $\mathcal{V}_\Omega(I)$ est irréductible (puisque $\mathfrak{J}(\mathcal{V}_\Omega(I))$ est premier). <u>L'application $V \longmapsto \mathfrak{J}(V)$ est une bijection de l'ensemble des k-variétés irréductibles de Ω^n sur l'ensemble des idéaux premiers de $k[X_1, \ldots, X_n]$</u>

Avant de démontrer le théorème 4 (ce qui sera long, car c'est un théorème profond), on va en donner d'autres formulations équivalentes.

Rappelons que les points de Ω^n correspondent bijectivement aux k-homomorphismes $\varphi : k[X_1, \ldots, X_n] \longrightarrow \Omega$; dire qu'un point $x = (x_1, \ldots, x_n)$ appartient à $\mathcal{V}(I)$,

c'est dire que l'idéal I est contenu dans le noyau de l'homomorphisme φ_x défini par x. Le théorème 4 exprime que si un $P \in k[X_1, \ldots, X_n]$ appartient au noyau de φ_x quel que soit $x \in \mathcal{V}(I)$, alors $P \in I$. Autrement dit, I est l'intersection des noyaux de φ_x lorsque x parcourt $V = \mathcal{V}(I)$. Une formulation du théorème 4 est donc la suivante :

Théorème 4' .- Si $P \notin I$, il existe un k-homomorphisme $\varphi : k[X_1, \ldots, X_n] \longrightarrow \Omega$ dont le noyau contient I mais ne contient pas P.

Considérons l'anneau quotient

$$A = k[X_1, \ldots, X_n] / I ;$$

c'est un anneau intègre, et k s'identifie à un sous-anneau de A au noyau de l'homomorphisme composé

$$k \longrightarrow k[X_1, \ldots, X_n] \longrightarrow k[X_1, \ldots, X_n] / I,$$

qui est injectif parce que $k \cap I$ est un idéal de k ne contenant pas 1, d'où $k \cap I = \{0\}$. On appellera k-homomorphisme $A \longrightarrow \Omega$ un homomorphisme d'anneaux qui prolonge l'injection $k \longrightarrow \Omega$ (k étant identifié à un sous-anneaux de A).

Observons que tout k-homomorphisme $\varphi : k[X_1, \ldots, X_n] \longrightarrow \Omega$ qui s'annule sur I définit, par passage au quotient, un k-homomorphisme $A \longrightarrow \Omega$. On obtient ainsi une bijection de l'ensemble des k-homomorphismes $k[X_1, \ldots, X_n] \longrightarrow \Omega$ qui s'annulent sur I, sur l'ensemble des k-homomorphismes $A \longrightarrow \Omega$. Le théorème 4' se reformule comme suit, en appelant $a \in A$ l'image de P par l'application canonique de $k[X_1, \ldots, X_n]$ sur son quotient A :

Théorème 4". Soit A l'anneau intègre $k[X_1, \ldots, X_n] / I$ (I premier). Etant donné un $a \in A$, $a \neq 0$, il existe un k-homomorphisme $\psi : A \longrightarrow \Omega$ tel que $\psi(a) \neq 0$.

[Rappelons que le corps Ω a été supposé algébriquement clos].

On va ramener la démonstration du théorème 4" à celle d'un autre théorème. En effet, soit K le corps des fractions de l'anneau intègre A, et soit A' le sous-anneau de K engendré par A et $a^{-1} \in K$; A' est isomorphe à un quotient de l'anneau des polynômes $k[X_1, \ldots, X_n, Y]$. Si nous trouvons un k-homomorphisme $\psi : A' \longrightarrow \Omega$,

il est clair que la restriction de ψ à A satisfera à $\psi(a) \neq 0$, puisque

$$\psi(a)\,\psi(a^{-1}) = 1.$$

Il suffit donc (en changeant les notations et récrivant A au lieu de A') de prouver le théorème suivant :

Théorème 5. Soit A un anneau commutatif contenant k, et engendré (comme anneau) par k et un nombre fini d'éléments [nous exprimerons cette condition en disant que A est une k-algèbre de type fini ; cela exprime que A est isomorphe au quotient d'une algèbre de polynômes $k[X_1, \ldots, X_n]$ par un idéal I, premier ou non].

Alors, si $\Omega \supset k$ est un corps algébriquement clos, il existe un k-homomorphisme $A \to \Omega$.

Tel est le théorème qu'il nous faut maintenant démontrer. Observons que lorsque A est un corps K, et que le degré $[K : k]$ est fini, l'existence d'un k-homomorphisme $K \to \Omega$ nous est déjà connue (cf. la partie de ce cours relative aux extensions algébriques de degré fini) ; on a même étudié le nombre de ces k-homomorphismes : il est fini, et c'est un diviseur du degré $[K : K]$; il est égal à $[K : k]$ lorsque K est une extension séparable de k.

Toute l'astuce, pour démontrer le théorème 5, va consister à se ramener au cas d'un surcorps de k, de degré fini sur k.

11- Démonstration du théorème 5.

Soit $\mathfrak{m}$ un idéal maximal de A (élément maximal de l'ensemble des idéaux de A, distincts de A). On sait qu'il existe (théorème de Zorn), et que $A/\mathfrak{m}$ est un corps K. L'injection $k \to A$ définit, par passage au quotient, un homomorphisme de corps $k \to K$, qui est donc injectif et identifie k à un sous-corps de K. On va montrer que, sous les hypothèses du théorème 5, le degré $[K : k]$ est fini. Alors on sait qu'il existe un homomorphisme $\varphi : K \to \Omega$ qui prolonge l'injection $k \to \Omega$; prenons pour ψ l'homomorphisme composé

$$A \to A/\mathfrak{m} = K \xrightarrow{\varphi} \Omega ;$$

il répond à la question, ce qui prouve le théorème 5.

Tout revient donc à démontrer le

Lemme 1. Si un corps K, contenant k, est engendré, comme k-algèbre, par un nombre fini d'éléments $a_i \in K$, alors le degré $[K : k]$ est fini.

Or le lemme 1 se prouvera à l'aide du

Lemme 2. ("lemme de normalisation" d'Emmy Noether).-

Soit A une k-algèbre de type fini. Alors il existe un sous-anneau B de A, contenant k, tel que :

(i) $B \approx k[Y_1, \ldots, Y_p]$ (algèbre de polynômes) :

(ii) A soit un B-module de type fini (i.e. : il existe des $a_i \in A$, en nombre fini, tels que tout élément de A soit combinaison linéaire des a_i à coefficients dans B).

Ce lemme sera démontré plus loin. Admettons-le pour le moment, et voyons comment le lemme 1 peut s'en déduire. L'hypothèse du lemme 1 est que le corps K est une k-algèbre de type fini ; soit $B \subset K$ un sous-anneau ayant les propriétés énoncées au lemme 2. Utilisons le :

Lemme 3. Soit K un corps commutatif, et soit B un sous-anneau de K tel que K soit un B-module de type fini. Alors B est un sous-corps de K.

Alors on conclut ici que B est un corps ; or, d'après le lemme 2, $B \approx k[Y_1, \ldots, Y_p]$; mais une algèbre de polynômes ne peut être un corps que s'il n'y a pas de variable du tout, i.e. si $p = 0$. Donc $B = k$; et comme (lemme 2) K est un B-module de type fini, on conclut que K est un k-espace vectoriel de dimension finie, c'est-à-dire $[K : k] < +\infty$, ce qui prouve le lemme 1.

Démonstration du lemme 3 : soit $b \in B$, $b \neq 0$. On veut montrer que $b^{-1} \in K$ est en réalité dans B. Or soient u_j $(i = 1, 2, \ldots, h)$ des éléments de K qui engendrent K comme B-module. Il existe des $b_{ij} \in B$ tels que

$$b^{-1} u_i = \sum_{j=1}^{h} b_{ij} u_j \quad , \quad 1 \leq i \leq h.$$

Posons $\delta_{ij} = \begin{cases} 0 & \text{si } i \neq j \\ 1 & \text{si } i = j. \end{cases}$

Les relations précédentes s'écrivent :

$$\sum_{j=1}^{p} (b_{ij} - \delta_{ij}\, b^{-1})\ u_i = 0, \qquad i = 1, \ldots, p.$$

Ces relations ont lieu dans le corps K. Comme les u_i ne sont pas tous nuls et satisfont à un système de p équations linéaires homogènes, on conclut que

$$\det (b_{ij} - \delta_{ij}\, b^{-1}) = 0.$$

Si on développe ce déterminant, on trouve

$$b^{-p} = \text{combinaison linéaire de } 1,\ b^{-1}, \ldots,\ b^{-p+1}$$

à coefficients dans B. Donc, en multipliant par b^{p-1}, b^{-1} est combinaison linéaire de $b^{p-1}, b^{p-2}, \ldots, b, 1$ à coefficients dans B. Donc $b^{-1} \in B$. C.Q.F.D.

Le lemme 3 est donc démontré, et par suite le théorème 5 est démontré (ainsi que le théorème 4) sous réserve que nous prouvions le lemme de normalisation (lemme 2 ci-dessus).

Le genre de raisonnement qui interviendra dans la preuve du lemme de normalisation intervient déjà, en plus simple, dans la théorie de degré de transcendance ; c'est pourquoi nous allons commencer par celle-ci.

12- Dimension d'une variété irréductible ; degré de transcendance.

Ce qui va suivre est indépendant des théorèmes 4 et 5 ; il n'y a donc aucun inconvénient logique à traiter de ces questions avant d'avoir terminé la démonstration des théorèmes 4 et 5.

Soit $V \subset \Omega^n$ une k-variété irréductible. Nous allons lui attacher un corps $K = K(V)$ comme suit. Soit $I = \mathfrak{J}(V)$ l'idéal de V, qui est premier, et soit $A = k[X_1, \ldots, X_n] / I$ l'anneau quotient, qui est intègre. Alors K(V) est, par définition, le corps des fractions de l'anneau intègre A ; k s'identifie à un sous-corps de K.

Définition. On appelle dimension de V (ou, plus précisément, k-dimension de la variété k-irréductible V) le degré de transcendance du corps $K = K(V)$ sur le corps k.

Reste à définir le degré de transcendance ! Observons que le corps K est engendré (comme corps) par k est un nombre fini d'éléments de K, à savoir les classes des polynômes $X_1, \ldots, X_n$ dans $A = k[X_1, \ldots, X_n] / I$.

Nous dirons qu'un surcorps K de k est de type fini sur k si K est engendré (comme corps) par k et un nombre fini d'éléments a_i ; cela veut dire que tout sous-corps de K qui contient k et les a_i est identique à K. Il ne faut pas confondre cette notion avec celle intervenue au lemme 1 : là il s'agissait d'un surcorps K engendré, comme k-algèbre, par un nombre fini d'éléments a_i, ce qui signifiait que tout sous-anneau de K contenant k et les a_i était identique à K.

La théorie du degré de transcendance qui va suivre s'applique à un corps K de type fini sur k (comme corps !)

Définition. Des éléments $a_1, \ldots, a_p \in K$ sont dits algébriquement indépendants sur k si tout polynôme $P \in k[X_1, \ldots, X_p]$ tel que $P(a_1, \ldots, a_p) = 0$ est identiquement nul.

On peut aussi formuler cette condition comme suit : la donnée de $a_1, \ldots, a_p \in K$ définit un k-homomorphisme

$$\varphi : k[X_1, \ldots, X_p] \longrightarrow K,$$

à savoir l'unique φ tel que $\varphi(X_i) = a_i$ pour $i = 1, \ldots, p$. Dire que les a_i sont algébriquement indépendants sur k revient à dire que le noyau de φ est réduit à 0 ; alors l'image de φ est un sous-anneau de K isomorphe à l'anneau des polynômes $k[X_1, \ldots, X_p]$, et le sous-corps engendré par les a_i est isomorphe au corps des fractions de $k[X_1, \ldots, X_n]$, c'est au corps des fractions rationnelles en $X_1, \ldots, X_p$, à coefficients dans k ; ce corps se note

$$k(X_1, \ldots, X_p).$$

Définition. Si le corps K est engendré, sur k, par des éléments $a_1, \ldots, a_p$ algébriquement indépendants sur k, on dit que K est une extension transcendante pure de k.

Théorème 6. Si K est un surcorps de type fini de k, il existe un sous-corps K' de K tel que :

(i) $k \subset K'$, K' étant une extension transcendante pure de k ;

(ii) le degré $[K : K']$ soit fini (donc K est une extension algébrique de K').

[Le lecteur comparera cet énoncé à celui du lemme de normalisation].

Définition. Dans la situation du théorème 6, tout système $(a_1, \ldots, a_p)$ d'éléments de K, algébriquement indépendants sur k, tels que K soit de degré fini sur le sous-corps K' engendré par k et $a_1, \ldots, a_p$, s'appelle une base de transcendance de K sur k.

Théorème 7. Si K est un surcorps de type fini de k, toute les bases de transcendance de K sur k ont le même cardinal. On l'appelle le degré de transcendance de K sur k.

[Par exemple, dire que le degré de transcendance est nul équivaut à dire que K est une extension algébrique de degré fini de k].

On va démontrer successivement le théorème 6 et le théorème 7.

Première démonstration du théorème 6: cela va être une démonstration "en montant". Soient $a_1, \ldots, a_n \in K$ tels que K soit engendré (comme corps) par k et les éléments $a_1, \ldots, a_n$. Si tous les a_i sont algébriques sur k, alors K est une extension algébrique de k, obtenue par adjonction successive d'éléments algébriques $a_1, \ldots, a_n$; on sait que le degré $[K : k]$ est fini dans ce cas. Le théorème 6 est alors vrai en prenant $K' = k$.

Sinon, il existe au moins un a_i (on peut supposer que c'est a_1, quitte à changer la numérotation) qui est transcendant sur k : l'homomorphisme

$$\varphi : k[X] \longrightarrow K$$

qui envoie X en a_1 a un noyau nul. [Dire que a_1 est transcendant sur k équivaut à dire que l'ensemble (a_1) est algébriquement libre sur k]. Le sous-corps K_1 engendré par k et a_1 est isomorphe à $k(X)$.

Le corps K est alors engendré par K_1 et les éléments $a_2, \ldots, a_n$. Si tous ces éléments sont algébriques sur K_1, le théorème est démontré en prenant $K' = k_1$. Sinon, a_2 par exemple est transcendant sur K_1 ; mais alors a_1 et a_2 sont algébriquement indépendants sur k (vérification immédiate). Soit K_2 le sous-corps qu'ils engendrent avec k. On peut évidemment continuer ce processus ; on trouvera donc, de proche, $a_1, \ldots, a_p$ algébriquement indépendants sur k, et si K_p désigne le sous-corps

qu'ils engendrent avec k, les éléments restants $a_{p+1}, \ldots, a_n$ (s'il y en a) seront algébriques sur K_p. Il suffit de prendre $K' = K'_p$ pour obtenir le théorème 6.

Deuxième démonstration du théorème 6: ce sera une démonstration "en descendant" ; c'est à cette seconde démonstration que ressemblera la démonstration du "lemme de normalisation" qu'on donnera plus loin. Si $a_1, \ldots, a_n$ sont algébriquement indépendants sur k, le théorème est démontré en prenant $K' = K$. Sinon, soit $P \in k[X_1, \ldots, X_n]$ non identiquement nul, tel que $P(a_1, \ldots, a_n) = 0$. On va montrer que l'un au moins des éléments $a_1, \ldots, a_n$ est algébrique sur le sous-corps engendré par k et les autres. Prouvons-le par récurrence sur n ; c'est évidemment vrai pour $n = 1$. Supposons-le vrai pour $n - 1$ $(n \geq 2)$, et prouvons-le pour n. Le polynome P contient effectivement l'une des variables (sinon il serait de degré 0, et comme $P(a_1, \ldots, a_n) = 0$ il serait identiquement nul) ; supposons que ce soit X_n :

$$P(X_1, \ldots, X_n) = \alpha_0 (X_n)^d + \alpha_1 (X_n)^{d-1} + \ldots + \alpha_d ,$$

où $\alpha_0, \ldots, \alpha_d \in k[X_1, \ldots, X_{n-1}]$, α_0 non identiquement nul, $d \geq 1$. Alors $\alpha_0(a_1, \ldots, a_{n-1}), \ldots, \alpha_d(a_1, \ldots, a_{n-1})$ sont des éléments de K, et on a dans K la relation

$$\alpha_0(a_1, \ldots, a_{n-1})(a_n)^d + \alpha_1(a_1, \ldots, a_{n-1})(a_n)^{d-1} + \ldots + \alpha_d(a_1, \ldots, a_{n-1}) = 0 .$$

Si $\alpha_0(a_1, \ldots, a_{n-1}) \neq 0$, cette relation montre que a_n est algébrique sur le sous-corps K_{n-1} engendré par k et les éléments $a_1, \ldots, a_{n-1}$. Si $\alpha_0(a_1, \ldots, a_{n-1}) = 0$, alors l'hypothèse de récurrence montre que l'un des éléments $a_1, \ldots, a_{n-1}$ est algébrique sur le sous-corps engendré par k et les autres, et a fortiori sur le sous-corps engendré par k, les autres et a_n.

Ainsi nous pouvons supposer que a_n (par exemple) est algébrique sur le sous-corps K_{n-1} engendré par k et les éléments $a_1, \ldots, a_{n-1}$. Donc $[K : K_{n-1}] < +\infty$, étudions maintenant l'extension K_{n-1} de k ; on peut recommencer. Ou bien K_{n-1} est

une extension transcendante pure de k, et alors le théorème 6 est démontré en prenant $K' = K_{n-1}$; ou bien a_{n-1} (par exemple) est algébrique sur le sous-corps K_{n-2} engendré par k et les éléments $a_1, \ldots, a_{n-2}$. Alors

$$[K : K_{n-2}] = [K : K_{n-1}] \cdot [K_{n-1} : K_{n-2}]$$

est fini, et on étudie l'extension K_{n-2} de k. En poursuivant ainsi, on trouvera que K est une extension algébrique de degré fini du corps K_p engendré par $a_1, \ldots, a_p$ et k, tandis que K_p est une extension transcendante pure de k. Le théorème sera donc démontré en prenant $K' = K_p$.

Démonstration du théorème 7 : elle va être analogue à la démonstration de l'invariance du cardinal des bases d'un espace vectoriel de dimension finie. On va prouver, par récurrence sur l'entier p, la proposition suivante :

Si un corps K est de type fini sur k, et si K possède une base de transcendance ayant p éléments, toute autre base de transcendance a aussi p éléments.

Ceci est vrai si $p = 0$; car l'hypothèse est alors que le degré $[K : k]$ est fini, et on doit montrer que toute base de transcendance est vide. Or c'est évident, car si $a \in K$ appartenait à une base de transcendance, a serait transcendant sur k, donc le corps $k\langle a \rangle$ engendré par k et a serait de degré infini sur k, et a fortiori K serait de degré infini sur k.

Faisons la récurrence, l'assertion étant supposée vraie pour $p-1$ ($p \geq 1$). Soit B une base de transcendance de K sur k, ayant p éléments. Il suffit de montrer que pour toute autre base de transcendance B' on a

$$\text{Card } B' \leq p \tag{1}$$

(car ensuite on échange les rôles de B et B').

Si B' est vide, la relation (1) est vraie ; sinon, prenons un élément $x \in B'$.

Lemme : Il existe une base de transcendance B'' contenant x et telle que $B''-\{x\}$ soit contenue dans B.

On le voit en reprenant la démonstration du théorème 6 "en montant" : K est engendré sur k par l'élément x et les éléments de B ; on rajoute à x, l'un après l'autre, des éléments de B qui, avec x, soient algébriquement indépendants sur k,

dépendants], et ceci de manière que les autres éléments de B soient algébriquement dépendants sur le sous-corps obtenu. D'où le lemme.

Posons alors

$$B' = \{x\} \cup B'_1, \quad x \notin B'_1 ,$$

$$B'' = \{x\} \cup B''_1 , \quad x \notin B''_1 .$$

On a $B''_1 \neq B'_1$, car x appartient au sous-corps engendré par k et les éléments de B'_1, donc x et les éléments de B ne sont pas algébriquement indépendants sur k. On a donc

$$\text{Card } B''_1 \leq \text{Card } B - 1 = p - 1.$$

Appliquons l'hypothèse de récurrence au corps K et au sous-corps $k\langle x\rangle$: B'_1 et B''_1 sont des bases de transcendance de K sur $k\langle x\rangle$, donc

$$\text{Card } B'_1 = \text{Card } B''_1 \leq p - 1,$$

et par suite

$$\text{Card } B' = 1 + \text{Card } B'_1 \leq p . \qquad \text{C.Q.F.D.}$$

13 - Démonstration du lemme de normalisation.

Soit A un anneau commutatif contenant un corps k, et engendré (comme anneau) par k et un nombre fini d'éléments.

La notion d'éléments de A algébriquement indépendants sur k est encore valable. Si $a_1, \ldots, a_p \in A$ sont algébriquement indépendants sur k, le sous-anneau de A qu'ils engendrent avec k est isomorphe à l'anneau des polynômes $k[X_1, \ldots, X_p]$.

Le lemme de normalisation (cf. ci-dessus, § 11, lemme 2) va résulter du lemme suivant :

Lemme.- Supposons que l'anneau A soit engendré (comme anneau) par le sous-corps k et des éléments $a_1, \ldots, a_n$. Si ces éléments ne sont pas algébriquement indépendants sur k, il existe des éléments $c_1, \ldots, c_{n-1} \in A$ tels que, si on note C le sous-anneau qu'ils engendrent avec k, A soit un C-module de type fini.

Voyons d'abord pourquoi ce lemme entraîne le lemme de normalisation. Supposons en effet que A soit engendré (comme anneau) par k et des éléments $a_1, \ldots, a_n$. S'ils sont algébriquements indépendants, on a $A \approx k[X_1, \ldots, X_n]$; il suffit de prendre

$B = A$, et on obtient le lemme de normalisation. Sinon, d'après le lemme ci-dessus, A est un C_1-module de type fini, où C_1 est engendré par k et $n-1$ éléments. Si ceux-ci sont algébriquement indépendants sur k, le lemme de normalisation est prouvé en prenant $B = C_1$; sinon, on recommence : C_1 est un module de type fini sur un sous-anneau C_2 engendré par k et $n-2$ éléments. Etc... Ces opérations ont une fin. On a alors une suite d'anneaux emboîtés

$$A \supset C_1 \supset C_2 \supset \dots \supset C_r ,$$

tels que :

(i) C_r soit isomorphe à une algèbre de polynômes $k[Y_1, \dots, Y_{n-r}]$;

(ii) A soit un C_1-module de type fini, C_1 un C_2-module de type fini, etc...

On voit aussitôt, par récurrence sur r, que A est un C_r-module de type fini, et il suffit de prendre $C_r = B$ pour obtenir le lemme de normalisation.

[Remarque : cette démonstration s'est faite "en descendant".] Reste à démontrer le lemme ci-dessus. Par hypothèse, il existe $P \in k[X_1, \dots, X_n]$, non identiquement nul, tel que $P(a_1, \dots, a_n) = 0$. Soit d le degré de P en X_n :

$$P = u_o(X_n)^d + u_1(X_n)^{d-1} + \dots + u_d ,$$

où $u_o, \dots, u_d \in k[X_1, \dots, X_{n-1}]$, avec $u_o \neq 0$. Supposons d'abord (cas favorable) que $u_o \in k$ (c'est-à-dire que $u_o(X_1, \dots, X_{n-1})$ soit un polynôme de degré zéro). Quitte à multiplier P par une constante $\neq 0$, on peut supposer que $u_o = -1$; alors

$$(a_n)^d = u_1(a_1, \dots, a_{n-1})(a_n)^{d-1} + \dots + u_d(a_1, \dots, a_n)$$

est combinaison linéaire de $1, a_n, \dots, (a_n)^{d-1}$ à coefficients dans le sous-anneau C engendré par k et les éléments $a_1, \dots, a_{n-1}$. Par récurrence sur $r \geq d$, on voit alors que $(a_n)^r$ est combinaison linéaire de $1, a_n, \dots, (a_n)^{d-1}$ à coefficients dans C. Il en résulte que A est engendré par $1, a_n, \dots, (a_n)^{d-1}$ comme C-module, et le lemme est démontré dans ce cas [en prenant $c_1 = a_1, \dots, c_{n-1} = a_{n-1}$].

Reste le cas général, qu'on va ramener au cas favorable par une astuce. Faisons sur les variables $X_1, \dots, X_n$ la substitution

(1) $$X_i = Z_i + (X_n)^{m_i} \quad , \quad i = 1, 2, \ldots, n-1$$

où les m_i sont des exposants entiers ≥ 0 qu'on déterminera dans un instant. De (1) on tire inversement

(2) $$Z_i = X_i - (X_n)^{m_i} \quad , \quad 1 \leq i \leq n-1 \ .$$

Tout polynôme en $X_1, \ldots, X_{n-1}, X_n$ devient un polynôme en $Z_1, \ldots, Z_{n-1}, X_n$, et vice-versa. Voyons ce que devient le polynôme $P(X_1, \ldots, X_n)$; il devient un polynôme $Q(Z_1, \ldots, Z_{n-1}, X_n)$ dont on va chercher le degré en X_n. Soit

$$X_1^{\alpha_1} \ldots X_{n-1}^{\alpha_{n-1}} X_n^{\alpha_n}$$

l'un quelconque des monômes figurant effectivement dans P ; il devient

(3) $$(Z_1 + (X_n)^{m_1})^{\alpha_1} \ldots (Z_{n-1} + (X_n)^{m_{n-1}})^{\alpha_{n-1}} X_n^{\alpha_n} \ ,$$

polynôme en X_n de degré

(4) $$\alpha_1 m_1 + \ldots + \alpha_{n-1} m_{n-1} + \alpha_n \ ,$$

le terme de plus haut degré en X_n ayant pour coefficient 1.

Le polynôme $Q(Z_1, \ldots, Z_{n-1}, X_n)$ est une combinaison linéaire, à coefficients dans k, des polynômes (3) ; si les degrés (4) de ces polynômes en X_n sont <u>tous distincts</u>, le terme de plus haut degré en X_n dans celui qui a le plus grand degré sera le terme de plus haut degré en X_n dans le polynôme Q ; donc le coefficient du terme du plus haut degré en X_n dans $Q(Z_1, \ldots, Z_{n-1}, X_n)$ <u>sera un élément</u> de k : on sera dans le cas favorable !

La condition pour qu'il en soit ainsi est donc que les formes linéaires en $u_1, \ldots, u_{n-1}$!

$$\sum_{i=1}^{n-1} \alpha_i u_i + \alpha_n \ ,$$

relatives aux différents monômes du polynôme P, prenent des valeurs distinctes lorsqu'on donne aux variables $u_1, \ldots, u_{n-1}$ des valeurs entières $m_1, \ldots, m_n$ convenablement choisies. Considérons les différences deux à deux de ces formes linéaires, et formons leur produit ; c'est un polynôme

$$R(u_1, \ldots, u_{n-1}) \not\equiv 0$$

à coefficients entiers ; on doit montrer qu'on peut choisir les entiers positifs

$m_1, \ldots, m_{n-1}$ de façon que

$$R(m_1, \ldots, m_{n-1}) \neq 0.$$

Ceci se prouve par récurrence sur le nombre $n-1$ des variables. Pour $n - 1 = 1$, le polynôme $R(m)$ n'a qu'un nombre fini de zéros, tandis qu'il y a une infinité d'entiers > 0 ; donc la récurrence démarre, et on laisse au lecteur le soin de l'achever.

Ainsi, par le changement de variables (1), $P(X_1, \ldots, X_n)$ s'est transformé en un polynôme $Q(Z_1, \ldots, Z_{n-1}, X_n)$ qui est dans le cas favorable. Posons alors

$$c_i = a_i - (a_n)^{m_i} \quad , \quad i = 1, \ldots, n-1 \ ;$$

on a $Q(c_1, \ldots, c_{n-1}, a_n) = 0$, et puisqu'on est dans le cas favorable, A est un module de type fini sur le sous-anneau C engendré par k et les éléments $c_1, \ldots, c_{n-1}$.

C.Q.F.D.

Nous avons ainsi achevé la démonstration du lemme de normalisation. En même temps, le théorème fondamental (th. 4 du § 10) est entièrement établi. Nous allons maintenant pouvoir exploiter ce théorème.

14 - Le théorème des zéros de Hilbert.

Soit $\mathfrak{P}$ un idéal premier de $k[X_1, \ldots, X_n]$. Le théorème 4 nous dit que si Ω est algébriquement clos, on a

$$\mathfrak{I}(\mathfrak{V}_\Omega(\mathfrak{P})) = \mathfrak{P}.$$

Proposons-nous maintenant de déterminer $\mathfrak{I}(\mathfrak{V}_\Omega(I))$ lorsque I est un idéal quelconque, non nécessairement premier. Soit

$$V = \mathfrak{V}_\Omega(I) \quad ;$$

d'après le théorème 3 (§ 7), on a

$$V = \bigcup_i V_i \ ,$$

les V_i étant les composantes irréductibles de V, en nombre fini.

On a donc

$$\mathfrak{I}(V) = \bigcap_i \mathfrak{I}(V_i) \ .$$

Or $\mathfrak{I}(V_i) = \mathfrak{P}_i$ est un idéal premier.

Proposition 8. *Ω étant toujours supposé algébriquement clos, l'idéal $\mathfrak{I}(\mathfrak{V}_\Omega(I))$ est l'intersection de tous les idéaux premiers contenant I.*

Démonstration: on sait déjà que $\mathfrak{J}(V) = \bigcap_i \mathcal{P}_i$ est intersection d'une famille finie d'idéaux premiers. Il reste à montrer que si $\mathcal{P}$ est un idéal premier contenant I, alors $\mathcal{P}$ contient aussi $\mathfrak{J}(\mathcal{V}_\Omega(I))$. Or on a

$$\mathcal{V}(\mathcal{P}) \subset \mathcal{V}(I),$$

donc $$\mathfrak{J}(\mathcal{V}(\mathcal{P})) \supset \mathfrak{J}(\mathcal{V}(I)).$$

Mais, d'après le théorème 4, on a $\mathfrak{J}(\mathcal{V}(\mathcal{P})) = \mathcal{P}$, d'où $\mathcal{P} \supset \mathfrak{J}(\mathcal{V}(I))$, ce qui prouve la proposition.

Définition. Dans tout anneau commutatif A, si I est un idéal de A, on appelle radical de I, et on note $\mathrm{Rad}(I)$, l'idéal intersection de tous les idéaux premiers contenant I.

La proposition 8 exprime donc que $\mathfrak{J}(\mathcal{V}_\Omega(I)) = \mathrm{Rad}\, I$ lorsque Ω est algébriquement clos. En particulier, si $1 \notin I$, alors $1 \notin \mathrm{Rad}(I)$ (car $\mathrm{Rad}(I)$ est contenu dans tout idéal maximal contenant I), donc $\mathcal{V}_\Omega(\mathfrak{J}(\mathcal{V}_\Omega(I))) \neq \emptyset$. Ceci signifie que $\mathcal{V}_\Omega(I)$ n'est pas vide lorsque $1 \notin I$.

En d'autres termes : si des polynômes $P_\alpha \in k[X_1, \ldots, X_n]$ n'ont aucun zéro commun dans Ω^n (Ω étant supposé algébriquement clos), alors il existe des polynômes Q_α tels que

$$\sum_\alpha Q_\alpha P_\alpha = 1.$$

Il nous reste à donner une caractérisation commode du radical d'un idéal :

Proposition 9.- Le radical d'un idéal I, dans un anneau commutatif A, se compose des $a \in A$ tels qu'il existe un exposant entier $h \geq 1$ satisfaisant à $a^h \in I$.

1°/ Il est évident que $a^h \in I \Rightarrow a \in \mathrm{Rad}(I)$; car si $\mathcal{P}$ est un idéal premier contenant I, on a $a^h \in \mathcal{P}$, d'où l'on conclut $a \in \mathcal{P}$.

2°/ Reste à prouver que, réciproquement, si $a \in \mathrm{Rad}(I)$, il existe $h \geq 1$ tel que $a^h \in I$. C'est vrai, mais nous ne ferons la démonstration que dans le cas où A est intègre (ceci, pour éviter des considérations techniques qui alourdiraient l'exposé). Observons que ceci est bien suffisant pour le cas qui nous intéresse, et qui est celui où $A = k[X_1, \ldots, X_n]$.

Supposons donc A intègre. Soit $a \in A$; supposons $a^h \notin I$ pour tout entier $h \geq 1$; on veut trouver un idéal <u>premier</u> $\mathcal{P}$ tel que

$$\mathcal{P} \supset I, \quad a \notin \mathcal{P}.$$

Or considérons les fractions de la forme $\frac{x}{a^h}$, où $x \in A$, h entier ≥ 0 ; elles forment un sous-anneau B du corps des fractions de A, et B contient A. Les éléments $\frac{x}{a^h}$, où $x \in I$, forment un <u>idéal</u> J de B (vérification immédiate). De plus, $1 \notin J$, sinon on aurait

$$1 = \frac{x}{a^h}, \quad x \in I,$$

donc a^h appartiendrait à I, contrairement à l'hypothèse. Il s'ensuit qu'il existe dans B un <u>idéal maximal</u> $\mathcal{M}$ contenant J. L'intersection $\mathcal{M} \cap A = \mathcal{P}$ est un idéal premier de A qui contient I ; mais $a \notin \mathcal{P}$, sinon $1 = \frac{1}{a}$. a appartiendrait à $\mathcal{M}$. Ceci achève la démonstration.

Si nous mettons ensemble les propriétés 8 et 9, nous obtenons :

<u>Théorème 8.</u> ("théorème des zéros" de Hilbert).- <u>Soit</u> I <u>un idéal de</u> $k[X_1, \ldots, X_n]$, <u>et soit</u> $V = \mathcal{V}_\Omega(I)$ <u>la variété des zéros de</u> I <u>dans</u> Ω^n (où $\Omega \supset k$ est un corps algébriquement clos). <u>Alors si</u> $P \in k[X_1, \ldots, X_n]$ <u>s'annule en tout point de</u> V, <u>il existe un exposant entier</u> $h \geq 1$ <u>tel que</u> $P^h \in I$. [La réciproque est évidente : si $P^h \in I$, P s'annule en tout point de V].

15- <u>Variétés algébriques dans l'espace projectif.</u>

L'espace projectif $P_n(\Omega)$ est le quotient de $\Omega^{n+1} - \{0\}$ par la relation d'équivalence définie par les homothéties de rapport $\lambda \in \Omega$ $(\lambda \neq 0)$. Soit

$$p : \Omega^{n+1} - \{0\} \longrightarrow P_n(\Omega)$$

l'application canonique de $\Omega^{n+1} - \{0\}$ sur son quotient.

<u>Définition.</u> Un sous-ensemble $W \subset P_n(\Omega)$ est une variété linéaire projective si et seulement si

$$p^{-1}(W) \cup \{0\}$$

est un sous-espace vectoriel de Ω^{n+1} ; si h est la dimension de cet espace vectoriel, on dit que W est de dimension $h - 1$.

Soit à nouveau k un sous-corps de Ω.

Définition. On dit que $W \subset P_n(\Omega)$ est une k-variété algébrique (projective) si $p^{-1}(W) \cup \{0\}$ est une k-variété algébrique dans Ω^{n+1}.

Observons que $p^{-1}(W) \cup \{0\}$ est stable par les homothéties (et contient 0) ; autrement dit, c'est un cône de sommet 0 ; et l'on demande que ce cône soit une variété algébrique sur k. Ainsi les k-variétés algébriques de $P_n(\Omega)$ sont en correspondance bijective avec les cônes algébriques (sur k) dans Ω^{n+1}.

On appelle idéal d'une variété algébrique projective W l'idéal du cône correspondant de Ω^{n+1}.

Etudions donc brièvement les cônes algébriques. Pour cela, on supposera désormais que le corps Ω est infini ; ce n'est pas une restriction grave, puisque le cas le plus intéressant est celui où Ω est algébriquement clos ; or tout corps algébriquement clos est infini.

Proposition 10.- $\{0\}$ et Ω^{n+1} sont des cônes algébriques ; la réunion de deux cônes algébriques est un cône algébrique ; toute intersection de cônes algébriques est un cône algébrique (et c'est déjà l'intersection d'un nombre fini d'entre eux).

C'est évident. On en déduit que, dans $P_n(\Omega)$, $\emptyset$ et $P_n(\Omega)$ sont des variétés algébriques projectives (sur k) ; que la réunion de deux variétés algébriques est une variété algébrique, et que l'intersection d'une famille de variétés algébriques est une variété algébrique. D'où la k-topologie de Zariski sur l'espace projectif $P_n(\Omega)$.

Soit Γ un cône algébrique sur k ; que peut-on dire de l'idéal $\mathfrak{J}(\Gamma)$ de tous les $P \in k[X_0, X_1, \ldots, X_n]$ qui s'annulent en tout point de Γ ?

Proposition 11. Si $P \in \mathfrak{J}(\Gamma)$, toutes les composantes homogènes de P sont dans $\mathfrak{J}(\Gamma)$.

Démonstration. Soit $P = \sum_{i=0}^{p} P_i$, où P_i est un polynôme homogène de degré i. On a

$$P(\lambda X_0, \ldots, \lambda X_n) = \sum_{i=0}^{p} \lambda^i P_i(X_0, \ldots, X_n)$$

pour tout $\lambda \in \Omega$. Si $(x_0, \ldots, x_n) \in \Gamma$, et si P s'annule sur Γ, on a $P(\lambda x_0, \ldots, \lambda x_n) = 0$ pour tout $\lambda \in \Omega$, c'est-à-dire

$$\sum_{i=0}^{p} \lambda^i P_i(x_0, \ldots, x_n) = 0$$

pour tout $\lambda \in \Omega$. Comme le corps Ω est infini, le polynôme en T :

$$\sum_{i=0}^{p} P_i(x_0, \ldots, x_n)\, T^i$$

est identiquement nul, autrement dit on a

$$P_i(x_0, \ldots, x_n) = 0 \quad \text{pour tout } i,$$

et ceci quel que soit $(x_0, \ldots, x_n) \in \Gamma$. C.Q.F.D.

Définition. On dit qu'un idéal $I \subset k[X_0, \ldots, X_n]$ est homogène si chaque fois qu'un polynôme F appartient à I, toutes ses composantes homogènes appartiennent à I.

Un idéal engendré par des polynômes homogènes est un idéal homogène (exercice facile laissé au lecteur), la réciproque étant évidente.

La proposition 11 exprime que l'idéal $\mathfrak{I}(\Gamma)$ d'un cône Γ est un idéal homogène. Il est évident, en sens inverse, que si I est un idéal homogène, $\mathfrak{Z}(I)$ est un cône.

Naturellement, un idéal homogène est engendré par une famille finie de polynômes homogènes (conséquence du théorème 1, § 5).

Exercice. Pour qu'un idéal homogène I soit premier, il suffit (et il faut, bien entendu) que : (i) $1 \notin I$;

(ii) P et Q sont deux polynômes homogènes tels que $PQ \in I$, alors $P \in I$ ou $Q \in I$.

Théorème 9. Les composantes irréductibles d'un cône algébrique sont des cônes algébriques.

Démonstration. Observons d'abord qu'un cône Γ n'est jamais vide, puisque $0 \in \Gamma$. Soit

$$\Gamma = \bigcup_i V_i \qquad (V_i \not\subset V_j \text{ pour } i \neq j)$$

la décomposition de Γ en ses composantes irréductibles V_i. On va montrer que les V_i sont des cônes. Soit $\lambda \in \Omega$, $\lambda \neq 0$; notons λV le transformé d'une variété V par l'homothétie de rapport λ. Les λV_i sont des variétés algébriques irréductibles, on a $\lambda V_i \not\subset \lambda V_j$ pour $i \neq j$; comme $\lambda \Gamma = \Gamma$, on a

$$\Gamma = \bigcup_i (\lambda V_i).$$

Donc les λV_i sont les composantes irréductibles de Γ, et par suite sont égales aux V_i à l'ordre près. Soit σ_λ la permutation de l'ensemble des indices, telle que

$$\lambda V_i = V_{\sigma_\lambda(i)} .$$

On vérifie que $\sigma_{\lambda\mu} = \sigma_\lambda \circ \sigma_\mu$, donc $\lambda \longmapsto \sigma_\lambda$ est un homomorphisme du groupe multiplicatif $\Omega - \{0\}$ (qui est infini) dans le groupe des permutations de l'ensemble des indices, groupe qui est fini. Le noyau de cet homomorphisme est donc infini. Autrement dit, il existe une infinité de $\lambda \in \Omega - \{0\}$ tels que $\lambda V_i = V_i$ pour tout i, c'est-à-dire tels que chaque V_i soit stable par l'homothétie de rapport λ. Soit alors $P \in \mathfrak{J}(V_i)$,

$$P = \sum_{\alpha=0}^{p} P_\alpha , \quad P_\alpha \text{ homogène de degré } \alpha .$$

Le même raisonnement que plus haut montre que chacun des P_α appartient à $\mathfrak{J}(V_i)$; donc l'idéal $\mathfrak{J}(V_i)$ est homogène, et par suite $V_i = \Psi(\mathfrak{J}(V_i))$ est un <u>cône</u> C.Q.F.D.

Par la correspondance bijective entre les cônes algébriques de Ω^{n+1} et les variétés algébriques de l'espace projectif $P_n(\Omega)$, le théorème 9 donne la <u>décomposition d'une variété algébrique projective en ses composantes irréductibles</u>.

16- <u>Relation entre variétés algébriques affines et variétés algébriques projectives</u>.

Soit $j : \Omega^n \longrightarrow \Omega^{n+1} - \{0\}$ l'injection canonique, définie par

$$j(x_1, \ldots, x_n) = (1, x_1, \ldots, x_n).$$

L'application composée

$$\Omega^n \xrightarrow{j} \Omega^{n+1} - \{0\} \xrightarrow{p} P_n(\Omega)$$

est une <u>injection</u> de Ω^n dans $P_n(\Omega)$, qui identifie Ω^n au complémentaire de l'<u>hyperplan à l'infini</u> dans $P_n(\Omega)$ [l'hyperplan à l'infini est l'image par p des points $(x_0, x_1, \ldots, x_n) \in \Omega^{n+1} - \{0\}$ tels que $x_0 = 0$]. On fera désormais cette identification. Alors tout sous-ensemble de Ω^n est identifié à un sous-ensemble de $P_n(\Omega)$.

<u>Définition</u>. A toute k-variété algébrique V de Ω^n on associe $\bar{V} \subset P_n(\Omega)$, la plus petite k-variété algébrique projective contenant V. [$\bar{V}$ est donc l'adhérence de V pour la topologie de Zariski de $P_n(\Omega)$]. Ceci s'explicite comme suit : $j(V)$ est un sous-ensemble de Ω^{n+1}, on lui associe $\Gamma(V)$, <u>le plus petit cône algébrique</u> (sur k) contenant $j(V)$; et alors $\bar{V}$ est la variété algébrique projective définie par le cône $\Gamma(V)$.

$\Gamma(V)$ est évidemment l'ensemble des zéros communs à tous les polynômes homogènes $P(X_0, X_1, \ldots, X_n)$ tels que $P(1, X_1, \ldots, X_n) \in \mathfrak{J}(V)$. Ceci conduit à une définition.

Définition. A chaque idéal $I \subset k[X_1, \ldots, X_n]$ on associe l'idéal homogène $\overline{I} \subset k[X_0, X_1, \ldots, X_n]$ engendré par les $P(X_0, X_1, \ldots, X_n)$ homogènes tels que

$$P(1, X_1, \ldots, X_n) \in I.$$

Il résulte des définitions précédentes que l'idéal $\mathfrak{J}(\overline{V})$ (qui est, par définition, l'idéal $\mathfrak{J}(\Gamma(V))$) n'est autre que l'idéal homogène $\overline{\mathfrak{J}(V)}$.

Lemme. Tout $Q(X_1, \ldots, X_n) \in I$ est de la forme $P(1, X_1, \ldots, X_n)$, où $P(X_0, X_1, \ldots, X_n)$ est homogène.

En effet, soit

$$Q = \sum_{\alpha=0}^{p} Q_\alpha \quad , \quad Q_\alpha \text{ homogène de degré } \alpha .$$

Alors

$$P = \sum_{\alpha=0}^{p} (X_0)^{p-\alpha} \, Q_\alpha(X_1, \ldots, X_n)$$

répond à la question. Il est d'ailleurs évident que $P \in \overline{I}$, puisque $P(1, X_1, \ldots, X_n) \in I$.

Il résulte de ce lemme que $\Gamma(V) \cap j(\Omega^n) = j(V)$. Or ceci exprime simplement que

$$\boxed{\overline{V} \cap \Omega^n = V .}$$

Autrement dit, tous les points de $\overline{V}$ qui n'appartiennent pas à V sont des points à l'infini de $P_n(\Omega)$.

Proposition 12.- L'application $V \longmapsto \overline{V}$ respecte la réunion finie, mais pas l'intersection.

Autrement dit, on a

$$\overline{V_1 \cup V_2} = \overline{V}_1 \cup \overline{V}_2$$

[Cela résulte du fait que $\overline{V}$ est l'adhérence de V pour la topologie de Zariski de $P_n(\Omega)$], mais en général

$$\overline{V_1 \cap V_2} \neq \overline{V}_1 \cap \overline{V}_2 .$$

Par exemple, dans le plan, prenons pour V_1 et V_2 deux droites parallèles et distinctes ; alors $V_1 \cap V_2$ est vide, mais $\overline{V}_1 \cap \overline{V}_2$ ne l'est pas, car les deux droites se coupent à l'infini.

Proposition 13. $(V \subset W) \Longleftrightarrow (\overline{V} \subset \overline{W})$, et de plus, : (V irréductible) $\Leftarrow$ (... réductible).

La première assertion est évidente. Montrons la seconde ; il suffit d'examiner le cas où $V \neq \emptyset$. Si V est réductible, $V = V_1 \cup V_2$, $V_1 \neq V$, $V_2 \neq V$, on a

$$\overline{V} = \overline{V}_1 \cup \overline{V}_2 \text{ , et on a bien } \overline{V}_1 \neq \overline{V} \text{ et } \overline{V}_2 \neq \overline{V},$$

car si $\overline{V}_1 = \overline{V}$ par exemple, on aurait

$$V_1 = \overline{V}_1 \cap \Omega^n = \overline{V} \cap \Omega^n = V.$$

Inversement, si $\overline{V}$ est réductible, soit $\overline{V} = W_1 \cup W_2$, $W_1 \neq \overline{V}$, $W_2 \neq \overline{V}$; alors $V = V_1 \cup V_2$, avec

$$V_1 = W_1 \cap \Omega^n, \qquad V_2 = W_2 \cap \Omega^n,$$

et on a $V_1 \neq V$ et $V_2 \neq V$; car si $V_1 = V$ par exemple, alors $\overline{V}_1 = \overline{V}$ $\overline{V}_1 \subset \overline{W}_1 \neq \overline{V}$; contradiction.

Corollaire. Si les V_i sont les composantes irréductibles d'une V algébrique affine, alors les $\overline{V}_i$ sont les composantes irréductibles de la variété algébrique projective correspondante $\overline{V}$.

Exercice. Pour qu'une k-variété algébrique projective W soit de la forme $\overline{V}$, où V est une k-variété algébrique affine, il faut et il suffit qu'aucune des composantes k-irréductibles de W ne soit contenue dans l'hyperplan à l'infini.