UNIVERSITÉ PARIS XI

U.E.R. MATHÉMATIQUE

91405 ORSAY FRANCE

Nº 84

COURS DE C_3

SCIENCES MATHEMATIQUES

- I -

ALGEBRE et ARITHMETIQUE

TABLE DES MATIERES

CHAPITRE I

ANNEAUX PRINCIPAUX.

§ 1. Brèves généralités.

§ 2. Exemples.

§ 3. Résultats valables pour un anneau principal quelconque.

§ 1. Brèves généralités.

A est un anneau unitaire (existence de l'élément neutre 1 pour la multiplication), commutatif ($ab = ba$) et intègre ($ab = 0 \Rightarrow a = 0$ ou $b = 0$).

On rappelle la définition d'un idéal I dans l'anneau A. L'idéal particulier $I = A$ s'appelle idéal impropre, l'idéal particulier $I = \{0\}$ est l'idéal nul.

L'idéal $I = Aa = \{xa \mid x \in A\}$ est dit principal. L'élément a est un générateur.

Propriété 1. Deux générateurs a et b d'un même idéal principal non nul sont associés : $b = \varepsilon a$, $\varepsilon \in U$, où U désigne le groupe des unités de A

Démonstration (à faire en détail).

Rappel de la définition d'une unité u (telle que $uu' = 1$). Les unités forment un groupe multiplicatif U. La relation $\mathcal{R}$ entre éléments associés est une relation d'équivalence.

Définition 1. A est un anneau principal s'il est unitaire, commutatif, intègre, avec la propriété suivante : tout idéal est principal.

Avant de voir certaines propriétés générales des anneaux principaux, donnons dès maintenant quelques exemples.

§ 2. Exemples.

1°. L'anneau $\mathbb{Z}$ des entiers relatifs est principal.

(Rappel de la démonstration).

2°. L'anneau $k[X]$ des polynômes à une indéterminée X et à coefficients dans un corps commutatif k est principal.

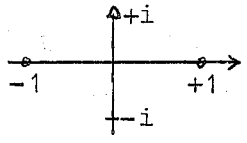
(Rappel de la démonstration s'appuyant sur la division des polynômes ordonnés suivant les puissances décroissantes de X).

3°. L'anneau $A = \mathbb{Z}[i]$ des entiers de Gauss est principal.

Rappels : $K = \mathbb{Q}(i) = \mathbb{Q}[i] = \{a + bi \mid a, b \in \mathbb{Q}\}$ est l'extension quadratique de $\mathbb{Q}$ engendrée par i. $E_1(K) = \mathbb{Z}[i] = \{a + bi \mid a, b \in \mathbb{Z}\}$ est un sous-anneau de $\mathbb{Q}(i)$ qui coïncide (on le verra plus loin) avec l'anneau $E(K)$ des entiers algébriques de K sur $\mathbb{Z}$. On l'appelle l'anneau des entiers de Gauss.

Si $a + bi = \alpha \in \mathbb{Z}[i]$, on a $N(\alpha) = a^2 + b^2 \in \mathbb{N} \cup \{0\}$ (norme de α) $N(\alpha) = 0$ si et seulement si $\alpha = 0$; donc : $\alpha \neq 0 \implies N(\alpha) \geqslant 1$. De plus $N(\alpha\beta) = N(\alpha)N(\beta)$ (propriété du module d'un produit de 2 nombres complexes).

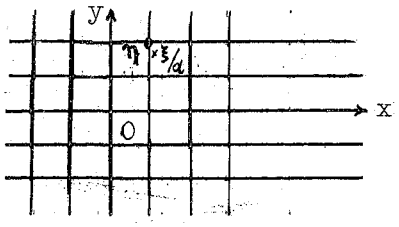
Eléments inversibles de $\mathbb{Z}[i]$. Si $\alpha\beta = 1$, α et $\beta \in \mathbb{Z}[i]$, on a $N(\alpha\beta) = N(\alpha)N(\beta) = N(1) = 1$. Comme α et β sont non nuls, $N(\alpha)$ et $N(\beta)$ sont des entiers $\geqslant 1$, ce qui exige $N(\alpha) = N(\beta) = 1$. Les seuls entiers de Gauss de norme égale à 1 sont ± 1, $\pm i$. Réciproquement ± 1, $\pm i$ sont inversibles. Donc le groupe des unités est $U = \{\pm 1, \pm i\}$



Théorème 1. L'anneau $\mathbb{Z}[i]$ est principal.

Lemme (de division). Soit $\alpha = a + ib \in A$, $\alpha \neq 0$. $\forall \xi \in A$, $\exists \eta$ et $\rho \in A$ tels que $\xi = \alpha\eta + \rho$, $N(\rho) < N(\alpha)$.

Démonstration : considérons $\frac{\xi}{\alpha} = u + iv$, $u, v \in \mathbb{Q}$.



L'image de $\frac{\xi}{\alpha}$ dans le plan complexe tombe dans l'un des carrés du réseau des points à coordonnées entières (images des éléments

de l'anneau des entiers de Gauss). Soit η l'affixe du sommet le plus proche de $\frac{\xi}{\alpha}$. (Il peut y avoir 1, 2 ou 4 choix possibles de η selon la position de $\frac{\xi}{\alpha}$). On a donc : $N(\frac{\xi}{\alpha} - \eta) \leqslant \frac{1}{4} + \frac{1}{4} = \frac{1}{2}$. Posons $\rho = \xi - \alpha\eta$. On a donc $\rho \in A$ et $N(\rho) = N(\alpha)\, N(\frac{\xi}{\alpha} - \eta) \leqslant \frac{1}{2} N(\alpha)$. Il en résulte bien $N(\rho) < N(\alpha)$.

Preuve du Théorème. Soit I un idéal de l'anneau A. Si $I = \{0\}$, I est principal. Supposons $I \neq \{0\}$ et soit α un élément non nul de I dont la norme est minimum. On a donc $\alpha \neq 0$. Soit $\xi \in I$. Le lemme s'applique avec $N(\rho) = 0$ (donc $\rho = 0$) à cause du choix de α. On a donc $\xi = \alpha\eta$ et $I \subseteq A\alpha$. Comme $A\alpha \subseteq I$, on a $I = A\alpha$.

Remarque. Les exemples précédents rentrent dans la classe des anneaux euclidiens : anneau A intègre, commutatif et unitaire, avec une application $g : A - \{0\} \to \mathbb{N} \cup \{0\}$, qui vérifie les 2 conditions :

1°) $g(\alpha\beta) \geqslant g(\alpha)$, $\forall\, \alpha, \beta \neq 0$.

2°) Soit $\alpha \neq 0$; $\forall\, \xi \in A$ $\exists\, r, q \in A$ tels que :

$$\xi = \alpha q + r \text{ , avec } r = 0 \text{ ou } g(r) < g(\alpha).$$

Alors $\mathbb{Z}$, $k[X]$, $\mathbb{Z}[i]$ sont euclidiens ; on le voit en prenant respectivement comme application g celle qui est définie par :

$$g(a) = |a| \quad \text{pour } a \in \mathbb{Z}$$

$$g(f) = \text{degré de } f \text{ pour } f \in k[X],\ f \neq 0$$

$$g(\alpha) = N(\alpha) \quad \text{pour } \alpha \in \mathbb{Z}[i].$$

Propriété 2. Tout anneau euclidien est principal.

(Faire la démonstration).

§ 3. Résultats valables pour un anneau principal quelconque.

Les définitions sont valables pour un anneau commutatif, unitaire et intègre.

Définition 2. Un élément $p \in A$ est premier si l'idéal principal Ap est premier, propre et non nul. (p est donc non nul et non inversible).

On rappelle que l'idéal P est premier si l'on a :

$$ab \in P \implies a \in P \text{ ou } b \in P .$$

Il revient au même de dire que l'anneau quotient A/P est intègre.

Définition 3. Un élément $p \in A$ est irréductible (ou indécomposable) s'il est non nul, non inversible, et s'il vérifie la condition suivante :

$$p = ab \implies a \in U \text{ ou } b \in U$$

U désigne le groupe des unités.

Propriété 3. Dans un anneau intègre quelconque, tout élément premier est irréductible.

élément premier $\implies$ élément irréductible.

En effet, si $p = ab$, on a : $ab \in Ap$, idéal premier, d'où $a \in Ap$ ou $b \in Ap$. L'hypothèse $a = up$ entraîne $a = uab$ d'où $1 = ub$ ($a \neq 0$ et A intègre) et $b \in U$.

Propriété 4. Dans un anneau principal, si p est irréductible, l'idéal Ap est maximal.

On rappelle que M est maximal s'il est maximal dans l'ensemble des idéaux propres :

$$M \subseteq I \implies I = M \text{ ou } I = A .$$

Cela revient à dire que l'anneau quotient A/M est un corps (exercice de révision).

En effet, supposons $Ap \subseteq I$ et A principal ; on a donc $I = Ab$ et $p = ab$. Comme p est irréductible il vient $a \in U$ ou $b \in U$, c'est-à-dire $I = Ap$ ou $I = A$. En corollaire, on a :

Théorème 2. Dans un anneau principal, tout idéal premier propre et non nul est maximal.

En effet si P est un idéal premier propre et non nul, on a $P = Ap$ où p est un élément prémier, d'où le théorème avec les propriétés 3 et 4.

Propriété 5. Dans un anneau principal, il y a coïncidence entre les notions

d'élément irréductible et d'élément premier.

On sait déjà que tout élément premier est irréductible. Réciproquement, si p est irréductible et l'anneau principal, l'idéal Ap est maximal (prop. 4) donc premier (tout idéal maximal est premier; le vérifier), et par suite p est premier.

La propriété 5 est la condition de Gauss : si p est irréductible et s'il divise un produit de 2 facteurs, p divise au moins l'un d'eux :

p irrédutible, $p|ab \implies p|a$ ou $p|b$.

Propriété 6. Dans un anneau principal, toute suite croissante d'idéaux est stationnaire.

Cela signifie que, si on a une suite infinie d'idéaux :

$I_1 \subseteq I_2 \subseteq \dots \subseteq I_n \subseteq \dots$, alors $I_n = I_{n+1} = \dots$ à partir d'un certain rang. Ou encore, si la suite est strictement croissante, elle est finie. Cette propriété caractérise ce qu'on appelle un anneau noethérien (voir plus loin Chap. VI, § 2).

En effet, considérons la réunion $\bigcup_{n=1}^{n=\infty} I_n$ des idéaux de la suite ; c'est un idéal I (du fait que les idéaux sont emboîtés ; ce n'est pas vrai en général pour une réunion d'idéaux quelconques). Comme A est principal, on a $I = Ab$. L'élément b appartient à la réunion des I_n et par suite à l'un d'eux, soit I_q . On a donc pour $n \geqslant q$:

$$I_q \subseteq I_n \subseteq I \subseteq I_q$$

d'où $I_n = I_q$.

Un anneau principal est donc noethérien. (La réciproque est fausse : $K[X,Y]$ est noethérien (Chap. VI, § 5) et non principal).

D'autres propriétés intéressantes des anneaux principaux font appel à la décomposition d'un élément quelconque comme produit d'un nombre fini d'éléments irréductibles. Elles seront vraies dans le cadre plus général des anneaux factoriels que nous étudions au Chap. II.

CHAPITRE II

ANNEAUX FACTORIELS

§ 1. Anneaux à factorisation unique.

A est encore un anneau commutatif intègre et unitaire. Nous avons donné au chapitre I la définition d'un élément irréductible (ou indécomposable) et celle d'éléments associés (équivalents selon la relation d'équivalence $a \equiv b\ (\mathcal{R}) \iff a = \varepsilon b$, $\varepsilon \in U$, U étant le groupe des unités). La théorie de la décomposition d'un élément quelconque a $(a \neq 0,\ a \notin U)$ en un produit fini d'éléments irréductibles, d'une manière unique, va être valable en particulier, pour les anneaux principaux, ainsi que pour des anneaux plus généraux que nous appellerons factoriels.

Définition 1. On appelle anneau factoriel un anneau A, commutatif, intègre et unitaire, satisfaisant aux deux conditions suivantes :

1°) Condition d'existence d'une factorisation : tout élément $a\ (\neq 0$ et $\notin U)$ est égal à un produit fini d'éléments irréductibles.

2°) Condition d'unicité de la factorisation : si un élément $a\ (\neq 0$ et $\notin U)$ s'exprime de deux manières sous la forme d'un produit d'éléments irrédutibles

$$(1) \qquad a = p_1 p_2 \cdots p_n = q_1 q_2 \cdots q_m .$$

On a $n = m$, et on peut ranger les éléments q_j de façon que $p_i \equiv q_i\ (\mathcal{R})$.

Autrement dit, si l'on considère les facteurs irréductibles distincts $p_i\ (\mathrm{mod}\,\mathcal{R})$ qui interviennent dans la décomposition (1), ceux-ci sont bien déterminés à la relation d'équivalence $\mathcal{R}$ près, ainsi que les exposants α_i

dont chacun est affecté

$$a = \varepsilon \prod_{i=1}^{i=k} p_i^{\alpha_i}, \quad \varepsilon \in U, \quad p_i \not\equiv p_j \pmod{\mathcal{R}} \text{ si } i \neq j .$$

Dans la définition, la condition 2° d'unicité va pouvoir, compte tenu de la condition 1° d'existence, être remplacée par la condition de Gauss. Plus précisément :

Théorème 1. Pour qu'un anneau soit factoriel, il faut et il suffit qu'il vérifie les deux conditions suivantes :

1°) condition d'existence d'une factorisation (inchangée)

2°) condition de Gauss : tout élément irréductible est premier.

(autrement dit : si p est irréductible et s'il divise un produit de 2 facteurs, il divise au moins l'un d'eux : p irréductible, $ab = cp \Longrightarrow a = mp$ ou $b = tp$).

Démonstration : à faire en détails, condition nécessaire, condition suffisante.

Les conditions du théorème 1 sont déjà plus applicables que la définition puisqu'on a vu par exemple qu'un anneau principal vérifie la condition de Gauss (propriété 5 du chapitre I).

Une autre forme équivalente encore plus élaborée est la suivante :

Théorème 2. Pour qu'un anneau soit factoriel, il faut et il suffit qu'il vérifie les 2 conditions suivantes :

1°) l'intersection de 2 idéaux principaux est un idéal principal

2°) toute suite infinie croissante d'idéaux principaux est stationnaire.

Preuve : condition suffisante. Etablissons d'abord la condition **P** d'existence de la factorisation. En la supposant non vérifiée, on choisirait un élément a ne vérifiant pas **P** tel que l'idéal principal $Aa = (a)$ soit maximal parmi les idéaux principaux dont les générateurs ne vérifient pas **P**. Ce choix est possible en vertu de la condition 2° du th. 2 qui implique la

condition maximale pour les idéaux principaux (à expliquer plus en détail). Alors a n'est pas irréductible (sinon il vérifierait P) et il existe une décomposition $a = bc$, avec $(a) \subsetneq (b)$ et $(a) \subsetneq (c)$. Comme (a) est maximal parmi ..., b et c vérifient la propriété P : $b = \prod_{\text{fini}} p_i$, $c = \prod_{\text{fini}} q_j$, d'où $a = bc = \prod p_i \prod q_j$ (contradiction).

Etablissons maintenant la condition de Gauss. Soit a irréductible divisant bc, donc : $bc = ka$. D'après la condition 1° du théorème 2 on a : $(a) \cap (b) = (m)$, où m est un p.p.c.m. de a et b ; en particulier : $m = aa' = bb'$. L'élément ab est multiple commun à a et b,, d'où : $ab = dm = daa' = dbb'$; et par suite :

$$a = db', \quad b = da'.$$

L'élément bc $(= ka)$ est multiple commun à a et b, d'où : $bc = ka = \ell m = \ell \frac{ab}{d}$. Il en résulte :

$$\ell a = cd .$$

Comme a est irréductible, d ou b' sont des unités. Si b' est inversible : $b'b'' = 1$ et $d = ab'' \implies b = ab''a'$ qui est multiple de a . Si d est inversible : $dd' = 1$ et $c = \ell ad'$ est multiple de a . La condition de Gauss est vérifiée.

Condition nécessaire. La propriété 1° du théorème 2 découle de l'existence du p.p.c.m. dans un anneau factoriel. La propriété 2° est une conséquence des propriétés de divisibilité dans un anneau factoriel (propriétés à expliciter au moyen de la décomposition en facteurs premiers).

Les conditions intervenant dans le théorème 2 sont vérifiées pour un anneau principal (propriété 6 du chap. I). On en déduit aussitôt :

Théorème 3. Tout anneau principal est factoriel.

Mais il existe des anneaux factoriels non principaux ($K[X,Y]$, voir plus loin, § 2, 3°).

§ 2. Exemples.

1°) $\mathbb{Z}$ est un anneau factoriel.

En effet $\mathbb{Z}$ est un anneau principal (cf. Chap. I). On retrouve ainsi les propriétés de factorisation d'un nombre non nul en puissances de nombres premiers.

Rappelons cependant les démonstrations élémentaires. Un nombre inversible de $\mathbb{Z}$ est égal à $+1$ ou à -1. Donc : $U = \{+1, -1\}$. Tout élément de $\mathbb{Z}$ est donc associé à un élément de $\mathbb{N}$. On appelle nombre premier un élément de $\mathbb{N}$, différent de 1, et n'admettant comme facteurs que ± 1 et $\pm p$. Cette définition correspond bien à celle d'élément irréductible dans le cas d'un anneau intègre quelconque.

Tout nombre naturel $\neq 1$ est un produit de nombres premiers. (Démonstration adaptée de la théorie générale : si cette propriété P n'est pas vraie, soit a un nombre minimum ne la vérifiant pas ; a n'est pas premier, d'où $a = bc$ avec $1 < b < a$, $1 < c < a$. b et c vérifient donc la propriété P , ainsi que leur produit $bc = a$; contradiction. C.Q.F.D.. Autre variante de la démonstration, en deux étapes : tout nombre naturel $a \neq 1$ possède un diviseur premier (par exemple un diviseur minimum de a autre que 1) puis : tout nombre naturel $a \neq 1$ est un produit de nombres premiers (récurrence sur a). Remarque : il est possible de présenter aussi la démonstration pour un anneau quelconque par une variante analogue ; cf. Cours Cartan, p. 16 et 17.

La décomposition d'un nombre naturel $\neq 1$ en un produit de nombres premiers est unique à l'ordre près

$$a = p_1 p_2 \cdots p_n = q_1 q_2 \cdots q_m \implies n = m$$

et, à l'ordre près des q_j : $p_i = q_i$ $(i = 1, 2, \ldots, n)$. C'est une conséquence (comme dans la théorie générale) de la condition de Gauss : p premier et $p \mid bc \implies p \mid b$ ou $p \mid c$. Pour établir cette dernière condition, on peut utili-

ser l'égalité de Bezout : si p et b sont premiers entre eux (c'est-à-dire s'ils n'ont pas d'autres diviseurs communs que ± 1) ils sont liés par une relation de la forme : $up + vb = 1$. Alors, supposons p premier, $pa = bc$, b non divisible par p. De la relation $up + vb = 1$, on déduit :

$c = upc + vbc = upc + vpa = kp$.

Exercices : énoncer et étendre l'égalité de Bezout dans le cas d'un anneau principal quelconque. Donner un exemple d'anneau factoriel ne la vérifiant pas (Cours Cartan, p. 21).

Démontrer que la suite des nombres premiers est illimitée.

Former la suite des nombres premiers au moyen du crible d'Erasthostène.

2°) $k[X]$ est un anneau factoriel (k = corps commutatif) en tant qu'anneau principal (cf. Chap. I).

Les éléments inversibles sont les polynômes réduits à des constantes non nulles (le vérifier). Le groupe des unités est donc le groupe multiplicatif $k^* = k - \{0\}$. Les éléments irréductibles sont les polynômes irréductibles sur k qui ont été définis et qui interviennent dans la théorie des extensions de corps (cf. Cours Lesieur, C_1). Ils ne sont pas toujours aisés à reconnaître, mais on a vu cependant des cas simples de polynômes irréductibles sur k (en citer). La factorisation d'un polynôme de degré non nul peut donc se faire d'après la théorie générale, mais on peut aussi la retrouver directement comme dans le cas de $\mathbb{Z}$ (à traiter en exercice : au lieu de considérer $|a|$, on envisage le degré du polynôme dans le cas de $k[X]$, et on utilise l'égalité de Bezout pour la condition de Gauss).

3°) L'anneau $k[X_1, X_2, \ldots, X_n]$ est factoriel.

Ce résultat intéressant donne un exemple d'anneau factoriel non principal. Il se démontre au moyen du théorème de transfert suivant :

Théorème 4.(de transfert). Si A est factoriel, $A[X]$ est factoriel.

Avant d'en donner la démonstration, disons qu'il s'applique au cas

précédent par récurrence sur n. $A = k[X_1]$ est factoriel, donc aussi $k[X_1][X_2] = k[X_1, X_2]$, et ainsi de suite.

Preuve du théorème 4. Remarquons d'abord que $A[X]$ est intègre. Ses unités sont celles de A. Quels sont ses éléments irréductibles ? Il y a d'abord ceux de A, mais d'autres également. Nous allons les déterminer en introduisant, d'une part la notion de polynôme primitif, et d'autre part en considérant le corps des fractions K de l'anneau intègre A et l'anneau de polynômes $K[X]$.

Définition. Un polynôme $f = a_o + a_1X + \ldots + a_nX^n$ est dit primitif si le p.g.c.d. des coefficients $a_i \in A$ est égal à 1. Remarquons que le p.g.c.d. des éléments $a_i \in A$ a un sens, car A est factoriel, et qu'il n'est défini qu'à une unité multiplicative de A près.

Voici quelques lemmes utiles sur les polynômes primitifs

Lemme 1. Le produit de 2 polynômes primitifs est primitif.

Soient : $f = a_o + a_1X + \ldots + a_nX^n$, $g = b_o + b_1X + b_2X^2 + \ldots + b_mX^m$, f et g primitifs. Supposons $fg = h$ non primitif. Les coefficients auraient donc un diviseur irréductible p en commun. Comme f est primitif, p ne divise pas tous les a_i ; soit donc a_1 le premier coefficient non divisible par p. On a : $a_o \equiv 0\ (p)$, $a_1 \not\equiv 0\ (p)$. De même, soit $b_o \equiv b_1 \equiv 0\ (p)$ et $b_2 \not\equiv 0\ (p)$. Le coefficient de X^3 dans le produit fg est :

$$c_3 = a_ob_3 + a_1b_2 + a_2b_1 + a_3b_o .$$

On en déduit : $a_1b_2 \equiv 0\ (p)$, ce qui est impossible.

Exercice : démontrer le lemme 1 en considérant l'anneau quotient $A/(p)$ qui est intègre.

Lemme 2. Tout polynôme $f \in A[X]$ s'écrit sous la forme : $f = af^*$, $a \in A$, f^* primitif. De plus il y a "unicité" :

$$af^* = bg^* \implies a = \varepsilon b\ ,\quad g^* = \varepsilon f^*\ ,\quad \varepsilon \in U$$

(U est le groupe des unités de A).

En effet, si $f = a_o + a_1X + \ldots + a_nX^n$, on peut considérer le p.g.c.d. a des coefficients a_i. Il vient : $a_i = aa_i^*$, et $f = af^*$, avec $f^* = a_o^* + a_1^*X + \ldots + a_n^*X^n$ qui est primitif.

De plus, $af^* = bg^* \Longrightarrow aa_i^* = bb_i^*$, $i = 1, \ldots, n$. Soit p un facteur irréductible de a ; il ne peut diviser tous les b_i^* puisque g^* est primitif. Il existe i tel que p divise bb_i^* sans diviser b_i ; par suite, p divise b (condition de Gauss dans un anneau factoriel). Dans la relation $af^* = bg^*$ on peut simplifier par p, puis on recommence. On aboutit à $\varepsilon f^* = kg^*$, et, comme f^* est primitif, k est une unité (C.Q.F.D.).

Introduisons maintenant le corps des fractions K de l'anneau intègre A (un rappel sur cette notion, au moins en T.D., serait peut être utile). On a donc : $A \subset K$ et $A[X] \subset K[X]$. Un polynôme $f \in A[X]$ peut donc être considéré comme un polynôme à coefficients dans K.

Lemme 3. Les éléments irréductibles de $A[X]$ sont alors :

1°) les éléments de A irréductibles dans A.

2°) les éléments f de $A[X]$ de degré > 0 tels que :

f est primitif et f est irréductible dans $K[X]$.

Il suffit de caractériser les polynômes irréductibles de $A[X]$ de degré > 0 par la propriété 2°, ceux qui sont réduits à des constantes étant évidemment caractérisés par la propriété 1°.

f irréductible dans $K[X]$, f primitif $\Longrightarrow$ f irréductible dans $A[X]$. En effet, si $f = gh$, g ou h sont des constantes car f est irréductible dans $k[X]$. Cette constante est une unité de A car f est primitif.

f irréductible dans $A[X] \Longrightarrow$ f primitif et f irréductible dans $K[X]$. En effet, f irréductible dans $A[X]$ est nécessairement primitif car $f = af^*$, $d^\circ f^* > 0$, d'où, f^* n'étant pas une unité, a en est une et f est bien primitif. f est également irréductible dans $K[X]$; supposons en effet :

$f = g(X)h(X)$, $f \in A[X]$, $g(X) \in K[X]$, $h(X) \in K[X]$.

On peut réduire les coefficients de g (resp. h) au même dénominateur $d \in A$ (resp. δ) et écrire :

$$g(X) = \frac{g_1(X)}{d}, \quad h(X) = \frac{h_1(X)}{\delta}, \quad g_1(X) \in A[X], \quad h_1(X) \in A[X].$$

Mettons f, g_1, h_1 sous la forme du lemme 2 :

$$f = af^*, \quad g_1 = bg_1^*, \quad h_1 = ch_1^*, \quad a, b, c \in A ;$$

il vient :

$$ad\delta f^* = bcg_1^*h_1^* .$$

Or $g_1^*h_1^*$ est primitif (lemme 1) et, d'après l'unicité du lemme 2 :

$$f^* = \varepsilon g_1^*h_1^* , \quad \varepsilon \in U .$$

Il en résulterait : $f = a\varepsilon g_1^*h_1^*$, d'où la réductibilité dans $A[X]$, ce qui est contraire à l'hypothèse. Le lemme 3 est démontré.

Revenons à la preuve du théorème de transfert. Pour montrer que $A[X]$ est factoriel nous prouvons le théorème d'existence et d'unicité de la factorisation. Soit $f \in A[X]$. Si $d^\circ f = 0$, $f \in A$, A factoriel, c'est vrai. Si $d^\circ f > 0$, f est décomposable dans $K[X]$ en facteurs que l'on écrit : $f = \prod_{i=1}^{n} \frac{a_i f_i^*}{d_i} = af^*$, d'où :

$$a\Big(\prod_{i=1}^{n} d_i\Big)f^* = \Big(\prod a_i\Big)\Big(\prod f_i^*\Big).$$

Il en résulte (lemmes 1 et 2) : $f^* = \varepsilon\big(\prod f_i^*\big)$; donc

$$f = \varepsilon a \prod_{i=1}^{m} f_i^* = \varepsilon\, p_1\, p_2 \cdots p_m\, f_1^* \cdots f_n^* .$$

D'après le lemme 3, il s'agit d'une décomposition en facteurs irréductibles dans $A[X]$.

L'unicité est encore une application des lemmes 2 et 3, avec l'unicité de la factorisation dans A et $K[X]$ (le lecteur le précisera en 2 lignes).

Le théorème de transfert s'applique, non seulement pour montrer que $K[X_1, \ldots, X_n]$ est factoriel, mais il permet également de démontrer que :

$\mathbb{Z}[X_1, X_2, \ldots, X_n]$ est un anneau factoriel.

4°) $\mathbb{Z}[i]$ est un anneau factoriel puisque $\mathbb{Z}[i]$ est un anneau principal (Chap. I). Nous allons revenir en détail sur cet exemple, et sur l'étude des éléments irréductibles au Chapitre suivant.

CHAPITRE III

L'ANNEAU DES ENTIERS DE GAUSS ET LES SOMMES DE 2 CARRES

§ 1. Nombres premiers dans l'anneau des entiers de Gauss.

§ 2. Sommes de 2 carrés.

§ 3. Restes quadratiques modulo p .

§ 1. Nombres premiers dans l'anneau des entiers de Gauss.

Continuant l'étude des éléments premiers dans les exemples classiques, nous allons chercher ceux de l'anneau $\mathbb{Z}[i]$. Tout élément de $\mathbb{Z}[i]$ irréductible est associé, soit à un entier naturel positif, soit à un nombre complexe $a+bi$ $(a \neq 0$ et $b \neq 0)$. (Le vérifier). Il faut préciser dans chacun de ces cas

Lemme 1. Soit $p \in \mathbb{N}$; si p est premier dans $\mathbb{Z}[i]$, alors p est premier dans $\mathbb{Z}$.

En effet, $p = a\,b$, a et $b \in \mathbb{Z}$, implique : a ou b sont des unités de $\mathbb{Z}[i]$, donc ± 1, et p est premier dans $\mathbb{Z}$.

Cela ne veut pas dire que tout nombre premier dans $\mathbb{Z}$ est premier dans $\mathbb{Z}[i]$; par exemple : $2 = (1+i)(1-i)$, $5 = (2+i)(2-i)$ sont des nombres premiers dans $\mathbb{Z}$ et non dans $\mathbb{Z}[i]$.

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

En effet, soit $p = (a+bi)(c+di)$. Alors, en prenant les normes, on a : $p^2 = (a^2+b^2)(c^2+d^2)$, ce qui implique dans $\mathbb{N}$: $a^2+b^2 = 1$ ou p^2 ou p . L'égalité $a^2+b^2 = 1$ est incompatible avec $a \neq 0$ et $b \neq 0$. L'égalité $a^2+b^2 = p^2$ implique $c^2+d^2 = 1$, et $c+di$ serait une unité de

$\mathbb{Z}[i]$ et par suite p serait associé à $a+bi$ $(a \neq 0,\ b \neq 0)$ (impossible). Il reste : $p = a^2+b^2$.

Démontrons maintenant que $a+bi$ est premier dans $\mathbb{Z}[i]$. Supposons $a+bi = (u+vi)(u'+v'i)$. On en déduit : $p = a^2+b^2 = (u^2+v^2)(u'^2+v'^2)$ et l'un des facteurs, soit $u'^2+v'^2$, est égal à 1. On en déduit que $u'+iv'$ est inversible, et par suite que $a+bi$ est premier.

Le lemme 2 permet déjà de caractériser les nombres premiers de $\mathbb{Z}$ qui sont premiers dans $\mathbb{Z}[i]$.

Corollaire. Les nombres premiers de $\mathbb{Z}$ qui sont premiers dans $\mathbb{Z}[i]$ sont exactement ceux qui ne sont pas une somme de 2 carrés

$$p \text{ premier, } p \text{ premier dans } \mathbb{Z}[i] \iff \begin{cases} p \neq a^2+b^2 \\ p \text{ premier dans } \mathbb{Z} \end{cases} .$$

En effet : supposons p premier et premier dans $\mathbb{Z}[i]$, alors on ne peut avoir $p = a^2+b^2$ $(a \neq 0,\ b \neq 0)$ car $p = a^2+b^2 = (a+bi)(a-bi)$ serait le produit de 2 éléments non inversibles de $\mathbb{Z}[i]$. On ne peut avoir non plus $p = a^2$ c'est-à-dire $p = a^2+b^2$ avec $b = 0$, car p est premier dans $\mathbb{Z}$. Réciproquement, si p premier dans $\mathbb{Z}$ n'est pas une somme de 2 carrés, p est irréductible dans $\mathbb{Z}[i]$; sinon : $p = (a+bi)(a'+b'i)$, a et $b \neq 0$, et le lemme 2 nous apprend que $p = a^2+b^2$ (contradiction).

Il reste alors à étudier les éléments irréductibles de la forme $a+bi$, $a \neq 0$ et $b \neq 0$.

Lemme 3. Les éléments irréductibles $a+bi$, a et $b \neq 0$, sont exactement ceux pour lesquels $p = a^2+b^2$ est premier dans $\mathbb{Z}$.

Supposons $a+bi$ irréductible dans $\mathbb{Z}[i]$, a et $b \neq 0$; la décomposition de a^2+b^2 en facteurs premiers dans $\mathbb{Z}$ donne

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

d'où

$$(a+bi)(a-bi) = p_1\, p_2 \cdots p_n \ .$$

D'après la condition de Gauss dans l'anneau factoriel $\mathbb{Z}[i]$, $a+bi$ divise

l'un des facteurs, soit p_1 , et le lemme 3 nous donne $p_1 = a^2+b^2$.

Inversement, si $p = a^2+b^2$ est premier, avec $a \neq 0$, $b \neq 0$, on a $p = (a+bi)(a-bi)$ et le lemme 3 nous indique que $a+bi$ est premier.

En rassemblant, on obtient :

Théorème 1. Les classes de nombres premiers dans $\mathbb{Z}[i]$ sont :

1°) Les classes des nombres premiers p dans $\mathbb{Z}$ qui ne sont pas de la forme $p = a^2+b^2$ $(a, b \in \mathbb{Z})$.

2°) Les classes des nombres de Gauss $a+bi$ $(a \neq 0, b \neq 0)$ tels que $p = a^2+b^2$ soit premier dans $\mathbb{Z}$.

Exercices : 1. Soit $p = a^2+b^2 = c^2+d^2$ premier. On a :

$$a = \pm c \ , \ b = \pm d \quad \text{ou} \quad a = \pm d \ , \ b = \pm c \ .$$

2. Le nombre 2 est le seul nombre premier de $\mathbb{Z}$ qui soit équivalent à un carré dans $\mathbb{Z}[i]$,

$$2 = i(1-i)^2.$$

§ 2. Sommes de 2 carrés.

L'étude des nombres premiers de $\mathbb{Z}[i]$ nous ramène d'après le th. 1 à celle des nombres premiers de $\mathbb{Z}$ qui sont une somme de 2 carrés. La réponse est donnée par le beau résultat arithmétique suivant :

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

$$p = 2 \quad \text{ou bien} \quad p \equiv 1 \pmod 4.$$

Le cas $p = 2$ est immédiat : $2 = 1+1$ est somme de 2 carrés. Supposons $p > 2$ et premier, donc impair. Démontrons : p premier impair, $p = a^2+b^2 \Longrightarrow p \equiv 1 \pmod 4$. En effet, l'un des nombres a ou b doit être pair, et l'autre impair, pour que la somme a^2+b^2 soit impaire. Si $a = 2h$, $b = 2k+1$, on a : $a^2 = 4h^2 \equiv 0 \pmod 4$, $b^2 = 4k^2+4k+1 \equiv 0 \pmod 4$; d'où $p = a^2+b^2 \equiv 1 \pmod 4$.

La réciproque est plus difficile :

p premier (impair), $p \equiv 1 \pmod 4 \implies p = a^2+b^2$.

Il suffit de prouver que p n'est pas un nombre premier de $\mathbb{Z}[i]$ (Th. 1). On admet provisoirement le lemme suivant qui sera démontré dans le paragraphe consacré aux restes quadratiques mod. p :

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

Donc, si $p \equiv 1 \pmod 4$, p premier, il existe x tel que $p \mid x^2+1 = (x+i)(x-i)$ dans $\mathbb{Z}[i]$. Si p était premier dans $\mathbb{Z}[i]$, p diviserait l'un des facteurs, par exemple : $p \mid x+i \implies x+i = p(a+bi) \implies pb = 1$, ce qui est impossible pour b entier. C.Q.F.D.

En conséquence, on voit d'après le théorème 1, que les nombres premiers p dans $\mathbb{Z}$ qui sont premiers dans $\mathbb{Z}[i]$ sont ceux qui ne sont pas congrus à 1 (mod. 4) ; comme ils ne peuvent pas être congrus à 0 ou 2, ce sont ceux qui sont congrus à 3 (mod. 4) (ou, ce qui revient au même, à -1) soit :

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

Par contre :

2, 5, 13, 17, 29,...

sont premiers dans $\mathbb{Z}$ et non premiers dans $\mathbb{Z}[i]$; ils sont égaux à des sommes de 2 carrés

$2 = 1+1$, $5 = 2^2+1$, $13 = 3^2+2^2$, $17 = 4^2+1$, $29 = 5^2+2^2$,...

Une question naturelle un peu plus générale se pose : quels sont les nombres naturels qui sont égaux à une somme de 2 carrés ? Soit E leur ensemble ; nous connaissons déjà : les nombres premiers impairs congrus à 1 (mod. 4), le nombre 2, les carrés parfaits (somme de 2 carrés dont l'un est nul). Par multiplication on en obtient d'autres, d'après le lemme suivant

Lemme 5. Le produit de 2 sommes de 2 carrés est une somme de 2 carrés.

Démonstration :

$$(a^2+b^2)(c^2+d^2) = (ad+bc)^2 + (ac-bd)^2$$

(identité de Lagrange qu'on vérifie directement, et qui résulte aussi du produit des normes dans l'anneau $\mathbb{Z}[i]$:

$$N[(a+bi)(c+di)] = N(a+bi)\ N(c+di).$$

Théorème 3. Pour que n soit égal à une somme de 2 carrés, il faut et il suffit que, dans la décomposition de n en facteurs premiers, les exposants des nombres premiers $p \equiv 3 \pmod 4$ soient pairs.

Condition suffisante. $n = 2^{\alpha}a^2b$, où b est un produit de facteurs premiers congrus à 1 (mod. 4). On applique alors le théorème 2 et le lemme 5.

Condition nécessaire. Soit $n = a^2+b^2$ $(a \neq 0,\ b \neq 0)$. Considérons le p.g.c.d. $d = (a,b)$ et posons $a = da'$, $b = db'$, d'où : $n = d^2(a'^2+b'^2)$. Soit p un diviseur premier de $a'^2+b'^2$; alors p n'est pas premier dans l'anneau $\mathbb{Z}[i]$ car $p \mid a'^2+b'^2 = (a'+b'i)(a'-b'i) \Longrightarrow p \mid a'+b'i$ par exemple $\Longrightarrow p \mid a'$ et $p \mid b'$ ce qui est en contradiction avec $(a',b') = 1$. D'après les théorèmes 1 et 2, p est donc égal à 2 ou est impair congru à 1 modulo 4. Ainsi, tous les $p \equiv 3 \pmod 4$ figurent dans la décomposition de d^2 et leurs exposants sont pairs (C.Q.F.D.).

Remarque. Contrairement au cas premier, la décomposition de n quelconque en somme de 2 carrés n'est pas nécessairement unique :

$$65 = 64+1 = 49+16 \ ; \quad 65 = 5 \times 13.$$

§ 3. Restes quadratiques modulo p . (p premier dans $\mathbb{Z}$).

La démonstration du lemme 4 : -1 est un carré mod. p lorsque $p \equiv 1 \pmod 4$ fait appel à quelques propriétés simples du corps $F_p = \mathbb{Z}/p\mathbb{Z}$, p premier.

Définition. $a \in \mathbb{Z}$ est un reste quadratique modulo p s'il existe $x \in \mathbb{Z}$ tel que $a \equiv x^2 \pmod p$. Cela revient à dire que la classe $\bar{a}$ de a mod. p est un carré dans F_p : $\bar{a} = \bar{x}^2$.

Comme 0 est un carré, il suffit de considérer les éléments non nuls mod. p , donc les éléments du groupe multiplicatif $F_p^* = F_p - \{0\}$. On peut d'ailleurs exclure le cas $p = 2$ pour lequel les 2 éléments $\bar{0}$ et $\bar{1}$ sont des carrés.

Les éléments de F_p^* sont les classes de :

$$1, 2, \ldots, p-1$$

en nombre $p-1$. Ils vérifient le :

Petit Théorème de Fermat : $x^{p-1} = 1$.

Rappelons une démonstration : le groupe multiplicatif F_p^* étant fini et d'ordre $p-1$, un élément quelconque $x \in F_p^*$ a pour ordre un diviseur d de $p-1$, soit $p-1 = dk$ (Théorème de Lagrange, Théorie des groupes). On a donc : $x^d = 1$, d'où $x^{p-1} = (x^d)^k = 1$.

Quels sont les carrés de F_p^* ? Ils forment un sous-groupe G_p qui est l'image de F_p^* par l'endomorphisme $u : x \mapsto x^2$. Il s'agit d'un endomorphisme pour la structure de groupe multiplicatif abélien : $u(xy) = (xy)^2 = x^2y^2 = u(x)u(y)$. Le noyau N de u est l'ensemble des éléments $x \in F_p^*$ tels que $x^2 = 1$, soit $(x-1)(x+1) = 0$, et par suite (propriétés de corps, donc d'anneau intègre) : $x = +1$ ou $x = -1$. On a ainsi : $N = \{+1,-1\}$ et Card $N = 2$. (Noter que $-1 \neq 1$ car $p \neq 2$). On en déduit d'après le théorème d'isomorphisme de la théorie des groupes :

$$G_p \simeq F_p^*/N$$

et par suite : Card G_p = Card F_p^*/Card N, d'où :

Lemme 6. G_p étant le groupe des carrés de F_p^* , on a

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

L'indice de G_p est donc égal à 2, c'est-à-dire qu'il n'y a dans F_p^* que deux classes modulo G_p, la classe 1 formée de tous les carrés et l'ensemble complémentaire (qui ne contient pas forcément -1).

Les éléments de G_p vont être caractérisés par le théorème suivant :

Théorème 4. Soit p premier impair. Les éléments x qui sont des carrés dans F_p^* sont caractérisés par :

$$x^{\frac{p-1}{2}} = 1 .$$

Les autres, en nombre égal, sont caractérisés par :

$$x^{\frac{p-1}{2}} = -1 .$$

Preuve : $x \in G_p \iff x^{\frac{p-1}{2}} = 1$. En effet, si $x = y^2$, $y \in F_p^*$, on a : $x^{\frac{p-1}{2}} = y^{p-1} = 1$ (Fermat).

$x \in F_p^*$, $x^{\frac{p-1}{2}} = 1 \iff x \in G_p$. En effet, il y a déjà $\frac{p-1}{2}$ racines connues distinctes dans F_p pour l'équation $X^{\frac{p-1}{2}} - 1 = 0$, qui sont les éléments de G_p. Or cette équation, qui est de degré $\frac{p-1}{2}$, ne peut admettre plus de $\frac{p-1}{2}$ racines distinctes dans le corps F_p. Il en résulte bien $x \in G_p$.

Enfin : $x \in F_p^* - G_p \iff x^{\frac{p-1}{2}} = -1$, car $x \in F_p^*$, $y = x^{\frac{p-1}{2}}$ vérifie l'équation $y^2 = 1$, donc $y = +1$ ou $y = -1$, le cas $y = +1$ étant exclu si $x \notin G_p$. De plus, si $x^{\frac{p-1}{2}} = -1$ on a $x \notin G_p$.

Application. Cherchons à quelle condition -1 est un reste quadratique modulo p. Il faut et il suffit d'après le théorème 4 que $(-1)^{\frac{p-1}{2}} = 1$, donc que $\frac{p-1}{2}$ soit pair, c'est-à-dire $p = 1+4h$. Le lemme 4 est démontré.

Exercices : 1) $(p-1)! \equiv -1 \pmod{p}$, p premier, (th. de Wilson)

2) 2 est un reste quadratique modulo p si et seulement si $p \equiv \pm 1 \pmod{8}$, ou encore :

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

Cours CARTAN, p. 41 ou SERRE, Cours d'arithmétique, Presses Universitaires, p. 16. Nous reviendrons sur la démonstration de ce résultat par le calcul du symbole de Legendre $(\frac{2}{p})$ au chapitre IX, § 2.

CHAPITRE IV

QUATERNIONS ET SOMMES DE 4 CARRES

§ 1. Les quaternions.

§ 2. Sommes de 4 carrés.

§ 3. Sommes de 3 carrés.

Nous avons vu au chapitre III à quelle condition un nombre entier positif pouvait s'écrire sous la forme d'une somme de 2 carrés. Pour p premier impair, cette condition est $p \equiv 1 \pmod 4$, ce qui prouve en même temps que n'importe quel nombre n'est pas susceptible de s'écrire comme somme de 2 carrés. Nous allons complèter cette étude de la représentation d'un nombre entier positif comme somme de carrés en démontrant le théorème suivant :

Théorème 1. (Lagrange). Tout nombre entier positif est égal à une somme de 4 carrés[1].

Ce résultat est le meilleur possible pour la représentation d'un nombre entier positif quelconque comme somme de carrés, car il existe des entiers positifs qui ne sont pas des sommes de 3 carrés, exemple : le nombre 7. Nous reviendrons plus loin sur les sommes de 3 carrés. Mais, de même que l'étude de l'anneau des entiers de Gauss éclaire certaines questions liées aux sommes de 2 carrés, l'étude de l'anneau des quaternions entiers va nous servir quelque peu dans les sommes de 4 carrés.

§ 1. Les quaternions.

Une définition possible des nombres complexes est le sous-corps de l'anneau $M_2(\mathbb{R})$ formé des matrices $\begin{pmatrix} a & b \\ -b & a \end{pmatrix}$, a et $b \in \mathbb{R}$. Nous allons

---

[1] dont un, deux ou trois peuvent être nuls. Certains entiers positifs peuvent être égaux à 1 carré, à une somme de 2 carrés, ou à une somme de 3 carrés.

donner une définition des quaternions inspirée de cette méthode.

Définition 1. On appelle quaternion toute matrice de la forme

$$q = \begin{pmatrix} \alpha & \beta \\ -\bar{\beta} & \bar{\alpha} \end{pmatrix}, \quad \alpha \in \mathbb{C}, \quad \beta \in \mathbb{C}.$$

Propriété 1. Les quaternions constituent un sous-corps non commutatif Q de l'anneau $M_2(\mathbb{C})$.

On vérifie que Q est stable pour les opérations d'addition et de multiplication dans $M_2(\mathbb{C})$. Si $q = (\alpha,\beta)$, $r = (\gamma,\delta)$ sont deux quaternions, on a : (le vérifier)

$$q+r = (\alpha+\gamma,\ \beta+\delta), \quad qr = (\alpha\gamma-\beta\bar{\delta},\ \alpha\delta+\beta\bar{\gamma}).$$

Les propriétés d'associativité et de distributivité sont automatiques dans Q au même titre que dans $M_2(\mathbb{C})$. On a : $q = 0 \iff \alpha = \beta = 0$; le quaternion $e = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ est élément unité, et tout quaternion $q \neq 0$ est inversible, avec pour inverse $\dfrac{1}{|\alpha|^2+|\beta|^2} \begin{pmatrix} \bar{\alpha} & -\beta \\ \bar{\beta} & \alpha \end{pmatrix}$. Q n'est pas commutatif (cf. propriété 2).

Propriété 2. Q est un espace vectoriel sur $\mathbb{R}$ de dimension 4, ayant pour base : e, i, j, k tels que : $i^2 = j^2 = k^2 = -1$; $ij = -ji = k$; $jk = -kj = i$; $ki = -ik = j$; e élément neutre unité.

En effet, il suffit d'expliciter, dans la définition 1, les nombres complexes $\alpha = a_0 + a_1 i$, $\beta = a_2 + a_3 i$ pour trouver :

$$(1) \quad q = a_0 e + a_1 i + a_2 j + a_3 k$$

avec : $e = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$, $i = \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix}$, $j = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$, $k = \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix}$.

Propriété 3. $\mathbb{R} \subset \mathbb{C} \subset Q$.

En effet, Q contient les quaternions réels $a_0 e$, identifiés à a_0, et les quaternions complexes $a_0 e + a_1 i$, identifiés à $a_0 + a_1 i = \alpha$. (Faire $a_2 = a_3 = 0$). En exercice, le lecteur vérifiera que Q est un espace vectoriel à gauche et à droite sur $\mathbb{C}$, de dimension 2, et il précisera la règle de multiplication à gauche et à droite, ainsi qu'une base.

Propriété 4. Le centre de Q est $\mathbb{R}$.

Rappelons que le centre d'un corps (ou d'un anneau) est le sous-

corps (ou sous-anneau) constitué par les éléments qui commutent avec tous les éléments du corps (ou de l'anneau),

$$Z = \text{Centre de } Q = \{a \in Q \mid \forall x \in Q,\ xa = ax\}.$$

La recherche en est facile ici (prière de l'effectuer en écrivant que a commute avec i, j, k).

Désormais nous prenons q sous la forme (1). En effectuant la multiplication de deux quaternions q et r sous la forme :

$$q = a_o + a_1 i + a_2 j + a_3 k\ ,\quad r = b_o + b_1 i + b_2 j + b_3 k$$

on obtient :

$$qr = c_o + c_1 i + c_2 j + c_3 k\ ,$$

avec :

$$(2)\qquad \begin{cases} c_o = a_o b_o - a_1 b_1 - a_2 b_2 - a_3 b_3 \\ c_1 = a_o b_1 + a_1 b_o + a_2 b_3 - a_3 b_2 \\ c_2 = a_o b_2 - a_1 b_3 + a_2 b_o + a_3 b_1 \\ c_3 = a_o b_3 + a_1 b_2 - a_2 b_1 + a_3 b_o\ . \end{cases}$$

Quaternions conjugués : le conjugué de $q = a_o + a_1 i + a_2 j + a_3 k$ est $\bar{q} = a_o - a_1 i - a_2 j - a_3 k$.

Propriétés : $\overline{q+r} = \bar{q} + \bar{r}$; $\overline{qr} = \bar{r}\bar{q}$ (le vérifier avec (2)).

Norme d'un quaternion. C'est le nombre réel $\geqslant 0$:

$$(3)\qquad \boxed{N(q) = q.\bar{q} = a_o^2 + a_1^2 + a_2^2 + a_3^2}\ .$$

Propriété 5. $N(qr) = N(q)N(r)$.

En effet : $qr\ \overline{qr} = qr\ \bar{r}\ \bar{q} = r\bar{r}\ q\bar{q}$ (puisque $r\bar{r}$ est un réel commutable avec q (propriété 4)).

Enfin, notons que : $q = 0 \iff N(q) = 0$, et que l'inverse de $q \neq 0$ et $\bar{q} \cdot \frac{1}{N(q)}$.

Quaternions entiers. L'ensemble des quaternions de la forme :

$$q = a_o + a_1 i + a_2 j + a_3 k\ ,\qquad a_o, a_1, a_2, a_3 \in \mathbb{Z}$$

constitue un sous-anneau unitaire non commutatif de Q qu'on appelle l'anneau des quaternions entiers (le vérifier).

§ 2. Sommes de 4 carrés.

Pour démontrer que tout entier positif est une somme de 4 carrés nous démontrerons les deux lemmes suivants :

Lemme 1. Le produit de 2 sommes de 4 carrés est une somme de 4 carrés.

Lemme 2. Tout nombre premier p est une somme de 4 carrés.

De ces deux lemmes résulte aussitôt par la décomposition de n facteurs premiers le :

Théorème 1. (de Lagrange). Soit $n \in \mathbb{N}$. Il existe des entiers a, b, c, $d \geqslant 0$ tels que :

$$n = a^2 + b^2 + c^2 + d^2 .$$

Preuve du lemme 1. On interprète $a_o^2 + a_1^2 + a_2^2 + a_3^2$ comme la norme du quaternion entier $q = a_o + a_1 i + a_2 j + a_k k$, et de même $b_o^2 + b_1^2 + b_2^2 + b_3^2 = N(r)$; $r = b_o + b_1 i + b_2 j + b_3 k$. On a donc d'après la propriété 5 :

$$(a_o^2 + a_1^2 + a_2^2 + a_3^2)(b_o^2 + b_1^2 + b_2^2 + b_3^2) = c_o^2 + c_1^2 + c_2^2 + c_3^2 ,$$

c_o, c_1, c_2, c_3 étant donnés par les formules (2).

Preuve du lemme 2. Elle est plus difficile. Une 1ère étape consiste à démontrer qu'un multiple mp de p est une somme de 4 carrés, puis dans une 2ème étape, on démontre par une méthode de "descente" sur m que le coefficient de p peut être ramené à la valeur 1. (Cf. Hardy et Wright, Chap. XX, p. 302). Nous allons l'expliquer en détail.

Propriété 6. Soit p premier impair[1]. Il existe des entiers $x \geqslant 0$ et $y \geqslant 0$ tels que $1 + x^2 + y^2 = mp$, $0 < m < p$.

Démonstration. Les $\frac{p+1}{2}$ nombres x^2 $(0 \leqslant x \leqslant \frac{p-1}{2})$ sont différents (mod p) car si $x^2 = x'^2 \pmod p$ on a, soit $x = x'$ (exclu) soit $x \equiv -x' \pmod p$ donc $x = p-x'$ (exclu). Il en est de même des nombres $-1-y^2$ $(0 \leqslant y \leqslant \frac{p-1}{2})$. Si ces 2 ensembles $\{x^2\}$ et $\{-(1+y^2)\}$ étaient disjoints, on aurait au total $2 \times \frac{p+1}{2} = p+1$ nombres distincts mod p, alors qu'il y en a au plus p. Il existe donc un élément commun soit $x^2 = -(1+y^2) \pmod p$ ou $1+x^2+y^2 = mp$. De plus $1+x^2+y^2 < 1+2\frac{p^2}{4} < p^2$, et par suite $m < p$. Evidemment, m n'est

[1] Le cas $p = 2$ est vite résolu ! 2 est somme de 2 carrés.

pas nul.

La propriété 6 exprime qu'un multiple de p est somme de 4 carrés (et même de 3) non tous nuls. Soit

$$(4) \qquad m_o p = x_1^2 + x_2^2 + x_3^2 + x_4^2 , \quad 1 \leqslant m_o < p .$$

Choisissons m_o minimum pour la relation (4), et démontrons que m_o est égal à 1.

Si m_o est pair, on a $m_o = 2m'$, et en faisant le calcul de $x_1^2 + x_2^2 + x_3^2 + x_4^2$ modulo 2, on voit que 1) ou bien les quatre x_i sont pairs 2) ou bien les quatre sont impairs 3) ou bien deux sont pairs et les deux autres impairs. Dans tous les cas, on peut grouper deux d'entre eux, soit x_1 et x_2, et les deux autres, soit x_3 et x_4, de façon que :

$$x_1 + x_2,\ x_1 - x_2,\ x_3 + x_4,\ x_3 - x_4$$

soient pairs, et ainsi :

$$\frac{1}{2} m_o p = m'p = \left(\frac{x_1+x_2}{2}\right)^2 + \left(\frac{x_1-x_2}{2}\right)^2 + \left(\frac{x_3+x_4}{2}\right)^2 + \left(\frac{x_3-x_4}{2}\right)^2$$

est somme de 4 carrés avec $1 \leqslant m' < m_o$, ce qui est impossible.

On peut donc supposer m_o impair. Effectuons la "division" de x_i par m_o sous la forme :

$$(5) \qquad y_i = x_i - b_i m_o \quad (i = 1, 2, 3, 4), \quad |y_i| < \frac{1}{2} m_o .$$

(Remarquer que l'on ne peut avoir $|y_i| = \frac{1}{2} m_o$ du fait que m_o est impair et que le point $b_i m_o$ est celui qui est le plus proche de x_i par excès ou par défaut, ce qui explique le reste sous la forme indiquée). On a d'après (5) : $y_i \equiv x_i \pmod{m_o}$, et d'après (4) :

$$\sum_{i=1}^{4} y_i^2 \equiv 0 \pmod{m_o}.$$

Posons :

$$\sum_{i=1}^{4} y_i^2 = m'm_o$$

$m' \neq 0$ car $m' = 0 \Rightarrow y_i = 0 \Rightarrow x_i \equiv 0 \pmod{m_o} \Rightarrow p = m_o k$, ce qui est impossible pour p premier et $1 < m_o < p$.

On a d'après (5) : $m'm_o < 4 \frac{m_o}{4}$, d'où $\underline{0 < m' < m_o}$.

Considérons les quaternions : $x = x_1 + x_2 i + x_3 j + x_4 k$ et $y = y_1 + y_2 i + y_3 j + y_4 k$. Ils sont entiers et on a :

$$y \equiv x \pmod{m_o} \quad [\text{i.e. } y_i \equiv x_i \pmod{m_o}]$$

qui entraîne évidemment par passage aux conjugués, et multiplication par le quaternion x :

$$x\bar{y} \equiv x\bar{x} \pmod{m_o}$$

et, comme $x\bar{x} = m_o p$, il en résulte :

$$z = x\bar{y} = m_o z'$$

où z' est un quaternion entier. Calculons :

$$N(z) = N(x)N(\bar{y}) = N(x)N(y) = (m_o p)(m' m_o) = m_o^2 m' p,$$

d'où :

$$N(z') = \frac{1}{m_o^2} N(z) = m' p \ .$$

Ainsi $m'p$ est somme de 4 carrés, avec $0 < m' < m_o$, ce qui est contraire au choix de m_o . On a bien $m_o = 1$. C.Q.F.D.

§ 3. Sommes de 3 carrés.

Le théorème 1 prend toute sa portée si l'on remarque qu'on ne peut l'améliorer par un théorème du genre : tout entier > 0 est somme de s carrés, avec les valeurs de s moindre que 4 . Pour $s = 1$ ou $s = 2$, c'est clair. Pour $s = 3$ signalons la proposition suivante :

Proposition. Les nombres de la forme $8m+7$ ne peuvent être égaux à des sommes de 3 carrés.

En effet : $x^2 \equiv 0, 1,$ ou $4 \pmod 8$. (Prendre les carrés modulo 8 de $0, \pm 1, \pm 2, \pm 3, 4$) d'où

$$x^2 + y^2 + z^2 \not\equiv 7 \pmod 8.$$

(Calculer toutes les sommes possibles mod. 8 de 3 carrés $0, 1$ ou 4 avec répétition admise).

CHAPITRE V

L'ANNEAU DES ENTIERS D'UN CORPS QUADRATIQUE

§ 1. Corps quadratique $K = \mathbb{Q}(\sqrt{d})$.

Définition 1. Un corps quadratique est un corps K tel que $\mathbb{Q} \subset K \subset \mathbb{C}$, avec $[K : \mathbb{Q}] = 2$.

Rappeler la définition de $[K : \mathbb{Q}]$: dimension de K comme e.v. sur $\mathbb{Q}$.

Propriété 1. $\forall \alpha \in K, \alpha \notin \mathbb{Q}$, on a : $K = \mathbb{Q}(\alpha) = \mathbb{Q}[\alpha]$,

c'est-à-dire K est une extension algébrique monogène de $\mathbb{Q}$.

En effet, soit un tel α ; on a : $\mathbb{Q}(\alpha) \subset K$, avec

$1 < [\mathbb{Q}(\alpha) : \mathbb{Q}] \leqslant 2$, d'où $[\mathbb{Q}(\alpha) : \mathbb{Q}] = 2$ et $\mathbb{Q}(\alpha) = K$.

Propriété 2. $K = \mathbb{Q}(\alpha)$ avec $\alpha^2 - d = 0$ (i.e. $\alpha = \sqrt{d}$), où $d \in \mathbb{Z}$ est sans facteurs carrés ($d = \varepsilon\, p_1 p_2 \cdots p_n$, $p_i \neq p_j$, $\varepsilon = \pm 1$). Réciproquement, si d est ainsi choisi, $K = \mathbb{Q}(\alpha)$ est quadratique.

Démonstration. D'après la propriété 1, $K = \mathbb{Q}(\alpha)$, le polynôme minimal de α sur $\mathbb{Q}$ étant du second degré, soit : $\alpha^2 + p\alpha + q = 0$. On peut l'écrire : $(\alpha + \frac{p}{2})^2 + q - \frac{p^2}{4} = 0$, et, en posant $\beta = \alpha + \frac{p}{2}$, on a évidemment : $K = \mathbb{Q}(\alpha) = \mathbb{Q}(\beta)$, où β vérifie : $\beta^2 - \frac{h}{r} = 0$ (h et $r \in \mathbb{Z}$), d'où $r\beta^2 - h = 0$. Posons $r\beta = \gamma$, d'où $\mathbb{Q}(\beta) = \mathbb{Q}(\gamma)$ et $\gamma^2 - rh = 0$, c.à.d. $\gamma^2 - d = 0$. Si d possède un facteur carré : $d = n^2\delta$, $\gamma^2 - n^2\delta = 0$ et avec $\frac{\gamma}{n} = \theta$, $K = \mathbb{Q}(\theta)$, $\theta^2 - \delta = 0$. C'est aux notations près la propriété 2.

Réciproque : si $\alpha^2 - d = 0$, $d \in \mathbb{Z}$, d sans facteurs carrés, on a : $[\mathbb{Q}(\alpha) : \mathbb{Q}] = 2$, car le polynôme minimal irréductible de α sur $\mathbb{Q}$ est $X^2 - d$. (Si $X^2 - d$ était réductible, il aurait un zéro dans $\mathbb{Q}$, soit $\frac{p^2}{q^2} = d$ et $d = p^2$ lorsque $(p,q) = 1$).

Exemples : $d = -1$, $K = \mathbb{Q}(i) = \mathbb{Q}(\sqrt{-1})$ corps quadratique imaginaire

$d = 2$, $K = \mathbb{Q}(\sqrt{2})$ corps quadratique réel

$d = 6$, $K = \mathbb{Q}(\sqrt{6})$ " " "

Remarques. 1. $d = 1$ est exclu puisque $X^2 - 1$ n'est pas irréductible sur $\mathbb{Q}$

2. Les éléments de $K = \mathbb{Q}(\sqrt{d})$ sont de la forme

$$a + b\sqrt{d}, \quad a \in \mathbb{Q}, \ b \in \mathbb{Q}.$$

Cette dernière propriété résulte de la théorie des extensions algébriques monogènes (Cours Lesieur de C 1) ; on la retrouve immédiatement en notant que $\alpha = \sqrt{d}$ vérifie $\alpha^2 - d = 0$, ce qui permet de remplacer tout polynôme en α à coefficients dans $\mathbb{Q}$ par un polynôme en α du 1^{er} degré. L'expression $a + b\alpha$ ainsi obtenue a une écriture unique car

$$a + b\alpha = 0 \implies a = 0 \text{ et } b = 0.$$

En effet : $\alpha^2 = d = \frac{a^2}{b^2}$ est impossible pour $b \neq 0$ (d est sans facteurs carrés). Autrement dit $\{1,\alpha\}$ forme une base de l'espace vectoriel $\mathbb{Q}(\alpha)$ sur $\mathbb{Q}$. De plus, l'application $\sigma : a + b\alpha \longmapsto a - b\alpha$ obtenue en changeant $\sqrt{d}$ en $-\sqrt{d}$ est un $\mathbb{Q}$-automorphisme de $\mathbb{Q}(\alpha)$,

$$\sigma(x+y) = \sigma(x) + \sigma(y) \ ; \ \sigma(xy) = \sigma(x)\sigma(y) \ ; \ \sigma(1) = 1 \ ;$$

$$\sigma(c) = c \text{ pour tout } c \in \mathbb{Q} \ ; \ \sigma(\sqrt{d}) = -\sqrt{d}.$$

§ 2. Entiers d'un corps quadratique $K = \mathbb{Q}(\sqrt{d})$.

Définition 2. On appelle entier algébrique sur $\mathbb{Z}$ du corps quadratique K, tout élément $x \in K$ qui vérifie une équation algébrique normée à coefficients entiers :

$$P(x) = x^n + a_1 x^{n-1} + \ldots + a_n = 0, \quad a_i \in \mathbb{Z}, \ i = 1, \ldots, n.$$

Propriété 3. Si x est un entier algébrique sur $\mathbb{Z}$ de $\mathbb{Q}(\sqrt{d})$, x vérifie une équation algébrique normée de degré $\leqslant 2$ à coefficients entiers.

En effet, l'anneau $\mathbb{Z}[X]$ étant factoriel, le polynôme $P(X)$ se décompose en un produit fini de polynômes irréductibles $P_i^*(X)$ dans $\mathbb{Z}[X]$, soit : $P(X) = \prod_{i=1}^{k} P_i^*(X)$. Les polynômes $P_i^*(X)$ sont primitifs dans $\mathbb{Z}[X]$ et irréductibles dans $\mathbb{Q}[X]$ (chap. II, th. de transfert, lemme 3), et on peut les prendre normés car le coefficient de X^n est $1 = a_1 a_2 \dots a_k$. L'entier algébrique α est alors racine d'un polynôme $P_i^*(X)$; ce polynôme est de degré $\leqslant 2$, sans quoi $\mathbb{Q}(\alpha)$ serait de dimension plus grande que 2.

Propriété 4. $E(K)$ désignant l'ensemble des entiers algébriques de K, on a :

$$\boxed{E(K) \cap \mathbb{Q} = \mathbb{Z}} \quad .$$

C'est connu (refaire la démonstration) ; mais cela résulte aussi de la propriété 3. Si x est un entier algébrique sur $\mathbb{Z}$ et rationnel, le polynôme minimal de x sur $\mathbb{Q}$ est du 1^{er} degré, normé à coefficients entiers ; or ce polynôme est $X-x$, ce qui prouve : $x \in \mathbb{Z}$.

Théorème 1. Pour que $x = a + b\sqrt{d}$, $(a, b \in \mathbb{Q})$, soit un entier algébrique sur $\mathbb{Z}$, il faut et il suffit que :

$$\text{Tr } x = 2a \in \mathbb{Z} \quad \text{et} \quad N(x) = a^2 - db^2 \in \mathbb{Z}.$$

$\text{Tr } x = 2a$ s'appelle la trace de x ; $N(x) = a^2 - db^2$ la norme de x.

Condition nécessaire. Si $x \in E(K)$ et si $x \in \mathbb{Q}$, on a $x = a \in \mathbb{Z}$ et $b = 0$. Si $x \notin \mathbb{Q}$, le polynôme minimal de x sur $\mathbb{Q}$ est de degré 2 et normé à coefficients entiers (propriété 3). Or ce polynôme est :

$$(X - a)^2 - db^2 = X^2 - 2aX + a^2 - db^2 .$$

Condition suffisante. $X^2 - 2aX + a^2 - db^2$ est annulé par $x = a + b\sqrt{d}$.

Propriété 5. Propriétés de la trace et de la norme :

$$\text{Tr}(x+y) = \text{Tr } x + \text{Tr } y \; ; \; N(xy) = N(x)N(y) \; ; \; N(x) = 0 \Longleftrightarrow x = 0 .$$

(A vérifier directement) ; on peut également utiliser l'automorphisme σ défini au § 1 et noter que :

$$\text{Tr } x = x + \sigma(x) \quad ; \quad N(x) = x.\sigma(x) .$$

Recherche des entiers de $\mathbb{Q}(\sqrt{d})$. Elle s'effectue au moyen du théorème 1.

Soit $x = a + b\sqrt{d} \in E$; $a, b \in \mathbb{Q}$. Je dis que : $2a = u \in \mathbb{Z}$, $2b = v \in \mathbb{Z}$. En effet : $2a = u = \mathrm{Tr}\, x$; $a^2 - db^2 = h = N(x)$; d'où $db^2 = \frac{u^2}{4} - h$, et $4db^2 = u^2 - 4h \in \mathbb{Z}$, c'est-à-dire : $d(2b)^2 = w \in \mathbb{Z}$. Il en résulte $2b = v \in \mathbb{Z}$, car si $2b = \frac{p}{q}$, $(p,q) = 1$, il vient : $d\frac{p^2}{q^2} = w$, $dp^2 = wq^2$ ce qui entraînerait q^2 divise d. Or d est supposé sans facteurs carrés. En conclusion :

$$(1) \quad 2a = u \in \mathbb{Z}, \quad 2b = v \in \mathbb{Z}, \quad u^2 - dv^2 = 4h \equiv 0 \pmod 4.$$

Réciproquement, si l'on a (1) : $\mathrm{Tr}\, x \in \mathbb{Z}$, $N(x) = a^2 - db^2 = h \in \mathbb{Z}$. Si u est pair, v doit être pair car la relation $dv^2 \equiv 0 \pmod 4$ avec $v \equiv 1 \pmod 4$ entraîne $d \equiv 0 \pmod 4$ alors que d n'est pas divisible par $4 = 2^2$. Donc : $x = a + b\sqrt{d}$ est un entier si $a \in \mathbb{Z}$, $b \in \mathbb{Z}$, quel que soit d, (on le savait !).

Si u est impair, il faut v impair pour avoir (1) ; mais alors : $u^2 - dv^2 \equiv 1 - d \equiv 0 \pmod 4$ et $d \equiv 1 \pmod 4$. Réciproquement, si $d \equiv 1 \pmod 4$, $x = a + b\sqrt{d}$ est entier lorsque $a = \frac{1+2a'}{2}$, $b = \frac{1+2b'}{2}$ sont des moitiés de nombres impairs. On a alors $x = (1+2b')(\frac{1+\sqrt{d}}{2}) + \frac{1+2a'}{2} - \frac{1+2b'}{2} = \ell + m\,(\frac{1+\sqrt{d}}{2})$ ($\ell \in \mathbb{Z}$, $m \in \mathbb{Z}$). Inversement $\ell + m(\frac{1+\sqrt{d}}{2}) = \frac{2\ell+m}{2} + \frac{m}{2}\sqrt{d}$ est un entier. On remarque que la forme $\ell + m\,(\frac{1+\sqrt{d}}{2})$ englobe le cas $a+b\sqrt{d}$, $a \in \mathbb{Z}$, $b \in \mathbb{Z}$, en prenant m pair. D'où :

Théorème 2. Si $d \equiv 1 \pmod 4$, les entiers de $\mathbb{Q}(\sqrt{d})$ sont les éléments du groupe abélien additif $\mathbb{Z}.1 + \mathbb{Z}.\frac{1+\sqrt{d}}{2}$.

Si $d \equiv 2$ ou $3 \pmod 4$, ce sont les éléments du groupe abélien additif $\mathbb{Z}.1 + \mathbb{Z}.\sqrt{d}$.

Il en résulte immédiatement que E est stable pour l'addition. On vérifie même que E est stable pour la multiplication, compte tenu de :

$$(\frac{1+\sqrt{d}}{2})^2 = \frac{1+2\sqrt{d}+d}{4} = \frac{d+1}{4} + \frac{\sqrt{d}}{2} \in E \text{ si } d \equiv 1 \pmod 4.$$

Par suite :

Théorème 3. Si $d \equiv 1 \pmod 4$ les entiers de $\mathbb{Q}(\sqrt{d})$ forment l'anneau $\mathbb{Z}[\frac{1+\sqrt{d}}{2}]$. Si $d \equiv 2$ ou $3 \pmod 4$, les entiers de $\mathbb{Q}(\sqrt{d})$ forment l'anneau $\mathbb{Z}[\sqrt{d}]$.

On a retrouvé directement dans ce cas particulier une propriété que l'on connaissait dans le cas général : les entiers d'un corps de nombres algébriques K forment un anneau $E(K)$. (Revoir à cette occasion la démonstration, cours de C 1).

Exemples $d = -1$. Les entiers de $K = \mathbb{Q}(\sqrt{-1})$ forment l'anneau des entiers de Gauss $\mathbb{Z}[i]$. (A retrouver directement en exercice).

$d = 2$. Les entiers de $K = \mathbb{Q}(\sqrt{2})$ forment l'anneau $\mathbb{Z}[\sqrt{2}]$.

$d = 5$. Les entiers de $K = \mathbb{Q}(\sqrt{5})$ forment l'anneau $\mathbb{Z}\left[\frac{1+\sqrt{5}}{2}\right]$. On constate sur cet exemple la présence de l'entier $x = \frac{1+\sqrt{5}}{2}$ qui vérifie l'équation $X^2 - X - 2 = 0$ et, par suite, le sous-anneau de E constitué par $E_1(K) = \mathbb{Z}[\sqrt{5}]$ est un sous-anneau propre.

$d = -3 \equiv 1 \pmod 4$ donne un exemple de corps quadratique imaginaire pour lequel $E = \mathbb{Z}\left[\frac{1+i\sqrt{3}}{2}\right] \supsetneq E_1(K) = \mathbb{Z}[i\sqrt{3}]$.

§ 3. Groupe des unités de l'anneau des entiers d'un corps quadratique.

Soit $K = \mathbb{Q}(\sqrt{d})$ un corps quadratique, $E = E(K)$ l'anneau des entiers algébriques de K sur $\mathbb{Z}$.

Définition 3. Les unités de l'anneau E des entiers algébriques de K sur $\mathbb{Z}$ sont les éléments de E inversibles dans E.

Ils forment un groupe multiplicatif U. Par abus de langage on les appelle aussi unités du corps quadratique.

Propriété 6. Soit $x \in E$; alors : $x \in U \iff N(x) = \pm 1$.

En effet, si $xy = 1$, $x \in E$, $y \in E$, on a : $N(xy) = N(x)N(y) = 1$, et comme $N(x)$ et $N(y)$ sont des entiers de $\mathbb{Z}$ (prop. 5), il vient : $N(x) = \pm 1$. Réciproquement, si $N(x) = \varepsilon = \pm 1$, $x = a + b\sqrt{d} \in E$, l'inverse de x est $y = \varepsilon(a - b\sqrt{d})$ et $y \in E$ d'après le théorème 2.

Selon les cas, tous les entiers algébriques sur $\mathbb{Z}$ unités de E peuvent avoir pour norme 1 (exemple : $E = \mathbb{Z}[i] = E(K)$ avec $K = \mathbb{Q}(i) = \mathbb{Q}(\sqrt{-1})$) ou bien certains ont pour norme $+1$ et d'autres pour norme -1 (exemple :

$K = \mathbb{Q}(\sqrt{2})$, $E = \mathbb{Z}[\sqrt{2}]$; $1 + \sqrt{2}$ est unité de normé -1 tandis que 1 est unité de norme 1). Les unités de norme 1 forment un sous-groupe de U qui est soit U tout entier, soit un sous-groupe propre d'indice 2 (exercice). Attention : les unités de norme -1 ne forment pas un sous-groupe.

Nous allons étudier le groupe des unités d'un corps quadratique, d'abord dans le cas imaginaire, puis dans le cas réel.

Cas d'un corps quadratique imaginaire $\mathbb{Q}(\sqrt{d})$, $d = -d' < 0$.

$$x = a + b\sqrt{d}\ ,\ x \in E\ .\quad N(x) = a^2 - db^2 = a^2 + d'b^2\ .$$

Si $d \equiv 2$ ou $3 \pmod 4$, on a : $d' \equiv 2$ ou $1 \pmod 4$ et $E = \mathbb{Z}[\sqrt{d}]$. La condition $x = a + b\sqrt{d} \in U$ s'écrit : $a \in \mathbb{Z}$, $b \in \mathbb{Z}$, $a^2 + d'b^2 = 1$. Si $d' \geqslant 2$ les solutions sont $b = 0$, $a = \pm 1$ et les seules unités ± 1 . Si $d' = 1$, on a $U = \{+1, -1, +i, -i\}$. Si $d \equiv 1 \pmod 4$, on a : $d' \equiv 3 \pmod 4$ et $E = \mathbb{Z}\left[\frac{1+\sqrt{d}}{2}\right]$. La condition $x = a + b\sqrt{d} \in U$ s'écrit : $a = \frac{u}{2}$, $b = \frac{v}{2}$, $u \in \mathbb{Z}$, $v \in \mathbb{Z}$, $u + v \equiv 0 \pmod 2$, $u^2 + d'v^2 = 4$. Si $d' = 3$, les solutions sont $(u = \pm 1,\ v = \pm 1)$ et $(u = \pm 2,\ v = 0)$, d'où le groupe des unités $U = \{\pm 1, \frac{\pm 1 \pm i\sqrt{3}}{2}\}$.

En résumé le groupe des unités est toujours $U = \{\pm 1\}$ sauf pour les cas singuliers des corps $\mathbb{Q}(i)$ et $\mathbb{Q}(i\sqrt{3})$ où l'on a respectivement le groupe des racines $4^{\text{èmes}}$ de l'unité et le groupe des racines $6^{\text{èmes}}$ de l'unité.

§ 4. Groupe des unités de l'anneau des entiers d'un corps quadratique réel.

Sa recherche va donner lieu à des résultats plus profonds qui s'appliquent à la résolution de certaines équations en nombres entiers.

Remarquons d'abord que, si $x \in U$ est une unité de $K = \mathbb{Q}(\sqrt{d})$, $x \in E$, alors x^{-1}, $-x$, $-x^{-1}$ sont aussi des unités. Il en résulte que toutes les unités s'obtiennent à partir du sous-groupe des unités positives, et même à partir de l'ensemble multiplicativement stable des unités > 1 . De plus, si $x = a + b\sqrt{d} \in E$, on a : $a^2 - db^2 = \varepsilon = \pm 1$, de sorte que l'inverse de x

$x_i \in K'$, $i = 1,\ldots, n$. Le corps $k(x_1, x_2,\ldots, x_n)$ est alors un corps de décomposition de $f(X)$ sur k.

Unicité à un k-isomorphisme près. Théorème 2. Soient $K = k(x_1, x_2,\ldots, x_n)$ et $K' = k(x'_1, x'_2,\ldots, x'_n)$ deux corps de décomposition de $f(X)$ sur k. Il existe un isomorphisme $\sigma : K \to K'$ qui laisse invariant les éléments de k.

Nous démontrons la proposition suivante dont le théorème 2 n'est qu'un cas particulier.

Théorème 2'. Soit $\varphi : k \to k'$ un isomorphisme de k sur k'. Soit $f(X) = a_o X^n +\ldots+ a_n \in k[X]$, $\bar{f}(X) = a'_o X^n +\ldots+ a'_n \in k'[X]$, avec $a'_o = \varphi(a_o)$, $a'_1 = \varphi(a_1),\ldots, a'_n = \varphi(a_n)$.

Supposons $K = k(x_1,\ldots, x_n)$, corps de décomposition de f sur k

$K' = k'(x'_1,\ldots,x'_n)$, corps de décomposition de $\bar{f}$ sur k'.

Alors il existe un isomorphisme $\sigma ; K \to K'$ qui prolonge $\varphi : k \to k'$ (c'est-à-dire tel que la restriction de σ à k coïncide avec φ).

Cette proposition est vraie pour $n = 1$, quels que soient k, k' et φ. En effet : $f(X) = a_o(X-x_1) \in k[X]$, $K = k(x_1) = k$

$\bar{f}(X) = a'_o(X-x'_1) \in k'[X]$, $K' = k'(x_1) = k'$.

Il suffit alors de prendre $\sigma = \varphi$. On remarque de plus que, nécessairement, $x'_1 = \varphi(x_1)$, puisque la relation $f(X) = a_o(X-x_1)$ dans $k[X]$ donne $\bar{f}(X) = a'_o(X-\varphi(x_1)) = a'_o(X - x'_1)$ dans $k'[X]$.

Supposons la proposition vraie pour $n-1$, quels que soient les corps k, k' et l'isomorphisme $\varphi : k \to k'$.

Soient K et K' deux corps de décomposition de $f(X)$ et $\bar{f}(X)$ sur k et k' respectivement. On a donc :

(1) $f(X) = a_o(X-x_1)\ldots(X-x_n) \in k[X]$, $K = k(x_1,\ldots, x_n)$

(2) $\bar{f}(X) = a'_o(X-x'_1)\ldots(X-x'_n) \in k'[X]$, $K' = k'(x'_1,\ldots, x'_n)$.

Je sais que $a'_o = \varphi(a_o)$, mais je ne peux pas dire que $x'_1 = \varphi(x_1)$ car φ est défini sur k et non sur l'extension K. Rappelons que, si

$f(X) = a_o X^n + a_1 X^{n-1} + \ldots + a_n \in k[X]$, on a : $\bar{f}(X) = a'_o X^n + a'_1 X^{n-1} + \ldots + a'_n \in k'[X]$; $a'_i = \varphi(a_i)$.

Décomposons $f(X) = f_1(X) \ldots f_k(X)$ en facteurs irréductibles dans $k[X]$. Considérons la racine x_1 ; elle vérifie $f(x_1) = 0$, d'où $f_1(x_1) \ldots f_h(x_1) = 0$, et elle annule l'un des polynômes $f_i(X)$. Supposons que ce soit $f_1(X)$. Donc x_1 est racine de $f_1(X) = 0$. Par l'isomorphisme φ on obtient la décomposition :

$$\bar{f}(X) = \bar{f}_1(X) \ldots \bar{f}_h(X) \quad \text{en facteurs irréductibles dans } k'[X].$$

Comme $k' \subset K'$, on a dans $K'[X]$:

$$\bar{f}(X) = \bar{f}_1(X) \ldots \bar{f}_h(X) = a'_o(X-x'_1)\ldots(X-x'_n).$$

La décomposition de $\bar{f}(X)$ dans $K'[X]$ se faisant en facteurs linéaires (donc irréductibles sur K'), celle du premier membre doit se faire aussi en facteurs linéaires d'après l'unicité de la factorisation dans $K'[X]$. En particulier $\bar{f}_1(X)$ se décompose en facteurs linéaires dans $K'[X]$ et ses zéros sont à prendre parmi $x'_1, \ldots, x'_n$, toujours d'après l'unicité de la factorisation. Supposons par exemple que x'_1 soit un zéro de $\bar{f}_1(X)$. Alors d'après le théorème de l'adjonction symbolique pour l'unicité, les deux extensions $k_1 = k(x_1)$ et $k'_1 = k'(x'_1)$ sont isomorphes dans un isomorphisme φ_1 qui prolonge $\varphi : k \to k'$, et qui envoie x_1 sur x'_1 . En appliquant φ_1 on a :

$$f(X) = (X-x_1)g(X), \quad g(X) = (X-x_2)\ldots(X-x_n) \in k_1[X]$$

$$\bar{f}(X) = (X-x'_1)\bar{g}(X), \quad \bar{g}(X) = (X-x'_2)\ldots(X-x'_n) \in k'_1[X]$$

$$\bar{g}(X) = \varphi_1(g(X)).$$

Mais alors on voit que $k_1(x_2, \ldots, x_n) = k(x_1, \ldots, x_n) = K$ est un corps de décomposition de $g(X)$ sur k_1 , et de même, $k'_1(x'_2, \ldots, x'_n) = K'$ est un corps de décomposition de $\bar{g}(X)$ sur k'_1 . D'après la proposition valable pour le degré $n-1$ de $g(X)$, il existe un isomorphisme $\sigma : K \to K'$ qui étend φ_1 , donc φ . La proposition 2' est démontrée, donc le théorème 2 en prenant pour φ l'identité sur k .

CHAPITRE VIII

CORPS FINIS

§ 1. Nombre d'éléments d'un corps fini.

L'exemple le plus simple de corps fini est le corps $F_p = \mathbb{Z}/\mathbb{Z}p$, qui possède $q = p$ éléments et qui est de caractéristique p. Mais on a vu aussi un autre exemple, celui du corps de décomposition de X^2+X+1 sur F_2, qui possède $q = 4$ éléments : 0, 1, j, j^2 (Chap. VII). C'est aussi le corps de décomposition de X^3-1 (ou X^4-X) sur F_2 ; il est de caractéristique $2 = p$, et l'on a : $q = p^2$. Plus généralement, nous avons le résultat suivant :

Théorème 1. *Un corps fini F est de caractéristique $p \neq 0$, et le nombre des éléments de F est p^r $(r \geqslant 1)$.*

En effet, le groupe cyclique abélien $\mathbb{Z}e$ ($e = 1$ élément neutre de F pour la multiplication) est nécessairement d'ordre fini p. La caractéristique de F est alors un nombre premier p. Le corps F est donc une extension du corps $F_p \simeq \mathbb{Z}e$, que l'on peut considérer comme plongé dans F. Comme F est fini, la dimension $[F : F_p] = r$ est également finie, et il existe une base $\{1 = \alpha_1, \ldots, \alpha_r\}$ de r éléments, sur F_p, tout élément de F s'écrivant, d'une

manière unique

$$x = a_1\alpha_1 + a_2\alpha_2 + \ldots + a_r\alpha_r , \qquad a_i \in F_p .$$

Comme chaque coefficient a_i peut prendre p valeurs, il y a p^r éléments x distincts :

$$\text{Card } F = p^r .$$

§ 2. Existence d'un corps F_q ayant $q = p^r$ éléments.

Problème : p premier et $r \in \mathbb{N}$ étant donnés, existe-t-il un corps ayant p^r éléments ? Si oui, quelle relation y a-t-il entre deux corps à p^r éléments, par exemple sont-ils isomorphes ?

Traitons d'abord le problème d'existence. Remarquons que, si un corps F de caractéristique p existe avec $p^r = q$ éléments, tous les éléments non nuls forment un groupe multiplicatif F^* ayant $q-1$ éléments et ils vérifient la relation $x^{q-1}-1 = 0$; si l'on veut une relation vérifiée aussi par $x = 0$, il suffit de prendre $x(x^{q-1}-1) = x^q - x = 0$.

Considérons alors le corps de décomposition de $f(X) = X^q - X$ sur F_p. Toutes les racines sont distinctes car la dérivée de $f(X)$ est $q\,X^{q-1}-1 = -1$ en caractéristique p, et elle ne peut s'annuler. Il y a donc q racines distinctes $x_1, x_2, \ldots, x_q$ $(q = p^r)$; parmi ces racines se trouvent d'ailleurs les p éléments du corps F_p, car si $x \in F_p$, on a : $x^p = x \Longrightarrow (x^p)^p = x^p = x$ c'est-à-dire $x^{p^2} = x$, et par récurrence sur r : $x^{p^r} = x$.

Démontrons que l'ensemble $E = \{x_1, x_2, \ldots, x_q\}$ forme lui-même un corps K . Soient $x \in E$, $y \in E$; on a donc : $x^{p^r} = x$, $y^{p^r} = y$, d'où en caractéristique p :

$$(x-y)^{p^r} = x^{p^r} - y^{p^r} = x-y$$

ce qui prouve que $x-y \in E$. De même :

$$(xy)^{p^r} = x^{p^r} \cdot y^{p^r} = xy , \text{ et } xy \in E .$$

Enfin l'inverse d'une racine non nulle est encore une racine. Donc E est un

corps ayant $q = p^r$ éléments (C.Q.F.D.) et on voit que $E = K = F_p(x_1, \ldots, x_q)$ qui est le corps de décomposition de $X^{p^r} - X$ sur F_p. Ici l'expression de corps de racines est parfaitement justifiée.

Exemples : il existe un corps F_8 à 8 éléments qui est le corps de décomposition de X^8-X, ou X^7-1, sur F_2 ; il existe un corps à 9 éléments qui est le corps de décomposition de X^9-X, ou X^8-1 sur F_3.

§ 3. Unicité du corps F_q à $q = p^r$ éléments, à un isomorphisme près.

Soit F un corps à $q = p^r$ éléments. Notons d'abord que sa caractéristique est $p' = p$, car d'après le § 1, on doit avoir $\text{Card } F = p'^{r'} = p^r$, ce qui exige $p' = p$, $r' = r$. Ensuite, tous les éléments de F doivent être racines de l'équation X^q-X sur F_p. Or toutes les racines de cette équation sont distinctes (la dérivée est égale à -1), et par suite F coïncide avec l'ensemble E de ces racines et avec un corps de décomposition de X^q-X sur F_p. D'après le théorème d'unicité du corps de décomposition, on a donc démontré le théorème suivant :

Théorème 2. Le nombre p premier étant donné, ainsi qu'un nombre naturel r quelconque, il existe un corps F_q à $q = p^r$ éléments. F_q a pour caractéristique p, et deux corps F_q à $q = p^r$ éléments sont isomorphes entre eux, et isomorphes au corps des racines de l'équation $X^{p^r}-X$ sur F_p.

§ 4. Le groupe multiplicatif F_q^* est cyclique.

En effet, ses éléments sont les racines de l'équation :

$$X^{q-1}-1 = 0$$

sur le corps F_p. Or on a vu au théorème 5, Chap. VII, que le groupe multiplicatif des racines $n^{\text{èmes}}$ de l'unité est cyclique si p ne divise pas n, ce qui est le cas ici puisque $n = q-1 = p^r-1$. Le groupe F_q^* sera donc engendré par une racine primitive α.

Exemple : $q = p = 5$. Les éléments non nuls de F_5 sont ± 1, ± 2 et ce sont les racines de l'équation X^4-1 . Les éléments ± 1 ne sont pas des racines primitives $4^{\text{èmes}}$ de l'unité puisque $1^2 = (-1)^2 = 1$; elles sont d'ordre 2 et non 4. Donc $+2$ et -2 sont les racines primitives cherchées. Le polynôme cyclotomique d'ordre 4 est : $P_4(X) = (X-2)(X+2) = X^2-4 = X^2+1$ sur le corps F_5 . Les puissances successives de 2 redonnent tous les éléments de F_5 .

Remarque. Si α est une racine primitive de $X^{p-1}-1 = 0$ dans F_p , α ne peut être un reste quadratique mod p . On sait en effet que α est un carré dans F_p si et seulement si $\alpha^{\frac{p-1}{2}} = 1$. Or $\alpha^{\frac{p-1}{2}} \neq 1$ si α est primitive, d'où $\alpha^{\frac{p-1}{2}} = -1$. La condition : α n'est pas un carré dans F_p est donc nécessaire pour que α soit une racine primitive ; elle n'est pas suffisante : considérer $\alpha = 6 = -1$ dans F_7 .

§ 5. Interprétation de r pour le groupe F_q , $q = p^r$.

On a vu au § 1 que $r = [F_q : F_p]$. Mais, si α est un générateur du groupe multiplicatif F_q^* , on a : $F_q^* = \{1, \alpha, \alpha^2, \ldots, \alpha^{q-2}\}$ et $F_q = F_p(\alpha)$ est une extension algébrique simple de F_p engendrée par α . Or, on sait que la dimension de $F_p(\alpha)$ sur F_p est égal au degré du polynôme minimal de α sur F_p , celui-ci étant un facteur irréductible du polynôme cyclotomique $P_{q-1}(X)$, de degré $\varphi(q-1)$. Il en résulte :

Propriété 1. Tous les facteurs irréductibles du polynôme cyclotomique $P_{q-1}(X)$ ont le même degré r , et r est un diviseur de $\varphi(q-1)$, où $q = p^r$.

On voit en passant que, dans le cas d'un corps k de caractéristique non nulle, le polynôme cyclotomique $P_n(X)$ n'est pas toujours irréductible sur k . Exemple : dans F_p lui-même, $P_{p-1}(X)$ se décompose en facteurs linéaires ($q = p$, $r = 1$). Un autre exemple est donné par $P_8(X)$ que l'on étudie au § 7.

§ 6. Le groupe de Galois $G(F_q,F_p)$.

Définition. k étant un sous corps de K, on appelle groupe de Galois $G(K,k)$ de K sur k, le groupe des k-automorphismes de K (c.à.d. des automorphismes de K qui laissent invariants les éléments de k).

Si $f(X) \in k[X]$ est un polynôme, K son corps de décomposition, le groupe de Galois de K sur k s'appelle encore le groupe de Galois du polynôme f sur k, ou de l'équation $f(X) = 0$ sur k, soit $G(f,k)$.

Ces définitions s'appliquent aux corps $F_p \subset F_q$ $(q = p^r)$ et à l'équation $X^{q-1}-1 = 0$ pour le groupe de Galois $G(F_q,F_p)$ que nous allons étudier.

Propriété 2. Card $G(F_q,F_p)= r$, $q = p^r$.

Cela donne une troisième interprétation de r . Cherchons les automorphismes du corps F_q ; ils conservent l'unité e , donc les éléments du sous-corps $F_p = \mathbb{Z}e$ et ce sont des F_p-automorphismes. Soit α une racine primitive de $X^{q-1}-1 = 0$. Elle est racine d'une composante irréductible $Q \in F_p[X]$ du polynôme cyclotomique $P_{q-1}(X)$, composante qui est de degré r d'après la propriété 1. Comme on a : $F_q = F_p(\alpha)$, un automorphisme σ de F_q est déterminé par le transformé $\beta = \sigma(\alpha)$ qui est une racine de $Q = 0$; toute racine de $Q = 0$ convient d'après le théorème de l'adjonction symbolique. Il y a r racines, toutes distinctes, et par suite r automorphismes.

Propriété 3. Le groupe de Galois $G(F_q,F_p)$ est cyclique d'ordre r , engendré par l'automorphisme $\sigma : x \mapsto x^p$.

L'application $\sigma : x \mapsto x^p$ est un automorphisme du corps F_q . En effet, F_q étant de caractéristique p , on a : $(x+y)^p = x^p+y^p$, $(xy)^p = x^py^p$, d'où un endomorphisme, évidemment injectif, qui laisse d'ailleurs invariants les éléments de $F_p \subset F_q$. Donc σ est une application F_p-linéaire injective de l'espace vectoriel F_q sur F_p qui est de dimension finie r ; σ est donc surjective. (Plus simplement, considérer une application injective d'un ensemble fini dans lui-même, elle est surjective). Formons la suite d'automorphismes :

σ, $\sigma^2 = \sigma \circ \sigma : x \mapsto (x^p)^p = x^{p^2}$, $\sigma^3 : x \mapsto x^{p^3}$,..., $\sigma^r : x \mapsto x^{p^r} = x$. On obtient ainsi r automorphismes de F_q qui sont tous distincts. En effet, supposons $\sigma^{k_1} = \sigma^{k_2}$, k_1 et $k_2 \leqslant r$, $k_1 < k_2$. En posant $k = k_2 - k_1 < r$ on aurait $\sigma^k = I$ (identité), c'est-à-dire $x^{p^k} = x$, $x \in F_q$. Mais cela est impossible puisque cette équation ne peut avoir p^r racines ; elle en a au plus p^k . La propriété 3 est démontrée.

Cette propriété entraîne que, si α est une racine d'un polynôme Q irréductible sur F_p , facteur du polynôme cyclotomique P_{q-1} , toutes les racines sont données par les transformations σ^k $(k = 1,..., r)$, soit

$$\alpha \ , \ \alpha^p \ , \ \alpha^{p^2} \ ,..., \ \alpha^{p^{r-1}} \ .$$

§ 7. Exemple. Etude de F_9 $(p = 3, r = 2)$.

Ses éléments non nuls sont les racines de $X^8 - 1 = 0$ dans le corps de décomposition sur F_3 . Le polynôme cyclotomique est $P_8(X) = X^4 + 1$ (Le vérifier) Les facteurs irréductibles de $P_8(X)$ sur F_3 sont de degré 2 . On a en fait :

$$X^4 + 1 = (X^2 + X - 1)(X^2 - X - 1) \ (= X^4 - 3X^2 + 1) \ .$$

Prenons $Q(X) = X^2 - X - 1$. Le corps F_9 est obtenu en adjoignant à F_3 une racine de ce polynôme irréductible sur F_3 , soit α . Comme le degré $[F_9 : F_3]$ est égal à 2, $\{1, \alpha\}$ constitue une base de F_9 sur F_3 ; d'où :

$$x \in F_9 \ , \ x = a + b\alpha \ , \ a \text{ et } b \in F_3 = \{0, +1, -1\}.$$

D'autre part $x \neq 0$ est une puissance de α . On retrouve ces résultats en calculant les puissances de α , compte tenu de $\alpha^2 - \alpha - 1 = 0$, ce qui donne :

$\alpha = \alpha$; $\alpha^2 = \alpha + 1$; $\alpha^3 = \alpha(\alpha+1) = \alpha + 1 + \alpha = -\alpha + 1$;

$\alpha^4 = (\alpha+1)^2 = \alpha^2 + 2\alpha + 1 = 3\alpha + 2 = -1$ (α racine de Q l'est de P_8) ;

$\alpha^5 = -\alpha$; $\alpha^6 = -\alpha - 1$; $\alpha^7 = \alpha - 1$; $\alpha^8 = 1$.

On a ainsi tous les éléments de F_9^* .

D'autre part, l'autre racine de $Q = 0$ est l'image de α par l'automorphisme $\sigma : x \to x^3$; elle est donc égale à α^3 .

Exercice. Etudier (ou retrouver) de la même façon le corps F_4 .

CHAPITRE IX

SYMBOLE DE LEGENDRE ET LOI DE RECIPROCITE QUADRATIQUE

Dans ce chapitre, l'existence des corps de décomposition et des racines primitives de $X^n - 1 = 0$, va jouer un rôle d'outil très utile.

§ 1. Symbole de Legendre.

Rappelons le résultat qui nous a servi pour l'étude des sommes de 2 carrés au Chapitre III.

Soit p un nombre premier impair. Les éléments x qui sont des carrés dans F_p^* sont caractérisés par l'égalité :

$$x^{\frac{p-1}{2}} = 1 .$$

Les autres, en nombre égal, sont caractérisés par :

$$x^{\frac{p-1}{2}} = -1 .$$

Donc, si $n \in \mathbb{Z}$, n est un reste quadratique mod p si et seulement si $n^{\frac{p-1}{2}} \equiv 1 \pmod{p}$; sinon on a : $n^{\frac{p-1}{2}} \equiv -1 \pmod{p}$. (On suppose $n \not\equiv 0 \pmod{p}$).

Définition. Soit p premier impair et $n \in \mathbb{Z}$, on appelle symbole de Legendre $(\frac{n}{p})$, l'expression définie ainsi :

$$\begin{cases} (\frac{n}{p}) = +1 & \text{si } n \text{ est un reste quadratique non nul mod } p \\ (\frac{n}{p}) = -1 & \text{si } n \not\equiv 0 \pmod p \text{ et n'est pas un reste quadratique} \\ (\frac{n}{p}) = 0 & \text{si } n \equiv 0 \pmod p. \end{cases}$$

En prenant la valeur $\bar{n} = x$ dans le corps F_p, on a d'après le résultat mentionné plus haut (th. 4, Chap. III)

$$(\frac{n}{p}) = x^{\frac{p-1}{2}}$$

cette expression étant encore valable pour $n \equiv 0 \pmod p \Rightarrow x = 0$.

En particulier :

$$(\frac{-1}{p}) = \begin{array}{ll} 1 & \text{si } p \equiv 1 \pmod 4 \\ -1 & \text{si } p \equiv 3 \pmod 4. \end{array}$$

Propriété 1. $(\frac{nn'}{p}) = (\frac{n}{p})(\frac{n'}{p})$.

En effet, en posant $\bar{n} = x$, $\overline{n'} = x'$ dans F_p, on a :

$$(\frac{nn'}{p}) = (\overline{nn'})^{\frac{p-1}{2}} = (xx')^{\frac{p-1}{2}} = x^{\frac{p-1}{2}} x'^{\frac{p-1}{2}} = (\frac{n}{p})(\frac{n'}{p}).$$

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 $\neq p$.

§ 2. Calcul de $(\frac{2}{p})$.

Propriété 2. On a :

$$\begin{cases} (\frac{2}{p}) = +1 & \text{si } p \equiv \pm 1 \mod 8 \\ (\frac{2}{p}) = -1 & \text{si } p \equiv \pm 3 \mod 8. \end{cases}$$

Soit α une racine primitive de l'unité dans le corps K des racines de l'équation $X^8 - 1 = 0$ sur le corps F_p. On a donc $x^8 - 1 = (\alpha^4+1)(\alpha^4-1) = 0$, d'où, comme α est primitive : $\alpha^4 = -1$. Posons $y = \alpha + \alpha^{-1} \in K$. Il vient :

$$y^2 = \alpha^2 + \frac{1}{\alpha^2} + 2 = \frac{\alpha^4+1}{\alpha^2} + 2 = 2 .$$

On en déduit :

$$y^p = y\, y^{p-1} = y.(y^2)^{\frac{p-1}{2}} = y.2^{\frac{p-1}{2}} = (\frac{2}{p})y .$$

Mais, comme K est de caractéristique p :

$$y^p = \alpha^p + \alpha^{-p} .$$

Si $p \equiv \pm 1 \pmod 8$, on a : $\alpha^{8h} = 1$, et $y^p = \alpha + \alpha^{-1} = y$. On en déduit :

$y = (\frac{2}{p})y \Rightarrow (\frac{2}{p}) = 1$ (car $y \neq 0$, $y^2 = 2$!!).

Si $p \equiv \pm 5 \pmod 8$, on a : $y^p = \alpha^5 + \alpha^{-5} = -\alpha - \alpha^{-1} = -y$. On en déduit :

$-y = (\frac{2}{p})y \Rightarrow (\frac{2}{p}) = -1$.

La propriété 2 est établie si l'on remarque que $\pm 5 \equiv \mp 3 \pmod 8$. On peut en déduire l'écriture commune aux 2 cas :

$$(\frac{2}{p}) = (-1)^{\frac{p^2-1}{8}} .$$

§ 3. Enoncé de la loi de réciprocité quadratique.

Soient p et q deux nombres premiers impairs distincts. On a :

$$\boxed{(\frac{p}{q})\,(\frac{q}{p}) = (-1)^{\frac{p-1}{2}\,\frac{q-1}{2}}}$$

Comme $(\frac{p}{q}) = \pm 1$, cette égalité permet d'exprimer :

$$(1) \qquad \boxed{(\frac{q}{p}) = (-1)^{\frac{p-1}{2}\,\frac{q-1}{2}}\,(\frac{p}{q})}$$

et d'en déduire :

$(\frac{q}{p}) = (\frac{p}{q})$ si p <u>ou</u> q est $\equiv 1 \bmod 4$

$-(\frac{q}{p}) = (\frac{p}{q})$ si p <u>et</u> q sont $\equiv -1 \bmod 4$.

Avant de donner la démonstration de la loi de réciprocité quadratique, nous allons expliquer comment elle sert dans le calcul de $(\frac{n}{p})$.

§ 4. Calcul de $(\frac{n}{p})$.

Le symbole de Legendre $(\frac{n}{p})$ ne dépend que de la classe de n mod p. On peut donc supposer :

$$-\frac{p}{2} < n < \frac{p}{2}$$

et même : $0 < n < \frac{p}{2}$ car : $(\frac{-n}{p}) = (\frac{-1}{p})(\frac{n}{p}) = (-1)^{\frac{p-1}{2}}\,(\frac{n}{p})$.

On décompose $n > 0$ en facteurs premiers. Comme le symbole $(\frac{2}{p})$ est connu (voir § 2), on est ramené au calcul de $(\frac{q}{p})$ pour q premier impair $< p$, ou même $< \frac{p}{2}$. Alors, par la loi de réciprocité (1) on est ramené à un calcul de

$(\frac{p}{q})$ pour un entier q inférieur. On recommence le même procédé, ce qui donne donc une méthode de calcul par récurrence sur p .

Exemples :

1°. $(\frac{29}{43}) = (\frac{43}{29}) = (\frac{14}{29}) = (\frac{2}{29})(\frac{7}{29})$

$= -(\frac{7}{29}) = -(\frac{29}{7}) = -(\frac{1}{7}) = -1$.

2°. $(\frac{23}{17}) = -1$ (Exercice, Cours Cartan, p. 104).

3°. $(\frac{-3}{p}) = (-1)^{\frac{p-1}{2}}(\frac{3}{p}) = +(\frac{p}{3}) = \begin{cases} 1 & \text{si } p \equiv 1 \pmod 3 \\ -1 & \text{si } p \equiv -1 \pmod 3. \end{cases}$

4°. $(\frac{5}{p}) = (\frac{p}{5})$. Or $(\frac{1}{5}) = 1$, $(\frac{2}{5}) = -1$; d'où :

$$(\frac{5}{p}) = \begin{cases} 1 & \text{si } p \equiv \pm 1 \mod 5 \\ -1 & \text{si } p \equiv \pm 2 \mod 5. \end{cases}$$

5°. Exercices. Calculer $(\frac{3}{p})$; $(\frac{4}{p})$.

§ 5. Démonstration de la loi de réciprocité quadratique.

Soient p et q deux nombres premiers impairs différents. On adjoint au corps F_p les racines du polynôme X^q-1 sur F_p , ce qui donne donc le corps de décomposition K de X^q-1 sur F_p . Les calculs se font dans K , qui est de caractéristique p .

Soit α une racine primitive de $X^q-1 = 0$. Toutes les racines sont donc $\alpha, \alpha^2, \ldots, \alpha^{q-1}, \alpha^q = 1$.

Considérons $x \in F_q$. On peut définir α^x puisque α^k ne dépend que de la classe de k mod. q. On pose :

$$\boxed{y = \sum_{x \in F_q} (\frac{x}{q})\alpha^x} \quad .$$

(Le coefficient de α^0 est $(\frac{0}{q}) = 0$; le symbole de Legendre $(\frac{x}{q})$ est égal à $+1$ ou -1 que l'on considère comme des éléments de F_p donc de $K \supset F_p$).

Calculons :

$$y^2 = \Big[\sum_{x \in F_q} (\frac{x}{q})\alpha^x\Big]\Big[\sum_{x' \in F_q} (\frac{x'}{q})\alpha^{x'}\Big] = \sum_{x,x'} (\frac{xx'}{q})\alpha^{x+x'} \quad .$$

Effectuons pour les variables x, x' le changement :

$$x = x, \quad x+x' = t .$$

Il vient :

$$y^2 = \sum_{x,t} \left(\frac{x(t-x)}{q}\right)\alpha^t = \sum_{t\in F_q} C_t \alpha^t \text{ , avec}$$

$$(3) \qquad C_t = \sum_{x\in F_q} \left(\frac{x(t-x)}{q}\right) = \sum_{x\in F_q^*} \left(\frac{x(t-x)}{q}\right)$$

puisque, pour $x = 0$, le coefficient est $\left(\frac{0}{q}\right) = 0$.

Cas $t = 0$.

$$C_o = \sum_{x\in F_q^*} \left(\frac{-x^2}{q}\right) ;$$

or : $$\left(\frac{-x^2}{q}\right) = (-1)^{\frac{q-1}{2}} \left(\frac{x^2}{q}\right) = (-1)^{\frac{q-1}{2}} \text{ , d'où}$$

$$(4) \qquad C_o = (-1)^{\frac{q-1}{2}} (q-1).$$

Cas $t \neq 0$.

On peut écrire : $\left(\frac{x(t-x)}{q}\right) = \left(\frac{(-x^2)(1-\frac{t}{x})}{q}\right) = \left(\frac{-1}{q}\right)\left(\frac{1-\frac{t}{x}}{q}\right)$.

Or quand x décrit F_q^*, $\frac{t}{x}$ décrit aussi F_q^* puisque $t \neq 0$ et $1 - \frac{t}{x}$ parcourt $F_q - \{1\}$. On a donc d'après (3) et compte tenu de $\left(-\frac{1}{q}\right) = (-1)^{\frac{q-1}{2}}$:

$$C_t = (-1)^{\frac{q-1}{2}} \sum_{z\in F_q-\{1\}} \left(\frac{z}{q}\right) = (-1)^{\frac{q-1}{2}} \left[\sum_{z\in F_q} \left(\frac{z}{q}\right) - \left(\frac{1}{q}\right)\right].$$

Mais $\left(\frac{1}{q}\right) = 1$ et $\sum_{z\in F_q} \left(\frac{z}{q}\right) = \sum_{z\in F_q^*} \left(\frac{z}{q}\right) = 0$ car il y a $\frac{q-1}{2}$ carrés dans F_q^* et autant d'éléments non carrés. Donc :

$$C_t = -(-1)^{\frac{q-1}{2}} .$$

Par suite :

$$y^2 = (-1)^{\frac{q-1}{2}} \left[q-1 - \sum_{t\in F_q^*} \alpha^t\right] \text{ , ou}$$

$$y^2 = (-1)^{\frac{q-1}{2}} \left[q - \sum_{t\in F_q} \alpha^t\right] .$$

Mais $\sum_{t\in F_q} \alpha^t = 0$, car la somme des racines de l'équation $X^q - 1 = 0$ est nulle.

Il vient donc :

$$(5) \qquad \boxed{y^2 = (-1)^{\frac{q-1}{2}} .q} \quad .$$

Nous allons maintenant calculer y^p . Le corps K étant de caractéristique p , on a :

$$y^p = \sum_{x \in F_q} \left(\frac{x}{q}\right)^p \alpha^{px}$$

avec $\left(\frac{x}{q}\right)^p = \left(\frac{x}{q}\right)$. (N'oublions pas que $u = \left(\frac{x}{q}\right) = \pm 1$ est pris dans le corps F_p et que p est impair, d'où $u^p = u$). On en déduit :

$$y^p = \sum_{x \in F_q} \left(\frac{x}{q}\right) \alpha^{px}$$

et :

$$(6) \quad \left(\frac{p}{q}\right) y^p = \sum_{x \in F_q} \left(\frac{px}{q}\right) \alpha^{px} = \sum_{x \in F_q} \left(\frac{x}{q}\right) \alpha^{x} = y \ .$$

Car lorsque x décrit F_q , px aussi du fait que $p \neq q$.

On déduit de (6) en simplifiant par y ($y \neq 0$, dire pourquoi ?) :

$$(7) \quad \boxed{\left(\frac{p}{q}\right) y^{p-1} = 1} \ .$$

Ecrivons, d'après (5) :

$$y^{p-1} = (y^2)^{\frac{p-1}{2}} = (-1)^{\frac{p-1}{2}\frac{q-1}{2}} q^{\frac{p-1}{2}}$$

$$= (-1)^{\frac{p-1}{2}\frac{q-1}{2}} \left(\frac{q}{p}\right)$$

et remplaçons dans (7) :

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right)(-1)^{\frac{p-1}{2}\frac{q-1}{2}} = 1 \ .$$

C'est la formule de réciprocité quadratique.

<u>Corollaire</u>. $\left(\frac{-q}{p}\right) = (-1)^{\frac{p-1}{2}\frac{q-1}{2}} \left(\frac{p}{q}\right)$.

En effet :

$$\left(\frac{-q}{p}\right) = \left(\frac{-1}{p}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}} (-1)^{\frac{p-1}{2}\frac{q+1}{2}} \left(\frac{p}{q}\right)$$

$$= (-1)^{\frac{p-1}{2}\frac{q+1}{2}} \left(\frac{p}{q}\right) \ .$$

CHAPITRE X

EXTENSIONS GALOISIENNES

§ 1. Définition.

Soit K une extension de degré fini du corps k. Soit $G(K,k)$ le groupe de Galois de K sur k, c'est-à-dire le groupe des k-automorphismes de K. Soit $F = K^G$ le sous-corps de K constitué par les éléments de K qui sont invariants par toutes les transformations σ du groupe G. (Vérifier qu'il s'agit d'un sous-corps). On emploie aussi les notations

$$G = \mathrm{Gal}(K,k), \qquad F = \mathrm{Fix}(K,G).$$

Il est clair que $k \subset F$. Nous allons démontrer le théorème suivant :

Théorème 1. *Les deux propriétés suivantes sont équivalentes*

(i) $\mathrm{Card}\ G = [K : k]$

(ii) $\mathrm{Fix}(K,G) = k$.

(ii) $\Rightarrow$ (i). Nous utiliserons plusieurs lemmes :

Lemme 1. *Soit m automorphismes distincts σ_i de G. La relation*

$$\sum_{i=1}^{m} \lambda_i \sigma_i(x) = 0, \quad \forall\, x \in K \quad \text{implique} \quad \lambda_i = 0 \ (i = 1, \ldots, m)$$
$$\lambda_i \in K$$

Récurrence sur m. La relation est vraie pour $m = 1$, car $\lambda_1 \sigma_1(x) = 0$,

$\forall x \in K \Rightarrow \lambda_1 \sigma_1(1) = \lambda_1 = 0$.

Supposons la vraie pour $m-1$. Dans l'hypothèse $\sum_{i=1}^{m} \lambda_i \sigma_i(x) = 0$, $\forall x \in K$ avec des coefficients non tous nuls, on peut supposer tous les $\lambda_i \neq 0$, car si l'un d'eux est nul on applique la propriété pour $m-1$. On a donc en divisant par λ_m :

$$(1) \qquad \sum_{i=1}^{m-1} \lambda_i \sigma_i(x) + \sigma_m(x) = 0 , \qquad \forall x \in K ,$$

d'où, en prenant $a \in K$ tel que $\sigma_1(a) \neq \sigma_m(a)$. (Un tel $a \in K$ existe, expliquer pourquoi, et n'est pas nul), et en remplaçant x par ax :

$$\sum_{i=1}^{m-1} \lambda_i \sigma_i(a)\ \sigma_i(x) + \sigma_m(a)\ \sigma_m(x) = 0$$

c'est-à-dire :

$$(2) \qquad \sum_{i=1}^{m-1} \lambda_i \sigma_i(a)\ \sigma_m^{-1}(a)\ \sigma_i(x) + \sigma_m(x) = 0 .$$

Retranchons (1) de (2) :

$$\sum_{i=1}^{m-1} \lambda_i (\sigma_i(a)\ \sigma_m^{-1}(a) - 1)\ \sigma_i(x) = 0 .$$

L'hypothèse de récurrence implique que tous les coefficients sont nuls, ce qui donne pour $i = 1$, $\lambda_1 = 0$. On arrive à une contradiction.

Lemme 2. Soit $r = [K : k]$; on a : Card $G = m \leqslant r$.

Ce lemme prouve en particulier que Card G est fini (ce qui peut s'établir directement à titre d'exercice). Considérons l'espace vectoriel K^r sur K et, avec une base $x_1, x_2, \ldots, x_r$ de K sur k, les vecteurs colonnes :

$$(3) \qquad \begin{matrix} \sigma_1(x_1) & \sigma_2(x_1) & \ldots & \sigma_m(x_1) \\ \sigma_1(x_2) & \sigma_2(x_2) & & \sigma_m(x_2) \\ \vdots & & & \\ \sigma_1(x_r) & \sigma_2(x_r) & & \sigma_m(x_r) \end{matrix}$$

obtenus en appliquant à $\begin{pmatrix} x_1 \\ \vdots \\ x_r \end{pmatrix}$ m automorphismes distincts $\sigma_i \in G$. Je dis que ces vecteurs sont linéairement indépendants sur K dans K^r . Supposons en effet :

$$\sum_{i=1}^{m} \lambda_i \sigma_i(x_p) = 0 , \qquad p = 1, \ldots, r .$$

Si $x \in K$, on a : $x = \sum_{p=1}^{r} \alpha_p x_p$, $\alpha_p \in k$, d'où :

$$\sum_{i=1}^{m} \lambda_i \sigma_i(x) = \sum_{i=1}^{m} \lambda_i \sigma_i\left(\sum_{p=1}^{r} \alpha_p x_p\right) = \sum_{i=1}^{m} \lambda_i \sum_{p=1}^{r} \alpha_p \sigma_i(x_p)$$

$$= \sum_{p=1}^{r} \alpha_p \sum_{i=1}^{m} \sigma_i(x_p) = 0 .$$

Il suffit alors d'appliquer le lemme 1 pour obtenir $\lambda_i = 0$ $(i = 1, \ldots, m)$. Comme l'espace K^r est de dimension r, on en déduit bien Card $G = m < r$.

Lemme 3. Soit $r = [K : k]$, Card $G = m$. Supposons (ii). Alors : $r \leqslant m$.

Considérons cette fois l'espace K^m et les r vecteurs lignes de la matrice (3). Je dis qu'ils sont linéairement indépendants sur K. Supposons en effet :

$$(4) \qquad \sum_{i=1}^{r} v_i \sigma_h(x_i) = 0, \quad v_i \in K, \quad h = 1, \ldots, m.$$

On raisonne par récurrence sur le nombre r de lignes. Si $r = 1$, en prenant $\sigma_1 = Id$, on aurait $v_1 x_1 = 0 \Rightarrow v_1 = 0$. Supposons la propriété vraie pour $r-1$. Si les coefficients v_i ne sont pas tous nuls dans (4), on peut supposer par exemple $v_r \neq 0$ et écrire après division par v_r :

$$(5) \qquad \sum_{i=1}^{r-1} v_i \sigma_h(x_i) + \sigma_h(x_r) = 0, \quad h = 1, \ldots, m .$$

Les coefficients v_i ne peuvent pas appartenir tous à k, car la relation (5) donnerait en prenant $\sigma_1 = Id$: $\sum_{i=1}^{r-1} v_i x_i + x_r = 0$, qui est impossible à cause de l'indépendance linéaire de $x_1, \ldots, x_r$ sur k. Dès lors si $v_1 \notin k$, il existe en vertu de (ii), un σ_q tel que $\sigma_q(v_1) \neq v_1$. Appliquons σ_q à (5) :

$$(6) \qquad \sum_{i=1}^{r-1} \sigma_q(v_i)\, \sigma_q \circ \sigma_h(x_i) + \sigma_q \circ \sigma_h(x_r) = 0 .$$

Lorsque $h = 1, \ldots, m$, σ_h décrit le groupe G, et $\sigma_q \circ \sigma_h$ aussi. On peut donc remplacer dans (6) $\sigma_q \circ \sigma_h$ par σ_h, ce qui donne :

$$(7) \qquad \sum_{i=1}^{r-1} \sigma_q(v_i)\, \sigma_h(x_i) + \sigma_h(x_r) = 0 .$$

Retranchons (5) de (7) :

$$\sum_{i=1}^{r-1} (\sigma_q(v_i) - v_i)\, \sigma_h(x_i) = 0, \quad h = 1, \ldots, m.$$

On obtiendrait une dépendance linéaire entre $r-1$ lignes avec un coefficient $\sigma_q(v_1) - v_1 \neq 0$, ce qui est contraire à l'hypothèse de récurrence.

L'application des lemmes 1, 2, 3 donne immédiatement $r = m$, c'est-à-dire (i) lorsque (ii) est supposé vérifié.

(i) $\Rightarrow$ (ii). Soit F le corps fixe de K pour G. Il est clair que G est encore le groupe des F-automorphismes de K. On a de plus :

$$\mathrm{Fix}(K,G) = F.$$

La condition (ii) est alors vérifiée pour F au lieu de k. La propriété (ii) $\Rightarrow$ (i) appliquée à F entraîne donc :

$$\mathrm{Card}\ G = [K : F].$$

Mais : $k \subseteq F \subseteq K \Rightarrow [K : k] = [K : F][F : k]$ d'où, avec (i) : $\mathrm{Card}\ G = [K : k]$, on obtient :

$$[F : k] = 1,$$

et, par suite :

$$F = k$$

(ii) est donc une conséquence de (i).

Définition 1. Une extension K de k, de degré fini, est dite Galoisienne si elle vérifie l'une ou l'autre des propriétés équivalentes du théorème 1.

§ 2. Extension séparable.

Définition. Soit $f(X) \in k[X]$. On dit que f est séparable sur k si toutes les racines de l'équation $f(X) = 0$ dans un corps de décomposition de $f(X)$ sur k sont simples.

Si f est décomposé en facteurs irréductibles sur k, f est séparable sur k si et seulement si tous les facteurs irréductibles sont distincts et séparables sur k. (A expliquer).

Propriété 1. Si k est de caractéristique nulle, tout polynôme $f(X) \in k[X]$ irréductible sur k est séparable.

Preuve : si $f(X) = 0$ avait une racine multiple α dans le corps de décomposition K de f sur k, celle-ci annulerait $f(X)$ et $f'(X)$, donc le p.g.c.d. $\Delta(X) \in k[X]$ qui serait donc de degré positif. Mais f étant irréductible sur k, l'égalité $f(X) = M(X)\,\Delta(X)$ entraîne $d^oM(X) = 0$, et $f(X)$ diviserait $f'(X)$. Si $f(X) = a_oX^n + a_1X^{n-1} + \ldots + a_n$, $a_o \neq 0$, $f'(X) = na_oX^{n-1} + \ldots$ ne peut être multiple de $f(X)$ que si $f'(X) = 0$, donc $na_o = 0$, ce qui est impossible en caractéristique nulle.

Etudions de plus près la condition obtenue en caractéristique p non nulle $na_o = 0 \Rightarrow n = m_1p$ est multiple de la caractéristique ; $(n-1)a_1 = 0 \Rightarrow a_1 = 0$ car $n-1$ n'est pas multiple de p ; d'une façon générale :

$$n = m_1p,\quad a_1 = 0, \ldots, a_h = 0 \text{ si } h \text{ n'est pas multiple de } p$$

et :

$$(1) \qquad f(X) = a_o(X^p)^{m_1} + b_1(X^p)^{m_2} + \ldots = g(X^p),$$

où $g(u) \in k[u]$ est un polynôme de degré $m_1 = \frac{n}{p}$. Il reste à étudier la compatibilité de ce résultat avec l'irréductibilité de f.

Propriété 2. Si $k = F_q$ est un corps fini ($q = p^r$), tout polynôme $f(X) \in k[X]$ irréductible sur k est séparable.

En effet, on a vu que l'application $\sigma : u \to u^p$ est un automorphisme du corps F_q. Cette application est donc surjective et par suite : $v = u^p$ possède une solution en u quand on se donne v. Tout élément possède une racine $p^{\text{ème}}$; on dit que F_q est un corps parfait. Mais alors, on peut poser dans (1) : $a_o = \beta_o^p$, $b_1 = \beta_1^p, \ldots,$ avec $\beta_i \in k$; et écrire en caractéristique p :

$$f(X) = (\beta_oX^{m_1} + \beta_1X^{m_2} + \ldots)^p \quad ; \quad \beta_i \in k .$$

Ce qui est en contradiction avec l'irréductibilité de f sur k.

Revenons au cas général d'un corps de caractéristique p.

Propriété 3. Si $f(X) \in k[X]$ est irréductible sur k, de caractéristique p, toutes les racines de $f(X) = 0$ dans le corps de décomposition ont le même ordre de multiplicité qui est une puissance de p.

On raisonne par récurrence sur le degré, qui est un multiple de p

$$f(X) = g(u) \qquad u = X^p .$$

Si $d^o g = 1$, on prend $g(u) = u-\alpha$; $\alpha \in k$. Soit β une racine de $f(X) = 0$, d'où $\alpha = \beta^p$ et $f(X) = X^p - \alpha^p = (X-\alpha)^p$.

Supposons maintenant f de degré quelconque.

$g(u)$ est aussi un polynôme irréductible dans $k[u]$ (si $g(u) = h(u)\,\ell(u)$ on a : $f(X) = h(X^p)\,\ell(X^p)$) et son degré est moindre que celui de f ; on a donc par récurrence :

$$g(u) = (u - \beta_1)^{p^r} \dots (u - \beta_s)^{p^r}$$

d'où

$$f(X) = (X^p - \beta_1)^{p^r} \dots (X^p - \beta_s)^{p^r} .$$

En prenant une racine γ_i de $X^p-\beta_i = 0$ dans le corps de décomposition de f sur K, il vient $\beta_i = \gamma_i^p$ d'où :

$$f(X) = (X - \gamma_1)^{p^{r+1}} \dots (X - \gamma_s)^{p^{r+1}} \qquad \text{C. Q. F. D.}$$

<u>Exemple</u>. Soit $h(X) = X^p-t$, le corps $k = F_p(t)$ étant une extension transcendante simple de F_p . Dans le corps de décomposition de $h(X)$ sur k, prenons une racine α ; elle vérifie $\alpha^p = t$, d'où $h(X) = X^p - \alpha^p = (X-\alpha)^p$.

Une composante irréductible de $h(X)$ sur k est donc un diviseur de la forme $(X-\alpha)^r$ avec $r = 0$ ou $r = p$. On ne peut avoir $r = 0$ car alors $\alpha \in k$ vérifierait :

$$\alpha^p = \left(\frac{a_o t^r + \dots + a_h}{b_o t^s + \dots + b_s}\right)^p = t$$

c'est-à-dire :

$$a_o^p t^{pr} + \dots = t(b_o^p t^{ps} + \dots)$$

et, en prenant les degrés dans chaque membre :

$$p(r+1) = p(s+1) + 1 \qquad \text{(impossible)}$$

d'où : <u>$h(X) = X^p - t$ est irréductible sur $k = F_p(t)$ et non séparable sur k</u> .

<u>Définition</u>. Soit $K \supset k$ une extension algébrique de k . On dit que $x \in k$ <u>est séparable sur</u> k si le polynôme minimal irréductible $f(X)$ de x sur k est séparable. On dit que K <u>est une extension séparable de</u> k si tout élément de K est séparable sur k .

Si k est de caractéristique nulle, ou bien est un corps fini F_q, toute extension algébrique K de k est séparable.

§ 3. Extension normale.

Définition. Soit $K \supset k$ une extension algébrique de k. On dit que K est une extension normale de k si, quel que soit le polynôme irréductible $f(X) \in k[X]$, l'hypothèse que $f(X) = 0$ admette une racine dans K entraîne que toutes les autres racines de $f(X) = 0$ (dans le corps de décomposition de $f(X) = 0$ sur k) sont également dans K.

Autrement dit, le polynôme minimal sur k de tout élément $x \in K$, admet toutes ses racines dans K.

Théorème 2. Soit K une extension galoisienne de k. Alors K est une extension normale et séparable de k.

Soit $x \in K$. Nous allons déterminer le polynôme minimal $f(X)$ de x sur k au moyen des transformés $\sigma(x)$ par les éléments σ du groupe de Galois $G(K,k)$. Désignons par x_i les transformés distincts de x par les éléments $\sigma \in G$. On peut prendre $\sigma_1 = Id$ d'où $\sigma_1(x) = x = x_1$. Ces éléments x_i sont en nombre m au plus égal à l'ordre de G qui est $[K : k] = r$. On a pour tout $\sigma \in G$, $\sigma(x_i) = \sigma \circ \sigma_i(x) \in \{x_1, \ldots, x_m\}$ et σ induit une permutation sur l'ensemble $x_1, \ldots, x_m$ (car c'est une bijection dans K). Considérons l'équation :

$$P(X) = (X - x_1)(X - x_2) \ldots (X - x_m).$$

Ses coefficients sont des fonctions symétriques élémentaires des x_i et ils restent donc invariants par tous les éléments $\sigma \in G$; ils appartiennent alors au corps fixe de K par G qui est k puisque l'extension est supposée Galoisienne. On a donc :

$$P(X) \in k[X].$$

De plus $P(X)$ est irréductible sur k, car si un facteur irréductible $Q(X)$

admet pour racine x_i , il aura également pour racine $\sigma(x_i)$, $\forall \sigma \in G$, c'est-à-dire tous les éléments distincts $x_1, \ldots, x_m$. Cela prouve que $Q(X)$ coïncide avec $P(X)$ qui est bien le polynôme irréductible de x sur k. Ce polynôme a effectivement toutes ses racines distinctes (c'est la séparabilité) et dans K (c'est la normalité).

§ 4. Apparition d'un corps de décomposition.

Théorème 3. Soit $K \supset k$ une extension de degré fini normale et séparable sur k. Alors K est le corps de décomposition d'un polynôme $f(X) \in k[X]$ séparable sur k.

Soit K de degré fini sur k et normal sur k. On prend $x \in K$, $x \notin k$. Le polynôme minimal $f_1(X)$ de x sur k a toutes ses racines dans K à cause de la normalité, et le corps des racines est $k_1 = k(x_1, \ldots, x_n) \subset K$. Toutes ces racines sont d'ailleurs distinctes à cause de la séparabilité. Si $k_1 = K$, le théorème est démontré. Sinon on prend $u \in K$, $u \notin k_1$ et le polynôme minimal f_2 de u sur K ; ce polynôme f_2 est différent de f_1 puisque $u \notin k_1$ et il admet des racines distinctes dans K et distinctes des précédentes, soit $y_1, \ldots, y_m$. Soit $k_2 = k_1(y_1, \ldots, y_m) \subset K$ avec $k_1 \subsetneq k_2$ (puisque u est dans k_2 et pas dans k_1).

L'extension K étant de degré fini sur k, le procédé s'arrête au bout d'un nombre fini d'opérations qui aboutissent sur K intervenant alors comme corps de décomposition du polynôme $f(X) = f_1(X)\, f_2(X) \ldots$ séparable sur k.

§ 5. Le corps de décomposition interprété comme une extension Galoisienne.

Théorème 4. Soit $f(X) \in k[X]$ un polynôme séparable sur k. Alors, le corps de décomposition K de $f(X)$ sur k est une extension Galoisienne de k.

Pour la démonstration, nous allons démontrer que le groupe de Galois $G(K,k)$ a pour ordre $[K : k]$. On utilise le lemme de prolongement suivant qui ne fait que préciser le théorème 2 "d'unicité" du corps de décomposition de f sur k lorsque f est séparable sur k.

Lemme de prolongement. (Cf. Mac-Lane-Birkhoff, Algèbre, Tome 2, p. 312).

Soit $f(X) \in k[X]$ séparable sur k ; on se donne un isomorphisme $\varphi : k \to k'$. On pose $\varphi(f) = \overline{f} \in k'[X]$. Soit K le corps de décomposition de $f(X)$ sur k, K' le corps de décomposition de $\overline{f}(X)$ sur k'. Alors, il existe exactement $d = [K : k]$ isomorphismes $K \to K'$ qui prolongent φ.

Récurrence sur le degré de f. Vrai pour $n = 1$. Soit $\sigma : K \to K'$, prolongeant $\varphi : k \to k'$. Il transforme x_1 racine donnée de $f(X) = 0$ en une racine x'_1 de $\overline{f}(X) = 0$, ou plus précisément, si $f(X) = f_1(X) \ldots f_h(X)$ est la décomposition de f en facteurs irréductibles sur k, et si x_1 est racine de $f_1(X) = 0$, x'_1 est racine de $\overline{f_1}(X)$ sur k'. Il y a exactement $[k_1 : k] = [k(x_1) : k]$ choix possibles pour x'_1 puisque toutes les racines sont distinctes (séparabilité de f_1 et de $\overline{f_1}$). Fixons l'un de ces choix. Nous avons un isomorphisme φ_1 induit par σ sur $k(x_1) \to k'(x'_1)$. Considérons $f(X) = (X-x_1)g(X)$, $g(X) \in k_1[X]$; $\overline{f}(X) = (X-x'_1)g_1(X)$; $g_1(X) = \varphi_1(g(X)) = \overline{g}(X) \in k'_1[X]$; $k'_1 = k'(x_1)$.

g est séparable sur k_1 et le corps des racines est $k_1(x_2, \ldots, x_n) = k(x_1, x_2, \ldots, x_n) = K$. Son degré est $n-1$, d'où par récurrence sur n, il existe exactement $[K : k_1]$ isomorphismes qui prolongent φ_1. On a ainsi trouvé : $[K : k_1] \times [k_1 : k] = [K : k]$ isomorphismes qui prolongent $\varphi : k \to k'$.

Le théorème 4 en résulte en prenant l'identité pour φ et $K = K'$.

§ 6. Théorème récapitulatif.

Soit K une extension de degré fini de k. On pose $G = \mathrm{Gal}(K,k)$, $F = \mathrm{Fix}(K,G)$. Il y a équivalence entre les propriétés suivantes :

(i) $\mathrm{Card}\ G = [K : k]$

(ii) $\mathrm{Fix}(K,G) = k$

(iii) K est une extension séparable et normale de k.

(iv) K est le corps de décomposition d'un polynôme $f(X) \in k[X]$ séparable sur k.

En effet : (i) $\Leftrightarrow$ (ii) d'après le théorème 1.

(ii) $\Rightarrow$ (iii) d'après le théorème 2.

(iii) $\Rightarrow$ (iv) d'après le théorème 3.

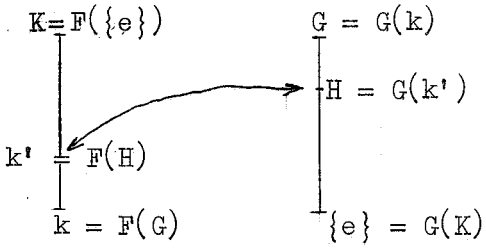
(iv) $\Rightarrow$ (i) d'après le théorème 4.

Si k est de caractéristique nulle ou est un corps fini, on peut se dispenser de l'hypothèse de séparabilité dans l'énoncé.

CHAPITRE XI

THEORIE DE GALOIS

K étant une extension Galoisienne de k, G le groupe des k-automorphismes de K, la théorie de Galois consiste à établir une correspondance biunivoque entre les sous-groupes de G et les sous-corps de K contenant k,



§ 1. Sous-corps k' associé à un sous-groupe H de G.

H étant un sous-groupe de G, on lui fait correspondre le sous-corps $k' = \mathrm{Fix}(K,H)$ des éléments de K qui sont fixes par toutes les transformations de H. Il est clair que k' est un sous-corps de K et que k' contient k. Posons $k' = F(H)$.

Propriété 1. Le groupe H' des k'-automorphismes de K est égal à H.

On a évidemment $H' \supseteq H$. Il en résulte que le corps fixe de H', qui est inclus dans le corps fixe de H, est inclus dans k'. D'autre part, il contient k' ; il lui est donc égal et K est une extension Galoisienne de k'. On a donc d'après le théorème 1 du Chap. X :

$$(1) \qquad [K : k'] = \mathrm{Card}\ H'.$$

Mais on peut également calculer l'ordre de H au moyen des lemmes du chapitre X, § 1, formulés de la façon suivante, avec démonstration calquée sur celle qui a été donnée.

Lemme. Soit H un groupe fini d'automorphismes du corps K ; soit $k' = F(H)$ le corps fixe de K pour H. On a :

(2) Card $H = [K : k']$.

En comparant (1) et (2), on obtient $H' = H$, donc la propriété 1. Cette propriété ne suppose pas que K est galoisien sur k, mais seulement que $[K : k]$ est fini.

§ 2. Sous-groupe H associé à un sous-corps k' de K contenant k.

Soit maintenant k' un sous-corps quelconque de K tel que

$$k \subseteq k' \subseteq K$$

(Le sous-corps $k' = F(H)$ du § 1 n'était peut-être pas quelconque). On lui fait correspondre le groupe $H = Gal(K,k') = G(k')$ des k'-automorphismes de K. Il est clair que H est un groupe et que ce groupe est inclus dans G. On pose $H = G(k')$.

Propriété 2. Le corps fixe de H est égal à k'.

Pour le démontrer, il suffit de vérifier que K est extension galoisienne de k'. Cela résulte du fait que K est extension galoisienne de k et de l'inclusion $k \subseteq k' \subseteq K$. On le vérifie en prenant l'une des propriétés équivalentes du théorème récapitulatif du chapitre X, par exemple la propriété IV : K est corps de décomposition d'un polynôme $f(X) \in k[X]$ séparable sur k ; alors K est également le corps de décomposition du polynôme $f(X) \in k'[X]$ séparable sur k'. (Explication : si $x_1, \ldots, x_n$ sont les racines de $f(X) = 0$ dans K, le corps de décomposition $K = k(x_1, \ldots, x_n)$ est aussi égal à $k'(x_1, \ldots, x_n)$ du fait de l'inclusion $k \subseteq k' \subseteq K$; la séparabilité sur k' est conservée puisque les racines $x_1, \ldots, x_n$ sont distinctes).

§ 3. Théorème fondamental de la théorie de Galois.

Soit K une extension galoisienne de k, et $G = \mathrm{Gal}(K,k)$ son groupe de Galois. Il existe une bijection décroissante entre l'ensemble $\mathcal{G}$ des sous-groupes H de G et l'ensemble $\mathcal{K}$ des sous-corps k' de K contenant k. Elle est donnée par les deux applications inverses l'une de l'autre :

$$H \longmapsto k' = \mathrm{Fix}(K,H) = F(H) \quad ; \quad k' \longmapsto \mathrm{Gal}(K,k') = G(k') = H .$$

On a de plus : $\mathrm{Card}\, H = [K : k']$, $i(H) = [k' : k]$. Enfin, le nombre des k-isomorphismes distincts de k' dans K est $[k' : k]$.

(index de H dans G)

Démonstration. La propriété 1 indique que $G \circ F(H) = H \quad \forall H \in \mathcal{G}$, c'est-à-dire que $G \circ F$ est l'identité sur $\mathcal{G}$. La propriété 2 démontre que $F \circ G(k') = k'$, $\forall k' \in \mathcal{K}$, donc que l'application $F \circ G$ est l'identité sur $\mathcal{K}$. Il en résulte aussitôt que F et G sont des bijections inverses l'une de l'autre entre $\mathcal{G}$ et $\mathcal{K}$. Elles sont décroissantes, c'est-à-dire :

$$k' \subseteq k'' \Rightarrow G(k'') \subseteq G(k').$$

(Les k''-automorphismes de K sont en particulier des k'-automorphismes) et :

$$H' \subseteq H'' \Rightarrow F(H'') \subseteq F(H').$$

(Le corps fixe par H'' l'est en particulier par H').

On a de plus $\mathrm{Card}\, H = [K : k']$ puisque K est extension galoisienne de k'. L'index $i(H)$ est égal à $\dfrac{\mathrm{Card}\, G}{\mathrm{Card}\, H} = [K : k] : [K : k'] = [k' : k]$. Enfin cherchons le nombre de k-isomorphismes de k' dans K (injections de k' dans K). Si $\varphi : k' \to k''$ en est une, K est le corps de décomposition de $f(X)$ sur k' et de $f(X) = \varphi(f(X))$ sur k''. D'après le théorème "d'unicité" sur le corps de décomposition (Chap. VII), il existe un isomorphisme $\sigma : K \to K$ qui prolonge φ et qui appartient donc à G. Ainsi, toute injection de k' dans K est la restriction à k' d'un k-isomorphisme σ de K. Inversement, si $\sigma \in G$, la restriction de σ à k' fournit une injection de k' dans K. Cherchons à quelle condition deux éléments σ et σ' de G définissent la même injection de k' dans K. Il faut et il suffit pour cela que $\sigma' \circ \sigma^{-1}$

soit l'identité sur k', donc $\sigma' \circ \sigma^{-1} = h \in H$, ou encore $\sigma' = h\sigma$, $h \in H$, c'est-à-dire que σ et σ' sont équivalents dans G modulo la relation d'équivalence définie par les classes à droite modulo H. Le nombre de ces classes est l'index de H dans G, égal à $\frac{\text{Card } G}{\text{Card } H} = [k' : k]$.

La correspondance bijective entre les sous-corps de K contenant k et les sous-groupes de G permet de traduire en termes de théorie des groupes des propriétés de la théorie des corps. Traitons par exemple le problème suivant :

§ 4. Condition pour que k' soit une extension Galoisienne de k.

Si K est toujours extension galoisienne de k', k' n'est pas toujours une extension galoisienne de k.

Théorème 2. Pour que k' soit une extension galoisienne de k, il faut et il suffit que $H = G(k')$ soit distingué dans G. On a alors :

$$\text{Gal}(k',k) \simeq G/H .$$

Si l'on suppose k' galoisien sur k, le nombre des k-automorphismes de k' est égal à $[k' : k]$, c'est-à-dire au nombre total des k-injections de k' dans K (théorème fondamental). Il en résulte que toute k-injection de k' dans K est un k-automorphisme de k', et par suite que :

(3) $\forall\, \sigma \in G$, on a $\sigma(k') = k'$.

Réciproquement si $\sigma(k') = k'$ pour tout $\sigma \in G$, les k-injections de k' dans K coïncident avec les k-automorphismes de k', qui sont donc en nombre $[k' : k]$ et k' est extension galoisienne de k. Il y a donc équivalence entre les deux propriétés : k' est galoisien sur k et la propriété (3).

Démontrons maintenant l'équivalence entre le propriété (3) et la propriété : $H = G(k')$ est distingué dans G. Supposons (3) et soit $\sigma \in G$, $\tau \in H$; formons $\sigma\tau\sigma^{-1}$ et démontrons que $\sigma\tau\sigma^{-1} \in H$; pour cela nous prenons $c \in k'$; alors $\sigma\tau\sigma^{-1}(c) = \sigma\sigma^{-1}(c) = c$ puisque $\sigma^{-1}(c) \in k'$ d'après (3) et que τ laisse invariants les éléments de k'. Maintenant supposons H distin-

gué dans G et démontrons (3). On a donc : $\sigma\tau\sigma^{-1}(c) = c$ pour tout $c \in k'$, $\tau \in H$, $\sigma \in G$; d'où : $\tau\sigma^{-1}(c) = \sigma^{-1}(c)$, $\forall\, \tau \in H$, de sorte que $\sigma^{-1}(c)$ appartient au corps fixe de H qui est précisément k'. Il en résulte $\sigma^{-1}(k') \subset k'$, $\forall \sigma \in G$, et par suite en prenant σ^{-1}, $\sigma(k') \subseteq k'$. Mais de $\sigma^{-1}(k') \subset k'$ on déduit en appliquant σ, $k' \subseteq \sigma(k')$, d'où $\sigma(k') = k'$.

L'application qui, à $\sigma \in G$, fait correspondre sa restriction à k' est un homomorphisme du groupe G sur le groupe $Gal(k',k)$ dont le noyau est $H = G(k')$. On a donc :

$$Gal(k',k) \simeq {}^{G}/_{H} .$$

Le groupe de Galois de k' sur k est isomorphe au groupe quotient de G par le sous-groupe distingué H.

(On suppose connues du lecteur les définitions de sous-groupe distingué et de groupe quotient, même dans le cas non abélien).

§ 5. Exemples et applications.

Donnons seulement quelques indications qui pourront être développées en travaux dirigés.

1. Groupe de Galois de l'équation $X^4-3 = 0$ sur $\mathbb{Q}$. (Mac-Lane, p. 306). Le polynôme $f(X) = X^4-3$ est irréductible sur $\mathbb{Q}$. Le corps de décomposition est $K = \mathbb{Q}(i,\alpha)$, où $i^2 = -1$, α réel tel que $\alpha^4 = 3$. K est une extension Galoisienne de $\mathbb{Q}$, d'après le théorème récapitulatif du Chap. X, la séparabilité étant assurée du fait que $\mathbb{Q}$ est de caractéristique nulle. On a $[K : \mathbb{Q}] = 8$ et le groupe de Galois $G(K,k)$ est un groupe non abélien d'ordre 8 isomorphe au groupe diédral Δ_4 des symétries du carré. La chaîne de sous-corps :

$$\mathbb{Q} \subset \mathbb{Q}(i) \subset \mathbb{Q}(i, \sqrt{3}) \subset K = \mathbb{Q}(i,\alpha)$$

donne par la bijection du théorème fondamental de la théorie de Galois une chaîne de sous-groupes :

$$G \supset H \supset L \supset \{e\}$$

que l'on précisera.

2. Groupe de Galois $G(F_q, F_p)$. Déjà vu au Chap. VIII sur les corps finis. Son ordre est r si $q = p^r$. F_q est extension galoisienne de F_p définie par le corps de décomposition du polynôme $f(X) = X^{q-1} - 1$ sur F_p, qui est séparable sur F_p (les racines sont toutes distinctes). G est cyclique, donc tous les sous-groupes de G sont cycliques et ils correspondent par la bijection fondamentale de Galois aux sous-corps de F_q, que l'on déterminera.

3. Groupe de Galois d'une équation binôme sur k.

$$X^n - a = 0 \qquad a \in k .$$

Dans bien des cas il est cyclique, donc abélien.

Dans tous les cas, il est résoluble.

Rappeler ou donner la définition d'un groupe résoluble (Voir Cours LESIEUR, Groupes).

4. Equation résoluble par radicaux.

Définition. On dit que l'équation : $f(X) = 0$ est résoluble par radicaux sur k, s'il existe une suite finie d'équations binômes intermédiaires séparables

$$X^{n_o} - a_o = 0, \quad a_o \in k, \quad \text{corps de décomposition } k_1 \text{ sur } k$$
$$X^{n_1} - a_1 = 0, \quad a_1 \in k_1, \quad \text{corps de décomposition } k_2 \text{ sur } k_1$$
$$\vdots$$
$$X^{n_h} - a_h = 0, \quad a_h \in k_h, \quad \text{corps de décomposition } k_{h+1} \text{ sur } k_h$$

telles que : $K \subseteq k_{h+1}$

où K désigne le corps de décomposition de $f(X)$ sur k.

Les racines de $f(X) = 0$ vont alors s'exprimer au moyen d'une suite finie d'opérations rationnelles et d'extractions de racines n^e (c.à.d. de radicaux). On a vu (Cours de C_1) qu'il en est ainsi pour les équations de degré $\leqslant 4$. k_{h+1} n'est pas nécessairement Galoisien sur k, mais on démontre qu'on peut se ramener à ce cas. Alors la suite de corps emboîtés :

$$k \subset k_1 \subset \ldots \subset k_i \subset k_{i+1} \subset \ldots \subset k_{h+1}$$

va donner par la bijection du théorème fondamental de Galois une suite décrois-

sante de sous-groupes

$$G_{h+1} \supset \ldots \supset G_{i+1} \supset G_i \supset \ldots \supset \{e\}.$$

k_{i+1} est une extension Galoisienne de k_i dont le groupe de Galois, d'après le théorème 2, est isomorphe au groupe quotient G_{i+1}/G_i qui est donc résoluble comme groupe de Galois d'une équation binôme. Il en résulte que G_{h+1} est résoluble ; de plus si G est le groupe de Galois de $f(X)$ sur k, l'inclusion $K \subseteq k_{h+1}$ entraîne que $G(K)$ est un sous-groupe distingué dans G_{h+1} (car K est extension galoisienne de k) et, d'après le théorème 2, le groupe de Galois G de K sur k est isomorphe à $G_{h+1}/G(K)$. Or ce groupe est résoluble si G_{h+1} l'est. (Résultats de théorie des groupes à admettre, ou à démontrer en exercices). On a donc un aperçu de la belle propriété suivante qui donne aux travaux originaux de Galois leur plus grande portée.

Théorème 3. Pour qu'une équation séparable $f(X) = 0$ soit résoluble par radicaux sur k , il faut et il suffit que son groupe de Galois $G(f,k)$ soit un groupe résoluble.

5. Equation générale de degré n.

Voir Cours LESIEUR, Nombres algébriques et transcendants pour la définition, ainsi que pour la propriété.

Théorème 4. Si $f(X)$ est l'équation générale de $d^o n$ sur k,

$$f(X) = a_o X^n + a_1 X^{n-1} + \ldots + a_n = 0$$

le groupe de Galois de $f(X)$ sur $k(a_o, a_1, \ldots, a_n)$ (et non pas sur k lui-même !) est le groupe symétrique $\mathcal{S}_n$.

Or on sait (résultat de pure théorie des groupes, pas très difficile à démontrer : voir cours LESIEUR, Groupes, que : le groupe symétrique $\mathcal{S}_n$ n'est pas résoluble pour $n \geqslant 5$, d'où :

Théorème 5. L'équation générale de degré n n'est pas résoluble par radicaux pour $n \geqslant 5$.

Cela n'empêche pas que certaines équations particulières le soient, par exemple $X^5 - a = 0$, $a \in k$. Les cas de résolubilité par radicaux sont justement éclairés par la résolubilité du groupe de Galois correspondant.

CHAPITRE XII

CONSTRUCTIONS AVEC LA REGLE ET LE COMPAS.

§ 1. Ensemble de points $\mathcal{E}(E)$, constructibles à partir de E .

§ 2. Exemples de points constructibles.

§ 3. Nombres réels constructibles.

§ 4. Propriétés des nombres constructibles.

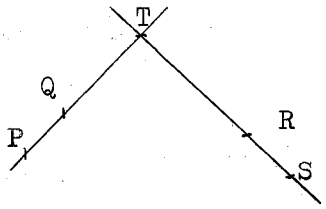
§ 5. Démonstration du théorème 2.

§ 1. Ensemble de points $\mathcal{E}(E)$, constructibles à partir de E .

Problème : à partir d'un ensemble de points, E, donné dans le plan euclidien réel, de règles de construction données, quel ensemble $\mathcal{E}(E)$ peut-on obtenir ?

* Règles de constructions.

1°) Intersection de deux droites :

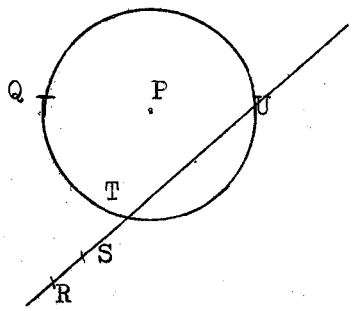


L'intersection des droites (PQ) et (RS), donne un nouveau point T

R, S, P, Q $\in$ E, T $\in \mathcal{E}(E)$

(On considèrera toujours l'intersection de deux droites différentes - c'est-à-dire non confondues-, de manière que la droite entière ne soit pas constructible).

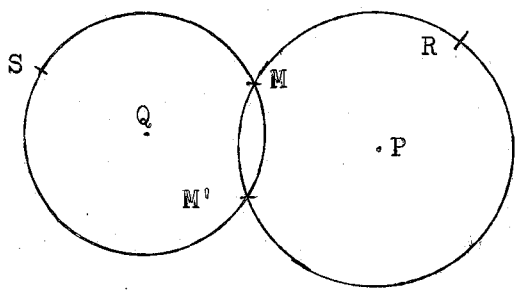
2°) Intersection d'un cercle et d'une droite :



L'intersection de la droite (RS) et du cercle P(PQ) donne deux nouveaux points T et U

R, S, P, Q $\in$ E, T, U $\in \mathcal{E}(E)$.

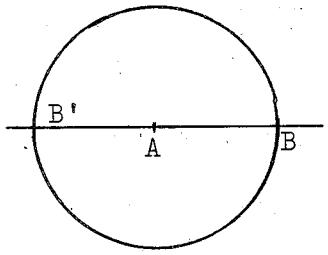
3°) Intersection de deux cercles :



De même, on obtient deux nouveaux points (et deux au plus, car les deux cercles doivent être distincts) en prenant l'intersection des deux cercles P(PR) et Q(QS) où P, Q, R, S ∈ E .

Définition. On appelle $\mathcal{C}_1(E)$ l'ensemble des points constructibles à partir de E en une opération, par une des 3 règles précédentes.

Propriété. Si Card E ⩾ 2 , $E \leqslant \mathcal{C}(E)$



E = {A, B,...}.

La figure montre que l'on obtient le point B par l'intersection du cercle A(AB) et de la droite AB .

Définition. On définit $\mathcal{C}_2(E)$ par $\mathcal{C}_1(\mathcal{C}_1(E))$ (ensemble des points constructibles en deux opérations au plus).

On définit ainsi par récurrence, $\mathcal{C}_n(E) = \mathcal{C}_1(\mathcal{C}_{n-1}(E))$ (points constructibles en n opérations au plus).

Définition. On appelle $\mathcal{C}(E)$: "ensemble des points constructibles à partir de E",

$$\mathcal{C}(E) = \bigcup_{n=1}^{\infty} \mathcal{C}_n(E).$$

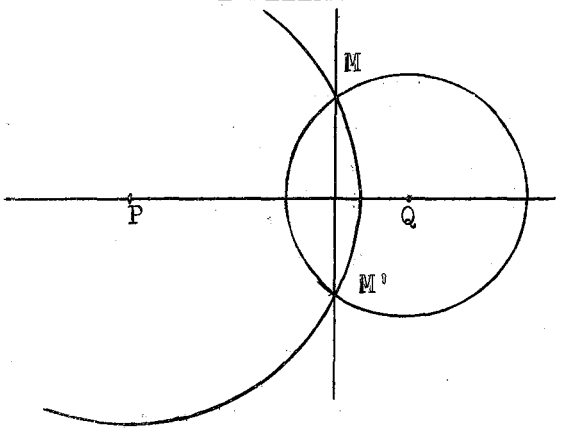
Définition. Soit P , un point. P est "constructible à partir de E ", si $P \in \mathcal{C}(E)$.

Définition. La droite (PQ) est "constructible" si elle joint deux points constructibles mais cela ne veut pas dire que tous les points de la droite sont constructibles.

§ 2. Exemples de points constructibles.

(A) La perpendiculaire à une droite constructible passant par un point donné est constructible.

α) M ∉ (PQ)



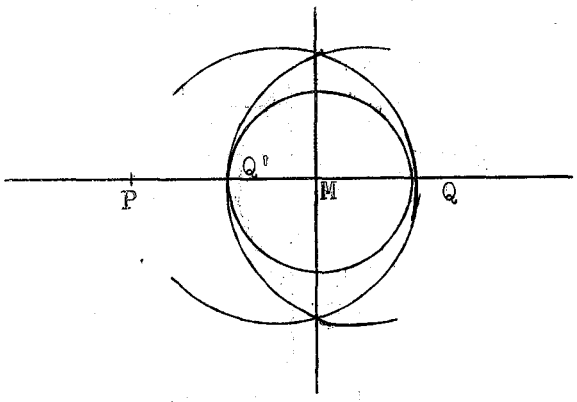
1°) On trace Q(QM)

2°) " " P(PM)

M' est le deuxième point d'intersection de ces deux cercles :

alors la droite (MM') est la perpendiculaire à (PQ).

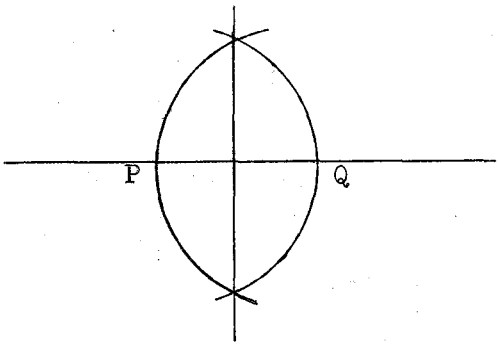
β) M ∈ (PQ)



1°) On trace M(MQ) et on obtient le symétrique Q' de Q par rapport à M .

2°) On trace Q(QQ') et Q'(QQ') ; leurs points d'intersection déterminant la perpendiculaire cherchée.

(B) La médiatrice d'un segment est constructible.

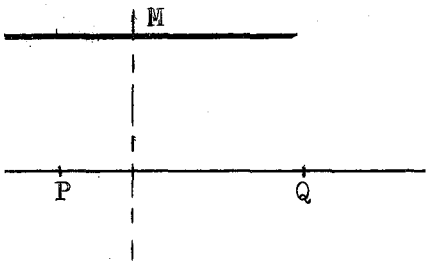


1°) On trace P(PQ)

2°) " " Q(PQ)

L'intersection de ces deux cercles définit la médiatrice de (PQ)

(C) La parallèle à une droite donnée constructible, passant par un point donné est constructible.



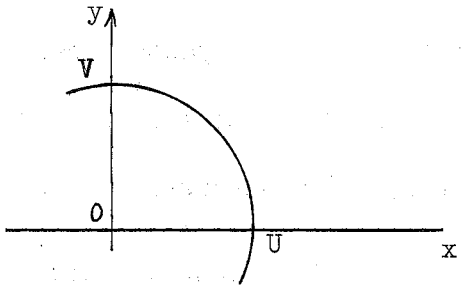
1°) On construit la perpendiculaire à (PQ) passant par M (voir, plus haut)

2°) On construit celle passant par M . C'est la droite cherchée.

§ 3. Nombres réels constructibles.

On s'intéresse maintenant à $E = \{0,U\}$, et à $\mathcal{E}(E)$.

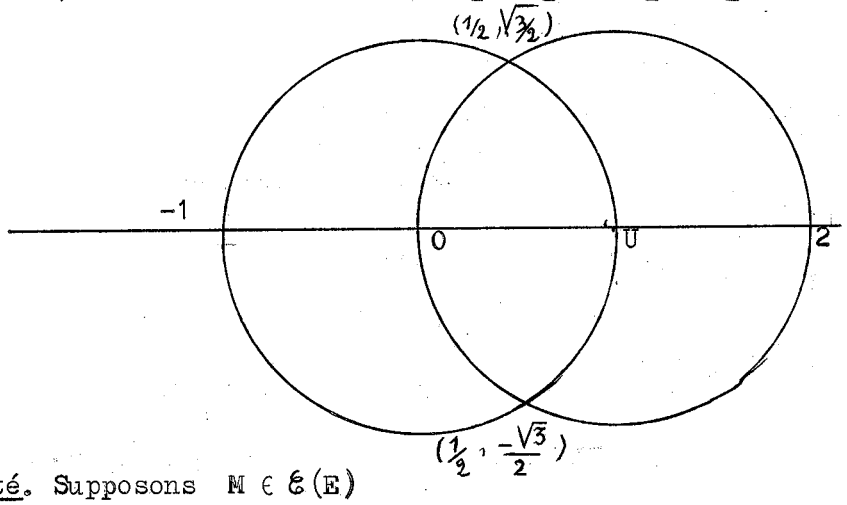
Pour représenter $\mathcal{E}(E)$, on construit un repère orthonormé OU, OV dans le plan euclidien réel, isomorphe à $\mathbb{R}^2$. Un point M constructible sera représenté par ses coordonnées x,y dans le repère OU, OV.



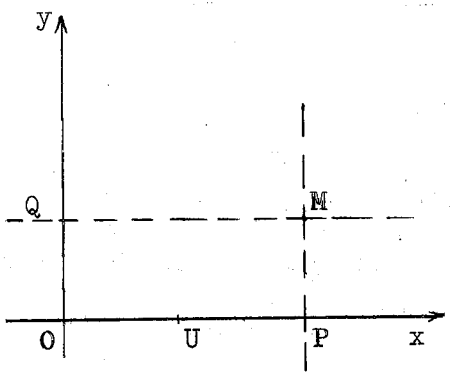
. V est constructible

- On construit la perpendiculaire à (OU) passant par 0
- On construit le cercle O(OU), et V est l'intersection

$$\mathcal{E}_1(E) = \{0 \ ; \ 1 \ ; \ 2 \ ; \ -1 \ ; \ (\tfrac{1}{2} \ , \ \tfrac{\sqrt{3}}{2}) \ ; \ (\tfrac{1}{2} \ , \ \tfrac{-\sqrt{3}}{2})\}$$



Propriété. Supposons $M \in \mathcal{E}(E)$



Alors $P \in \mathcal{E}(E)$

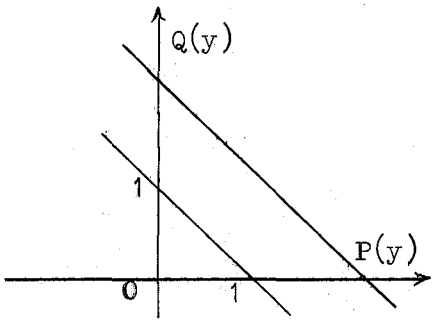
et $Q \in \mathcal{E}(E)$

(On trace la perpendiculaire à (OU) passant par M, puis celle à (OQ) passant par M)

. Réciproquement, si P et $Q \in \mathcal{E}(E)$, $M \in \mathcal{E}(E)$.

Définition. $x \in \mathbb{R}$ est un nombre constructible si le point $M \in Ox$, d'abscisse x est constructible.

Remarque : si $Q(y)$ est constructible $\Rightarrow$ y est constructible



. On trace V

. On trace (UV)

. puis la parallèle à (UV) passant par $Q(y)$

. le point $P(y)$ est intersection de Ox et de $(Q(y)P(y))$. Son abscisse est y .

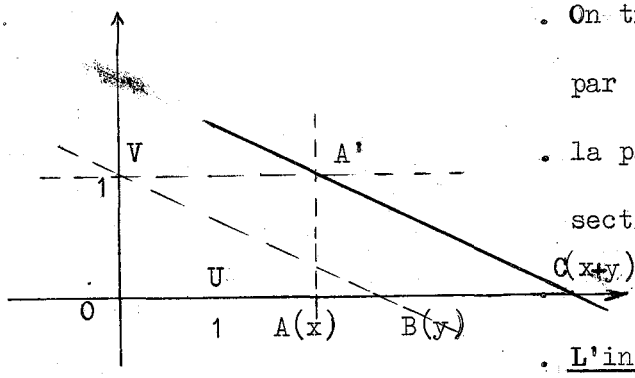
Définition. On appelle K , l'ensemble des points de $\mathbb{R}$ constructibles à partir de $\{0,U\}$.

Propriété. $M(x,y) \in \mathcal{C}(E) \iff x$ et $y \in K$.

(On trace par $M(x,y)$ les parallèles à Oy et Ox).

Théorème 1. $\begin{cases} K \text{ est un corps} \\ \mathbb{Q} \subsetneq K \subsetneq \mathbb{R} \end{cases}$

Démonstration : 1°) $x \in K, y \in K, \Rightarrow x+y \in K$



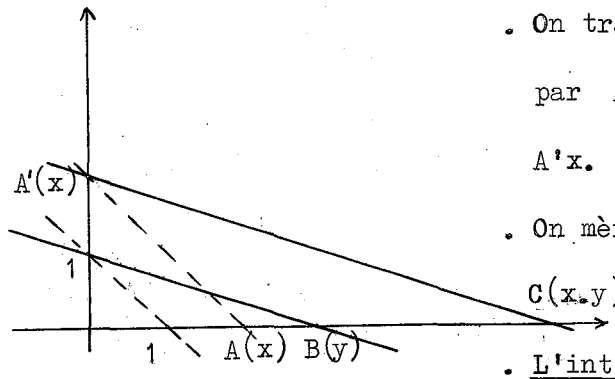
. On trace la perpendiculaire à Ox passant par $A(x)$

. la parallèle à Ox passant par U . L'intersection de ces deux droites est A' . Par A', on mène la parallèle à (V $B(y)$).

. L'intersection avec Ox est $C(x+y)$.

donc $x+y \in K$.

2°) $x \in K, y \in K, \Rightarrow x.y \in K$

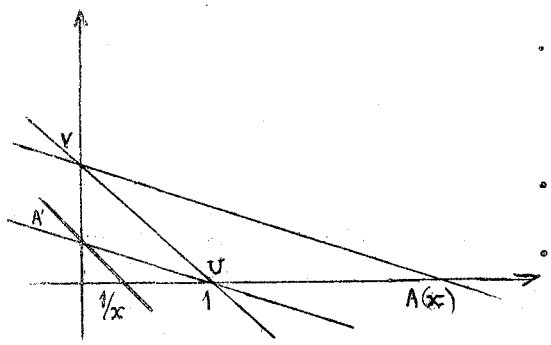


. On trace (UV) et la parallèle passant par Ax . L'intersection avec Oy donne A'x.

. On mène (V By) et la parallèle passant par A'x .

. L'intersection avec Ox donne $x.y$.

3°) Si $x \neq 0$, $\frac{1}{x} \in K$



. (V A(x)) et sa parallèle passant par U qui coupe Oy en A'

. (VU) et sa parallèle passant par A'

. L'intersection avec Ox donne $^1/_x$.

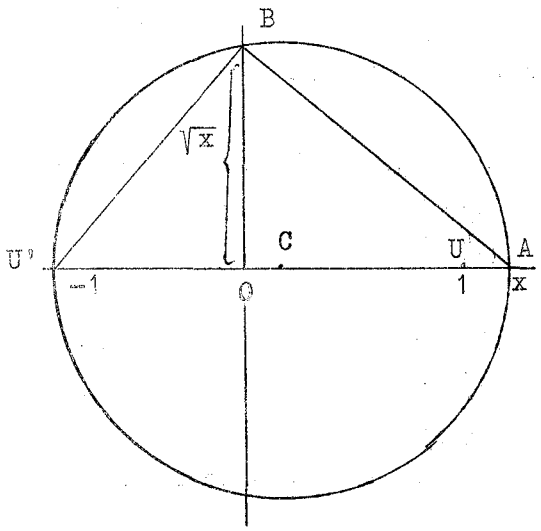
$\mathbb{Q} \not\subset K$, * . Le plus petit sous corps de $\mathbb{R}$ est $\mathbb{Q}$ donc $\mathbb{Q} \subset K$ ou : $\{0,1\} \subset K \Rightarrow \forall p \in \mathbb{N}$, $p \in K$ (translation) comme K est un corps, $\frac{1}{p} \in K$, donc $\frac{q}{p} \in K$ et $\mathbb{Q} \subset \mathbb{R}$.

$\mathbb{Q} \neq \mathbb{R}$, car $A(\sqrt{3}) \in \mathcal{C}(E)$ et $\sqrt{3} \notin \mathbb{Q}$ (voir plus haut)

$K \subset \mathbb{R}$ (évident). On verra que $K \not\subset \mathbb{R}$.

§ 4. Propriétés des nombres constructibles.

Si $x \in K$: $\sqrt{x} \in K$
$x > 0$



. On trace C , milieu de $[-1,x]$.

. C(Cx)

. La perpendiculaire à Ox passant par O : A l'intersection avec C(Cx)

. $OB = y = \sqrt{x}$.

En effet :

. Les triangles (AOB) et (BOU') sont semblables donc $\frac{x}{y} = \frac{y}{1} \Rightarrow x = y^2$.

Théorème 2. Propriété caractéristique d'un nombre constructible.

$x \in \mathbb{R}$: $x \in K \Leftrightarrow (\exists\, \alpha_1, \ldots, \alpha_n \in \mathbb{R} \mid \alpha_1^2 \in \mathbb{Q}, \ldots, \alpha_n^2 \in \mathbb{Q}(\alpha_1 \ldots \alpha_{n-1}))$

et $x \in \mathbb{Q}(\alpha_1, \alpha_2 \ldots \alpha_n)$

(i.e. $\mathbb{Q} \subset k_1 \subset \ldots \subset k_{n-1} \subset k_n$ et $k_1 = \mathbb{Q}(\alpha_1)$, $k_2 = \mathbb{Q}(\alpha_1, \alpha_2)$ ... $x \in k_n$ où k_i est une extension quadratique de k_{i-1} (on néglige les extensions triviales)).

Corollaire. Si $x \in K$, x est algébrique sur $\mathbb{Q}$, et $[\mathbb{Q}(x) : \mathbb{Q}] = 2^q$

évident d'après le théorème 2.

Applications.

1°) La quadrature du cercle

Est-il possible de construire un carré ayant même surface que le cercle unité ?

Soit x le côté du carré : on a alors

$$x^2 = \pi \qquad (\pi R^2 \text{ où } R = 1)$$

$$x = \sqrt{\pi} .$$

Si $x \in K$, $x^2 \in K$, et x^2 est algébrique sur $\mathbb{Q}$. Or, π est transcendant sur $\mathbb{Q}$ (Cours de M. LESIEUR, C 1, Orsay, et travaux de LINDEMANN), donc $x \notin K$. Donc $K \neq \mathbb{R}$.

2°) Duplication du cube

Peut-on construire un cube ayant un volume double du cube unité ?

Soit x son arête.

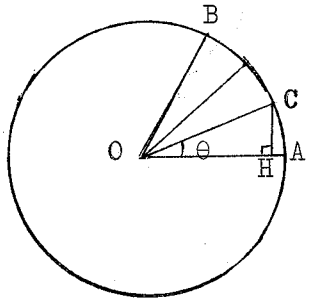
Alors $x^3 - 2 = 0$, donc x est algébrique sur $\mathbb{Q}$.

Comme $x^3 - 2$ est irréductible sur $\mathbb{Q}$,

$$[\mathbb{Q}(x) : \mathbb{Q}] = 3$$

donc x n'est pas constructible puisque $3 \neq 2^q$.

3°) Trisection de l'angle.



$$\theta = \frac{\pi}{9} = 20°$$

C constructible $\iff$ H constructible

H constructible $\iff$ $\overline{OH} \in K$

$\overline{OH} = \cos\theta = x$. $\cos 3\theta = \frac{1}{2}$

$\cos 3\theta = 4\cos^3\theta - 3\cos\theta = \frac{1}{2}$

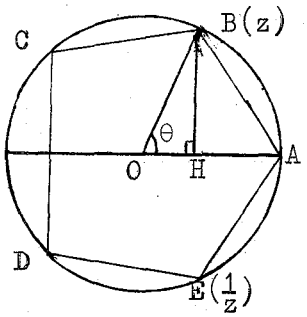
$$4x^3 - 3x - \frac{1}{2} = 0 \iff 8x^2 - 6x - 1 = 0 .$$

Posons $2x = y$ ($x \in K \iff y \in K$), $y^3 - 3y - 1 = 0$. Ce polynôme est irréductible sur $\mathbb{Q}$, n'ayant pas de racine rationnelle. Donc $[\mathbb{Q}(y) : \mathbb{Q}] = 3$, $3 \neq 2^m$.

Donc $y \notin K$ et $x \notin K$.

Impossibilité de la trisection de l'angle de 60° à la règle et au compas.

4°) Construction du pentagone régulier.



B est d'affixe z . $\theta = \frac{2\pi}{5}$, $|z| = 1$ donc $z = e^{\frac{2i\pi}{5}}$ et $z^5 - 1 = 0$, $\overline{OH} = \text{Cos } \theta$, $z + \frac{1}{z} = 2 \text{ Cos } \theta = y$.

B constructible $\Leftrightarrow$ H constructible

H constructible $\Leftrightarrow$ Cos $\theta \in K \Leftrightarrow y \in K$.

$z^5 - 1 = (z-1)(z^4 + z^3 + z^2 + z + 1) = 0$, $z \neq 1$ car z est l'affixe de B .

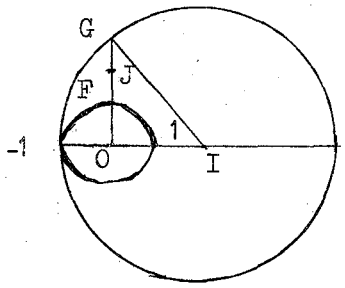
z est donc racine du polynôme cyclotomique $P_5(X)$ irréductible sur $\mathbb{Q}$

$$z^4 + z^3 + z^2 + z + 1 = 0$$

$$z^2 + z + 1 + \frac{1}{z} + \frac{1}{z^2} = 0 \qquad y = z + \frac{1}{z}$$

$y^2 + y - 1 = 0$. L'abscisse de H étant positive on obtient $y = \frac{-1 + \sqrt{5}}{2}$.

Montrons que $y \in K$.



Le rayon du grand cercle est 3 .

$\overline{OI} = 2$, $OG^2 = IG^2 - IO^2 = 9-4 = 5$.

Donc $\overline{OG} = \sqrt{5}$, $\overline{FG} = -1 + \sqrt{5}$.

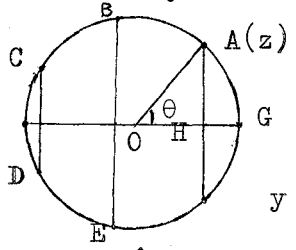
Soit J le milieu de FG ; $\overline{JG} = \frac{-1 + \sqrt{5}}{2}$

Donc $\overline{JG} = y = 2 \text{ Cos } \theta = 2\,\overline{OH} = \overline{OH'}$

$y \in K$ C.Q.F.D.

5°) Construction du polygone régulier de 7 côtés.

Soit A d'affixe $z = e^{\frac{2i\pi}{7}}$, $\theta = \frac{2i\pi}{7}$, $z^7 - 1 = 0$. $y = z + \frac{1}{z} = 2\,\overline{OH}$ $= 2 \text{ Cos } \theta$. z est racine du polynôme cyclotomique $P_7(X)$ irréductible sur $\mathbb{Q}$



$$z^6 + z^5 + z^4 + z^3 + z^2 + z + 1 = 0$$

$$z^3 + z^2 + z + 1 + \frac{1}{z} + \frac{1}{z^2} + \frac{1}{z^3} = 0$$

$y = z + \frac{1}{z}$ $\qquad y^3 + y^2 - 2y - 1 = 0$.

Ce polynôme n'ayant pas de racine rationnelle est irréductible sur $\mathbb{Q}$.

Donc $[\mathbb{Q}(y) : \mathbb{Q}] = 3$. $3 \neq 2^m$. Donc $y \notin K$ et A n'est pas constructible.

Le polygone régulier de 7 côtés n'est pas constructible à la règle et au compas.

§ 5. Démonstration du théorème 2.

$x \in K \iff$ (1) $\exists\ \alpha_1, \alpha_2 \ldots \alpha_n,\ \alpha_1^2 \in \mathbb{Q},\ \alpha_2^2 \in \mathbb{Q}(\alpha_1), \ldots,\ \alpha_n^2 \in \mathbb{Q}(\alpha_1, \ldots, \alpha_n)$

avec $\mathbb{Q} \subset \mathbb{Q}(\alpha_1) \subset \ldots \subset \mathbb{Q}(\alpha_1, \alpha_2, \ldots, \alpha_{n-1}) \subset \mathbb{Q}(\alpha_1, \ldots \alpha_n)$ et $x \in \mathbb{Q}(\alpha_1, \alpha_2, \ldots \alpha_n)$.

On peut dire également

(1') $\exists\ k_1, k_2, \ldots, k_n$

avec $k_o = \mathbb{Q} \subset k_1 \subset k_2 \subset \ldots \subset k_n$ avec $[k_i : k_{i-1}] = 2$ et $x \in k_n$. k_n est une extension de $\mathbb{Q}$ par racines carrées. (Nombre fini d'extensions quadratiques).

Condition suffisante. $x \in k_n = \mathbb{Q}(\alpha_1, \alpha_2, \ldots, \alpha_n) \Rightarrow x \in K$?

Faisons une récurrence sur n .

$n = 1 \quad \exists\ \alpha_1\ ,\ \alpha_1^2 \in \mathbb{Q}$ et $x \in \mathbb{Q}(\alpha_1)$

$(1, \alpha_1)$ est une base de $\mathbb{Q}(\alpha_1)$ donc $x = u\alpha_1 + v \qquad u, v \in \mathbb{Q}$.

$\alpha_1^2 = r \in \mathbb{Q}$. Donc $\alpha_1 = \sqrt{r}$ et $\alpha_1 \in K$. Donc $x \in K$ C.Q.F.D.

Passage de n-1 à n . Hypothèse : $x \in k_{n-1} \Rightarrow x \in K$.

$x \in k_n$, $\exists\ \alpha_1, \ldots, \alpha_n$, $\alpha_n^2 = c \in \mathbb{Q}(\alpha_1, \ldots, \alpha_{n-1}) = k_{n-1}$,

$x \in k_{n-1}(\alpha_n)$. Donc $x = u\,\alpha_n + v \qquad u, v \in k_{n-1}$,

$\alpha_n^2 = c \in k_{n-1} \Rightarrow c \in K$ (hypothèse de récurrence) et donc $\sqrt{c} \in K$

$u, v \in k_{n-1} \Rightarrow u, v \in K$ (" " ")

Donc $x = u\alpha_n + v \in K$ C.Q.F.D.

Condition nécessaire.

Lemme. K_1 et K_2 étant des extensions de $\mathbb{Q}$ par racines carrées, il en est de même du corps engendré par K_1 et K_2 soit $(K_1 \vee K_2)$

$K_1 = \mathbb{Q}(\alpha_1, \alpha_2, \ldots, \alpha_n) \qquad K_2 = \mathbb{Q}(\beta_1, \beta_2, \ldots \beta_m)$

$(K_1 \vee K_2) = \mathbb{Q}(\alpha_1, \alpha_2, \ldots, \alpha_n, \beta_1, \beta_2, \ldots, \beta_m)$

$\alpha_1^2 \in \mathbb{Q}$; $\alpha_2^2 \in \mathbb{Q}(\alpha_1)$ ... ; $\alpha_n^2 \in \mathbb{Q}(\alpha_1, \alpha_2, \ldots, \alpha_{n-1})$

$\beta_1^2 \in \mathbb{Q}$ mais également $\beta_1^2 \in \mathbb{Q}(\alpha_1, \alpha_2 \ldots \alpha_n)$

$\beta_2^2 \in \mathbb{Q}(\beta_1)$ " " $\beta_2^2 \in \mathbb{Q}(\alpha_1, \ldots, \alpha_n, \beta_1)$

$\vdots$

$\beta_m^2 \in \mathbb{Q}(\beta_1 \ldots \beta_{m-1})$ mais aussi $\beta_m^2 \in \mathbb{Q}(\alpha_1 \ldots \alpha_n, \beta_1 \ldots \beta_{m-1})$

$K_1 \cup K_2$ est donc obtenu par extension de $\mathbb{Q}$ par racines carrées C.Q.F.D.

Preuve de la condition nécessaire du théorème.

Soit $x \in K$. Soit M de coordonnées (x,y) $y \in K$

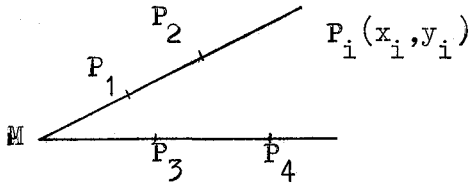
$M \in C_n(E) \iff$ M est constructible au moyen d'un nombre fini n d'opérations.

Faisons une récurrence sur n .

n = 1. Nous avons vu que les points M avaient alors des abscisses dans $\mathbb{Q}(\sqrt{3})$. On a $\mathbb{Q} \subset \mathbb{Q}(\sqrt{3})$ et $3 \in \mathbb{Q}$ et $x \in \mathbb{Q}(\sqrt{3})$ C.Q.F.D.

Passage de n-1 à n $M \in C_n(E) = C(C_{n-1}(E))$. M se construit alors de 3 façons possibles.

(1) Intersection de deux droites



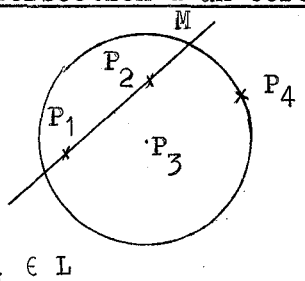
L'hypothèse de récurrence s'applique aux (x_i,y_i) qui sont donc dans des corps ayant la propriété (1'). Soit K_i ces corps $(x_i,y_i) \in K_i$. Considérons alors le corps $L = K_1 \vee K_2 \vee K_3 \vee K_4$. D'après le lemme il vérifie aussi (1'). Ecrivons que M est l'intersection des deux droites $\frac{y-y_1}{x-x_1} = \frac{y_2-y_1}{x_2-x_1}$ droite $(P_1\ P_2)$. $P_1\ P_2$ est donc de la forme $y = ax + b$ $a, b \in L$

de même $P_3\ P_4$ est de la forme $y = a'x + b'$ $a', b' \in L$

$$ax + b = a'x + b' \quad \text{et donc} \quad x = \frac{b'-b}{a-a'} \in L .$$

Donc x est dans un corps obtenu par extensions quadratiques successives C.Q.F.D.

(2) Intersection d'un cercle et d'une droite



La droite $P_1\ P_2$ a pour équation $y = ax+b$, $a, b \in L$. Le cercle de centre P_3 et de rayon $P_3\ P_4$ a pour équation :

$x_i\ y_i \in L$

$(x-x_3)^2 + (y-y_3)^2 = (x_4-x_3)^2 + (y_4-y_3)^2$ ou $x^2+y^2 + a'x + b'y + c' = 0$

a', b', $c' \in L$, $x_i y_i \in L$.

M vérifie donc l'équation suivante (l'abscisse de M)

$$x^2 + (ax+b)^2 + a'x + b'(ax+b) + c' = 0$$

ou $$ux^2 + vx + w = 0 \qquad u, v, w \in L .$$

Donc x est de la forme $\alpha+y$ avec $y^2 \in L$

$$x \in L(y) = Q(\alpha_1, \alpha_2, \ldots, \alpha_n, y) \qquad [L(y) : L] \leqslant 2$$

x est dans un corps ayant la propriété (1').

(3) Intersection de deux cercles.

C_1 d'équation $x^2 + y^2 + ax + by + c = 0$ $\qquad a, b, c \in L$

C_2 d'équation $x^2 + y^2 + a'x + b'y + c' = 0$ $\qquad a', b', c' \in L .$

M est situé sur Δ droite joignant les deux points d'intersection.

Δ a pour équation $(a'-a)x + (b'-b)y + (c'-c) = 0$, coefficients dans L

M est donc obtenu à partir de C_1 et Δ par exemple,

et on se ramène au cas (2).

Le théorème est démontré.

CHAPITRE XIII

POLYGONES REGULIERS

§ 1. Condition suffisante de constructibilité d'un nombre réel.

§ 2. Généralités sur la construction d'un polygône régulier de n côtés.

§ 3. Réduction au cas $n = p^2$.

§ 4. Théorème récapitulatif (Gauss).

§ 1. Condition suffisante de constructibilité d'un nombre réel.

Lemme 1. Soit L une extension galoisienne réelle de $\mathbb{Q}$.

$[L : \mathbb{Q}] = 2^n$, $x \in L \Rightarrow x$ est constructible. i.e. $L \subseteq K$.

Démonstration. Récurrence sur n .

Si $n = 1$ $[L : \mathbb{Q}] = 2$. Donc $L = \mathbb{Q}(\alpha_1)$ avec $\alpha_1^2 \in \mathbb{Q}$ et $\alpha_1 \in \mathbb{R}$ puisque L est réelle. Donc $\alpha_1 \in K$ (théorème 2 du chapitre XII). Donc $L \subseteq K$.

On suppose le lemme démontré jusqu'à $n-1$. Soit L telle que $[L : \mathbb{Q}] = 2^n$. L est galoisienne sur $\mathbb{Q} \Rightarrow$ Card $G = 2^n$, $G = \mathrm{Gal}(L,\mathbb{Q})$. Donc $\exists\, g \in G$ tel que $g^2 = e$ et $g \in Z(G)$ = centre de G . $S = \{e,g\}$ est un sous-groupe d'ordre 2 de G. Soit $k_{n-1} = \mathrm{Fix}(L,S)$. $\mathbb{Q} \subset k_{n-1} \subset L$. $[L : k_{n-1}] = O(S) = 2 \Rightarrow [k_{n-1} : \mathbb{Q}] = 2^{n-1}$ et S est distingué dans G car

$$\forall g \in S\ ,\ \forall \sigma \in G\ ,\ \sigma g \sigma^{-1} = \sigma\sigma^{-1} g \quad \text{car} \quad g \in Z(G)$$

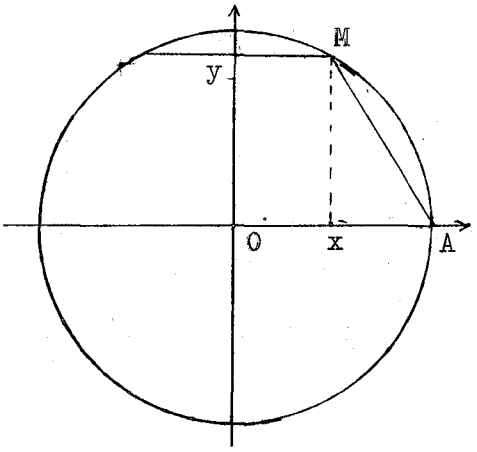
$$\sigma g \sigma^{-1} = g \in S\ .$$

Donc k_{n-1} est une extension galoisienne réelle de $\mathbb{Q}$. Alors, d'après l'hypothèse de récurrence, $k_{n-1} \subseteq K$. Or $L = k_{n-1}(\alpha)$ est une extension quadratique de k_{n-1}

$$\alpha^2 \in k_{n-1}\ ,\ \alpha \in \mathbb{R}\ .$$

Donc $\alpha \in K$ et $L \subseteq K$. Le lemme est démontré.

§ 2. Généralités sur la construction d'un polygone régulier de n côtés.



On dira que n convient ou $n \in C$ si le polygone régulier à n côtés est constructible avec la règle et le compas.

Exemples : $5 \in C$, $7 \notin C$ (voir Chap. XII).

Remarque : la construction du polygone revient à celle du point M d'affixe $z = e^{2i\pi/n}$, $z^n - 1 = 0$.

Soit $z = x + iy$. M constructible $\iff$ z constructible $\iff$ x et y constructibles. Or M $\in$ au cercle (O, OA) qui est constructible.

Donc M constructible $\iff$ x ou y constructible.

$x, y \in K \implies z = x + iy \in K' \subset \mathbb{C}$. K' est un corps.

K' est le corps des nombres complexes constructibles.

§ 3. Réduction au cas $n = p^2$.

Lemme 2. $n \in C$, $m \mid n \implies m \in C$.

Démonstration. Soit $n = md$.

Le polygone régulier à n côtés étant construit on peut joindre les sommets d à d .

Le premier sommet obtenu aura pour affixe

$$z = e^{2i\pi d/n} = 2\, e^{2i\pi/m} .$$

On obtient donc ainsi le polygone régulier à m côtés.

Lemme 3. $n \in C$, $n' \in C$, $(n,n') = 1 \implies nn' \in C$.

Démonstration. $(n,n') = 1 \implies \exists\, a, b \in \mathbb{Z}$ tels que $na + n'b = 1$.

Soit $\frac{1}{nn'} = \frac{a}{n'} + \frac{b}{n}$. $n \in C$, donc on sait construire l'angle $\frac{2\pi}{n}$. Donc en la reportant b fois, on sait construire l'angle $b\,\frac{2\pi}{n}$. De même $n' \in C \implies$ on sait construire l'angle $a\,\frac{2\pi}{n'}$. Donc on peut construire l'angle $a\,\frac{2\pi}{n'} + b\,\frac{2\pi}{n} = \frac{2\pi}{nn'}$. Donc le polygone régulier à nn' côtés est constructible

et $nn' \in C$.

Démonstration algébrique.

Le premier sommet du polygone régulier à n côtés a pour affixe $\alpha = e^{2i\pi/n}$. α est une racine primitive $n^{\text{ième}}$ de l'unité. Donc α engendre un groupe cyclique d'ordre n . De même β , affixe du premier sommet de polygone régulier à n' côtés engendre un groupe cyclique d'ordre n' .

$(n,n') = 1 \Rightarrow$ le produit de ces 2 groupes cycliques est un groupe cyclique d'ordre nn' . De plus, si $an + bn' = 1$, un générateur du groupe produit est

$$\gamma = \alpha^b \beta^c .$$

Or $\alpha \in K'$, $\beta \in K'$ et K' est un corps donc $\gamma \in K' \Rightarrow nn' \in C$.

Application. $n = \pi\, p_i^{\alpha_i}$.

$$n \in C \iff \forall i \ , \ p_i^{\alpha_i} \in C .$$

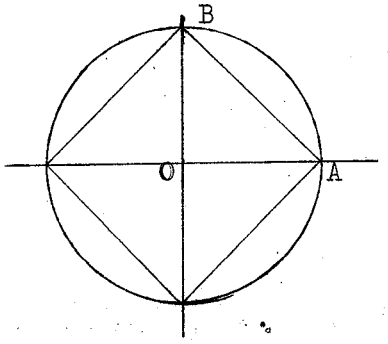
Démonstration.

($\Rightarrow$). Lemme 2 $\quad p_i^{\alpha_i} | n$

($\Leftarrow$). Lemme 3 + récurrence sur le produit.

Lemme 4. $\forall \alpha \in \mathbb{N} \ , \ 2^\alpha \in C$.

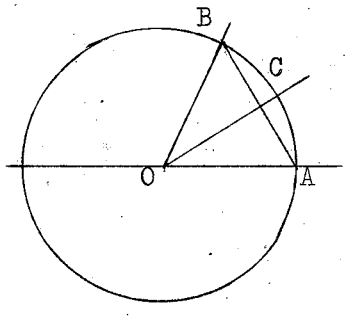
Récurrence sur α .



$\alpha = 2$. B est constructible

Le carré inscrit dans le cercle est constructible $2^2 \in C$.

Passage de $\alpha-1$ à α .



Soit B le premier sommet du polygone régulier à $2^{\alpha-1}$ côtés. OC, médiatrice de AB , est constructible. Le polygone régulier ayant C pour 1er sommet a

$$2 \times 2^{\alpha-1} = 2^\alpha \text{ côtés.}$$

Donc $2^\alpha \in C$, $\forall \alpha \in \mathbb{N}$.

Théorème 1. (Gauss). Soit p premier $\neq 2$.

1°) $p^m \notin C$, si $m \geqslant 2$.

2°) $p \in C \iff p = 1 + 2^{2^n}$.

Démonstration. Soit z l'affixe du premier sommet du polygone régulier à n côtés. Si z est constructible, $z = x+iy$, x et $y \in K$. Donc x et $y \in k$ provenant de $\mathbb{Q}$ par extensions finies des racines carrées. i est racine de $X^2 + 1 = 0$. Donc $k(i)$ est une extension quadratique de k et $[k(i) : \mathbb{Q}] = 2^h$ or $z \in k(i) \implies \mathbb{Q}(z) \subset k(i) \implies [\mathbb{Q}(z) : \mathbb{Q}] = 2^r$.

Soit $n = p$ premier différent de 2. z est racine de $z^p - 1 = 0$

$X^p - 1 = (X-1)(X^{p-1} + \ldots + X+1)$

$X^{p-1} + \ldots + X + 1$ est irréductible sur $\mathbb{Q}$.

Donc le polynôme minimal de z est $X^{p-1} + \ldots + X + 1$.

Soit $n = p^2$. $X^{p^2} - 1 = (X^p)^p - 1 = (X^p - 1)(X^{p(p-1)} + \ldots + X^p + 1)$

$= (X^p - 1)\, g(X)$.

z étant une racine primitive $p^{2\text{ième}}$ de l'unité, $0(z) = p^2$. Donc $z^p \neq 1$ et $g(z) = 0$.

Soit $X = 1+t$

$$(1+t)^{p^2} - 1 = ((1+t)^p - 1)g(t)$$

$$t^{p^2} + p\,H(t) = [t^p + p\,K(t)]\, g(t) .$$

Soit en faisant la division

$$g(t) = t^{p(p-1)} + p\,L(t).$$

D'autre part le terme constant de $g(t)$ est p . Donc d'après le critère d'Eisenstein. $g(t)$ est irréductible sur $\mathbb{Q}$. Donc $g(X)$ est irréductible sur $\mathbb{Q}$. Donc le polynôme minimal de z est $g(X)$.

Application à la démonstration du théorème.

Supposons que $p^m \in C$ avec $m \geqslant 2$. $p^2 \mid p^m$. Donc d'après le lemme 2, $p^2 \in C$. D'après ce qui précède, le degré du polynôme minimal de z , affixe du premier sommet du polygone régulier à p^2 côtés est alors $p(p-1)$ et $[\mathbb{Q}(z) : \mathbb{Q}] = 2^r$.

Donc $p(p-1) = 2^r$. Or p est premier différent de 2, donc c'est impossible.

Donc $p^m \notin C$ si $m \geqslant 2$.

Supposons que $p \in C$. Le polynôme minimal de z $X^{p-1} + \ldots + X + 1$ et $[\mathbb{Q}(z) : \mathbb{Q}] = 2^r$. Donc $p-1 = 2^r$

$$p = 1 + 2^r .$$

D'autre part si p est premier et $p = 1+2^r$, alors $r = 2^n$; en effet si $r \neq 2^n$ $r = ab$ avec a impair

$$p = 1 + (2^b)^a$$

$$p = (1+2^b)(2^{b(a-1)} - 2^{b(a-2)} + \ldots + 1)$$

avec $1 + 2^b > 1$ et $1 + 2^b < 1 + 2^{ab}$ ce qui est impossible car p est premier.

Donc si $p \in C$

$$p = 1 + 2^{2^n} .$$

Montrons que la condition est suffisante. p premier - $p = 1 + 2^r$.

z affixe du premier sommet du polygone régulier à p côtés.

z est une racine primitive $p^{\text{ième}}$ de l'unité.

Son polynôme minimal est $X^{p-1} + \ldots + X + 1$. Donc $[\mathbb{Q}(z) : \mathbb{Q}] = p-1$. Donc $[\mathbb{Q}(z) : \mathbb{Q}] = 2^r$. Soit $z = x + iy$, $z \in K' \iff x \in K$

$$x = \frac{z+1/z}{2} \in \mathbb{Q}(z) \quad \text{et} \quad x \in \mathbb{R} .$$

Donc $x \in k = \mathbb{Q}(z) \cap \mathbb{R}$. D'autre part $\mathbb{Q}(z)$ est le corps de décomposition de $X^{p-1} + \ldots + X + 1$ sur $\mathbb{Q}$. Donc c'est une extension galoisienne de $\mathbb{Q}$. Soit $G = \mathrm{Gal}(\mathbb{Q}(z), \mathbb{Q})$. G est commutatif, cyclique d'ordre 2^r . $\mathrm{Gal}(k,\mathbb{Q})$ est un sous-groupe de G commutatif, donc distingué . Donc k est une extension galoisienne réelle de $\mathbb{Q}$. Son degré divise 2^r donc est une puissance de 2. Alors d'après le lemme 1, $x \in k \Rightarrow x \in K$. Donc le polynôme régulier à p côtés est constructible. Le théorème est démontré.

§ 4. Théorème récapitulatif (Gauss).

$n \in C \iff n = 2^\alpha p_1 \ldots p_r$ avec $p_i \neq p_j$ si $i \neq j$ et p_i premier $1 + 2^{2^n}$, $\forall i = 1, \ldots, r$.

Définition. Un nombre de Fermat est un nombre de la forme $F_n = 1 + 2^{2^n}$.

Fermat avait conjecturé en 1640 que ces nombres étaient premiers. Euler a donné en 1732 un nombre de Fermat non premier (F_n pour $n = 5$).

On étudiera en application des résultats précédents la constructibilité des polygones réguliers de n côtés pour $n < 20$. En particulier, le polygone régulier de 17 côtés est constructible. Sa construction effective avec la règle et le compas est un problème de géométrie que nous ne traiterons pas ici.

APPENDICE AUX CHAPITRES XII ET XIII

Application de la théorie de Galois à une condition nécessaire et suffisante de constructibilité.

Théorème. Pour que x soit constructible, il faut et il suffit que le corps K de décomposition du polynôme minimal $P(X)$ de x sur $\mathbb{Q}$ ait pour degré une puissance de 2 :

$$[K : \mathbb{Q}] = 2^q .$$

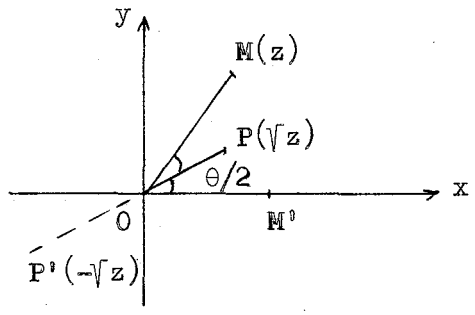
Rappel : Le corps K' des nombres complexes constructibles est :

$$K' = \{z = x+iy \mid x, y \in K\} .$$

On a pour K' un lemme analogue à celui du cas réel :

Lemme. $z \in K' \implies \sqrt{z} \in K'$.

La démonstration repose sur la construction du point $P(\sqrt{z})$ à partir de $M(z)$.



Si $z = re^{i\theta}$, on a $\sqrt{z} = \pm \rho\, e^{\frac{i\theta}{2}}$ avec $\rho = \sqrt{r}$. Or $r = \sqrt{x^2+y^2}$ est constructible réel, donc $\sqrt{r}$ l'est aussi, ainsi que le cercle de centre O et de rayon OP . La droite OP est également constructible comme bissectrice de l'angle des deux demi-droites (Ox, OM), par exemple par la médiatrice de MM' , où M' est le point de Ox d'abscisse $r = OM$.

Démonstration du théorème.

1°. La condition est suffisante. En remarquant que K est une extension galoisienne de $\mathbb{Q}$ (pas nécessairement réelle), il suffit de l'établir sous la forme suivante :

(1) Si k' est une extension galoisienne de $\mathbb{Q}$ de degré 2^n , et si $z \in k'$, alors z est constructible : $z \in K'$.

On raisonne par récurrence sur n. Si $n = 1$, on a : $k' = \mathbb{Q}(z_1)$, avec $z_1^2 \in \mathbb{Q}$ (z_1 réel ou complexe). D'après le lemme, $z_1 \in K'$ et, comme $z = uz_1 + v$, $u, v \in \mathbb{Q}$, on a également $z \in K'$.

Supposons la propriété (1) vérifiée pour l'ordre 2^{n-1} et démontrons là pour n. Le groupe de Galois G de k' sur $\mathbb{Q}$ est d'ordre 2^n. Il en résulte, d'après

$$\begin{array}{|l} k' \\ | \\ k_{n-1} \\ | \\ \mathbb{Q} \end{array} \qquad \begin{array}{|l} G \\ | \\ \\ S=\{e,g\} \\ \{e\} \end{array}$$

une propriété de pure théorie des groupes, que G contient un élément g d'ordre 2 situé dans le centre de G. Le sous-groupe $S = \{e,g\}$ est alors distingué dans G car $\sigma \in G$, $\sigma g \sigma^{-1} = \sigma\sigma^{-1} g = g \in S$. (On utilise ici le fait que $g \in Z(G)$, centre de G, pour permuter g et σ^{-1}). D'après le théorème fondamental de la théorie de Galois, la propriété $S \lhd G$ implique que le corps fixe $k_{n-1} = F(S)$ des éléments de k' qui sont invariants par g est une extension galoisienne de $\mathbb{Q}$, de degré égal à $\frac{\text{Card } G}{\text{Card } S} = \frac{2^n}{2} = 2^{n-1}$. On a donc $[k_{n-1} : \mathbb{Q}] = 2^{n-1}$, k_{n-1} extension galoisienne de $\mathbb{Q}$, et l'hypothèse de récurrence s'applique, d'où $k_{n-1} \subset K'$. Mais $[k' : k_{n-1}] = \text{Card } S = 2$, de sorte que k' est une extension quadratique de k_{n-1}. Ainsi $k' = k_{n-1}(z_n)$ avec $z_n^2 \in k_{n-1}$. D'après le lemme, on a : $z_n \in K'$, et si $z = u z_n + v$, $u, v \in k_{n-1}$, on a également $z \in K'$. La propriété (1) est démontrée et la condition du théorème est suffisante.

2°. La condition est nécessaire. Supposons x constructible. On sait que x appartient à une extension provenant de $\mathbb{Q}$ par un nombre fini d'extensions quadratiques successives (réelles) :

$$\mathbb{Q} \subset \mathbb{Q}(\alpha_1) \subset \mathbb{Q}(\alpha_1, \alpha_2) \subset \ldots \subset \mathbb{Q}(\alpha_1, \alpha_2, \ldots, \alpha_n) = k_n$$

$$(2) \qquad \alpha_1^2 \in \mathbb{Q}, \ \alpha_2^2 \in \mathbb{Q}(\alpha_1) = k_1, \ldots, \ \alpha_n^2 \in \mathbb{Q}(\alpha_1, \alpha_2, \ldots, \alpha_{n-1}) = k_{n-1}.$$

On a bien $[k_n : \mathbb{Q}] = 2^n$, mais le théorème n'en résulte pas encore car k_n

n'est pas en général une extension galoisienne de $\mathbb{Q}$. Il est assez facile d'obtenir la plus petite extension galoisienne de $\mathbb{Q}$ contenant k_n . Ici, extension galoisienne signifie extension normale puisque $\mathbb{Q}$ est de caractéristique nulle. Soit $m_i(X)$ le polynôme minimal de α_i sur $\mathbb{Q}$. Toute extension normale de k_n contient évidemment les racines β_{ij} de l'équation $m_i(X) = 0$, et par suite le corps de décomposition du polynôme :

$$M(X) = m_1(X)\, m_2(X) \ldots m_n(X)$$

sur $\mathbb{Q}$. Or ce corps de décomposition est lui-même une extension normale de $\mathbb{Q}$; il coïncide donc avec la plus petite extension normale de $\mathbb{Q}$ contenant k_n , soit

$$N = \mathbb{Q}(\alpha_1, \alpha_2, \ldots, \beta_{ij}, \ldots).$$

On va lui donner une autre forme mieux adaptée pour calculer son degré. Soit $\sigma \in G$, groupe de Galois de N sur $\mathbb{Q}$; numérotons ses éléments $\sigma_1 = e, \sigma_2, \ldots, \sigma_r$. Nous allons démontrer l'égalité :

$$N = N' = \mathbb{Q}(\alpha_1, \ldots, \alpha_n, \sigma_2(\alpha_1), \ldots, \sigma_2(\alpha_n), \ldots, \sigma_r(\alpha_1), \ldots, \sigma_r(\alpha_n)).$$

Le second membre est inclus dans N , de sorte qu'il suffit d'établir l'inclusion opposée, ou encore :

$$\beta_{ij} \in N' .$$

Notons pour abréger $\beta_{ij} = \beta_i$ une racine quelconque de l'équation $m_i(X) = 0$ vérifiée par α_i sur $\mathbb{Q}$. Il existe, d'après le théorème de l'adjonction symbolique, un $\mathbb{Q}$ isomorphisme $\varphi : \mathbb{Q}(\alpha_i) \longrightarrow \mathbb{Q}(\beta_i)$, qui transforme α_i en β_i. Celui-ci laisse invariant les coefficients de $M(X) \in \mathbb{Q}[X]$, et peut donc être étendu à un $\mathbb{Q}$-automorphisme σ du corps de décomposition N de $M(X)$ sur $\mathbb{Q}$. Ainsi, il existe un élément $\sigma_s \in G$ tel que $\beta_{ij} = \sigma_s(\alpha_i)$, ce qui prouve que $N \subseteq N'$, d'où $N = N'$. En d'autres termes, le corps $N = N'$ est engendré par les corps $\sigma(k_n)$ isomorphes à k_n qui proviennent des injections de k_n dans N . (On sait d'ailleurs que ces corps sont en nombre égal à $[k_n : \mathbb{Q}] = 2^n$). Mais alors, les égalités (2) vont donner en appliquant σ_2 :

$$(\sigma_2(\alpha_1))^2 \in \mathbb{Q},\ (\sigma_2(\alpha_2))^2 \in \mathbb{Q}(\sigma_2(\alpha_1)),\ldots,(\sigma_2(\alpha_n))^2 \in \mathbb{Q}(\sigma_2(\alpha_1),\ldots,\sigma_2(\alpha_{n-1}))$$

ce qu'on peut encore écrire :

$$(\sigma_2(\alpha_1))^2 \in \mathbb{Q}(\alpha_1,\ldots,\alpha_n)\ ;\ (\sigma_2(\alpha_2))^2 \in \mathbb{Q}(\alpha_1,\ldots,\alpha_n,\sigma_2(\alpha_1))\ ;\ \ldots$$

et ainsi de suite. Il en résulte que N provient de $\mathbb{Q}$ par un nombre fini d'extensions quadratiques ou triviales, d'où :

$$[N : \mathbb{Q}] = 2^h .$$

Mais alors, en revenant à $x \in k_n \subset N$ (normale sur $\mathbb{Q}$), le corps de décomposition K du polynôme minimal $P(X)$ de x sur $\mathbb{Q}$ est contenu dans N ; c'est un sous-corps K de N, dont le degré divise celui de N, et par suite est une puissance de 2 (C.Q.F.D.).

Remarque. Si x est constructible, on sait que $[\mathbb{Q}(x) : \mathbb{Q}]$ est une puissance de 2, mais cette condition ne suffit pas pour que x soit constructible. La condition du théorème donne une condition nécessaire et suffisante qui fait intervenir le corps engendré par les racines du polynôme minimal $P(X)$ de x sur k. Par exemple, un nombre algébrique x de degré 4 n'est pas toujours constructible. (Voir un exemple en exercices).