N° d'ordre :

République Algérienne Démocratique et Populaire
Ministère de l'Enseignement Superieur et de la Recherche Scientifique

UNIVERSITÉ D'EL-OUED

FACULTÉ DES SCIENCES ET DE TECHNOLOGIE

Mémoire de fin d'étude

LICENCE ACADEMIQUE

Domaine: Mathématiques et Informatique
Filière: Mathématiques
Spécialité: Modélisation mathématiques & simulation numérique

Présenté par : **KHENFOUR Fatma**
REZIG Meriem
TAMMA Manel

Thème

L'anneau des entiers d'un corps de nombre

Soutenu le …juin 2014

Devant le jury composé de:

Mr. HAMROUNI Ahmed	MC (B) Univ. El-Oued	Président
Mr. Chayae Ahmed	MA (B) Univ. El-Oued	Examinateur
Mr. Youmbai Ahmed El Amine	MA (A) Univ. El-Oued	Rapporteur

Année universitaire: 2013 – 2014

Remerciements

En premier lieu, nous tenons à remercier ALLAH nos créateur pour nous avoir donne la force pour accomplir ce travail.

Nous tenons à notifier un remerciement spécial à tous nos professeurs qui ont contribué a notre formation de mathématique, en particulier, notre encadreur pédagogique Mr YOUMBAI Ahmed Elamine.

Nous tenons a remercie tous les étudiants de La promotion 2013/2014 de Math de l'université d'El-oued.

Sans oublier un grand merci à tous les membres de l'Association de l'Alkhawayrismia pour la science à son soutenir permanent.

En fin, nous remercions vivement notre famille pour l'aide matérielle et morale durant la période préparation.

Table des matières

Introduction générale

En mathématiques, un entier algébrique est un élément d'un corps de nombres qui y joue un rôle analogue à celui d'un entier relatif dans le corps des nombres rationnels. L'étude des entiers algébriques est à la base de l'arithmétique des corps de nombres, et de la généralisation dans ces corps de notions comme celles de nombre premier ou de division euclidienne. Par définition, un entier algébrique est une racine d'un polynôme unitaire à coefficients dans . Par exemple, le nombre $1+\sqrt{3}$ est un entier algébrique, car il est une racine du polynôme unitaire à coefficients entiers x^2-2x-2. Les nombres de la forme $a+bi$ où a et b sont des entiers relatifs et où i désigne une racine du polynôme x^2+1 sont aussi des entiers algébriques particuliers ; ils sont appelés entiers de Gauss.

Cette définition a émergé au cours du xixe siècle, en particulier dans les travaux de Richard Dedekind, car elle donne une notion adéquate pour développer l'arithmétique dans des corps de nombres. Un autre usage de ces nombres est la résolution d'équations diophantiennes, c'est-à-dire d'équations polynomiales à coefficients dans les entiers relatifs, et dont on recherche les solutions entières. Des exemples sont le théorème des deux carrés de Fermat, le dernier théorème de Fermat ou encore l'équation de Pell-Fermat. Par ailleurs, la compréhension de la structure d'un anneau d'entiers permet de mieux comprendre le corps d'origine. Les techniques développées pour décrire les propriétés de tels anneaux sont utilisées pour démontrer des théorèmes fondamentaux sur les corps de nombres comme celui de Kronecker-Weber.

Chapitre 1

Théorie des anneaux

1.1 Groupes

Un ensemble G est un groupe s'il est muni d'une loi de composition interne $*$:

– associative $(x * y)*z = x*(y * z)$.

– qui posséde un élément neutre e:

$e * x = x * e = x$.

– telle que tout élément $x \in G$ posséde un symétrique $x' \in G$: $x' * x = x * x' = e$.

Un ensemble G qui est un groupe et où la loi $*$ est commutative est dit groupe commutatif ou abélien. Si G est un groupe (loi interne $*$) on dit que $G' \subset G$ est un sous-groupe si l'ensemble G' constitue un groupe avec la même loi de composition interne $*$.

1.1.1 Anneau

Un ensemble A muni d'une addition et d' une multiplication posséde une structure d'anneau pour l'addition et la multiplication si: A posséde une structure de groupe commutatif pour l'addition, la multiplication est associative, la multiplication est distributive à gauche et à droite par rapport à l'addition.

Les axiomes de la structure d'anneau sont donc: [4]

1. $(\forall\ a,b,c \in A)\ (a + b) + c = a + (b + c)$.

2. $(\exists\ \varepsilon \in A)\ (\forall\ a \in A)\ a + \varepsilon = \varepsilon + a = a$.

3. $(\forall\ a \in A)\ (\exists\ a' \in A)\ a + a' = a' + a = \varepsilon$, a' est note $-a$.

4. $(\forall\ a,b \in A)\ a + b = b + a$.

5. $(\forall\ a,b,c \in A)\ (ab)c = a(bc)$.

6. $(\forall\ a,b,c \in A)a(b + c) = ab + ac$.

7. $(\forall\ a,b,c \in A)\ (b + c)a = ba + ca$.

Si la multiplication est commutative, on dit que l'anneau est abélien ou commutatif.
Si la multiplication possède un élément neutre, on dit que l'anneau est unitaire.
les anneaux que l'on considérera par la suite seront tous unitaire commutatifs.

1.1.2 Sous-groupe

On appelle sous-groupe de $(G, *)$ toute partie H de G qui est stable pour la loi $*$ et qui est un groupe pour la loi induite sur H par la loi $*$.

H est un sous-groupe propre de G si H est un sous-groupe de G distinct de $\{e\}$ et G.

– Une partie H non vide de G est un sous-groupe de G si et seulement si:

$(\forall\,(x, y) \in H^2, x * y \in H)$ et $(\forall x \in H, x^{-1} \in H)$

– Une partie H non vide de G est un sous-groupe de G si et seulement si $\forall\,(x, y) \in H^2$, $x * y^{-1} \in H$.

1.1.3 Sous-anneaux

On appelle sous-anneau d'un anneau A toute partie non vide B de A, stable pour les lois de A; et telle que la structure induite sur B par ces lois soit une structure d'anneau.

Un sous-anneau B de A est donc un sous-groupe du groupe additif A, et une partie stable de A pour la multiplication.

Réciproquement une partie B de A vérifiant ces deux conditions est un sous-anneau de A. En effet la multiplication induite sur la partie stable B de A est associative, et distributive à gauche et à droite par rapport à l'addition.

1.1.4 Anneau intègre

Un anneau A est dit intègre si l'ensemble $A - \{0\}$ est non vide et multiplicativement stable. un élément a est dit diviseur de zéro s'il existe un élément b non nul, tel que $a \cdot b = 0$. Un anneau intègre n'a donc pas de diviseur de zéro propre, c'est-à-dire distinct de zéro.

1.1.5 Anneau factoriel

On appelle factoriel un anneau commutatif unitaire intégre où tout élément non nul est produit d'élément premiers.

Un anneau factoriel est donc, en particulier, un anneau de Gauss, et il posséde toute les propriétés de ces anneaux.

1.1.6 Idéaux

On appelle idéal d'un anneau A, tout sous-groupe I groupe additif A, stable pour la multiplication par un élèment quelconque de l'anneau.

1.1.7 Idéal premier

Un idéal I d'un anneau A est dit premier si et seulement s'il est différent de A et si

$\forall a,b \in A : ab \in I \Rightarrow a \in I$ ou $b \in I$.

1.1.8 Idéal maximal

Un idéal I d'un anneau A est dit maximal s'il est différent de l'anneau A, et si tout idéal contenant I est égale à I, ou à A lui-même.

1.1.9 Idéal principal

Un idéal I d'un anneau A est dit principal s'il est engendré par un singleton$\{x\}$, et non le note par (x) ou Ax.

1.1.10 Idéal de type fini

Un idéal I d'un anneau A est dit de type fini, s'il est engendré par une famille finie d'élément de A.

1.1.11 Anneau quotient

Etant donné I un idéal de A, on définit une relation d'équivalence $\Re$ par

$$a\Re b \Longleftrightarrow a - b \in I.$$

L'ensemble quotient pour cette relation, muni des opérations induites par les opérations sur A, est un anneau appelle anneau quotient de A par l'idéal I, et noté $\frac{A}{I}$.

1.1.12 Module

Un A-module$(E, +, \cdot)$ est un ensemble muni d'une loi interne $+$ et d'une loi externe
$A \times E \to E$: $(a, e) \to \alpha e$ vérifiant.

1. $(E, +)$ est un groupe abélien.
2. $\alpha(e + e') = \alpha e + \alpha e'$.
3. $(\alpha + \beta)e = \alpha e + \beta e$.
4. $(\alpha\beta)e = \alpha(\beta e)$.
5. $1e = e$.

pour tous α, $\beta \in A$ et tous e, $e' \in E$.

Sous-module

Soit E un A-module, un sous-module F de E est sous groupe de $(E, +)$ qui est en plus stable pour la multiplication externe par tout élément de A.

Autrement dit une partie F de E est un sous-module si et seulement s'il contient 0, et si pour tous x, y de F et tous α de A, on a $x + y \in F$ et $\alpha x \in F$.

Module de type fini

Soit A un anneau. Rappelons qu'un $A-$module E est dit de type fini s'il est engendré par un nombre fini d'élément de A.

Module libre

Un module est dit libre s'idmet une base, c'est-à-dire un systéme de générateurs indépendant.

Chapitre 2

Éléments entiers sur un anneau

Parmi les nombres complexes, on va s'occuper dans ce mémoire des nombres algébriques, c'est-à-dire ceux qui satisfsont à une équation de la forme

$$x^n + a_{n-1}x^{n-1} + ... + a_1x + a_0 = 0$$

où les $a_\imath$ sont des nombres rationnels. Lorsque les a_i sont des nombres entiers ($a_\imath \in \mathbb{Z}$) le nombre algébrique x est appelé un entier algébrique, ainsi $\sqrt{2}$, $\sqrt{3}, \imath, \exp^{2\imath\pi/5}$ sont des entiers algébriques. Il n'est pas évident à priori que des sommes ou des produits de nombres algébriques (resp. d'entiers algébriques) sont encore des nombres algébriques (resp. des entiers algébriques). Regardons l'exemple de $x = \sqrt{2} + \sqrt{3}$; on calcule $x^2 = 2 + 3 + 2\sqrt{6}$; on isole la racine carrée et il vient $x^2 - 5 = 2\sqrt{6}$; encore une élévation au carré, $(x^2 - 5)^2 = 24$, ce qui montre que x est un entier algébrique. Le lecteur pourra s'exercer sur $\sqrt[3]{5} + \sqrt[5]{7}$, et sera convaincu que la série d'astuces qui méne au résultat n'est pas facilement généralisable.

Pour surmonter cette difficulté, les algébristes du siécle dernier, Dedekind en particulier, ont eu l'idée de ≪linéariser≫ le probléme, c'est-a'-dire d'y introduire des modules. C'est ce que nous allons faire. Le remplacement de $\mathbb{Z}$ (ou $\mathbb{Q}$) par un anneau commutatif quelconque ne coûte aucun effort supplémentaire, et sera fort utile pour la suite. Nous commencerons par le cas général des éléments entiers sur un anneau, et particulariserons ensuite aux éléments algébriques sur un corps.

Théorème 2.0.1 [7]

Soient R un anneau, A un sous-anneau de R, et x un élément de R.

Les propriétés suivantes sont équivalentes:

a) il existe a_0 , $a_1, \cdots$, $a_{n-1} \in A$ tel que:

$$x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0 = 0 \ldots\ldots\ldots\ldots\ldots\ldots (1)$$

(autrement dit x est racine d'un polynôme unitaire sur A).

b) l'anneau $A[x]$ est un $A-$module de type fini.

c) il existe un sous-anneau B de R tel que:

$A \subset B \subset R$

$x \in B$

B est un $A-$module de type fini.

Montrons d'abore que a entraîne B.

Notons M le sous$-A-$module de R engendré par $1, x, ..., x^{n-1}$ par a) on a $x^n \in M$. Par récurrence sur J montrons que $x^{n+j} \in M$, en effet, par multiplication par x^j, (1) donne

$$x^{n+j} = -a_{n-1}x^{n+j-1} - ... - a_0 x^j.$$

Comme $A[x]$ est le $A-$module engendré par les $x^k (K \geq 0)$, on a $A[x] = M$, ce que démontre b).

Comme l'anneau commutatif $A[x]$ est un module fidéle sur lui-méme, b) entraîne c)

c) $\Rightarrow$a):

on a

$$B = Ab_1 + ... + Ab_q$$

$b_i \in B$ et $x \in B$, donc $xb_i \in B$; on peut écrire

$$xb_i = a_{i1}b_1 + ... + a_{iq}b_q$$

$a_{ij} \in A$, on a donc un systéme linéaire homogéne de q équations à q inconnues

$b_i \sum_j (\delta_{ij} x - a_{ij}) b_j = 0 \qquad \begin{cases} \delta_{ij} = 1 & i = j \\ 0 & i \neq j \end{cases}.$

Soit d le déterminant $d = \det(\delta_{ij}x - a_{ij})$. On en déduit par les formules de cramer $d \times b_i = 0\ \forall i$. Mais B a un élèment neutre1 $1 = \sum \lambda_i b_i$, $\lambda_i \in A$. On a donc

$$1 \times d = \sum \lambda_i d b_i = 0.$$

On voit immédiatement que $d = 0$ constitue une équation de dépendance intégrale.[5]

Définition

Soient R un anneau et A un sous-anneau de R. Un élèment x de R est dit entier sur A s'il satisfait aux conditions équivalentes a), b), c), du théoréme précédent. Soit $P \in A[x]$ un polynôme unitaire tel que $P(x) = 0$ (polynôme dont l'existence est affirmée par a)); la relation $P(x) = 0$ est appelée une équation de dépendance intégrale de x sur A.

Exemple: 1. L'élément $x = \sqrt{2}$ de $\mathbb{R}$ est entier sur $\mathbb{Z}$; une équation de dépendance intégrale est donnée par $x^2 - 2 = 0$.

2. Les éléments de $\mathbb{Q}(i)$ entiers sur l'anneau $\mathbb{Z}$ sont les éléments de la forme $a + ib$avec $a \in \mathbb{Z}$ et $b \in k$(<< entiers de gauss>>); les élé ments de $\mathbb{Q}\left(\sqrt{5}\right)$ entiers sur $\mathbb{Z}$ sont les éléments de la forme $\left(a + b\sqrt{5}\right)/2$, où a et b appartiennent a' $\mathbb{Z}$ et sont tous deux pairs ou tous deux impairs.

3. Les nombres complexes entiers sur $\mathbb{Z}$ sont encore appelés entiers algébriques.[3]

Remarque:[7] Soient R un anneau, A un sous-anneau de R, et (x_i) $1 \leq i \leq n$ une famille finie d'éléments de R. Si, pour tout i, x_i est entier sur $A[x_1, ..., x_{i-1}]$ (en particulier si tous les x_i sont entiers sur A), alors $A[x_1, ..., x_n]$ est un $A-$module de type fini.

Raisonnons par récurrence sur n. Pour $n = 1$ c'est l'assertion b) du théoréme précédent.

Supposons la propositions vraie jusqu'a' $n-1$. Alors $B = A[x_1, ..., x_{n-1}]$ est un A-module de type fini, soit $B = \sum_{j=1}^{p} Ab_j$.

Par application du cas $n = 1$, $A[x_1, ..., x_n] = B[x_n]$ est un $B-$module de type fini, soit $\sum_{k=1}^{q} Bc_k$, on a alors

$$A[x_1, ..., x_n] = \sum_{k=1}^{q} Bc_k = \sum_{k=1}^{q}(\sum_{j=1}^{p} Ab_j)c_j = \sum_{j,k} Ab_j c_k.$$

Ainsi $(b_j c_k)$ est un systéme générateur fini du $A-$module $A[x_1, ..., x_n]$

Corollaire 2.0.1 *Si x et y sont entiers sur l'anneau A, alors $x+y$, $x-y$, et xy sont également entiers sur A* [5] .

En effet on a $x+y$, $x-y$, $xy \in A[x,y]$, d'aprés la propotions précédent, $A[x,y]$ est un $A-$module de type fini. Donc, d'aprés le c) du théoréme (2.0.1) $x+y$, $x-y$, et xy sont entiers sur A.

Corollaire 2.0.2 *Soient R un anneau et A un sous$-$anneau de R. L'ensemble A' des éléments de R qui sont entiers sur A est un sous$-$anneau de R, qui contient A. En effet A' est un sous-anneau de R d'apres le corollaire précédent; il contient A car tout $a \in A$ est racine du polynôme unitaire $X-a$, donc est sur A.*[7]

Définition 2.0.1 *L'ensemble des éléments d'un anneau R entiers sur un sous-anneau A frome un anneau A' intermédiaire entre A et B: on l'appelle la fermeture intégrale de A dans R. Il suffit d'appliquer le corollaire 1* [5]

Soient A un anneau intégre et K son corps des fractions; la fermeture intégrale de A dans K s'appelle la clôture intégrale de A. Soient B un anneau et A un sous-anneau de B; on dit que B est entier sur A (autrement dit, si la fermeture intégrale de A dans B est B lui-même). [7]

Proposition 2.0.1 *La dépendance intégrale est transitive on a trois anneaux $A \subset B \subset C$. Si B est entier sur A et si C est entier sur B, alors C est entier sur A.Soit alors x un élément de C : il est entier sur B et vérifie donc*

$$x^n + b_{n-1}x^{n-1} + ... + b_1 x + b_0 = 0.$$

Il est ainsi entier sur le sous-anneau

$$B^1 = A[b_0, b_1, ..., b_{n-1}].$$

Comme B est entier sur A, ce sous-anneau est un $A-$module de type fini (la proposition 1) [5]

par le c) du Théoréme (2.0.1), on en conclut que x est entier sur A. Donc C est entier sur A. [7]

Théorème 2.0.2 [6]

Soient A' un anneau, A un sous-anneau de A' tel que A' soit entier sur A et p un idéal premier de A. Il existe un idéal premier p' de A' tel que $p' \cap A = p$.

Démonstration. ■

a) supposons que A soit local et que p soit l'idéal maximal de A. Soit p' un idéal maximal quelconque de A'

puisque $[A/p' \cap A = A + p'/p' \subset A'/p']$ et comme A'/p' est entier sur $A/p' \cap A$, alors A'/p' est un corps si et seulement si $A/p' \cap A$ l'est aussi. Donc, p'est maximal si et seulement si $p' \cap A$ l'est et comme $p' \cap A \subset p$ ceci entraîne $p' \cap A = p$. Pour achever la démonstration, on va démontrer le lemme suivant :

Lemme 2.0.1 *Soient B' un anneau intégre, B un sous-anneau de B' tel que B' soit entier sur B. Alors B' est un corps si et seulement si B est aussi un corps. Supposons que B soit un corps et soit $y \in B'$, $y \neq 0$. Alors*

$$y^n + b_{n-1}y^{n-1} + ... + b_1 y + y_0 = 0$$

avec $b_\imath \in B$ $(\imath = 0, 1, ..., n-1)$ et l'on peut supposer $b_0 \neq 0$, car si non on peu simpliffier par y puisque B' est intégre. Donc, $y(y^{n-1} + b_{n-1}y^{n-2} + ... + b_2 y + b_1)$ est inversible dans B, car b_0 l'est. Il existe un $U \in B$ tel que:

$$y(y^{n-1} + b_{n-1}y^{n-2} + ... + b_1)U = 1$$

et comme $(y^{n-1} + b_{n-1}y^{n-2} + ... + b_1)U \in B'$, alors y est inversible dans B'. Reciproquement, supposons que B' soit un corps et soit $x \in B$, $x \neq 0$. Alors $x^{-1} \in B'$ et donc

$$x^{-n} + b_{n-1}x^{-(n-1)} + ... + b_1 x^{-1} + b_0 = 0$$

avec $[B_\imath \in B(\imath = 0, 1, ..., n-1)]$ En multipliant la derniére équation par x^{n-1}, on a $x^{-1} = -(b_{n-1} + b_{n-2}x + ... + b_1 x^{n-2} + b_0 x^{n-1}) \in B$.

2.1 Anneaux intégralement clos

Définition 2.1.1 *On dit qu'un anneau A est intégralement clos s'il est intégre et si sa clôture intégrale est A lui-méme.*

Autrement dit, tout élément x du corps des fractions K de A, qui est entier sur A, est élément de A [7].

On notera qu'un anneau intégralement clos n'est pas nécessairement intégrlement fermé dans un anneau qui le contient.

Proposition 2.1.1 *Soient A un anneau, R une $A-$algébre. La fermeture intégrale A' de A dans R est un sous-anneau intégralement fermé dans R.*

En effet, la fermeture intégrale de A' dans R est entiére sur A; elle est donc égale a' A'.

Corollaire 2.1.1 *La clôture intégrale d'un anneau intégre A est un anneau intégralement clos. En effet, soient K le corps des fractions de A, B la clôture intégrale de A. Il est clair que K est le corps des fractions de B, et il suffit d'appliquer la proposition précédent a' $R = K$.*

Proposition 2.1.2 *Soient R un anneau, $(B_\lambda)_{\lambda \in L}$ une famille de sous-anneaux de R et pour chaque $\lambda \in L$, soit A_λ un sous-anneau de B_λ. Si chaque $A_\lambda$est intégralement fermé dans B_λ, alors $A = \bigcap_{\lambda \in L} A_\lambda$ est intégralement fermé dans $B = \bigcap_{\lambda \in L} B_\lambda$* 3

2.2 Exemples d'anneaux intégralement clos

Exemple 2.2.1 [7]

1. Soient A un anneau intégre et K son corps des fractions. Alors la clôture intégrale A' de A (c-a'-d la fermeture intégrale de A dans K) est un anneau intégralement clos. En effet la clôture intégrale de A' est entiére sur A', donc sur A (d'apres le proposition de la dépendance intégrale est transitive); elle est donc égale a'A'.

2. Tout anneau principal est intégralement clos.

En effet un anneau principal A est intégre par définition. Soit x un élément entier sur A de son corps des fractions; on a une équation de dépendance intégrale.

$$x^n + a_{n-1}x^{n-1} + ... + a_1x + a_0 = 0 \qquad (a_i \in A)$$

or on peut écrire $x = a\ /b$, avec $a, b \in A$ premiers entre eux, d'où, en reportant dans (1) et en multipliant par b^n.

$$a^n + b\left(a_{n-1}a^{n-1} + ... + a_1ab^{n-2} + a_0b^{n-1}\right)$$

Ainsi b divise a^n, comme il est prmier avec a, l'application répétée du lemme d'Euclide montre qu'il divise a; donc $x = a\ /\ b \in A$, et A est intégralement clos.

on notera qu'on a seulement utilisé les propriétés multiplicatives des anneaux principaux (éléments premiers entre eux, lemme d'Euclide).

Le raisonnement montre ainsi que tout anneau factoriel est intégralement clos.

2.3 Éléments algébriques sur un corps. Extensions algébriques

Soient R un anneau, et K un sous-corps de R. On dit qu'un élément x de R est algébrique sur K s'il existe des éléments non tous nuls $a_0, ..., a_n$ de K tels que:[7]

$$a_nx^n + ... + a_1x + a_0 = 0$$

il revient au même de dire que les monômes $(x^J)_{J\in N}$ sont linéairement dépendants sur K. Un élément non algébrique sur K est dit tranxendant sur K; ceci veut dire que les monômes $(x^J)_{Je N}$ sont linéairement indépendants sur K.

1. Dans la relation de la définition 1, on peut supposer a_n non mul; il admet alors un inverse a_n^{-1} car K est un corps; en multipliant par a_n^{-1} on obtient une équation de dépendance intégrale. Donc:

   sur un corps, algébrique = entier, on peut donc appliquer la théorie des éléments entiers; par exemple, pour $K \subset R$ et $x \in R$, le théoréme (2.0.1), b) donne:

2. x algébrique sur $K \Longleftrightarrow [K\,[x] : K]$ finie .on dit qu'un anneau R contenant un corps K est algébrique sur K si tout élément de R est algébrique sur K; si R lui-méme est un corps on dit alors que R est une extension algébrique de K. E'tant donnés un corps

L et un sous-corps K de L, la dimension $[L : K]$ s'appelle aussi le degré de L sur K. le théoréme (2.0.1), c) donne alors:

3. Si le degré de L sur K est fini, L est extension algébrique de K on appelle corps de nombres algébriques (ou corps de nombres) toute extension de degré fini de $\mathbb{Q}$.

Proposition 2.3.1

Soient K un corps, L une extension algébrique de k et M une extension algébrique de L. Alors M est extension algébrique de L. De plus $[M : K] = [M : L]\,[L : K]$ (<< multiplicativité des degrés >>).

1. La premiére assertion est un cas particulier de la proposition 2. De puls, si $(x_\imath)_{\imath\in N}$ est une base de L sur K et $(y_\jmath)_{\jmath\in J}$ une base de M sur L, alors $(x_\imath y_\jmath)_{(\imath,\jmath)\in I\times J}$ est une base de M sur K: en effet, c'est un systéme générateur, comme dans la proposition 1; d'autre part une relation $\sum_{\imath,\jmath} a_{\imath\jmath}\, x_\imath\, y_\jmath = 0$ avec $a_{\imath\jmath} \in K$, donne $\sum_{\jmath} \left(\sum_{\imath} a_{\imath\jmath}\, x_\imath \right) y_\jmath = 0$ d'ou $\sum_{\imath} a_{\imath\jmath}\, x_\imath = 0$ pour tout $\jmath$ (car $\sum a_{\imath\jmath} x_\imath \in L$), et par conséquent $a_{\imath\jmath} = 0$ pour tous $\imath, \jmath$. Ceci démontre la formule de multiplicativite des degrés.

Proposition 2.3.2 *Soient R un anneau, et K un sous-corps de R. Alors*

a) l'ensemble K' des éléments de R algébriques sur K est un sous-anneau de R contenant K;

b) Si R est intégre, K' est un sous-corps de R En effet a) est un cas particulier du corollaire 2 de la proposition 1, et b) résulte de la lemme 3.

Nous allons maintenant étudier de plus prés les éléments algébriques sur un corps.

Soient R un anneau, K un sous-corps de R et x un élément de R. Il existe un homomorphisme φ et un seul de l'anneau de polynôme $K[X]$ dans R tel que $\varphi(X) = x$, et que $\varphi(a) = a$ pour tout $a \in K$; l'image de φ est $K[x]$. la définétion des éléments algébriques se traduit par.

4. x algébrique sur $K \Longleftrightarrow$ Ker $(\varphi) \neq (0)$.

si x est elgébrique sur K, l'idéal Ker (φ) est un idéal principal $(F(X))$ (car $K[X]$ est un anneau pricipal), engendré par un polynôme non nul $F(X)$ qu'on peut supposer unitaire car K est un corps; ce polynôme unitaire est déterminé de façon unique par K et x, et on l'appelle le polynôme minimal de x sur K. Traduisons sa définition:

5. Soient $F(X)$ le polynôme minimal de x sur K, et $G(X) \in K[X]$; pour qu'on ait $G(x) = 0$, il faut et il suffit que $F(X)$ divise $G(X)$ dans $K[X]$. De plus, par passage au quotient, on obtient un isomorphisme canonique.

6. $K[X]/(F(X)) \underset{\hookleftarrow}{\backsim} K[X]$

Avec les mêmes notations, supposons toujours x algébrique sur K, et soit $F(X)$ son polynôme minimal; en appliquant (5) est le lemme1 on obtient les équivalences.

7. $K[x]$ corp $\iff$ $K[x]$ intégre $\iff$ $F(X)$ irréductible inverstement soient K un corps et $F(X) \in K[X]$ un polynôme irréductible alors $K[x]/(F(x))$ est un corps contenant K, et, en notant x la classe de X dans ce corps, on a $F(X) = 0$. Ainisi $F(X)$ est divisible par $X - x$ sur ce corps $K[x]$. Plus généralement :

Proposition 2.3.3 *Soient K un corps, et $P(X) \in K[X]$ un polynôme non constant. Il existe une extension algélrique K' de degré fini de K telle que $P(X)$ se décompose en facteurs du premier degré dans $K'[X]$.*

On raisonne par récurrence sur le degré d de $P(X)$ .C'est évident pour $d = 1$. Supposons l'assertion démontrée jusqu'au degré $d - 1$.

Soit $F(X)$ un facteur irréductible de $P(X)$. On vient de voir qu'il existe une extension K'' de degré fini de K (a'savoir $K[X]/F(X)$) et un élèment $x \in K$"tels que $F(X)$ soit multiple de $X - x$ dant $K"[X]$ .On a alors $P(X) = (X - x)P_1(X)$ avec $P_1(X) \in K"[X]$. D'aprés l'hypothése de récurrence, $P_1(X)$ se décompose en facteurs du premier degré sur une extension K' de degré fini de K". Alors K' est une extension de degré fini de K (proposition1), et $P(X)$ se décompose en facteurs du premier degré dans $K'[X]$.

Remarque 2.3.1 *Crops algébriquement clos. On dit qu'un corps K est algébriquement clos si tout polynôme non constant $P(X) \in k[X]$ se décompose en facteurs du premier degré dans $K[X]$; il suffit pour cela, par récurrence sur le degré, que tout polynôme non constant $P(X) \in K[X]$ admette une racine $x \in K$. Par application (transfinie) de le lemme1 (c'est-a'-dire en combinant le lemme1 et le théoréme de Zorn).*

On démontre que tout corps est un sous-corps d'un corps algébriquement clos.

On démontre en Analyse, par des méthodes variées, que le corps G des nombres complexes est algébriquement clos. Cela Suffira a' nos bresoins.

2.4 Éléments conjugués,et corps conjugués

E'tant donnés deux corps, L, L'contenant un corps K on appelle $K-$isomorphisme de L sur L' tout isomorphisme $\varphi = L \longrightarrow L'$ tel que $\varphi(a) = a$ pour tout $a \in K$; dans ces conditions on dit que L et L' sont $K-$isomorphes, ou (s'ils sont algébriques sur K) sont des corps conjugés sur K. E'tant données deux extensions L, L' de K, on dit que deux éléments $x \in L$ et $x' \in L'$ sont conjugués sur K s'il existe un $K-$isomorphisme $\varphi : K(x) \longrightarrow K'(x')$ tel que $\varphi(x) = x'$; alors φ est unique. Ceci signifie que, ou bien x et x' sont tous deux tranxendants sur K, ou bien x et x' sont tous deux algébriques sur K et admettent le même polynôme minimal.

Soit $F(X)$ un polynôme irréductible de degré n sur K, et $x, ..., x_n$ ses racines dans un extension K' de K (proposition 6). Alors les x_i sont deux a' deux conjugués sur K, et les corps $K[x_i]$ sont aussi deux a' deux conjugués sur K.

Soient K un corps de caractéristique 0 ou un corps fini, $F(X) \in K[X]$ un polynôme unitaire irréductible, et $F(X) = \prod_{i=1}^{n} (X - x_i)$ sa décomposition en facteurs du premier degré dans une extension K' de K (proposition 6). Alors les n racines $x_1, ..., x_n$ de $F(X)$ sont distinctes Raisonnons par l'absurde. Dans le cas contraire, $F(X)$ admettrait une racine multiple x, qui serait donc aussi racine du polyonôme dérivé $F'(X)$; alors $F(X)$ divriserait $F'(X)$. Comme $d^\circ F' \langle d^\circ f$ ceci implique que $F'(X)$ est le polynôme nul. Or si

$$F(X) = X^n + a_{n-1}X^{n-1} + ... + a_0 \qquad (a_i \in K)$$

1. pour une démonstration utilisant les propriétés des fonctions continues sur un espace compact, pour une démostration utilisant les propriétés des fonctions homolorphes d'une variable complexe. On a

$$F'(X) = nX^{n-1} + (n-1)\, a_{n-1}X^{n-2} + ... + a_1$$

on a donc $n \cdot 1 = 0$ et $\jmath \cdot a_\jmath = 0$ pour $\jmath = 1, ..., n-1$. ceci est impossible en caractéristique 0.

En caractéristique $\rho \neq 0$, ceci implique que ρ divrise n ,et qu'on $a : a_\jmath = 0$ pour $\jmath$ non multiple de ρ (on rappelle que ρ est un nombre premier). Ainsi $F(X)$ est de la forme.

$$F(X) = X^{qp} + b_{q-1}X^{(q-1)p} + ... + b_1X^p + b_0 \qquad (b_\imath \in K)$$

si chacun des $b_\imath$ est une puisance $p^{-éme}$, soit $b_\imath = c_\imath^p$ avec $c_\imath \in K$, on a:

$F(X) = (X^p + c_{q-1}X^{q-1} + ... + c_0)^p$, et $F(X)$ n'est par irréductible. Or, si K est un corps fini et si on note p $(\neq 0)$ sa caractéristique, l'application $x \longmapsto x^p$ de K dans K est injective (car $x^p = y^p$ implique $x^p - y^p = o, (x-y)^p = 0$ et $x - y = 0$); elle est donc surjective car K est fini. On a donc une contradiction.

Les corps K de caractéristique $p \neq 0$ tel que $x \longmapsto x^p$ soit surjective ($\imath.e$.que tout élément de K soit une puissance $p^{-éme}$) sont appelés les corps parfaits; on vient de montrer que tout corps fini est parfait; on convient qu'un corps de caractéristique 0 est parfait. Nous avons démontré que la conclusion du lemme reste vraie sous la seule hypothése que K est un corps parfait. Le corps $F_p(T)$ des fractions rationnelles a' une variable sur F_p n'est pas parfait, car la variable T n'est pas une puissance $P^{-éme}$ dans $F_p(T)$.

Soient K un corps de caractéristique 0 on fini, K' une extension de degré fini n de K et, C un corps algébriquement clos contenant K. Alors il existe n K-isomorphismes distincts de K' dans C.

Notre assertion est vraie pour une extension monogéne K', c'est-a'-dire de la forme $K' = K[x]$ $(x \in K')$. En effet le polynôme minimal $F(X)$ de x sur K est alors de degré n.

Il admet n racine $x_1, ..., x_n$ dans C, qui sont distinctes d'aprés le lemme. Pour $\imath = 1, ..., n$, on a donc un $K-$isomorphisme.

$\nabla_\imath : K' \to C$ tel que $\nabla_\imath(x) = x_\imath$.

Nous procéderons alors par récurrence sur le degré n de K'. Soit $x \in K'$; considérons les corps $K \subset K[x] \subset K'$ et posons $q = [K[x] : K]$; on peut supposer $q \rangle 1$. D'aprés le cas monogéne, on a q K $-$isomorphismes distincts $\nabla_1, ..., \nabla_q$ de $K[x]$ dans C. Comme $K[\nabla_\imath(x)]$ et $K[x]$ sont isomorphes, on peut construire une extension $K'_\imath$ de $K[\nabla_\imath(x)]$ et un

isomorphisme $\tau_\imath : K^{'} \to K'_\imath$ qui prolonge $\nabla_\imath$. Or $K\left[\nabla_\imath(x)\right]$ est un corps de caratéristique 0 ou fini. Comme $[K'_\imath = K\left[\nabla_\imath(x)\right]] = [K' : K\left[x\right]] = \frac{n}{q}\langle n$.

L'hypothése de récurrence montre qu'on a $\frac{n}{q} K\left[\nabla_\imath(x)\right]$ $-$isomorphismes distincts $\theta_{\imath\jmath}$de $K'_\imath$ dans C. Alors les n composés $\theta_{\imath_\jmath} \circ \tau_\imath$ fournissent $q \cdot \frac{n}{q} = n$ $K-$isomorphismes de K' dans C. Ils sont distincts car $\theta_{\imath_\jmath} \circ \tau_\imath$ et $\theta_{\imath'\jmath'} \circ \tau_{\imath'}$ différent sur $K\left[x\right]$ si $\imath \neq \imath$, et, si $\imath = \imath'$, $\theta_{\imath_\jmath}$ et $\theta_{\imath\jmath'}$différent sur $K'_\imath$.GQFD. Le théoréme 1 s'étend a' un corps parfait K : on motre en effet que toute extension algébrique d'un corps parfait (en particulier $K\left[\nabla_\imath(x)\right]$) est un corps parfait; le reste de la démonstration est inchangé.

Corollaire 2.4.1 *(«théoréme de l'élément primitif»)*

Soient K un corps fini ou de caractéristique 0, et K' une extension de K de degré fini n. Il existe alors un élément x de K'(dit « primitif ») tels que $K' = K\left[x\right]$.

Si K est fini, K' est fini, et son groupe multiplictif K'^* est formé des puissances d'un méme élément x. On a alors $K' = K\left[x\right]$ supposons maintenant K de caractéristique 0, donc infini. Daprés le théoréme 1, on a n $K-$isomprhismes $\nabla_\imath$ de K' dans un corps algébriquement clos C contenant K.Pour $\imath \neq j$ l'équation $\nabla_\imath(y) = \nabla_j\ (y)\,(y \in K')$ définit une partie $V_{\imath_j}$ de K', qui est évidemment un sons $K-$espace vectoriel de K', et qui est distincte de K' car $\nabla_\imath \neq \nabla_\jmath$. Comme K est infini, l'algébre linéaire montre que la réunion des $V_{\imath_j}$ est distincte de K'. Prenons x en dehors de cette réunion. Les $\nabla_\imath(x)$ sont alors deux a' deux distincts, de sorte que le polynôme minimal $F(X)$ de x sur K a ou moins n racines distinctes (les $\nabla_\imath(x)$) dans C ; on a donc $d^0\ F \geqslant n$, c'est -a'-dire $[K\left[x\right] : K] \geqslant n$. Comme $K\left[x\right] \subset K'$ et que $[K' : K] = n$, on en déduit $K' = K\left[x\right]$.CQFD.

Chapitre 3

Application aux corps quadratiques et cyclotomiques

La théorie des corps se trouve les ouvrage de théorie des nombres algébriques.

3.1 Les corps quadratiques

On appelle corps quadratique toute extension du degré 2 du corps Q des nombres rationnels.

Si K est un corps quadratique, tout élément x de $K - Q$ est de degré 2 sur Q, donc est élément primitif de K $(i.e. K = Q[x], \text{et } (1, x) \text{ est une base de } K \text{ sur } Q)$.

Soit $F(X) = X^2 + bX + c$ $(b, c \in Q)$ le polynôme minimal d'un tel élément $x \in K$. La résolution de l'équation du second degré $x^2 + bx + c = 0$ donne $2x = -b \pm \sqrt{b^2 - 4c}$.Ainsi $K = Q\left(\sqrt{b^2 - 4c}\right)$[1].

Or $b^2 - 4c$ est un nombre rationnel

1. Par $\sqrt{b^2 - 4c}$ nous entendons l'un des deux éléments de K dont le carré est $b^2 - 4c$.

$\frac{u}{v} = \frac{uv}{v^2}$ avec u,$v \in Z$ on a donc aussi $K = Q(\sqrt{uv})$ avec $uv \in Z$.

Par le même procédé on voit qu'on peut enfin écrire $K = Q\left(\sqrt{d}\right)$ où d est un entier sans facteurs carrés dans sa décomposition en facteurs premiers.

On a ainsi prouvé:

Proposition 3.1.1 *Tout corps quadratique est de la forme* $Q\left(\sqrt{d}\right)$ *où* d *est un entier sans facteurs carrés.*

L'élément $\sqrt{d}$ est une racine du polynôme irréductible $X^2 - d$. Il admet un conjugué dans K, à savoir $-\sqrt{d}$. Il existe donc un automophisme σ de K qui applique $\sqrt{d}$ en $-\sqrt{d}$

L'élément général de K est la forme $a + b\sqrt{d}$ avec $a, b \in Q$, et on a

1. $\sigma\left(a + b\sqrt{d}\right) = a - b\sqrt{d}$

   Nous nous proposons d'étudier l'anneau A entiers de K, c'est-à-dire l'ensemble des $x \in K$ qui sont entiers sur Z. Si $x \in A$, $\sigma(x)$ est racine de la même équation de dépendance intégrale que x, donc $\sigma(x) \in A$. On a donc $x + \sigma(x) \in A$ et $x \cdot \sigma(x) \in A$. Or, si $x = a + b\sqrt{b}$ avec $a, b \in Q$, on a d'aprés (1),

2. $x + \sigma(x) = 2a \in Q \qquad x\sigma(x) = a^2 - db^2 \in Q$

   Comme Z est principal, et donc intègralement clos, on a donc

3. $2a \in Z \qquad a^2 - db^2 \in Z$

   Ces conditions (3) sont nécessaires pour que $x = a + b\sqrt{d}$ soit entier sur Z; elles sont aussi suffisantes car alors x est racine de $x^2 - 2ax + a^2 - db^2 = 0$ d'aprés (3) on a $(2a)^2 - d(2b)^2 \in Z$, comme $2a \in Z$, on a donc $d(2b)^2 \in Z$. Or d est sans facteurs carrés; si $2b$ n'était pas entier, son dénominateur comporterait un facteur premier p; ce facteur appaitrait sous la forme p^2 dans $(2b)^2$, et la multiplication par d ne pourrait pas le ramener dans Z ; on a donc $2b \in Z$ Bref on peut poser $a = \frac{u}{2}, b = \frac{v}{2}$ avec $u, v \in Z$; la condition (3) devient alors:

4. $u^2 - dv^2 \in 4Z.$

Si v est pair, (4) montre que u est pair aussi; on a alors $a, b \in Z$. Si v est impair,
on a $v^2 \equiv 1 \bmod 4$; or la classe
de u^2 mod. 4 est 0 ou 1 (écrire la table des carrés mod);
comme d est sans facteurs carrés, il n'est pas multiple de4;
Aainsi on amécessairement $u^2 \equiv 1$ mod. 4 et $d \equiv 1$ mod.4 On a donc prouvé ce qui suit:

Théorème 3.1.1 *Soit $K = Q\left(\sqrt{d}\right)$ un corps quadratique, avec $d \in Z$ sans facteurs carrés (et donc $\neq 0 \bmod 4$).*

a) Si $d \equiv 2$ ou $d \equiv 3$ mod.4, l'anneau A des entiers de K est l'ensemble des $a + b\sqrt{d}$, avec $a, b \in Z$.

b) Si $d \equiv 1 \bmod .4$, A est l'ensemble des $\frac{1}{2}\left(u + v\sqrt{d}\right)$ avec u,$v \in Z$ des même parité.

Dans le cas $d \equiv 2$ ou $3 \bmod .4$, une base de $Z-$module A évidemment $\left(1, \sqrt{d}\right)$.

Dans le cas $d \equiv 1 \bmod .4$, une base du $Z-$module A est $\left(1, \frac{1}{2}\left(1 + \sqrt{d}\right)\right)$.En effet, par b), les éléments 1 et $\frac{1}{2}\left(1 + \sqrt{d}\right)$ sont dans A.Inversement, pour montrer que $\frac{1}{2}\left(u + v\sqrt{d}\right)$ (avec $u, v \in Z$ de même parité) est combinaison $Z-$linéaire de 1 et $\frac{1}{2}\left(1 + \sqrt{d}\right)$, on se ramène au cas où u et v sont pairs par soustraction éventuelle de $\frac{1}{2}\left(1 + \sqrt{d}\right)$; dans ce cas on a

$\frac{1}{2}\left(u + v\sqrt{d}\right) = \left(\frac{u}{2} - \frac{v}{2}\right) \cdot 1 + v \cdot \frac{1}{2}\left(1 + \sqrt{d}\right)$.

Pour finir, un peu de terminologie. Si $d \succ 0$ on a dit que $Q\left(\sqrt{d}\right)$ est un corps quadratique réel (car il existe un sous-corps de R conjugué de $Q\left(\sqrt{d}\right)$ sur Q).

Si $d \prec 0$, on dit que $Q\left(\sqrt{d}\right)$ est un corps quadratique imaginaire.

3.2 Normes et traces

a) Rappels d'algèbre linéaire.

Soient un anneau, E un $A-$module libre de rang fini, et u un endomorphisme de E. On définit en algèbre linéaire la trace, le déterminant, et le polynôme caractéristique de u.

Si une base (e_i) de E a été choisie et si (a_{ij}) est la matrice de u dans cette base, quantités valent respectivement.

1. $Tr\ u = \sum_{i=1}^{a} a_{ii}, \det\ (u) = \det\left(a_{ij}\right)$ .et $\det\ (X \cdot I_E\ - u)$ NB. Ces quantités sont indépendantes de la base choisie. Les formules (1) montrent qu'on a:

2. $Tr\left(u + u'\right) = Tr\left(u\right) + Tr\left(u'\right)$

   $\det\left(uu'\right) = \det\left(u\right) \det\left(u'\right)$

   $\det\left(X \cdot I_E\ - u\right) = X^n - \left(Tr\ u\right) X^{n-1} + ... + (-1)^n \det\ u.$

b) Normes et traces dans une extension.

Soint B un anneau, et A un sous-anneau de B tel que B soit un $A-$module libre de rang fini n (par exemple A peut être un corps, et B une extension de degré n de A). Pour $x \in B$, la multiplucation m_x par x (soit $y \longmapsto xy$) est un endomorphisme du $A-$module B.

Définition 3.2.1 *On appelle trace (resp. norme, polynôme carectéristique) de $x \in B$, relativemment à B et A, la trace (resp, déterminant, polynôme carectéristique) de l'endomorphisme m_x de multiplication par x. La trace (resp. norme) de x est notée $Tr_{A/B}(x)$ (resp. $N_{A/B}(x)$) ou $Tr(x)$ (resp. $N(x)$) lorsqu'aucune confusion n'est à craindre; ce sont des élément de A. Le polynôme caractéristique de x est un polynôme unitaire à coefficient dans A.Pour $x, x \in B$ et $a \in A$ on a évidemment $m_x + m_{x'} = m_{x+x'}$, $m_x \circ m_{x'} = m_{xx'}$ et $m_{ax} = am_x$; de plus la matrice de ma, dans n'importe quelle base de B sur A, est la matrice diagonale dont tous les éléments diagonaux sont égaux à a. Il résulte alors des formules (1) et (2) qu'on a:*

3. $Tr(x + x') = Tr(x) + Tr(x')$, $Tr(a\,x) = aTr(x)$, $Tr(a) = n.a$

$N(xx') = N(x)\,N(x')$, $\quad N(a) = a^n$, $\quad N(a\,x) = a^n N(x)$

Proposition 3.2.1 *Soient K un corps caractéristique 0 ou fini, L une extention algébrique de degré n de K, x un élément de L, et $x_1, ..., x_n$ les racines du polynôme minimal*

de x sur K (dans une extension convenable de K; chacune répétie $[L : k\ [x]]$ fois. Alors $Tr_{L/K}(x) = x + ... + x_n$, $N_{L/K}(x) = x + ... + x_n$, de plus le polynôme caractéristique

de x, relativement à L et K, est $(X - x_1) ... (X - x_n)$.

Ainsi ce polynôme caractéristique est et la puissance $[L : K[x]] - éme$ du polynôme minimal de x sur K.

Traitons d'abord le cas où x est un élément primitif de L sur K .Soint $F(X)$ le polynôme minimal de x sur K; alors L est $K-$isomorphe à $K(X)/F(X)$, et $(1, x, ..., x^{n-1})$ est une base de L sur K.

Posons $F(X) = X^n + a_{n-1}X^{n-1} + ... + a_1X + a_0$.

La matrice de l'endomorphisme m_x dans cette base est:

$$\begin{vmatrix} 0 & 0 & \cdots & 0 & -a_0 \\ 1 & 0 & \cdots & 0 & -a_1 \\ 0 & 1 & \cdots & 0 & \vdots \\ \vdots & 0 & & \vdots & \vdots \\ \vdots & \vdots & & \vdots & \vdots \\ 0 & 0 & \vdots & 1 & -a_{n-1} \end{vmatrix}$$

Le determinant de $X \cdot 1_L - m_x$ est donc:

$$\begin{vmatrix} X & 0 & \cdots & 0 & a_0 \\ -1 & X & & 0 & a_1 \\ 0 & -1 & & 0 & \vdots \\ \vdots & \vdots & & \vdots & \vdots \\ \vdots & \vdots & & X & a_{n-2} \\ 0 & 0 & & -1 & X + a_{n-1} \end{vmatrix}$$

En développant on obtient le polynôme caractéristique de x, qui est donc égal au polynôme minimal $X^n + a_{n-1}X^{n-1} + ... + a_0$. D'aprés (2) on en déduit $Tr(x) = -a_{n-1}$ et $N(x) = (-1)^n a_0$.

Or, comme a est primitif, on a $F(X) = (X - x_1)...(X - a_n)$, d'où, en comparant,

$$Tr(x) = x_1 + ... + x_n \text{ et } N(x) = x_1...x_n$$

Passons maintenant au cas général, et posons $r = [L : k[x]]$ .Il nous suffit de montrer que le polynôme caractéristique $P(X)$ de x relativement à L et K est égal à la puissance $r\_éme$ du polynôme minimal de x sur K. On soint $(y\imath)_{\imath=1,...,q}$ une base de $K[x]$ sur K,et $(z_\imath)_{\jmath=1,...,r}$ une base de L sur $K[x]$,alors $(y_\imath z_\jmath)$ est une base de L sur Ket on a $n = qr$.

Soint $M = (a_{\imath\jmath})$ la matrice de la multiplication par x dans $K[x]$ par rapport à la base $(y_\imath)$: ainsi $xy_\imath = xy_\imath = \sum a_{\imath h} y_h$.On a alors

$$x(y_\imath z_\jmath) = \left(\sum_h a_{\imath h} y_h\right) z_\jmath = \sum_h a_{\imath h}(y_h z_\jmath)$$

Si on ordonne lexicographiquement la base $(y_\iota z_j)$ de L sur K, on voit donc que la matrice $M^{'}$ de la multiplication par x dans L par rapport à cette base se répresente sous la forme d'un tableau

diagonal de matrices

$$M_1 = \begin{vmatrix} M & 0 & \cdots & 0 \\ 0 & M & \cdots & 0 \\ - & - & \cdots & \vdots \\ 0 & 0 & \cdots & M \end{vmatrix}$$

La matrice $X \cdot I - M_1$ se présente donc comme tableau diagonal des matrices $X \cdot I_q - M_1$, d'où $\det(X \cdot I_n - M_1) = (\det(X \cdot I_q - M))^r$.

Or le premier membre est $P(X)$, et $\det(X \cdot I_n - M)$ est le polynôme minimal de x sur K d'aprés la première partie.

Donnons enfin un résultat sur les traces et normes d'éléments entiers.

Proposition 3.2.2 *Soint A un anneau intègre, K son corps des fractions, L une extension de degré fini de K, et x un élément de L entier sur A; on suppose K de caractéristique* 0.

Alors les coefficient du polynôme caractéristique $P(X)$ de x relativemment à L et K en particulier $Tr_{L/K}(x)$ et $N_{L/K}(x)$, sont entier sur A.

Utilisons la proposition 1: on a $P(X) = (X - x_1)...(X - x_n)$; les coefficients de $P(x)$ sont donc, au signe prés, des sommes de produits des $x_{\iota j}$ il suffit de montrer que les x_i sont entiers sur A.

Or chaque x_ι est un conjugué de x sur K et on a un $K-$isomorphisme $\sigma\iota : K[x] \to K[x_\iota]$ tel que $\sigma_\iota(x) = x_\iota$ En appliquant $\sigma = \sigma_\iota$ à une équation de dépendance intégrale de x sur A.

On obtient une équation de dépendance intégrale de $x\iota$ sur A.

Corollaire 3.2.1 *Supposonsde plus A intégralement clos.Alors les coefficients du polynôme caractéristique de x, en particuler $Tr_{L/K(x)}$ et $N_{L/K}(x)$,sont élément de A.*

En effet ces coefficients sont élément de K par définition entiers sur A par la proposition 2.

On remarquera que les quantités $x + \sigma(x)$ et $x \cdot \sigma(x)$ utilisées dans l'étude des corps quadratique sont la racine et la norme de x. On y a prouvé un cas particulier du corrolaire ci-dessus.

3.3 Corps cyclotomique

On appelle corps cyclotomique tous corps de nombres engendré sur Q par des racines de l'unité. Ètant donné un nombre prémier p, nous designerons par z une racine primitive $p^{-ème}$de l'unité

(dans C par exemple), et nous allons étudier le corps cyclotomique $Q[z]$. Le nombre z est racine du polynôme $X^P - 1$; comme z est $\neq 1$, il est aussi racine du polynôme :

$\frac{X^P - 1}{X - 1} = X^{P-1} + X^{P-2} + ... + X + 1$, appellé polynôme cyclotomique. Il n'est nullement évident que ce polynôme est irréductible sur Q (ce qui revient à dire que le corps $Q[z]$ est degré $p - 1$).

Pour le démontre nous aurons besoin du CRITÈRE D'EISENSTEIN. Soint A un anneau principal $p \in A$ un élément premier de A et $F(X) = X^n + a_{n-1}X^{n-1} + ... + a_1X + a_0$ un élément de $A[X]$

tel que p divise tous les $a_\imath (0 \leq \imath \leq n-1)$, mais que p^2 ne divise pas a_0.Alors $F[X]$ est irréductible sur le corps des fractions K de A.

Supposons en effets que l'on ait $F(X) = G.H$ avec $G, H \in K[X]$, G et H unitaires. Les racines de F sont entièrre sur A. Or toute racine de G (resp $.H$) est racine de F, donc est entièr sur A.

Or les coefficients de G (resp $.H$) sont des sommes de produits des racines de G (resp $.H$); ils sont donc entiers sur A. Comme A est principal, donc intégralement clos, on a

$G \in A[X]$ et $H \in A[X]$.

Soint alors $\overline{F}, \overline{G}, \overline{H}$ les images de F, G, H dans $(A/A_P)[X]$; on a $\overline{F} = \overline{G} \cdot \overline{H}$. d'aprés l'hypothése sur les $a_\imath$, on a $\overline{F} = X^n$. Comme A/A_p est un anneau intégre, la décomposition $X^n = \overline{G} \cdot \overline{H}$ est nécessairement de la forme $X^n = X^q \cdot X^{n-q}$ (car $\overline{G}$ et $\overline{H}$ sont unitaire); d'où $\overline{G} = X^q$ et $\overline{H} = X^{n-q}$. Si G et H sont tous deux non constant, on en déduit que p divise les termes constants de G et H

donc p^2 divise le terme constant a_0 de F; contrairement à l'hypothèse. Donc G ou H est constant, et F est irréductible.

Exemple 3.3.1 *Le polynôme* $X^3 - 2X + 6$ *est irréductible sur* Q *(prendre* $p = 2, A = Z$*).*

Théorème 3.3.1 *pout tout nombre premier* p*, le polynôme cyclotomique:*
$X^{p-1} + X^{p-2} ... + X + 1$ *est irréductible dons* $Q[X]$.

Posons en effet $X = Y + 1$. On a

$$X^{p-1} + ... + 1 = \frac{X^p - 1}{X - 1} = \frac{(Y+1)^p - 1}{Y}$$

$$= Y^{p-1} + \sum_{j=p-1}^{1} \begin{pmatrix} P \\ j \end{pmatrix} Y^{j-1} = F_1(Y)$$

Or p divise tous les coefficients binômiaux $\begin{pmatrix} p \\ j \end{pmatrix}$, mais p^2 ne divise pas le terme constant $\begin{pmatrix} p \\ 1 \end{pmatrix} = p$. Donc $F_1(Y)$ est irréductible par le critère d'Eisenstein, donc aussi le polynôme cyclotomique.

Soit toujours z une racine primitive $p-éme$ de l'unité. Il résulte du que le corps $Q[z]$ est de degré $p-1$; donc $(1, z, ..., z^{p-2})$ est unebase de $Q[z]$ sur Q. Nous allons étudier l'anneau des entiers

de $Q[z]$ et montrer que c'est $Z[z]$.

Pour cela nous aurons besoin de calculer quelque trace et normes (on écrira $Tr(x)$ et $N(x)$ au lieu de $Tr_{Q[z]/Q}(x)$ et $N_{Q[z]/Q}(x)$).

Notons que les congugués de z sur Q sont les $z^j \quad (j = 1, ..., p-1)$.

L'irréductibilité du polynôme cyclotomique donne aussitôt;

1. $Tr(x)$ et $N(x) = -1 \quad Tr(1) = p - 1$

   D'où $Tr(z^j) = -1$ pour $j = 1, ..., p-1$ et donc

2. $Tr(1-z) = Tr(1-z^2) = ... = Tr(1-z^{p-1}) = p.$

   D'autre part le calcule fait dans le montre que $N(z-1) = (-1)^{p-1} p$:∩

   d'où $N(1-z) = p$.Comme la norme de $1-z$ est le produit des conjugués de $1-z$, on a donc

3. $p = (1-z)(1-z^2)...(1-z^{p-1})$

   Notons A l'anneau des entiers de $Q[z]$ .Il contient évidemment z et ses puissances. On va montrer qu'on a

4. $A(1-z) \cap Z = pZ$

   En effet on a $p \in A(1-z)$ d'aprés (3), d'où $A(1-z) \cap Z \supset pZ$,comme pZ est idéal maximal de Z, la relation $A(1-z) \cap Z \neq pZ$ entrainerait $A(1-z) \cap Z = Z$, et $1-z$ serait inversible dans A; ses conjugués $1-z$, le seraient alors aussi, et donc p également d'aprés (4), ainsi $\frac{1}{p}$ serait entier sur Z, ce qui est sbsurde. montrons enfin que tout $y \in A$, on a

5. $Tr(y(1-z)) \in pZ$

En effet chaque conjugué $y_j(1-z^j)$ de $y(1-z)$ est multiple (dans A) de $1-z^j$, lequel est multiple de $1-z$ car

$$1-z^j = (1-z)\left(1+z+...+z^{j-1}\right)$$

comme la trace est la somme des conjugués, on a donc

$$Tr(y(1-z)) \in A(1-z)$$

d'où (5), d'aprés (4), car la trace d'un entier est dans Z

Ceci étant, nous sommes en mesure de déterminer l'anneau des entiers de $Q[z]$

Théorème 3.3.2 *Soint p un nombre premier et z une racine primitive $p-$éme de l'unité (dans C). Alors l'anneau A des entiers du corps cyclotomique $Q(z)$ est $Z[z]$, et $(1, z, ..., z^{p-1})$ est une base*

du $Z-$module A.

En effet soit $x = a_0 + a_1 z + ... + a_{p-2} z^{p-2}\,(a_i \in Q)$ un élément de A.

On a alors

$$x\,(1-z) = a_0\,(1-z) + a_1\left(z - z^2\right) + ... + a_{p-2}\left(z^{p-2} - z^{p-1}\right)$$

En prenant les traces, il résulte de 1 et de 2 que

$$Tr\,(x\,(1-z)) = a_0 Tr\,(1-z) = a_0 p$$

3.4 Racines de l'unité

On a appelé racines de l'unité dans un groupe l'ensemble des éléments d'ordre fini. Dans le groupe multiplicatif d'un corps $\mathbb{k}$, les racines $n^{iémes}$ de l'unité seront les racines du polynôme $X^n - 1$. Il n'y a aucune raison pour que ce polynôme ait n racines dans $\mathbb{k}$, mais peu importe, on peut considérer son corps de rupture sur $\mathbb{k}$. [8]

3.5 Racines n^{iémes} de l'unité

Pour tout $n \geqslant 1$, on appellera donc racine $n^{iéme}$ de l'unité sur $\mathbb{k}$ toute racine du polynôme $X^n - 1 \in \mathbb{k}\,[X]$. Ces racines ne sont pas, en général, dans $\mathbb{k}$, mais dans le corps de rupture de $X^n - 1$ sur $\mathbb{k}$.

En fait, les coefficients de $X^n - 1$ étant dans le sous-corps premier $\mathbb{k}_0$ de $\mathbb{k}$, les racines $n^{iémes}$ de l'unité seront dans le corps de rupture de $X^n - 1$ sur $\mathbb{k}_0$. De plus l'égalité

$$X^n - 1 = (X-1)(1 + X + ... + X^{n-1})$$

montre que c'est aussi le corps de rupture

$$1 + X + ... + X^{n-1}$$

sur $\mathbb{k}_0$.

Il en résulte que, pour étudier les racines de l'unité sur un corps, on peut supposer qu'il s'agit d'un corps premier: $\mathbb{k} = \mathbb{Z}/p$ (p premier) ou $\mathbb{k} = \mathbb{Q}$.

Ces racines $n^{iémes}$ forment un groupe multiplicatif dans le corps de rupture de X^n-1 sur $\Bbbk$. Ce groupe est d'ordre inférieur à n et, comme sous-gourpe multiplicatif fini du groupe multiplicatif d'un corps, il est cyclique.

Racines primitives et corps cyclotomiques.

Un générateur ω est générateur du groupe multiplicatif des racines $n^{iémes}$ et aussi élément primitif du corps de rupture de X^n-1 sur $\Bbbk$. On appelle un tel élément une racine primitive $n^{iéme}$ de l'unité sur $\Bbbk$.

On notera $\Omega_n(K)$, ou simplement Ω_n s'il n'y a pas de confusion, l'ensemble des racines primitives $n^{iémes}$ de l'unité sur $\Bbbk$. On a donc

$\omega \in \Omega_n(K) \Leftrightarrow \Bbbk(\omega)$ est le corps de rupture de X^n-1 sur $\Bbbk \Leftrightarrow$ toute racine $n^{iéme}$ de l'unité est puissance de ω.

Il résulte de cela que l'extension $\Bbbk(\omega)$ est normale, en tant que corps de rupture.

Le polynôme dérivé de X^n-1 est nX^{n-1}, d'où deux cas:

$*n \neq 0$ dans $\Bbbk$, c'est-à-dire n non multiple de car $\Bbbk$. Les seuls diviseurs de $nX^{n-1}n'$ont que 0 pour racine, donc X^n-1 est premier avec son dérivé, et il est séparable : il y a n racines $n^{iémes}$ de l'unité;

$*n=0$ dans $\Bbbk$, soit $n=mp^s$, avec $s \geqslant 1$ et m non multiple de p =car $\Bbbk$. Alors l'égalité $X^{\,n}-1=(X^m-1)^{p^s}$ montre que les racines $n^{iémes}$ de l'unité sont les m racines $m^{iémes}$, chacune répétée p^s fois.

Dans le cas où n n'est pas multiple de car $\Bbbk$ (ce qui se passe toujours si $\Bbbk$ est de caractéristique nulle) les n racines $n^{iémes}$ forment la suite

$\{1,\omega,\omega^2,...\omega^{n-1}\}$,

où ω est une racine primitive, et l'on a donc

$$X^n-1=\prod_{j=0}^{n-1}(X-\omega^\imath)$$

On déduit de cette égalité que les racines $n^{iémes}$ de l'unité sur $\mathbb{Z}/p$ sont alors les images canoniques modulo p des racines $n^{iémes}$ de l'unité sur $\mathbb{Q}$, et, en particulier les racines primitives sur $\mathbb{Z}/p$ sont, modulo p, celles sur $\mathbb{Q}$, (ceci en supposant toujours n non multiple de p).

Le corps engendré par $\Bbbk$ et les racines $n^{iémes}$ de l'unité, qui est l'extension $\Bbbk(\omega)$ où ω est primitive $n^{iéme}$, s'appelle **corps cyclotomique** d'ordre n sur $\Bbbk$.

En général, $\Bbbk$ est premier, et si l'on ne précise rien il s'agit de $\Bbbk = \mathbb{Q}$.

3.5.1 Racines primitives: premiéres propriétés

Les racines de l'unité sur $\mathbb{Q}$ sont toutes dans $\mathbb{C}$, car ce dernier contient une clôture algébrique de $\mathbb{Q}$. Une racine primitive $n^{iéme}$ de l'unité sur $\mathbb{Q}$ est $\exp \imath \frac{2\Pi}{n} \in \mathbb{C}$. sur $\mathbb{Z}/p$, $\exp \imath \frac{2\Pi}{n} \pmod p$ convient pour $n \notin p\mathbb{Z}$.

Supposons désormais n non multiple de car $\Bbbk$. Le corps $\Bbbk$ sera, au choix $\mathbb{Q}$ ou $\mathbb{Z}/p$, il suffira dans ce dernier cas de tout considérer modulo p. Si ω est racine primitive $n^{iéme}$ de l'unité sur $\Bbbk$, les autres sont les ω^q, où q est un entier positif inférieur à n premier avec n; ceci résulte du théoréme général sur les générateurs d'un groupe cyclique. Le nombre de racines primitives $n^{iémes}$ est le nombre $\varphi(n)$ d'entiers positifs inférieurs à n premiers avec n. On a donc card $\Omega_n = \varphi(n)$, et $\varphi(n)$ est aussi le degré sur $\Bbbk$ du corps cyclotomique d'ordre n, comme on le verra un peu plus loin. Il est clair que pour n premier toute racine $n^{iéme}$ de l'unité autre que 1est primitive. D'autre part, si α est une racine $n^{iéme}$ de l'unité, elle est d'ordre m diviseur de n dans le groupe des racines, donc c'est une racine primitive $\left(\frac{n}{m}\right)^{iéme}$ de l'unité. toute racine $n^{iéme}$ de l'unité est racine primitive $m^{iéme}$ pour un unique diviseur m de n On en déduit, en particulier, que l'ensemble des racines $n^{iémes}$ de l'unité est l'union disjointe $\cup d/n\Omega_{d,}$ d'où l'on retrouve l'égalité $n = \sum_{d/n} \varphi(d)$. Des exemples de racines primitives $n^{iémes}$ de l'unité sont, pour les petites valeurs de n, 1, -1, $\jmath$ et $\imath$ (respectivement $n = 1, 2, 3, 4$). Une porpriété des racines primitives en caractéristique nulle**.** plaçons-nous en caractéristique 0, donc dans le corps $\mathbb{Q}$. On va montrer que les racines primitives $n^{iémes}$ de l'unité sont toutes conjuguées les unes des autres. Pour cela, considérons pour tout $\omega \in \Omega_n$ son polynôme minimum P_ω. Il divise dans $\mathbb{Q}[x]$ le polynôme $X^n - 1$ qui est unitaire sur $\mathbb{Z}$, donc qu'en fait P_ω est le méme pour tous les $\omega \in \Omega_n$, et qu'il est de degré $\varphi(n)$.

1. Considérons pour cela le PPCM des polynômes P_ω quand ω parcourt Ω_n.

   C'est un polynôme $\Phi_n \in \mathbb{Q}[x]$ qui divise aussi $X^n - 1$ (car le dernier est un multiple commun des P_ω), donc il est unitaire sur $\mathbb{Z}$; c'est le générateur dans $\mathbb{Q}[x]$ de l'idéal

des polynômes ayant tous les éléments de Ω_n pour racines. Montrons qu'en fait Φ_n n'est autre que le poduit $\prod_{\omega\in\Omega_n}(x-\omega)$. Considérons pour cela un facteur irréductible $\mathbb{R}$ de Φ_n sur $\mathbb{Q}$; $\mathbb{R}$ est unitaire sur $\mathbb{Z}$. Si $\mathbb{R}$ ne s'annulait sur aucun des $\omega\in\Omega_n, \frac{\Phi_n}{R}$ serait dans l'idéal ci-dessus, donc multiple de Φ_n ce qui est absurde. Donc $\mathbb{R}$ s'annule en un point $\alpha\in\Omega_n$ et le $\mathbb{Q}-$isomorphisme $\mathbb{Q}[X]/\mathbb{R}=\mathbb{Q}(\alpha)$ montre que toutes les racines de $\mathbb{R}$ sont en fait des racines primitives $n^{iémes}$ de l'unité sur $\mathbb{Q}$. Ceci prouve bien

$\Phi_n(X)=\prod_{\omega\in\Omega_n}(x-\omega)$, polynôme de degré $\varphi(n)$, ou encore:

$\Phi_n(X)=\prod_{\substack{1\le s\le n\\ \text{spremieravecn}}}(X-\alpha^s)$,où α est un élément de Ω_n.

2. Il nous reste à montrer que le polynôme minimum d'un élément ω arbitraire de Ω_n est égal à Φ_n ce qui montrera que Φ_n est irréductible sur $\mathbb{Q}$ et que les racines primitives forment une classe de conjugasion.

On sait en tout cas que $P_\omega\in\mathbb{Q}[X]$ est irréductible, qu'il est unitaire sur $\mathbb{Z}$, et que c'est un diviseur dans $\mathbb{Q}[X]$, donc dans $\mathbb{Z}[X]$, du polynôme Φ_n unitaire sur $\mathbb{Z}$. On peut écrire, dans $\mathbb{Z}[X]$, $\Phi_n=P_\omega T$. On va montrer que, pour tout p premier non diviseur de n, ω^p est racine de P_ω, donc que ω^p est conjugué de ω; l'égalité $P_{\omega^p}=P_\omega$ pour p premier non diviseur de n implique bien $P_{\omega^m}=P_\omega$ pour tout m premier avec n, et les éléments de Ω_n auront alors méme polynôme minimum. Soit donc p premier non diviseur de n. Le polynôme minimum P_{ω^p} de ω^p vérifie aussi $\Phi_n=P_{\omega^pS}$ dans $\mathbb{Z}[X]$. Si P_ω est différent de P_{ω^p}, la relation P_ω/P_{ω^pS} implique, dans l'anneau factoriel $\mathbb{Z}[X]$, la divisibilité de S par P_ω, car P_ω et P_{ω^p} sont premiers. posons donc $S=P_\omega V$ dans $\mathbb{Z}[X]$, d'où il résulte

$\Phi_n=P_{\omega^p}P_{\omega V}$. Considérons alors $\mathbb{Q}(X)=P_{\omega^p}(X^p)$. C'est un polynôme sur $\mathbb{Q}$ nul pour $X=\omega$, donc il est multiple dans $\mathbb{Q}[X]$ et, par suite, dans $\mathbb{Z}[X]$, de P_ω, soit $\mathbb{Q}=P_\omega D$. Modulo p, on a $\overline{\mathbb{Q}}=(\overline{p}_{\omega^p})^p$ car dans $\mathbb{Z}/p$ un élément est égal à sa puissance $p^{iéme}$. Tout facteur irréductible de $\overline{p}_\omega$ dans $\mathbb{Z}/p\,[X]$ divise $(\overline{p}_{\omega^p})^p$, donc divise $\overline{p}_{\omega^p}$ et, par suite, son carré divise X^n-1.

Mais, comme n n'est pas multiple de P, X^n-1 est séparable sur $\mathbb{Z}/p$, donc n'y a pas de facteurs carrés, d'où la contradication quand on suppose P_ω différent de P_{ω^P}. On a donc montré: En caractéristique nulle les racines primitives $n^{iémes}$ de l'unité forment une classe

de conjugasion. Il en résulte, en notant comme toujours $\varphi(n)$ le nombre d'entiers inférieurs à n premiers avec n: Le degré sur $\mathbb{Q}$ d'une racine $n^{iéme}$ primitive de l'unité est $\varphi(n)$; c'est donc là le degré du corps cyclotomique. Polynômes cyclotomiques. On montré en passant que le polynôme minimum commun aux racines primitives $n^{iémes}$ de l'unité sur $\mathbb{Q}$

est $\Phi_n = \prod_{\omega \in \Omega_n} (X - \omega)$.

Ce polynôme à coefficients entiers, unitaire sur $\mathbb{Z}$, irréductible sur $\mathbb{Q}$, s'appelle le polynôme cyclotomique d'ordre n. Le fait que toute racine $n^{iéme}$ est primitive $n^{iéme}$ pour un unique diviseur de n se traduit par $\prod_{d/n} \Phi_d = X^n - 1$, formule qui premet de calculer le $n^{iéme}$ polynôme cyclotomique en fonction des précédents. En caractéristique non nulle, le polynôme cyclotomique $\Phi_n = \prod_{\omega \in \Omega_n} (X - \omega)$ est le méme $(\mathrm{mod}\, p)$, mais il n'est pa alors toujours irréductible.

3.6 Quelques exemples explicites

Pour n premier, le polynôme cyclotomique Φ_n est le quotient de $X^n - 1$ par $X - 1$, puisque seul 1 n'est pas racine primitive. On a donc en ce cas $\Phi_n = 1 + x + ... + x^{n-1}$. Une racine primitive est alors de norme 1 et de trace -1. D'ailleurs, dans le cas n premier, effectuons la substitution $X = Y - 1$ Il reste $Q(Y) = 1/y\left[(1+y)^n - 1\right]$,

Soit $Q(Y) = Y^{n-1} + \sum_{\imath=1}^{n-1} C_n^\imath Y^{\imath-1}$. L'irréductibilité de Φ_n peut alors se démontrer à l'aide de celle de Q, et ceci par Eisenstein, le facteur premier n divise tous les

$C_n^\imath = n\frac{(n-1)(n-2)...(n-\imath+1)}{\imath(\imath-1)...1}$, et n^2 ne divise pas $C_n^1 = 1$. De plus, cette substitution donne, pour toute racine $\alpha \neq 1$,

$N(\alpha - 1) = (-1)^{n-1} n$, d'où $N(1-\alpha) = n$, ce qui se traduit par:

$n = (1-\alpha)(1-\alpha^2)...(1-\alpha^{n-1})$ (N *désigne la norm*). Écrivons les premier exemples de racines primitives et de polynôme cyclotomiques:

$1\Phi_1 = -1 + x$,

$-1\Phi_2 = 1 + x$,

$\jmath\Phi_3 = 1 + x + x^2$,

$\imath\Phi_4 = 1 + x^2$,

$\frac{1}{4}\left(-1+\sqrt{5}\right) + \frac{\imath}{2\sqrt{\frac{5+\sqrt{5}}{2}}}\Phi_5 = 1 + x + x^2 + x^3 + x^4$,

$-\jmath\Phi_6 = 1 - x + x^2,$
$\sqrt[3]{\frac{7}{2}\left(1+\sqrt[3]{-3}\right)}\Phi_7 = 1 + x + x^2 + x^3$
$\frac{\imath+1}{\sqrt{2}}\Phi_8 = 1 + x^4,$
$\sqrt[3]{\jmath}\Phi_9 = 1 + x^3 + x^6,$
$-\sqrt[5]{-1}$
$\Phi_{10} = 1 - x + x^2 - x^3 + x^4.$

3.7 Sommes De 2 Carrés

L'étude des nombres premiers de $\mathbb{Z}[\imath]$ nous raméne à celle des nombres premiers de $\mathbb{Z}$ qui sont une somme de 2 carrés.

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: $P =$ ou bien $b \equiv 1 \,(\mathrm{mod}\, ulo)$. Le cas $P = 2$ est immédiat: $2 = 1 + 1$ est somme de 2 carrés. Supposons $P\rangle 2$ et premier, donc impair. Démontrons: P premier impair, $P = a^2 + b^2 \Rightarrow P \equiv 1 \,(\mathrm{mod}\, .4)$. 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 impair. Si $a = 2h$, $b = 2K + 1$, on a : $a^2 = 4h^2 \equiv 0 \,(\mathrm{mod}\, .4)$, $b^2 = 4K^2 + 4K + 1 \equiv 0 \,(\mathrm{mod}\, .4)$; d'où $P = a^2 + b^2 \equiv 1 \,(\mathrm{mod}\, .4)$. La réciproque est plus difficile: P premier $(impair)$, $P \equiv 1 \,(\mathrm{mod}\, .4) \Rightarrow P + a^2 + b^2$. Il suffit de prouver que P n'est pas un nombre premier de $\mathbb{Z}[\imath]$. On admet provisoirement le lemme suivant qui sera démontré dans le paragraphe consacré aux restes quadratiques mod. P. Soit P Premier dans $\mathbb{Z}$, $P \equiv 1 \,(\mathrm{mod}\, .4)$; il existe $x \in \mathbb{Z}$ telque $x^2 + 1 \equiv (\mathrm{mod}\, .P)$. Donc, si $P \equiv 1 \,(\mathrm{mod}\, .4)$, P Premier, il existe x telque $P/x^2 + 1 = (x + \imath)(x - \imath)$ dans $\mathbb{Z}[\imath]$. Si p était premier dans $\mathbb{Z}[\imath]$, P diviserait l'un des facteurs, par exemple:

$P/x + \imath \Rightarrow x + \imath = P(a + b\imath) \Rightarrow Pb = 1$, ce qui est impossible pour b entier. C. Q. F. D. En conséquence, on voit, que les nombres premiers P dans $\mathbb{Z}$ qui sont premiers dans $\mathbb{Z}[\imath]$ sont ceux qui ne sont pas congrus à 1 $(\mathrm{mod}\, .4)$; comme ils ne peuvent pas être congrus à 0 ou 2, ce sont ceux qui sont congurs à 3 $(\mathrm{mod}\, .4)$ $(ou, ce\ qui\ revientau\ même,\ à - 1)$. Soit: 3, 7, 11, 19, 23, 31, ... Par contre: $2, 5, 13, 17, 29, \ldots$ Sont premiers dans $\mathbb{Z}$ et non premiers dans $\mathbb{Z}[\imath]$; 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 $(\mathrm{mod}\,.4)$, le nombre 2, les carrés par faits (*somme de carrés dont l'unestnul*). Par multiplication on en obtient d'autres, d'aprés le lemme suivant.

Le produit de 2 sommes de 2 carre est une somme de 2 carrés.

$(a^2+b^2)(c^2+d^2) = (ad+bc)^2 + (ac-bd)^2$ identité de Lagrange qu' on vérifie directement, et qui résulte aussi du produit des Il en résulte bien $x \in G_P$. Enfin:

$x \in F_p^* - G_p \Leftrightarrow x^{\frac{p-1}{2}} = -1$, 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 mod *ulo* P . Il faut et il suffit que $(-1)^{\frac{p-1}{2}} = 1$, donc que $\frac{p-1}{2}$ soit pair, c'est-à-dire $P = 1 + 4h$.

Conclusion et Perspective

Dans la théorie algébriques des nombres, certains éléments sembles être spécial, il s'agit bien entendu des entiers algébriques.

Dans ce mémoire nous avons défini les entiers algébriques et établi une série de résultats, mais, c'est loi d'être un travail complet, car il existe pas mal de théorèmes importants concernant le sujet, ce qui fait un bon sujet de recherche en master et nous suggérons comme exemple d'étudié la distribution des entier (le théorème de Minkowski) ou aussi aborder la théorie de corps de classes.

Bibliographie

[1] Claude MUTAFIAN, Le défi Algébrique. Tome 2 Vuibert, Paris.

[2] J.E.Bertin, M.J.Bertin, Algébre Linéaire et Géométrie Classique. MASSON Paris 1981.

[3] N.Bourbaki, Eléments de Mathématiques, Algébre Commutative, Ch 5 et Ch 6. Hermann Paris.

[4] M. Queysanne, Algèbre, André Revue, Armond Colin, 1964.

[5] Pierre Samuel, Algèbre commutative, Secrétariat mathématiques de l'ENS Paris, 1969.

[6] Pierre Samuel, Corps de Fonctions Algébrique, Notas de Matematica n° = 28, Rio De Ganeiro, 1963.

[7] Pierre Samuel, Théorie Algébriques des nombres. Hermann, Paris, deuxième édition, 1971.

[8] Z. I. BOREVICH, and I. R. SHAFAREVICH, Number Theory,Academic Press, New York, 1966.

Résumé

Dans ce travail, nous avons étudié l'anneau des entiers d'un corps de nombres, particulièrement les extensions quadratiques et cyclotomiques.

Mots clés

Anneau des entiers, anneau intégralement clos, corps des quadratiques, corps des cyclotomiques.

Abstract

In this work we have studied the ring of a field, practically the quadratic extensions and cycloto.

Keys words

Ring of integers, integrally closd ring, quadratic corps, cyclotomi.

ملخص

تطرقنا في هذا العمل الى دراسة حلقة الأعداد الصحيحة للحقول التي تحوي Q وبصفة خاصة حقول الرباعيات و حقل دويراني

كلمات مفتاحية

حقل الأعداد الذي يحوي Q ودرجته منتهية,حلقة مغلقة كليا, حقول الرباعيات,حقل دويراني.