الجمهوريـة الجزائـريـة الديمقراطيـة الشعبيـة
République Algérienne Démocratique et Populaire
وزارة التعليـم العالـي والبحـث العلمـي
Ministère de l'Enseignement Supérieur et de la Recherche Scientifique

N° Réf :……

Centre Universitaire
Abd elhafid boussouf Mila

Institut des sciences et de la technologie **Département de Mathématiques et Informatique**

Mémoire préparé En vue de l'obtention du diplôme de Licence
En: - Filière mathématiques

Les Corps Quadratiques

Préparé par :Bourourou Loubna
Kassa raihane
Djouambi chafia
Tayebi kanza

Encadrer par :Bouguebina Mounir

Année universitaire :2014/2015

أنداء من الشكر و الثناء

أولا نشكر الله عز وجل فالفضل والمنة والثناء له سبحانه وحده، فهو الي وفقنا لإنجاز هذا العمل المتواضع فنسأله دائم التوفيق والسداد لما فيه الخير والصلاح.

كما نشكر الأستاذ المحترم، المشرف على هذا العمل، والذي نحمل له كل الحب والتقدير لإشرافه على مذكرتنا وعلى ما بذله من جهد وتحمله من مشقة جعلنا الله في موازين حسناتك نحن العارفات بفضلك العاجزات على شكرك على مجهوداتك التي بذلتها وعلى نصائحك وإرشاداتك التي قدمتها لنا شكرا لك أستاذنا.

بوغبينة منير.

وإلى كل اللذين عرفناهم وأحببناهم، والذين ساهموا في إنجاز هذا العمل من قريب أو بعيد، نهدي ثمرة جهدنا ونقول:

نتذكر أحبتنا ونحتار ...

ما هي أجمل دعوة للأخيار ...

نسأل الله العزيز الغفار ...

أن يبارك في رزقهم والأعمار ...

وأن يسعدهم

ما تعاقب الليل والنهار ...

وأن يسطر أسماءهم في عليين مع الأبرار ...

نحبكم في الله.

Les Corps Quadratiques

Bourourou Loubna
Djouambi Chafia
Kassa Raihane
Tayebi Kanza

avril

Table des matières

Introduction

Un corps de nombre est un sous corps $K \subseteq C$ tel que le degré de l'extension de corps $[K : Q]$ est fini. considérons $I_x = p \in Q[t]|p(x) = 0, x \in C$ l'ensemble des polynome annulateurs de x.on a $I_x = p(x)$ ou p_x est le polynome minimal de x.ceci implique que tout polynome annulateur $q \in I_x$ peut s'écrire de la forme $q = q_x s$ avec s un polynome quelconque. Les K conjugués de $\alpha \in K$ sont les éléments $\sigma_i(\alpha)(i = 1, ..., n)$ ou les $\sigma_i : K \longrightarrow C$ sont des monomorphismes associés á K. De plus,les élément $\sigma_i(\alpha)$ sont les n zéro distincts du polynome minimal. Un nombre complexe θ est un entier algébrique s'ils existe un polynome unitaire $p \in Q[t]$ avec des coefficients entiers tel que $P(\theta) = 0$. On définit $o = o_k = k \bigcap B$ l'anneau des entiers de k ou k est un corps de nombre et B est l'ensemble des entiers algébriques on a $Z \subseteq o$. Pour $k = Q(\theta)$ tel que $deg(P_\theta) = n, \{1, \theta, ..., \theta^{n-1}\}$ est une base pour K. De plus,$\{1, \theta, ..., \theta^{n-1}\}$ est une base d'entiers si elle engendre $Q(\theta)$.

Chapitre 1

Groupes, Anneaux et Corps

Dans ce premier chapitre on appelle prévement les notion de groupe,d'anneau et de corps dont nous aurons besoin par la suite.Un attention toute particulière est donnée aux idéaux dans un anneau et notamment aux idéaux premiers et maximaux.

1.1 Groupes

soit G un ensemble non vide muni d'une loi de composition interne $*$

Definition 1 *:*
$(G,*)$ *est un groupe si :*
- $*$ *est associative.*
$$\forall x,y,z \in G; (x*y)*z = x*(y*z)$$
- $*$ *admet un élément neutre* e*.*
$$\exists e \in G, \forall x \in G : x*e = e*x = x$$
- *tout élément de* G *admet un symetrique* $x^{'}$ *pour* $*$*.*
$$\forall x \in G, \exists x^{'} \in G : x*x^{'} = x^{'}*x = e$$

Si $*$ *est commutative, on dit que* $(G,*)$ *est un groupe commutatif ou abélien.*

Exemple :
1)$(\mathbb{Z},+),(\mathbb{Q},+),(\mathbb{R},+)$ et $(\mathbb{C},+)$ sont des groupes abélien.
2) $(\mathbb{N},+)$ n'est pas un groupe car aucun élément autre que 0 n'a de symétrique.

1.2 Anneaux

Definition 2 *:*
soit A un ensemble muni de deux loi de composition internes note $+$ et $.$ on dit que $(A,+,.)$ est un anneaux si :

- *$(A,+)$ est un groupe abélien le neutre de la loi $+$ est not 0.*
- *la loi $.$ est associative et doit admet un élément neutre pour $*$ noté 1_A.*
- *la loi $.$ est distributive par rapport á la loi $+$ on peut résumer par $\forall X,Y,Z \in A$ on a :*

$$X*(Y+Z) = X*Y + X*Z$$
$$(X+Y)*Z = X*Z + Y*Z$$

Exemple :
1)$(\mathbb{Z},+,*),(\mathbb{Q},+,*)$ et $(\mathbb{R}[x],+,*))$ sont des anneaux commutatifs.
2)l'ensemble des fonctions d'un ensemble X dans R est un anneau pour les lois :

$$(f+g)(x) = f(x) + g(x)$$
$$(f.g)(x) = f(x).g(x)$$

1.3 Corps

Definition 3 *:*
Soit K un ensemble et soit $+$. deux lois internes sur K.le triplet $(K,+,.)$ posséde une structure de corps si :

- *$(K,+,.)$ a une structure d'anneau commutatif unitaire.*
- *$(K \setminus \{0\})$ a une structure de groupe (abélien).*

Exemple :
$\mathbb{Q},\mathbb{R}$ et $\mathbb{C}$ sont des structures de corps pour leur addition et multiplication respectives,d'autre corps existent mais ils sont beaucoup moins accessibles.Nous pensons par exemple,au corps des quaternions d'hamilton.
Remarque : Par plus d'écriture et quand aucune confusion n'est á crainde nous noterons K le corps $(K,+,.)$.

Definition 4 *:*
Soit K un corps on dit qu'une partie K' de K est un sous corps de K si :
a) K' est un sous anneau de K.
b) les relations $x \neq 0$ et $x \in K'$ impliquent $x^{-1} \in K'$.

Exemple :

$\mathbb{Q}$ et un sous corps de $\mathbb{R}$ et $\mathbb{R}$ est un sous corps de $\mathbb{C}$.

Proposition 1 *:*

Les seuls idéaux d'un corps sont l'idéal nul et le corps tout entier.Réciproquement si A set un anneau n'ayant comme seuls idéaux que l'déal nul et lui même alors A est un corps.

Preuve :

1) Supposons que K est un corps.soit I un idéal non nul de A.Soit donc X un élément non nul de$I$.X est par définition d'un corps,inversible dans K soit X^{-1} l'inverse de X dans K.X^{-1}.X par définition d'un idéal,lélément de I mais X^{-1}.X est égale a l'élément unite de K donc $1 \in I$ et $I = K$.

2) Supposons maintenant que les seuls idéaux de l'anneau A sont l'idéal nul de A tout entier.il suffit de montrer que tout les élément non nul de A sont inversibles.soit $x \neq 0$ un élément de A. soit (x) l'idéal engendré par x comme x n'est pas nul,cet idéal n'est pas nul non plus .il est alors égale á A tout entier l'unité de A est donc élément de (x),ceci signifie qu'il existe y dans A tel que $x.y = 1.x$ est donc inversible d'inverce y.

Chapitre 2

Corps Quadratique

2.1 Extension du corps

En mathématique plus particulierement en algébre l'éxtension du corps commutatif K set un corps L qui contiet K comme sous corps.
par exemple : $\mathbb{C}$ le corps des nombres complexes est une extension de $\mathbb{Q}$.le corps des nombres réel lequel est lui méme un extension de $\mathbb{Q}$.le corps des nombres rationnels,on note parfois $L|K$ pour indiquer que L est une extension de K.

Definition 5 *:*
Soit K un corps ,extension de K est un couple (L, j) ou L est un corps et j un morphisme de corps de K dans L (les morphisme de corps étant systématiquement injectifs). on montrer qu'il existe un sur corps N de K et un morphisme corps $f : N \longrightarrow L$ tel que la restriction de f á K soit égal aj. ainsi l'extention (L, j) peut étre identifée á l'extension (N, i) avec l'iclusion i pour cette raison les extensions d'un corps sont généralement cosidérées comme dessur corps notont cependant que certains constructions d'extensions ne sont pas naturellement des sur corps (par exemple le corps de rupture) et que la definition d'extension ci dessus plus de souplesse.

une extension de$L|K$ est un sous corps de L contenant K si v est un sous ensemble de L alors on definit de corps $K(v)$ comme le plus petit sous corps de L contenant K et v il est constutié des éléments de L pouvant étre obtenus á partir d'élément de K et de v grâce á un nombre fini d'additions de multiplication et d'inversion,ou encore :pouvant étre obtenus en appliquant á

des lélément de v une fraction rationnelle (a plusieurs variables) á coefficients dans K si $L = K(v)$ on dit que L est engendré par v.
Morphisme d'extension :

si E et F des extensions de K un morphisme (ou K morphisme) de E dans F est un morphisme d'anneau qui quivant l'identité sur K un tel morphisme est toujours injectif car son noyan est un idéal propre de E.
un isomorphisme de K extensions est un K morphisme surjectif (donc bijectif) entre deux extensions de K.
un automorphisme de K extensions est un K morphisme surjectif (donc bijectif) d'une extension de K dans elle méme.

2.2 Le polynôme

Definition 6 *:*
Un polynôme et une expression formée uniquement de produits et de sommes de constants et d'indéterminées habituellement notées $X, Y, Z....$ ces objets sont largement utilisés en partique,ne serait ce que parce qu'ils donnent localement une valeur approchée de toute fonction dérivable et permettent de repésenter des formes lisses.

Un polynôme en algébre génerale,á une indéterminée sur un anneau (unitaire) est une expretion de la forme :

$$a_0 + a_1X^1 + a_2X^2 + ... + a_nX^n$$

óu X est un symbole appelé indéterminée du polynôme,supposé être distinct de tout élément de l'anneau,les coefficients a_i sont dans l'anneau,et n est un entier naturel. Si,en mathématique appliquées,en analyse et en algebre lineaire,il est frequent de confondre le polynôme avec la fonction polynôme,il n'en est pas de méme en algébre générale cet article traite principalement du polynôme formel á une indétermineé.

2.3 Corps quadratique

Definition 7 *:*

Un corps quadratique est un corps de nombres K de degré 2 sur $\mathbb{Q}$ on peut ecrire $K = \mathbb{Q}(\theta)$ ou θ est un entier algebrique .

De plus,on a vu $(cf[1.p22])$ *que le degré de l'extension,dans notre cas* $[Q(\theta) : Q] = 2$*,est égal au degré du pôlynome minimal.ceci implique que* θ *est zéro du pôlynome*

$$t^2 + at + b(a, b \in Z).....(1)$$

On peut donc defini θ *par :*

$$\theta = \frac{-a \pm \sqrt{(a^2-4b)}}{2}.....(2)$$

Exemple :
Le corps $Q(\sqrt{2})$ est un corps quadratique car $\sqrt{2}$ est un entier algebrique qui est zéro de $x^2 - 2$,pôlynome unitaire de degré 2.
le corps $Q(\frac{1}{2} + \frac{1}{2}\sqrt{5})$ est un corps quadratique car $\frac{1}{2} + \frac{1}{2}\sqrt{5}$ est un entier algebrique qui est zéro de $y^2 - y - 1$,pôlynome unitaire de degré 2.

Proposition 2 *:*
Les corps quadratiques sont précisément de la forme $Q(\sqrt{d})$ *pour* d *un entier rationnel sans facteur carré.*

Démonstration :
Soit $a^2 - 4b = r^2 d$ ou $r, d \in Z$ et d est sans facteur carré (i.e :d n'est pas divisible par le carré d'un nombre premiers) par (1),$a^2 - 4b \in Z$ peut s'écrire comme le produit de nombres premiers par la factorisation en facteurs premiers,il est donc toujours possible de trouver de tels r, d alors par (2)

$$\theta = \frac{-a \pm r\sqrt{d}}{2}$$

comme $a, r, 2 \in Z \subset Q$,on a $Q(\theta) = Q(\sqrt{d})$.
Exemple :
On a $Q(\sqrt{5}) = Q(\frac{1}{2} + \frac{1}{2}\sqrt{5})$ pour un $d < 0$ on peut prendre l'exemple $Q(e^{\frac{2\pi i}{3}}) = Q(\frac{-1+i\sqrt{3}}{2}) = Q(\sqrt{-3})$.
Théorem 1.2 :

Soit d un entier rationnel sans facteur careé,alors les entiers de $Q(\sqrt{d})$ sont :
a) $Z[\sqrt{d}]$ si $d \ncong 1(mod 4)$.
b) $Z[\frac{1}{2} + \frac{1}{2}\sqrt{d}]$ si $d \equiv 1(mod 4)$.
Demonstration :

$\alpha \in Q(\sqrt{d}) \backslash Q$ peut s'ecrire de la forme $\alpha = r + s\sqrt{d}$ pour $r, s \in Q$ suite á la réductibilité de r et s grâce á leurs facteurs communs,on obtient

$$\alpha = \frac{a+b\sqrt{d}}{c} a, b, c \in Z, c > 0 .....(3)$$

ou aucun nombre premier ne divise a, b, c.
De plus on a $(cf.[1, p45], lemme 2.13)$ α est entier algebrique $\Leftrightarrow$ les coefficients du pôlynome minimal sont des entiers rationnels
Calculons ce pôlynome minimal :

$$(t - (\frac{a+b\sqrt{d}}{c}))(t - (\frac{a-b\sqrt{d}}{c})) = t^2 - \frac{2a}{c}t + \frac{a^2+b^2d}{c^2}$$

par conséquent

$$\frac{a^2+b^2d}{c} \in Z \text{ et } \frac{2a}{c} \in Z .....(4)$$

dans le cas ou c et a (respectivement b) ont un facteur premier p en commun,alors p divise b car $\frac{a^2+b^2d}{c} \in Z$,il existe donc un nombre premier qui divise á la fois a, b, c ce qui contredit l'hypothése qu'aucun nombre ne divise a, b, c. Si c et a (respectivement b) n'ont pas de facteur premier en commun,comme $\frac{2a}{c}$ doit étre un entier,alors $c = 1$ ou $c = 2$.
Dans le cas $c = 2$,on a $\alpha = \frac{a+b\sqrt{d}}{2}$,de plus on sait par hypothése que c ne divise ni á ni b,alors a et b sont impairs,de plus par (4)

$$\frac{a^2+b^2d}{4} \in Z$$

ainsi

$$a^2 + b^2d = 0(mod4)$$

Considérons maintenant le carré de a et b (nombres impairs) :

$$a^2 = (2k+1)^2 = 4k^2 + 4k + 1 \equiv 1(mod4), k \in Z$$

par le méme raisonnement,on obtient

$$b^2 \equiv 1(mod4)$$

dans le cas ,$c = 1$ on a $\alpha = a + b\sqrt{d}$ par (3),il ensuit que α est un entier sur $Q(\sqrt{d})$ car $a, b \in Z \subset Q$.
Conclusion :

Si $d \equiv 1(mod4)$,alors $a, b \equiv 1(mod4)$ par conséquent $c = 2$ avec a, b impairs et b) est montré.
Si $d \ncong 1(mod4)$ alors $c = 1$ et a) est montré.
Exemple :

Les entiers de $Q(\sqrt{5})$ sont $Z[\frac{1}{2}+\frac{1}{2}\sqrt{5}]$ car $5 \equiv 1(mod4)$ tandis que les entiers de $Q(\sqrt{3})$ sont $Z[\sqrt{3}]$ car $3 \not\equiv 1(mod4)$.

Théoreme 1.3 :

Si$d \not\equiv 1(mod4)$,alors $Q(\sqrt{d})$ a une base d'entiers de la forme $\{1, \sqrt{d}\}$ et un discriminant égal á $4d$.

Si $d \equiv 1(mod4)$,alors $Q(\sqrt{d})$ á une base d'entiers de la forme $\{1, \frac{1}{2}+\frac{1}{2}\sqrt{d}\}$ et un discriminant égal á d.

Démonstration :

Les base d'entiers proviennent directement théoreme 1.2 d'aprés la nature de d,il ressort deux types de bases,$\{1, \sqrt{d}\}$ et $\{1, \frac{1}{2}+\frac{1}{2}\sqrt{d}\}$ permettant dengendrer 0_k ou $k = Q(\theta)$,comme $0_k = k \cap B$,ces bases seront des bases d'entiers pour $k = Q(\theta)$. Le discriminant sa calcule a l'aide des monomorphismes associés á $Q(o)$ pour $\alpha = r + s\sqrt{d} \in Q(o))$

$$\alpha 1(r + s\sqrt{d}) = r + s\sqrt{d}$$
$$\alpha 2(r + s\sqrt{d} = r - s\sqrt{d})$$

le discriminant par rapport á ces deux bases se calcule donc comme suit :

$$\begin{vmatrix} 1 & \sqrt{d} \\ 1 & -\sqrt{d} \end{vmatrix}^2 = (-2\sqrt{d})^2 = 4d$$

$$\begin{vmatrix} 1 & \frac{1}{2}+\frac{1}{2}\sqrt{d} \\ 1 & \frac{1}{2}-\frac{1}{2}\sqrt{d} \end{vmatrix}^2 = (-\sqrt{d}^2) = d$$

Exemple :

Le corps $Q(\sqrt{3})$ á pour base $1, \sqrt{3}$ et pour discriminant 12 car $3 \equiv 1(mod4)$ d'autre part,le corps $Q(\sqrt{5})$ á pour base $\{1, \frac{1}{2}+\frac{1}{2}\sqrt{5}\}$

Remarque :

on peut voir que $\{1, \sqrt{5}\}$ et $\{1, \frac{1}{2}+\frac{1}{2}\sqrt{5}\}$ sont des Q bases car $\{\sqrt{5}, \frac{1}{2}+\frac{1}{2}\sqrt{5}\}$ sont des entiers algebriques de $Q(\sqrt{5})$.Mais il n'est pas ceci implique que $1, \sqrt{5}$ n'est pas une base d'entiers.

Bibliographie

[1] Bouayda et Seddiki,localisation d'un anneau et corps de fraction,2011.

[2] Menoud Lorraine,corps quadratiques et corps cyclotomiques,2013.

[3] Chatelet Albert,L'arithmtique des quadratiques,1960.