République Algérienne Démocratique et Populaire
وزارة التعليم العالي و البحث العلمي
Minstère de l'Enseignement Supérieur et de la Recherche Scientifique

CENTRE UNIVERSITAIRE DE MILA
INSTITUT DES SCIENCES ET DE LA TECHNOLOGIE

Réf. ***/11***

Mémoire de fin d'étude
Présenté pour l'obtention du diplôme de

Licence Académique

Domaine : **Mathématiques et Informatique**
Filière : **Mathématiques**
Spécialité : **Mathématiques Appliquées**

Thème

Corps des nombres algèbrique

Présenté par :
Saheb Azzedine
Saad Azzeme Khaled

Dirigé par :
Boughbina Mounir

Année universitaire 2010-2011

Remerciement

Nos remerciements à nos très chers parents, frères, sœurs, collègues et amis respectives qui nous ont encouragés, soutenu durant tout notre parcours.

Un remerciement particulier à notre

encadreur Mr Boughbina Mounir.

pour sa présence, son aide et surtout

pour ses précieux conseils qui nous

ont assistés pour l'accomplissement de notre projet.

Nous tenons à exprimer nos sincères remerciements à tout le personnel de l'institut de sciences et de la technologie surtout les enseignants qui nous ont enseigné durant toutes nos années d'étude.

Enfin nous remercions toutes personnes qui ont contribué de prés ou de loin à l'achèvement de ce travail.

Merci bien.

Corps de Nombres Algébriques

avril 2011

Table des matières

Chapitre 1

Structures Algébriques

On passe en revue dans ce chapitre les différentes notions dont on aura besoin par la suite en donnant notamment les définitions et principales propriétés des groupes, anneaux et corps. Un soin particulier sera donné à l'anneau des polynômes sur un corps à la fin du chapitre. Comme on le verra les polynômes vont s'avérer être un outil puissant pour l'étude des extensions de corps et en particulier des corps de nombres.

1.1 Groupes

Soit G un ensemble muni d'une loi de composition interne c'est-à-dire d'une application $* : G \times G \longrightarrow G$ qui à deux éléments x, y dans G associe un troisième élément $z = x * y$.

Définition 1 *: L'ensemble G muni de la loi $*$ est appelé groupe si :*

1. *la loi $*$ est associative : pour tous x, y, z dans G on a*

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

2. *la loi $*$ a un élément neutre : Il existe un élément $e \in G$ tel que pour tout $x \in G$ on ait*

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

3. *Tout élément $x \in G$ a un symétrique $x^{'}$ qui est un'élément de G vérifiant :*

$$x * x^{'} = x^{'} * x = e.$$

On vérifie facilement que l'elément neutre e et le symétrique $x^{'}$ de x sont uniques. Si la loi $*$ est de plus commutative

$$x * y = y * x$$

pour tous $x, y \in G$ on dit que le groupe est commutatif ou encore abélien. Si tel est le cas la loi $*$ est notée additivement : $* = +, e = 0$ et $x^{'} = -x$. Dans le cas général elle est notée multiplicativement : $* = ., e = 1$ et $x^{'} = x^{-1}$.
Exemple : Prenons $G = \mathbb{Z}$ muni de la loi d'addition usuelle. l'addition dans $\mathbb{Z}$ est clairement associative et commutative et admet comme élément neutre $e = 0$. Le symétrique de x est $-x$. Donc $\mathbb{Z}$ est un groupe abélien pour l'addition. C'est d'ailleurs cet exemple qui a motivé la notation additive.

Définition 2 *: Une partie non vide H d'un groupe G est un sous-groupe si :*

1. *H est stable pour la la loi de G : si $x, y \in H$ alors $x.y$ est aussi dans H.*
2. *muni de la loi de G, H est lui même un groupe.*

Dans la pratique pour montrer qu'une partie non vide H est un sous-groupe il suffit de montrer que

$$x, y \in H \Longrightarrow x.y^{-1} \in H.$$

(En notation additive il suffit de montrer que $x - y \in H$). Par exemple la partie

$$H = n\mathbb{Z} = \{na, a \in \mathbb{Z}\}$$

de $\mathbb{Z}$ formée des multiples d'un entier naturel $n \in \mathbb{N}$ est un sous-groupe de $\mathbb{Z}$ pour l'addition. En effet si $x = na$ et $y = nb$ sont dans H alors $x - y = n(a - b)$ est aussi dans H. Le sous-groupe trivial de G est le sous-groupe formé de l'élément neutre.

Le nombre d'éléments d'un groupe G est appelé son ordre qui peut donc être fini ou infini. Un groupe fini est un groupe d'ordre fini. Soit S une partie de G. Le sous-groupe engendré par S est le plus petit sous-groupe de G contenant S. On le note $< S >$. C'est l'ensemble des produits finis $x_1 . . . . x_n$ avec $x_i \in S$ ou $x_i^{-1} \in S$. Quand $S = \{a\}$ avec $a \in G$, le sous-groupe $< S >=< a >$ est appelé le groupe cyclique engendré par a. Ses éléments sont les puissances a^n de a. Le groupe G est de type fini si $G =< S >$ avec S une partie finie de G. En particulier tout groupe cyclique (engendré par un

seul élément) est de type fini.
Remarque : De type fini ne veut pas dire fini. Par exemple $\mathbb{Z}$ muni de l'addition est un groupe de type fini et même cyclique engendré par 1. Mais il contient une infinité d'éléments.

Soit f une application du groupe G_1 vers le groupe G_2. On dit que f est un morphisme de groupes si

$$f(x.y) = f(x).f(y)$$

pour tous $x, y \in G_1$ (le produit de gauche étant dans le premier groupe et le produit de droite dans le second groupe). Autrement dit f préserve les structures de groupes de G_1 et G_2. Comme conséquence de cette définition on a

$$f(1_{G_1}) = 1_{G_2}$$

et

$$f(x)^{-1} = f(x^{-1}).$$

Le noyau du morphisme f est

$$Ker(f) = \{x \in G \mid f(x) = 1_{G_2}\} = f^{-1}(1_{G_2}).$$

C'est un sous-groupe de G qui détecte l'injectivité de f. En effet f est injective si et seulement si son noyau est le sous-groupe trivial de G_1. Si le morphisme f est bijectif on dit que c'est un isomorphisme (et un automorphisme si $G_1 = G_2$).

Si H est un sous-groupe du groupe abélien G (noté donc additivement) on définit une relation sur G par

$$x \Re y \Longleftrightarrow x - y \in H.$$

C'est clairement une relation d'équivalence et on dispose donc de l'ensemble quotient

$$\frac{G}{\Re} = \frac{G}{H} = \{\overline{x}, x \in G\}$$

des classes d'équivalence modulo H

$$\overline{x} = \{y \in G \mid x \Re y\}.$$

On peut définir une addition sur les classes d'equivlence par

$$\overline{x} \overline{+} \overline{y} = \overline{x + y}$$

qui fait de l'ensemble quotient un groupe commutatif (l'élément neutre est $\overline{0}$ et le symétrique de $\overline{x}$ est $\overline{-x}$). Le groupe ainsi obtenu est appelé le groupe quotient de G par H et on dispose d'un morphisme de groupes

$$\phi : G \longrightarrow \frac{G}{H}$$

qui à x associe sa classe $\overline{x}$ et de noyau exactement H.
Exemple : Soit $G = \mathbb{Z}$ muni de l'addition et soit $H = n\mathbb{Z}$ avec $n \in \mathbb{N}$. La relation d'équivalence modulo H est la relation des congruences modulo n de Gauss et on a donc

$$\frac{\mathbb{Z}}{n\mathbb{Z}} = \{0, 1, 2, \ldots, n-1\}.$$

Définition 3 *: Soit G un groupe abélien et soit H un sous-groupe de G. L'indice de H dans G noté $(G : H)$ est le cardinal du groupe quotient de G par H.*

Par exemple on a

$$(G : G) = 1$$

$$(G : 1) = \#G$$

et

$$(\mathbb{Z} : n\mathbb{Z}) = n.$$

Supposons de plus que G est fini. Par définition l'indice de H dans G est le nombre de classes d'équivalence modulo H. Chaque classe d'équivalence modulo H est de la forme $x + H = \{x + h, h \in H\}$ et son cardinal est donc celui de H. Toutes les classes d'équivalence ont donc même cardinal. On en déduit que l'ordre de G est le produit de celui de H par l'indice de H dans G :

$$(G : 1) = (G : H).(H : 1)$$

On aura donc montré le célèbre théorème de Lagrange :

Proposition 1 *: Soit G un groupe fini et soit H un sous-groupe de G. Alors l'ordre de H divise l'ordre de G.*

Exemple Tout groupe G d'ordre un nombre premier p est cyclique. En effet soit $a \neq 0 \in G$ et soit H le sous-groupe cyclique engendré par a. Alors l'ordre de H doit diviser l'ordre de G qui est p. Comme p est premier on doit avoir $H = G$.

1.2 Anneaux

Définition 4 *: Un anneau est un ensemble A muni de deux lois $+$ et $.$ telles que :*

1. *$(A, +)$ est un goupe commutatif.*
2. *la multiplication $.$ est assoxiative et a un élément neutre 1.*
3. *La multiplication est distributive par rapport à l'addition : pour tous $x, y, z \in A$ on a*
$$(x + y).z = x.z + y.z$$
et
$$z.(x + y) = z.x + z.y.$$

Si la multiplication est commutative on dit que l'anneau A est commutatif. L'élément neutre pour l'addition est noté 0. En général $1 \neq 0$ mais si $1 = 0$ alors l'anneau A est formé du seul élément 0. Par exemple $\mathbb{Z}$ muni de l'addition et de la multiplication est un anneau commutatif dans lequel $1 \neq 0$.

Un sous-groupe B (pour l'addition) d'un anneau A est appelé sous-anneau de A si $1 \in B$ et B est stable pour la multiplication : $x, y \in B \Longrightarrow x.y \in B$. Autrement dit muni des deux opérations de A, B est lui-même un anneau.

Soit A un anneau commutatif.

Définition 5 *: Une partie I d'un anneau A est un idéal de A si*

1. *$(I, +)$ est un sous-groupe de $(A, +)$.*
2. *$a.x \in I$ pour tout $a \in A$ et pour tout $x \in I$.*

Par exemple A et $\{0\}$ sont des idéaux de A. On les appelle des idéaux propres. Tous les autres idéaux sont non propres. Remarquer qu'un idéal I de A n'est pas forcément un sous-anneau de A car en gńéral il ne contient pas 1. En fait on a
$$1 \in I \Longleftrightarrow I = A.$$
Un idéal principal de A est un idéal de la forme
$$I = aA = \{a.x, x \in A\}$$
c'est l'idéal principal engendré par a. L'anneau A est dit principal si tous ses idéaux sont principaux.

Exemple : $(\mathbb{Z}, +, .))$ est un anneau principal. En effet en utilisant la division

euclidienne on montre facilement que tout sous-groupe pour l'addition de $\mathbb{Z}$ est de la forme $n\mathbb{Z}$ pour $n \in \mathbb{N}$ et donc tout idéal est de cette forme aussi.

Soient $a, b \in A$. On dit que a divise b ou que b est un multiple de a s'il existe $c \in A$ avec $b = ac$. L'idéal $I = aA$ est donc l'ensemble des multiples de a. Remarquer que a divise b si et seulement si $bA \subset aA$. Un élément a est une unité s'il a un inverse a^{-1} pour la multiplication. a est dit premier ou irréductible si $a = bc$ implique que b ou c est une unité. $a \neq 0$ est un diviseur de 0 s'il existe $b \neq 0$ tel que $a.b = 0$. Les anneaux qui n'ont pas de diviseurs de zéro sont appelés des anneaux intègres. Par exemple dans $\mathbb{Z}$, les éléments premiers sont (au signe prés) les nombres premiers p. L'equation $a.b = 0$ n'a pas de solution non nulle dans $\mathbb{Z}$ qui est donc un anneau intègre.

Définition 6 *: Un idéal propre I d'un anneau A est dit premier si $ab \in I$ implique $a \in I$ ou $b \in I$. I est dit maximal s'il n'est contenu dans aucun autre idéal propre de A.*

Proposition 2 *: Un idéal maximal est premier. Les idéaux premiers de $\mathbb{Z}$ sont de la forme $p\mathbb{Z}$ avec p un nombre premier et ils sont tous maximaux.*

Preuve : Soit I un idéal maximal. Soient $a, b \in A$ avec $ab \in I$. Supposons que $a \notin I$. Alors l'idéal $I + aA$ est égal à A, car I est maximal. Il existe alors $d \in I$ et $x \in A$ avec $d + a.x = 1$ et donc $d.b + a.b.x = b \in I$ (rappelons que A est commutatif). Ceci montre que I est premier. Tout idéal propre de $\mathbb{Z}$ est de la forme $n\mathbb{Z}$ avec $n \neq 0 \in \mathbb{N}$. Supposons que $n\mathbb{Z}$ premier. $ab \in n\mathbb{Z}$ implique $a \in n\mathbb{Z}$ ou $b \in n\mathbb{Z}$ s'écrit n divise ab implique n divise a ou n divise b, ce qui par le lemme de gauss veut dire que $n = p$ un nombre premier. Enfin $n\mathbb{Z} \subset m\mathbb{Z}$ si et seulement si m divise n. Ceci montre que tout idéal premier de $\mathbb{Z}$ est maximal.

Une application $f : A \longrightarrow B$ entre deux anneaux est un morphisme si :

$$f(x + y) = f(x) + f(y)$$

$$f(x.y) = f(x).f(y)$$

$$f(1_A) = 1_B$$

pour tous $x, y \in A$. Autrement dit f préserve les opérations d'anneau. Si f est de plus bijective, on dit que c'est un isomorphisme entre A et B. Si $A = B$, on parle d'endomorphisme et d'automorphismes, respectivement. Le noyau d'un morphisme f est :

$$Kerf = \{x \in A : f(x) = 0_B\} = f^{-1}(0_B).$$

C'est un idéal de A. L'image de f est :

$$Imf = \{f(x), x \in A\} = f(A).$$

C'est un sous-anneau de B.

Soit A un anneau et soit I un idéal de A. On définit une relation $\Re$ sur A par :

$$x\Re y \Leftrightarrow x - y \in I.$$

On verifie facilement que $\Re$ est une relation d'equivalence sur A. Sur l'ensemble quotient

$$\frac{A}{\Re} = \frac{A}{I} = \{\overline{x}, x \in A\},$$

on définit deux opérations $\overline{+}$ et $\overline{.}$ en posant : $\overline{x} \ \overline{+} \ \overline{y} = \overline{x+y}$ et $\overline{x} \ \overline{.} \ \overline{y} = \overline{x.y}$. Ces deux opérations sont bien définies et font de $\frac{A}{I}$ un anneau. C'est l'anneau quotient de A par I. Remarquer que $\overline{x} = x + I$. En particulier $\overline{0} = I$ est l'élément neutre de $\overline{+}$.

On a un morphisme canonique surjectif d'anneaux :

$$\phi : A \longrightarrow \frac{A}{I}$$

qui à x associe sa classe modulo I, $\overline{x} = x + I$ et de noyau $Ker\phi = I$. De plus il y a une correspondance bijective entre les idéaux J de A qui contiennent I et les idéaux $\overline{J}$ de $\frac{A}{I}$ donnée par $J = \phi^{-1}(\overline{J})$.

Exemple : On prend $A = \mathbb{Z}$ et $I = n\mathbb{Z}$. On a alors $x - y \in n\mathbb{Z} \Longleftrightarrow x \equiv y \ mod(n)$. L'ensemble quotient est donc l'ensemble des classes de congruence modulo n :

$$\frac{\mathbb{Z}}{n\mathbb{Z}} = \{\overline{0}, \overline{1}, \ldots, \overline{n-1}\}$$

et les opérations d'anneau sont celles bien connues de l'addition et de la multiplication des congruences.

Proposition 3 *: L'idéal I est premier si et seulement si l'anneau quotient $\frac{A}{I}$ est intègre.*

Preuve : Un anneau est intègre s'il n'a pas de diviseurs de 0. Supposons I premier et soient $\overline{a}$ et $\overline{b}$ tels que $\overline{a}.\overline{b} = \overline{0}$. donc $a.b \in I$. Comme I est premier, cela veut dire que $a \in I$ ou $b \in I$, c'est à dire que $\overline{a} = \overline{0}$ ou que $\overline{b} = \overline{0}$ et donc que l'anneau quotient est intègre. Inversement supposons l'anneau quotient intègre et soient $a, b \in A$ avec $a.b \in I$. Donc $\overline{a}.\overline{b} = 0$ et donc $\overline{a} = \overline{0}$ ou $\overline{b} = \overline{0}$, c'est à dire que $a \in I$ ou $b \in I$. Ceci montre que I est premier.

1.3 Corps

Définition 7 *: Un corps K est un anneau non nul dans lequel tout élément différent de 0 a un inverse pour la multiplication.*

Ainsi $K^* = K - \{0\}$ muni de la loi de multiplication devient un groupe qu'on appelle groupe multiplicatif de K. Par exemple $\mathbb{Q}$ l'ensemble des nombres rationnels, $\mathbb{R}$ l'ensemble des nombres réels ou $\mathbb{C}$ l'ensemble des nombres complexes sont des corps.
Un sous corps de K est une partie L de K stable pour les lois $+$ et $.$ et qui est, pour ces lois, elle-même un corps. Par exemple $\mathbb{Q}$ est un sous-corps de $\mathbb{R}$.
Un corps K est automatiquement intègre. En effet soit $a.b = 0$ et supposons $a \neq 0$. On a alors $a^{-1}.a.b = b = 0$.
Remarque : Un corps K n'a pas d'idéal propre. Autrement dit les seuls idéaux de K sont $\{0\}$ et K lui-même. En effet soit I un idéal de K non nul et soit $x \neq 0 \in I$, alors $x^{-1}.x = 1 \in I$ et donc $I = K$. En particulier tout morphisme non nul $f : K \longrightarrow L$ entre deux corps est injectif puisque, $Kerf$ etant un idéal, il doit-être égal à $\{0\}$.

Proposition 4 *: Un idéal I d'un anneau A est maximal si et seulement si l'anneau quotient $\frac{A}{I}$ est un corps.*

Preuve : Supposons I maximal et soit $\overline{x} \neq \overline{0} \in \frac{A}{I}$. Nous devons montrer que $\overline{x}$ a un inverse pour la multiplication. Comme $\overline{x} \neq \overline{0}$, $x \notin I$. L'idéal $I + xA$ doit donc être égal à A car I est maximal. Il existe donc $a \in A$ et $b \in I$ avec $b + x.a = 1$ ou encore $x.a = 1 - b \in 1 + I = \overline{1}$. Ce qui veut dire que $\overline{x}.\overline{a} = \overline{1}$ et donc $\overline{x}$ a un inverse. Inversement supposons que $\frac{A}{I}$ est un corps. Pour montrer que I est maximal, il suffit de montrer que pour tout $x \notin I$, l'idéal $I + xA$ doit être égal à A. Pour cela il faut montrer que $1 \in I + xA$. Or $x \notin I$ équivaut à $\overline{x} \neq 0$ et donc $\overline{x}$ a un inverse $\overline{y}$: $\overline{x}.\overline{y} = \overline{1}$. Donc $xy \in 1 + I$ et $1 \in I + xA$.
Exemple : On a vu que les idéaux maximaux de $\mathbb{Z}$ sont de la forme $p\mathbb{Z}$ avec p un nombre premier. Donc pour tout nombre premier p, les congruences modulo p :

$$\frac{\mathbb{Z}}{pZ} = \{\overline{0}, \overline{1}, \ldots, \overline{p-1}\}$$

forment un corps qu'on appelle le corps premier à p éléments et qu'on note $\mathbb{F}_p$.

Définition 8 *: Soit K un corps et soit S une partie non vide de K. Le sous-corps de K engendré par la partie S est le plus petit sous-corps de K contenant S. On le note $< S >$.*

Plus petit ici est entendu au sens de l'inclusion ensembliste. Remarquer aussi que la famille des sous-corps de K contenat S est non vide puisqu'elle contient toujours K. Le sous-corps engendré par S est donc l'intersection de tous les sous-corps contenant S.

1.4 Anneau des polynômes sur un corps

Soit K un corps. Un polynôme en la variable X à coefficient dans le corps K est une expression de la forme

$$P(X) = a_n X^n + a_{n-1} X^{n-1} + \ldots + a_1 X + a_0$$

avec $a_i \in K$. Si $a_n \neq 0$ l'entier n est appelé le degré du polynôme. Un polynoôme de degré n est dit unitaire si $a_n = 1$. Le polynôme nul est le polynôme dont tous les coefficients sont nuls. Notons $K[X]$ l'ensemble des polynômes à coefficients dans K. On peut définir une addition et une multiplication dans $K[X]$ par les formules

$$(\sum_i a_i X^i) + (\sum_i b_i X^i) = \sum_i (a_i + b_i) X^i$$

et

$$(\sum_i a_i X^i).(\sum_j b_j X^j) = \sum_k (\sum_{i+j=k} a_i b_j) X^k.$$

On vérifie facilement que ces deux opérations font de $K[X]$ un anneau commutatif. L'élément neutre pour l'addition est le polynôme nul et l'élément neutre pour la multiplication est $P(X) = 1$. On peut aussi multiplier un polynôme P par un scalaire $\lambda \in K$

$$(\lambda P)(X) = \lambda P(X) = \sum_i \lambda a_i X^i.$$

Ceci permet de regarder $K[X]$ comme un K-espace vectoriel de dimension infinie et de base $\{1, X, X^2, \ldots\}$.

L'anneau $K[X]$ a des propriétés trés similaires à celles de l'anneau $\mathbb{Z}$ des entiers relatifs et notamment en ce qui concerne la divisibilité. On dira qu'un polynôme Q divise un polynôme P s'il existe un autre polynôme R tel que

$$P = Q.R$$

Un polynôme sera dit irréductible si ses seuls diviseurs sont 1 et lui-même.

Chapitre 2

Extensions de Corps

Les corps de nombres seront par définition des extensions finies de $\mathbb{Q}$ le corps des nombres rationnels. L'objectif de ce chapitre est donc de définir la notion d'extension de corps et en particulier des extensions finies. On commence par rappeler les notions de caractéristique d'un corps et de corps premier. Ue extension de corps L/Ksera définie comme étant le plongement du corps K dans le corps L qui sera alors vu comme espace vectoriel sur K. Ceci permettra d'appliquer les résultats classiques de l'algèbre linéaire à cette situation et de donner un sens à des notions comme le degré d'une extension. Les polynômes vont reapparaitre ici pour définir la notion d'algébricité (éléments algébriques, extensions algébriques,...). Les extensions normales et séparables sont des exemples trés importants d'extension et on en donnera les principales propriétés à la fin du chapitre.

2.1 Caractéristique d'un Corps

Définition 9 *: Le sous-corps premier d'un corps K est le sous-corps de K engendré par $S = \{1_K\}$ avec 1_K l'élément neutre pour la multiplication de K.*

On remarque immédiatement que tout sous-corps de K contient son sous-corps premier (puisqu'il contient 1_K). En particulier le sous-corps premier est le plus petit sous-corps (non nul) de K.
Exemple : Le sous-corps premier de $\mathbb{Q}$ est $\mathbb{Q}$ lui-même. En effet comme le sous-corps premier contient 1, il va contenir tout entier $n = n.1 \in \mathbb{Z}$ et donc aussi son inverse $n^{-1} = \frac{1}{n}$. Ceci veut dire que le sous-corps premier va

contenir toute fraction $\frac{n}{m}$ avec $n, m \in \mathbb{Z}$ et $m \neq 0$, c'est-à-dire tout élément de $\mathbb{Q}$ qui s'identifie ainsi à son sous-corps premier. De même le sous-corps premier du corps fini $\mathbb{F}_p$ (pour p un nombre premier) est $\mathbb{F}_p$ lui-même. En effet les seuls sous-corps de $\mathbb{F}_p$ sont $\{0\}$ et $\mathbb{F}_p$ (car p n'a pas de diviseur et par utilisation du théorème de Lagrange sur les groupes). Comme ce sous-corps premier ne peut être égal à $\{0\}$, il doit être égal à $\mathbb{F}_p$.
Considérons le morphisme d'anneaux

$$\phi : \mathbb{Z} \longrightarrow K$$

défini par $\phi(n) = n.1_K$. Les choses seront différentes pour K selon que ce morphisme est injectif ou non :

Proposition 5 *: Soit K un corps quelconque. Le sous-corps premier de K est isomorphe soit à $\mathbb{Q}$ soit à $\mathbb{F}_p$ pour un nombre premier $p \geq 2$.*

Preuve : Si $Ker(\phi) = \{0\}$ (ϕ est injective), on peut identifier $\mathbb{Z}$ à un sous-anneau de K (en fait il est isomorphe à un sous-anneau de K). Le corps K contient donc comme sous-corps le corps $\mathbb{Q}$ des rationnels. Par un raisonnement analogue à celui de l'exemple le sous-corps premier de K contient le sous-corps $\mathbb{Q}$. Comme le sous-corps premier est par définition le plus petit sous-corps de K contenant 1, on en déduit qu'il est égal (en fait isomorphe) à $\mathbb{Q}$. Remarquer que dans ce cas le seul entier naturel n tel que $n.1_K = 0$ est $n = 0$.
Supposons maintenant que $Ker(\phi) \neq \{0\}$ (ϕ n'est pas injective). On sait que $Ker(\phi)$ est un idéal de $\mathbb{Z}$. Comme $\frac{\mathbb{Z}}{Ker(\phi)}$ est isomorphe à un sous-anneau de K, c'est un anneau intègre (sans diviseurs de 0) et donc l'idéal $Ker(\phi)$ est un idéal premier de $\mathbb{Z}$. On a donc

$$Ker(\phi) = p\mathbb{Z}$$

pour p un nombre premier et

$$\frac{\mathbb{Z}}{Ker(\phi)} = \frac{\mathbb{Z}}{p\mathbb{Z}} = \mathbb{F}_p$$

est un sous-corps de K (en fait il est isomorphe à un sous-corps de K). Ce sous-corps doit contenir le sous-corps premier de K et par le raisonnement de l'exemple il est égal (en fait isomorphe) à ce sous-corps premier. Remarquer que dans ce cas $p.1_K = 0$ et p est le plus petit entier naturel qui vérifie cette propriété.

Définition 10 *: La caractéristique de K est égale à 0 dans le premier cas et à p dans le second cas.*

Ains la caractéristique d'un corps est l'unique entier naturel k tel que $Ker(\phi) = k\mathbb{Z}$. Si K est de caractéristique 0 il contient $\mathbb{Q}$ comme sous-corps premier et si K est de caractéristique p il contient $\mathbb{F}_p$ comme sous-corps premier. On a vu que les corps $\mathbb{Q}$ et $\mathbb{F}_p$ ne contiennent pas de sous-corps propre (ils sont leurs propres sous-corps premiers).

Définition 11 *: Les corps $\mathbb{Q}$ et $\mathbb{F}_p$ sont appelés des corps premiers.*

Tout corps contient soit l'un soit l'autre (mais jamais les deux en même temps). C'est cette idée qui est derrière la définition de la caractéristique.

2.2 Extensions de Corps

Un morphisme de corps $\phi : K \longrightarrow L$ est nécéssairement injectif. En effet le noyau de ϕ est un idéal de K et comme dans un corps les seuls idéaux sont $\{0\}$ et K on doit avoir

$$Ker(\phi) = \{0\}.$$

Ceci nous amène à la définition suivante :

Définition 12 *: On appelle extension d'un corps K toute paire (L, ϕ) avec L un corps et $\phi : K \longrightarrow L$ un morphisme de corps.*

Comme ϕ est injective K est isomorphe à $Im(\phi)$ qui est un sous-corps de L. En identifiant K à son image on peut regarder K comme un sous-corps de L et on regarde ϕ comme une manière de plonger K dans L. Inversement si K est un sous-corps de L alors (L, i) est clairement une extension de K (avec i le morphisme d'inclusion $K \hookrightarrow L$). Ainsi la notion d'extension de corps est une géneralisation de celle de sous-corps.
Remarque : Si L est une extension de K alors les deux corps doivent avoir la même caractéristique. Dans la suite on omettra la mention du morphisme ϕ et on dira tout simplement que L est une extension de K. De plus on supposera que K est un sous-corps de L (puisque le plongement ϕ permet de faire ceci).
Exemple :
1) Tout corps de caractéristique 0 est une extension de $\mathbb{Q}$.

2) Tout corps de caractéristique un nombre premier p est une extension du corps fini $\mathbb{F}_p$.
3) L'inclusion $i : \mathbb{R} \hookrightarrow \mathbb{C}$ montre que $\mathbb{C}$ est une extension de $\mathbb{R}$.
4) Soit $L = \{a + ib \mid a, b \in \mathbb{Q} \wedge i^2 = -1\}$. L est un sous-corps de $\mathbb{C}$ contenant $\mathbb{Q}$ (faire $b = 0$ dans la définition de L). C'est donc une extension de $\mathbb{Q}$. De plus L est le sous-corps de $\mathbb{C}$ engendré par la partie $S = \{i\}$. En effet c'est le plus petit sous-corps de $\mathbb{C}$ contenant i.

Définition 13 *: Soient K et L deux corps avec L une extension de K. Pour toute partie non vide T de L, le sous-corps de L engendré par $K \cup T$ sera appelé l'extension de K obtenue par adjonction de T à K (dans L). On le notera $K(T)$.*

Si $T = \{\alpha\}$ est formée d'un seul élément $\alpha \in L$, on note plutôt $K(T) = K(\alpha)$ et on parle d'extension simple de K (une extension de K par adjonction d'un seul élement). De même si $T = \{\alpha_1, \alpha_2, \ldots, \alpha_n\}$, on pose $K(T) = K(\alpha_1, \ldots, \alpha_n)$.
Exemple :
1) $L = \{a + ib \mid a, b \in \mathbb{Q} \wedge i^2 = -1\}$ s'écrit donc $L = \mathbb{Q}(i)$.
2) De même $\mathbb{C} = \{a + ib \mid a, b \in \mathbb{R} \wedge i^2 = -1\}$ s'écrit $\mathbb{C} = \mathbb{R}(i)$.
3) On montre aussi facilement que $\mathbb{Q}(\sqrt{2}) = \{a + b\sqrt{2} \mid a, b \in \mathbb{Q}\}$. C'est le sous-corps de $\mathbb{R}$ engendré par $\sqrt{2}$ sur $\mathbb{Q}$.
Remarque : L'extension $K(\alpha_1, \alpha_2)$ peut-être considérée comme une adjonction successive de deux éléments sans ordre particulier : on peut écrire

$$K(\alpha_1, \alpha_2) = K(\alpha_1)(\alpha_2) = K(\alpha_2)(\alpha_1).$$

En effet on a $K(\alpha_1) \subseteq K(\alpha_1, \alpha_2)$ et $\alpha_2 \in K(\alpha_1, \alpha_2)$, donc

$$K(\alpha_1)(\alpha_2) \subseteq K(\alpha_1, \alpha_2)$$

Mais on a aussi

$$K(\alpha_1, \alpha_2) \subseteq K(\alpha_1)(\alpha_2)$$

puisque $K(\alpha_1, \alpha_2)$ est le plus petit sous-corps de L contenant K, α_1 et α_2. On peut généraliser ce résultat de 2 à n. Toute extension obtenue par l'adjonction d'un nombre fini d'éléments peut donc être vue comme une suite finie d'extensions simples par des extensions intermédiaires (si K est une extension de K tout corps M tel que $K \subseteq M \subseteq L$ est appelé extension intermédiaire entre K et L

Exemple : On peut donc écrire $\mathbb{Q}(\sqrt{2},\sqrt{3}) = \mathbb{Q}(\sqrt{2})(\sqrt{3}) = \mathbb{Q}(\sqrt{3})(\sqrt{2})$. Par exemple le corps $M = \mathbb{Q}(\sqrt{2})$ est une extension intermédiaire entre $K = \mathbb{Q}$ et $L = \mathbb{Q}(\sqrt{2},\sqrt{3})$:

$$\mathbb{Q} \subseteq \mathbb{Q}(\sqrt{2}) \subseteq \mathbb{Q}(\sqrt{2},\sqrt{3}).$$

Soit L une extension de K. Les opérations d'addition de L et de multiplication d'un élément de K par un élément de L (vus tous deux comme des éléments de L) font de L un K-espace vectoriel. On peut peut donc appliquer tous les résultats d'algèbre linéaire à notre situation. En particulier on peut parler de la dimension de L sur K comme étant le cardinal d'une base quelconque de L sur K.

Définition 14 *: Le degré de l'extension de corps $K \subseteq L$ est la dimension de L sur K. On le note $[L : K]$:*

$$[L : K] = dim_K L.$$

L'extension est dite finie si ce degré est fini et infinie dans le cas contraire.

Exemple : Tout élément x de $\mathbb{Q}(\sqrt{2})$ s'écrit $x = a.1 + b.\sqrt{2}$ avec $a, b \in \mathbb{Q}$. Donc $\{1, \sqrt{2}\}$ est une base de $\mathbb{Q}(\sqrt{2})$ sur $\mathbb{Q}$. Ainsi

$$[\mathbb{Q}(\sqrt{2}) : \mathbb{Q}] = 2.$$

De même on a

$$[\mathbb{C} : \mathbb{R}] = 2.$$

Proposition 6 *: Pour toute extension intermédiaire $K \subseteq M \subseteq L$ on a $[L : K] = [L : M].[M : K]$.*

Preuve : Ceci découle facilement du fait que si $\{x_i\}_{i\in I}$ est une base de M sur K et si $\{y_j\}_{j\in J}$ est une base de L sur M alors $\{x_i.y_j\}_{(i,j)\in I\times J}$ est une base de L sur K.
Exemple : Appliquons la proposition à l'extension intermédiaire $\mathbb{Q} \subseteq \mathbb{Q}(\sqrt{2}) \subseteq \mathbb{Q}(\sqrt{2},\sqrt{3})$. On a

$$[\mathbb{Q}(\sqrt{2}) : \mathbb{Q}] = 2$$

et en utilisant le fait que $\mathbb{Q}(\sqrt{2},\sqrt{3}) = \mathbb{Q}(\sqrt{2})(\sqrt{3})$

$$[\mathbb{Q}(\sqrt{2},\sqrt{3}) : \mathbb{Q}(\sqrt{2})] = 2$$

et donc

$$[\mathbb{Q}(\sqrt{2},\sqrt{3}) : \mathbb{Q}] = 2.2 = 4.$$

Définition 15 *: Soient L et M deux extensions du corps K. Un K-morphisme de L vers M est un morphisme de corps $\psi : L \longrightarrow M$ qui induit l'identité sur K :*

$$\psi_{|K} = Id_K.$$

Autrement dit le morphisme ψ laisse invariants les éléments de K :

$$\psi(x) = x.$$

pour tout $x \in K$. Un K-ismorphisme est un K-morphisme bijectif. Si $L = M$ on parle de K-automorphisme.

2.3 Corps de Rupture et de Décomposition d'un polynôme

Soit K un corps et soit $P \in K[X]$ un polynôme unitaire irréductible de degré superieur à 1. Comme P est irréductible l'idéal principal qu'il engendre, (P), est un idéal maximal de $K[X]$. L'anneau quotient

$$L = \frac{[K[X]}{(P)}$$

est un corps qui est une extension de K puisqu'on a le morphisme composé :

$$K \hookrightarrow K[X] \longrightarrow \frac{K[X]}{(P)} = L$$

où le deuxième morphisme est le morphisme canonique qui à un polynôme $Q \in K[X]$ associe sa classe $\overline{Q}$ modulo P. Posons

$$x = \overline{X}$$

la classe du polynôme $X \in K[X]$. On a $x \in L$ et

$$P(x) = P(\overline{X}) = \overline{P(X)} = 0.$$

Autrement dit même si le polynôme P n'a pas de racine dans K on peut toujours trouver une extension L de K dans laquelle ce polynôme acquiert une racine.

Définition 16 *: Le corps L est appelé le corps de rupture du polynôme P.*

Exemple : Prenons $K = \mathbb{R}$ et $P(X) = X^2+1$. Le polynôme P est irréductible sur $\mathbb{R}$ et est de degré 2. La classe $x = \overline{X}$ vérifie l'équation

$$x^2 = -1$$

et en envoyant x vers i on obtient un isomorphisme

$$L = \frac{\mathbb{R}[X]}{(X^2+1)} \cong \mathbb{C}.$$

Ainsi le corps $\mathbb{C}$ des nombres complexes peut-être vu comme le corps de rupture du plynôme $X^2 + 1$ sur $\mathbb{R}$.
Remarque : Le corps de rupture d'un polynôme P n'est pas unique tout simplement parce qu'en général le polynôme P a plusieurs racines. Mais en envoyant une racine vers l'autre on montre facilement qu'ils sont tous K-isomorphes.
Exemple : Prenons $K = \mathbb{Q}$ et $P(X) = X^3 - 2$. P est irréductible sur $\mathbb{Q}$ (il n'a pas de racine dans $\mathbb{Q}$) et est de degré 3. Les racines de P dans $\mathbb{C}$ sont $\sqrt[3]{2}, j\sqrt[3]{2}$ et $j^2\sqrt[3]{2}$ avec $j = exp(2i\pi/3)$ une racine primitive troisième de l'unité. Le polynôme P a trois corps de rupture correspondant chacun à une racine :

$$\mathbb{Q}(\sqrt[3]{2}),$$
$$\mathbb{Q}(j\sqrt[3]{2}),$$
$$\mathbb{Q}(j^2\sqrt[3]{2}).$$

Ils sont différents mais tous $\mathbb{Q}$-isomorphes.

Définition 17 *: Soit $K \subseteq L$ une extension de corps et soit $P \in K[X]$ un polynôme à coefficients dans K de degré ≥ 1. On dit que P est scindé dans L si toutes les racines de P sont dans L.*

Autrement dit P est scindé dans L s'il s'écrit dans $L[X]$ comme produit de facteurs linéaires :

$$P(X) = a\prod_{i=1}^{d}(X - \alpha_i).$$

Les α_i sont les racines de P.

Définition 18 *: Soit $P \in K[X]$ un polynôme de degré ≥ 1. Une extension L de K est un corps de décomposition de P sur K si P est scindé dans $L[X]$ et si L est engendré sur K par les racines de P :*

$$L = K(\alpha_1, \alpha_2, \ldots, \alpha_d).$$

où les α_i sont les racines de P.

Proposition 7 *: Tout polynôme $P \in K[X]$ de degré ≥ 1 a un corps de décomposition sur K et ce pour tout corps K.*

Preuve : Raisonnons par récurrence sur le degré n de P. Si $n = 1$ alors $P(X) = aX + b = a(X - b/a)$. Donc K est un corps de décomposition de P. Supposons le résultat vrai pour tout polynôme de degré $< n$ et soit $P \in K[X]$ de degré n. Soit M un corps de rupture de P. M contient une racine α de P qui s'écrit donc $P(X) = (X - \alpha)Q(X)$ dans $M[X]$ avec $Q \in M[X]$ de deré $n - 1$. Par hypothèse de récurrence il existe une extension L de M qui est un corps de décomposition de Q sur M. En rajoutant la racine α aux racines de Q on obtient toutes les racines de P. Ceci montre que L est un corps de décomposition de P sur K.

2.4 Eléments Algébriques et Transcendants

Définition 19 *: Soit $K \subseteq L$ une extension de corps. Un élément α de L est dit algébrique sur K s'il existe un polynôme $P \in K[X]$ avec $P(\alpha) = 0$. Sinon on dit que α est transcendant sur K.*

Si $\alpha \in L$ est algébrique sur K il existe un polynôme irréductible unitaire de degré minimal I_α avec $I_\alpha(\alpha) = 0$ (ceci résulte de la théorie de la divisibilité dans l'anneau $K[X]$).

Définition 20 *: Le polynôme I_α est appelé le polynôme minimal de α sur K. Son degré est appelé le degré de α sur K. On le note $deg_K(\alpha)$.*

Comme le polynôme I_α est unitaire irréductible il a un corps de rupture

$$M = \frac{[K[X]}{(I_\alpha)}.$$

En envoyant la classe x de $\overline{X}$ vers α on obtient un K-isomorphisme

$$\frac{K[X]}{(I_\alpha)} \cong K(\alpha)$$

avec $K(\alpha)$ le sous-corps de L engendré par α sur K.

Proposition 8 *: Si $\alpha \in L$ est algébrique sur K alors $K(\alpha)$ est une extension finie de K et on a $[K(\alpha) : K] = deg_K(\alpha)$.*

Preuve : On va montrer que les éléments $1, \alpha, \alpha^2, \ldots, \alpha^{d-1}$ (avec d le degré de I_α) forment une base de $K(\alpha)$ sur K. Par définition tout élément de $K(\alpha)$ est une combinaison linéaire à coefficients dans K de puissances de α. On sait qu'il existe des éléments $a_0, a_1, \ldots, a_{d-1}$ de K avec

$$\alpha^d + a_{d-1}\alpha^{d-1} + \ldots + a_1\alpha + a_0 = 0.$$

Donc

$$\alpha^d = -a_{d-1}\alpha^{d-1} - \ldots - a_1\alpha - a_0$$

s'exprime comme combinaison linéaire de $1, \alpha, \ldots, \alpha^{d-1}$. De même

$$\alpha^{d+1} = \alpha^d.\alpha = -a_{d-1}\alpha^d - \ldots - a_1\alpha^2 - a_0\alpha$$

s'exprime aussi comme combinaison linéaire de ces éléments et ainsi de suite pour toutes les puissances de α. On en déduit que les éléments $1, \alpha, \ldots, \alpha^{d-1}$ engendrent $K(\alpha)$ sur K. Supposons maintenant qu'il existe $b_0, b_1, \ldots, b_{d-2} \in K$ avec

$$\alpha^{d-1} + b_{d-2}\alpha^{d-2} + \ldots + b_1\alpha + b_0 = 0.$$

On doit alors avoir $b_0 = b_1 = \ldots = b_{d-2} = 0$ car sinon cela contredirait la définition de I_α (comme étant le polynôme de degré minimal annulant α). Ainsi $\{1, \alpha, \ldots, \alpha^{d-1}\}$ est une base de $K(\alpha)$ sur K.
Exemple : Considérons l'extension $\mathbb{Q} \subseteq \mathbb{C}$ et l'élément $\sqrt[3]{2} \in \mathbb{C}$. Le polynôme $X^3 - 2$ est un polynôme sur $\mathbb{Q}$ qui annule $\sqrt[3]{2}$. Cet élément est donc algébrique sur $\mathbb{Q}$. Le polynôme $X^3 - 2$ est unitaire et irréductible (puisqu'il n'a pas de racine dans Q). Il est donc le polynôme minimal de $\sqrt[3]{2}$:

$$I_{\sqrt[3]{2}}(X) = X^3 - 2$$

(Remarquer qu'il n y a pas de polynôme de degré ≤ 2 sur $\mathbb{Q}$ qui annule $\sqrt[3]{2}$). Une base de $\mathbb{Q}(\sqrt[3]{2})$ sur $\mathbb{Q}$ est $\{1, \sqrt[3]{2}, (\sqrt[3]{2})^2\}$ et donc

$$[\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}] = 3.$$

Remarque : Si α est transcendant sur K alors l'extension $K(\alpha)$ de K est nécéssairement infinie car sinon il existerait un polynôme sur K qui annule α

Définition 21 *: Une extension L de K est dite algébrique si tout élément de L est algébrique sur K.*

D'aprés la remarque précédente toute extension finie est algébrique. En effet supposons que l'extension L de K soit finie et supposons qu'il existe $\alpha \in L$ transcendant sur K. On a

$$K \subseteq K(\alpha) \subseteq L$$

et donc

$$[L : K] = [L : K(\alpha)].[K(\alpha) : K]$$

Comme $[K(\alpha) : K] = \infty$ on doit aussi avoir $[L : K] = \infty$. Contradiction.

2.5 Extensions Normales et Séparables

Définition 22 *: L'extension L de K est dite normale si elle est algébrique et si pour tout $\alpha \in L$ le polynôme minimal I_α a toutes ses racines dans L.*

Exemple : Tout corps K est une extension normale de lui-même : en effet K est algébrique sur K et pour tout $\alpha \in K$ le polynôme minimal de α est $I_\alpha = X - \alpha$ qui a une seule racine $\alpha \in K$. Le corps $\mathbb{Q}(\sqrt[3]{2})$ n'est pas une extension normale de $\mathbb{Q}$ car le polynôme minimal de $\sqrt[3]{2}$ qui est $I_{\sqrt[3]{2}} = X^3 - 2$ n'a pas toutes ses racines dans $\mathbb{Q}(\sqrt[3]{2})$ ($j\sqrt[3]{2}$ et $j^2\sqrt[3]{2}$ n'appartiennent pas à $\mathbb{Q}(\sqrt[3]{2})$). Le corps $\mathbb{C} = \mathbb{R}(i)$ est une extension normale de $\mathbb{R}$. En effet toute puissance de i est égale à ± 1 ou à $\pm i$. Il suffit donc de vérifier la normalité pour i. Mais le polynôme minimal de i est $X^2 + 1$ dont les racines i et $-i$ appartiennent à $\mathbb{C}$. Remarquer que dans ce cas $\mathbb{C}$ est le corps de décomposition de $X^2 + 1$.

Proposition 9 *: Soit $L = K(\alpha_1, \ldots, \alpha_n)$ une extension normale de K. Alors L est le corps de décomposition d'u polynôme non constant $P \in K[X]$.*

Preuve : L'extension étant algébrique chaque élément α_i est algébrique et a donc un polynôme minimal I_{α_i} sur K dont toutes les racines sont dans L par normalité. Le polynôme

$$P(X) = I_{\alpha_1}(X) \ldots I_{\alpha_n}(X)$$

a donc toutes ses racines dans L. Ainsi Le corps de décomposition M de P vérifie

$$K \subseteq M \subseteq L.$$

Comme $\alpha_1, \ldots, \alpha_n$ sont des racines de P on a aussi

$$L = K(\alpha_1, \ldots, \alpha_n) \subseteq M.$$

On en déduit que

$$L = M.$$

Remarque : Les extensions algébriques finies sont toutes de la forme $L = K(\alpha_1, \ldots, \alpha_n)$. La proposition aurait pu donc s'énoncer ainsi : toute extension normale finie est le corps de décomposition d'un polynôme non constant . On peut aussi montrer l'inverse (mais nous ne le ferons pas ici) : Tout corps de décomposition d'un polynôme est une extension normale finie.
Exemple : Le corps $\mathbb{Q}(\sqrt[3]{2}, j\sqrt[3]{2}, j^2\sqrt[3]{2})$ est le corps de décomposition du polynôme $X^3 - 2$ sur $\mathbb{Q}$. C'est donc une extension normale de $\mathbb{Q}$.

Définition 23 *: Soit $K \subseteq L$ une extension algébrique. Le groupe des K-automorphismes de L est noté $G = Aut(L/K)$. Si $\alpha \in L$ l'orbite de α sous l'action de G est*

$$G\alpha = \{g(\alpha) \mid g \in G\}$$

et le stabilisateur de α est le sous-groupe G_α de G donné par

$$G_\alpha = \{g \in G \mid g(\alpha) = \alpha\}.$$

Proposition 10 *: Pour tout $\sigma \in G = Aut(L/K)$, $\sigma(\alpha)$ est une racine de I_α.*

Preuve : Ecrivons $I_\alpha(X) = X^d + a_{d-1}X^{d-1} + \ldots + a_0$ avec $d = deg_K(\alpha)$ et $I_\alpha(\alpha) = 0$. Soit $\sigma \in Aut(L/K)$. On a alors

$$0 = \sigma(I_\alpha(\alpha) = \sigma(\alpha)^d + a_{d-1}(\sigma(\alpha))^{d-1} + \ldots + a_0 = I_\alpha(\sigma(\alpha)).$$

Donc $\sigma(\alpha)$ est une racine du polynôme minimal I_α.
la proposition montre que $X - \sigma(\alpha)$ divise I_α pour tout $\sigma \in G = Aut(L/K)$. Quand σ parcourt $Aut(L/K)$ les éléments $\sigma(\alpha)$ parcourent l'orbite $G\alpha$. Comme le polynôme I_α est de degré fini d on en déduit que pour tout α l'orbite $G\alpha$ est un ensemble fini et de cardinal $\leq d$. De plus I_α est divisible par le produit

$$\prod_{\beta \in G\alpha} (X - \beta).$$

On pourrait alors se poser la question suivante :
Question : Sous quelles conditions a-t-on $I_\alpha(X) = \prod_{\beta \in G\alpha}(X - \beta)$ pour tout $\alpha \in L$?
On voit immédiatement qu'une condition nécéssaire pour que cette égalité ait lieu est que toutes les racines de I_α soient dans L. Autrement dit une condition nécéssaire est que L soit une extension normale de K. Mais cette condition n'est pas suffisante car dans le produit $\prod_{\beta \in G\alpha}(X - \beta)$ les β sont tous distincts et le polynôme I_α pourrait trés bien avoir des racines multiples. Ceci nous amène à la notion de séparabilité.

Un polynôme $P \in K[X]$ irréductible est dit séparable si toutes les racines de P dans son corps de décomposition sont simples (de multiplicité 1) ou encore deux à deux distinctes.

Définition 24 *: Soit L une extension algébrique de K. On dit que $\alpha \in L$ est séparable sur K si son polynôme minimal est séparable. L'extension est dite séparable si tout élément est séparable.*

Proposition 11 *: Soit L une extension algébrique de K et soit M une extension intermédiaire*

$$K \subseteq M \subseteq L.$$

Si L est séparable sur K alors M est séparable sur K et L est séparable sur M.

Preuve : Comme $M \subseteq L$, M est clairement séparable sur K. Le polynôme minimal de $\alpha \in L$ sur K est multiple du polynôme minimal de α sur M. Si le premier est séparable le second doit l'être aussi.

Pour tout polynôme $P(X) = a_0 + a_1X + \ldots + a_nX^n \in K[X]$ on pose

$$D(P) = P^{'}(X) = a_1 + a_2X + \ldots + a_nX^{n-1}.$$

C'est l'opération de dérivation des polynômes. Si P est degré n sa dérivée $D(P)$ est un polynôme de degré $n-1$. On a bien sûr la propriété

$$D(PQ) = D(P)Q + PD(Q).$$

Supposons que le polynôme P a une racine α de multiplicité $n \geq 2$ dans son corps de décomposition M. P s'écrit donc

$$P(X) = (X-\alpha)^n Q(X)$$

avec $Q(X) \in M[X]$. En dérivant

$$D(P) = P^{'} = n(X-\alpha)^{n-1}Q + (X-\alpha)^n Q^{'}$$

et donc

$$P^{'}(\alpha) = 0.$$

Donc α est une racine commune à P et à $P^{'}$. Inversement supposons que P et $P^{'}$ ont une racine commune α. Alors α est nécéssairement une racine multiple de P. En effet si on avait

$$P(X) = (X-\alpha)Q(X)$$

avec $Q(\alpha) \neq 0$ on aurait

$$P^{'}(X) = Q(X) + (X-\alpha)Q^{'}(X)$$

et $P^{'}(\alpha) \neq 0$.

Proposition 12 *: Soit $P \in K[X]$ un polynôme irréductible. Alors P est séparable $\Longleftrightarrow P^{'} \neq 0$.*

Preuve : Si $P^{'} = 0$ alors toute racine de P est aussi racine de $P^{'}$ et est donc multiple. Ainsi P n'est pas séparable. Inversement soit $P^{'} \neq 0$ et supposons que P n'est pas séparable. Il a donc au moins une racine commune avec $P^{'}$. Ceci veut dire que le plus grand commun diviseur D de P et $P^{'}$ dans $K[X]$ est de degré ≥ 1 ce qui contredit le fait que P est irréductible.

Exemple : En caractéristique 0 tout polynôme irréductible est séparable. En effet soit P un polynôme irréductible qu'on peut supposer unitaire. Si d est le degré de P le terme dominant de $P^{'}$ est dX^{d-1} qui est non nul. Donc P est séparable. Pour un exemple en caractéristique p prenons $K = \mathbb{F}_p(T)$ le corps des fractions rationnelles sur le corps fini $\mathbb{F}_p$. Le polynôme $P(X) = X^p - T$ a pour dérivée $P^{'}(X) = pX^{p-1} = 0$ et il n'est donc pas séparable.

Cette étude nous permet de répondre à la question précédente : Pour les extensions normales et séparable on a

$$I_\alpha(X) = \prod_{\beta \in G\alpha} (X - \beta).$$

Finissons ce chapitre avec le célèbre théorème de l'élément primitif :

Proposition 13 *: Soit L une extension finie séparable de K. Alors il existe $\gamma \in L$ tel que $L = K(\gamma)$.*

Preuve : Nous ferons la démonstration pour $[L : K] = 2$. Le cas général s'en déduit par récurrence. Soit $\{\alpha, \beta\}$ une base de L sur K de sorte que $L = K(\alpha, \beta)$. L'extension étant finie elle est algébrique. Soient I_α et I_β les polynômes minimaux de α et β sur K. Posons $P = I_\alpha I_\beta$ et soit M le corps de décomposition de P. α et β étant des racines de P on a $L \subseteq M$. Soient $\alpha_1 = \alpha, \alpha_2, \ldots, \alpha_r$ les racines de I_α dans M et soient $\beta_1 = \beta, \beta_2, \ldots, \beta_s$ les racines de I_β dans M avec r le degré de I_α et s le degré de I_β. L étant séparable sur K les α_i et les β_j sont des racines distinctes et

$$M = K(\alpha_1, \ldots, \alpha_r, \beta_1, \ldots, \beta_s).$$

On peut toujours trouver $t \in K^*$ tel que

$$\alpha + t\beta \neq \alpha_i + t\beta_i$$

pour tout $i \geq 2$ et pour tout $j \geq 2$. Posons

$$\gamma = \alpha + t\beta.$$

γ vérifie

$$\gamma - t\beta_j \neq \alpha_i$$

pour tout $i \neq 1$ et tout $j \neq 1$. Soit $Q \in K(\gamma)[X]$ le polynôme défini par

$$Q(X) = I_\alpha(\gamma - tX).$$

On a

$$Q(\beta) = I_\alpha(\alpha) = 0$$

et

$$Q(\beta_j) = I_\alpha(\gamma - t\beta_j) \neq 0$$

pour tout $j \geq 2$. Ainsi β est algébrique sur $K(\gamma)$. De plus β est la seule racine commune de Q et I_β (en tant qu'éléments de $K(\gamma)[X]$). Soit $R \in K(\gamma)[X]$ le polynôme minimal de β sur $K(\gamma)$. Le polynôme R divise I_β et Q dans $K(\gamma)[X]$ (puisque $I_\beta(\beta) = 0$ et $Q(\beta) = 0$) et toute racine de R est donc une racine commune de I_β et Q. L étant séparable sur K, elle l'est aussi sur $K(\gamma)$. le polynôme R doit donc être de degré 1 de la forme

$$R(X) = X - \beta.$$

ce qui entraine que

$$\beta \in K(\gamma)$$

et aussi

$$\alpha \in K(\gamma)$$

puisque $\alpha = \gamma - t\beta$ et $t \in K^*$. On a donc bien

$$K(\alpha, \beta) = K(\gamma).$$

Exemple : Soit l'extension $\mathbb{Q}(\sqrt{2}, \sqrt{3})$ de $\mathbb{Q}$. Le polynôme minimal de $\sqrt{2}$ est $X^2 - 2$ de racines $\sqrt{2}$ et $-\sqrt{2}$ et celui de $\sqrt{3}$ est $X^2 - 3$ de racines $\sqrt{3}$ et $-\sqrt{3}$. Comme

$$\sqrt{2} + \sqrt{3} \neq -\sqrt{2} - \sqrt{3}$$

on peut prendre ici

$$t = 1$$

et donc

$$\mathbb{Q}(\sqrt{2}, \sqrt{3}) = \mathbb{Q}(\sqrt{2} + \sqrt{3}).$$

Chapitre 3

Corps de nombres

Les corps de nombres algébriques constituent l'objet d'étude d'une branche trés florissante (et difficile) des mathématiques : la théorie algébrique des nombres. Dans ce chapitre nous toucherons à peine au sujet en expliquant ce qu'est un corps de nombre et surtout en introduisant son anneau des entiers algébriques qui est d'un grande importance dans l'étude du corps. On présentera aussi quelques outils comme la norme et la trace. A la fin du chapitre, et comme application de toute la théorie, on présente l'exemple des corps de nombres les plus simples : les extensions quadratiques de Q en calculant notamment leurs anneaux des entiers.

3.1 Définition

Définition 25 *: Un nombre complexe $\alpha \in \mathbb{C}$ est dit algébrique s'il est racine d'un polynôme à coefficients dans $\mathbb{Q}$. Un nombre algébrique est dit entier s'il est de plus racine d'un polynôme unitaire à coefficients dans $\mathbb{Z}$.*

Par exemple $i, \sqrt{2}$ sont algébriques et entiers en tant que racines des polynômes X^2+1 et X^2-2. Par contre π et e ne sont pas algébriques. Ils sont transcendants. Remarquer aussi que si α est racine d'un polynôme à coefficients dans $\mathbb{Q}$ alors par reduction de ces coefficients au même dénominateur α devient solution d'un polynôme à coefficients dans $\mathbb{Z}$. On peut donc dire que α est algébrique s'il est racine d'un polynôme (pas nécessairement unitaire) à coefficients dans $\mathbb{Z}$.

Définition 26 *: Un corps de nombres est un sous-corps de $\mathbb{C}$ qui est une extension finie de $\mathbb{Q}$.*

Un corps de nombres K est donc caractérisé par les deux conditions :

$$\mathbb{Q} \subseteq K \subset \mathbb{C}.$$

$$[K : \mathbb{Q}] < \infty.$$

En particulier un corps de nombre est de caractéristique 0 puisqu'il contient le corps premier $\mathbb{Q}$.

Proposition 14 *: Les éléments d'un corps de nombres K sont tous des nombres algébriques.*

Preuve : Soit $\alpha \in K$. On a

$$\mathbb{Q} \subseteq \mathbb{Q}(\alpha) \subseteq K$$

et comme K est une extension finie de $\mathbb{Q}$ on en déduit que $\mathbb{Q}(\alpha)$ est aussi une extension finie de $\mathbb{Q}$. Il existe donc un entier m tels que les éléments $1, \alpha, \alpha^2, \ldots, \alpha^m$ de $\mathbb{Q}(\alpha)$ soient linéairement dépendants sur $\mathbb{Q}$. Il existe donc des coefficients $a_0, a_1, \ldots, a_m$ dans $\mathbb{Q}$ tels que

$$a_0 + a_1\alpha + a_2\alpha^2 + \ldots + a_m\alpha^m = 0.$$

Ceci veut dire que α est racine d'un polynôme à coefficients dans $\mathbb{Q}$ et donc que α est algébrique.

Le corps de nombres le plus simple est bien sûr $K = \mathbb{Q}$ lui même. Viennent ensuite les extensions simples engendrées par un nombre algébrique α sur $\mathbb{Q}$ comme $\mathbb{Q}(i)$ ou $\mathbb{Q}(\sqrt{2})$. Mais comme on est en caractéristique 0, et d'aprés le chapitre 2, toute extension algébrique (et en particulier finie) de $\mathbb{Q}$ est séparable. Ainsi tout corps de nombres est une extension finie séparable de $\mathbb{Q}$ et on peut donc lui appliquer le théorème de l'élément primitif : Pour tout corps de nombres K il existe $\alpha \in K$ tel que

$$K = \mathbb{Q}(\alpha).$$

Le degré de K sur $\mathbb{Q}$ est donc le degré du polynôme minimal de α sur $\mathbb{Q}$:

$$[K : \mathbb{Q}] = degI_\alpha$$

et l'ensemble $\{1, \alpha, \alpha^2, \ldots, \alpha^{n-1}\}$ (avec $n = degI_\alpha$) constitue une base de K sur $\mathbb{Q}$.

Exemple : $\mathbb{Q}(i)$ est de degré 2 sur $\mathbb{Q}$ puisque le polynôme minimal de i est X^2+1. Une base est formée de 1 et i et tout élément de $\mathbb{Q}(i)$ s'écrit donc sous la forme $a+ib$ avec $a,b \in \mathbb{Q}$. De même $\mathbb{Q}(\sqrt[3]{2})$ est de degré 3 sur $\mathbb{Q}$ puisque le polynôme minimal de $\sqrt[3]{2}$ sur $\mathbb{Q}$ est X^3-2. Une base est formée de 1, $\sqrt[3]{2}$ et $(\sqrt[3]{2})^2$ et tout élément de $\mathbb{Q}(\sqrt[3]{2})$ s'écrit $a+b\sqrt[3]{2}+c(\sqrt[3]{2})^2$ avec $a,b,c \in \mathbb{Q}$.

Les racines $\alpha_1=\alpha,\alpha_2,\ldots,\alpha_n$ du polynôme minimal de α dans son corps de décomposition L sont appelées les conjuguées de α. Les extensions simples $\mathbb{Q}(\alpha_i)$ sont toutes des sous-extensions de L et on a des $\mathbb{Q}$-isomorphismes

$$\phi_i : \mathbb{Q}(\alpha) \longrightarrow \mathbb{Q}(\alpha_i)$$

pour $i=2,\ldots,n$ qui consitent à envoyer α vers α_i.
Remarque : Les α_i pour $i=2,\ldots,n$ n'appartiennent pas forcément à K. Ce sera le cas si K est normal sur $\mathbb{Q}$ et on aura une identification entre le corps de décomposition et K. Par exemple pour $K=\mathbb{Q}(i)$ les deux racines i et $-i$ sont dans K. L'extension est normale et séparable (on dit qu'elle est galoisienne).

3.2 Trace et Norme

Les $\mathbb{Q}$-isomorphismes ϕ_i peuvent être considérés comme des plongements

$$\phi_i : K \hookrightarrow \mathbb{C}$$

de K dans le corps des complexes $\mathbb{C}$. Si $\phi_i(K) \subset \mathbb{R}$ le plongement est dit réel, sinon il est dit complexe. Il existe toujours un nombre pair de plongements complexes puisque si ϕ_i est complexe sa conjuguée $\overline{\phi_i}$ est aussi un plongement complexe (si α_i est racine du polynôme minimal de α il en est de même de sa conjuguée complexe $\overline{\alpha_i}$ et donc comme ϕ_i correspond à α_i, $\overline{\phi_i}$ va correspondre à $\overline{\alpha_i}$). Si r_1 dénote le nombre de plongements réels et si r_2 dénote le nombre des paires $(\phi_i,\overline{\phi_i})$ de plongements complexes on a

$$[K:\mathbb{Q}] = n = r_1 + 2r_2.$$

Comme $\mathbb{Q} \subset \mathbb{R}$ il n y a pas de plongement complexes pour $K=\mathbb{Q}$ et donc un seul plongement réel. Ainsi $r_1=1$ et $r_2=0$ et donc

$$[\mathbb{Q}:\mathbb{Q}] = 1 = 1+2.0$$

Pour donner un exemple moins trivial soit $K = \mathbb{Q}(i)$. Il y a deux plongements dans $\mathbb{C}$ correspondant aux racines i et $-i$ du polynôme minimal $X^2 + 1$ de i. Le premier ϕ_1 envoie i vers i et le second ϕ_2 envoie i vers $-i$. Plus exactement on a

$$\phi_1 : K \hookrightarrow \mathbb{C}$$

donné par $\phi_1(a + ib) = a + ib$ (ϕ_1 est donc l'identité sur K) et

$$\phi_2 : K \hookrightarrow \mathbb{C}$$

donné par $\phi_2(a + ib) = a - ib$ (ϕ_2 est donc la conjugaison complexe). Ces deux plongements sont clairement complexes (ici il n y a pas de plongements réels) et on a

$$\phi_2 = \overline{\phi_1}.$$

Donc $r_1 = 0, r_2 = 1$ et

$$[K : \mathbb{Q}] = 2 = 0 + 2.1.$$

En général r_1 est le nombre de racines réelles du polynôme minimal de α et r_2 est le nombre des paires $(\alpha_i, \overline{\alpha_i})$ formées des racines complexes.

Soit $x \in K$ et Soit $M_x : K \longrightarrow K$ la multiplication par x dans K définie par

$$M_x(y) = xy.$$

pour tout $y \in K$. M_x est une application linéaire sur K vu comme espace vectoriel sur $\mathbb{Q}$. Son polynôme caractéristique

$$\Delta_x = det(XId_K - M_x)$$

est un polynôme à coefficients dans $\mathbb{Q}$ de degré $n = [K : \mathbb{Q}]$. Il s'écrit donc sous la forme

$$\Delta_x(X) = X^n + a_{n-1}X^{n-1} + \ldots + a_1X + a_0$$

avec $a_i \in \mathbb{Q}$. On remarque que l'une des racines de M_x est $x_1 = x$:

$$M_x(x) = 0.$$

Si on note les autres racines de M_x dans $\mathbb{C}$ par $x_2, \ldots, x_n$ on a donc

$$\Delta_x(X) = \prod_{i=1}^{n}(X - x_i)$$

Proposition 15 *: On a* $\sum_{i=1}^{n} x_i \in \mathbb{Q}$ *et* $\prod_{i=1}^{n} x_i \in \mathbb{Q}^*$.

Preuve : Il suffit de remarquer que

$$\sum_{i=1}^{n} x_i = tr(M_x) = -a_{n-1} \in \mathbb{Q}$$

et

$$\prod_{i=1}^{n} x_i = detM_x = (-1)^n a_0 \in \mathbb{Q}.$$

Il y a une relation simple entre les racines x_i de Δ_x et les images $\phi_i(x)$ de x. En effet on a

$$\Delta_x(\phi_i(x) = \phi_i(\Delta_x(x)) = \phi_i(0) = 0.$$

(On a utilisé le fait que $\phi_i(a) = a$ pour tout $a \in \mathbb{Q}$). Autrement dit chaque $\phi_i(x)$ est une racine de Δ_x. En rearrangeant les x_i s'il faut on a donc

$$\phi_i(x) = x_i$$

pour $i = 1, \ldots, n$. Comme corollaire on obtient

$$\sum_{i=1}^{n} \phi_i(x) \in \mathbb{Q}$$

et

$$\prod_{i=1}^{n} \phi_i(x) \in \mathbb{Q}^*$$

pour tout $x \in K$.

Définition 27 *: la trace et la norme sur* K *sont les applications* $Tr_{K/\mathbb{Q}} : K \longrightarrow \mathbb{Q}$ *et* $N_{K/\mathbb{Q}} : K^* \longrightarrow \mathbb{Q}^*$ *définies par :*

$$Tr_{K/\mathbb{Q}}(x) = \sum_{i=1}^{n} \phi_i(x)$$

et

$$N_{K/\mathbb{Q}}(x) = \prod_{i=1}^{n} \phi_i(x).$$

Exemple :
1) si l'élément $x \in K$ est dans $\mathbb{Q}$ on a $\phi_i(x) = x$ pour tout i. Donc $Tr_{K/\mathbb{Q}}(x) = nx$ et $N_{K/\mathbb{Q}}(x) = x^n$.
2) Soit $x = a + ib \in K = \mathbb{Q}(i)$ non nul avec $a, b \in \mathbb{Q}$ (a et b ne s'annulant pas simultanément). On a $\phi_1(x) = x$ et $\phi_2(x) = \overline{x}$ le conjugué complexe de x. Donc

$$Tr_{K/\mathbb{Q}}(x) = x + \overline{x} = 2Re(x) = 2a$$

et

$$N_{K/\mathbb{Q}}(x) = x\overline{x} =\mid x \mid^2= a^2 + b^2.$$

Remarque : La trace est additive et la norme est multiplicative :

$$Tr_{K/\mathbb{Q}}(x + y) = Tr_{K/\mathbb{Q}}(x) + Tr_{K/\mathbb{Q}}(y)$$

et

$$N_{K/\mathbb{Q}}(x.y) = N_{K/\mathbb{Q}}(x).N_{K/\mathbb{Q}}(y).$$

3.3 Entiers algébriques

On s'interesse ici aux éléments d'un corps de nombres qui sont des entiers algébriques (racines d'un polynôme unitaire dans $\mathbb{Z}[X]$). On les appelle les éléments entiers du corps. Nous allons montrer qu'ils constituent un sous-anneau du corps de nombres.

Soit $\mathbb{Z}[\alpha]$ le sous-groupe (pour l'addition) de $\mathbb{C}$ engendré par les puissances de α sur $\mathbb{Z}$. Ses éléments sont les sommes finies $\sum_i a_i\alpha^i$ pour $i \in \mathbb{N}$.

Proposition 16 *: Les conditions suivantes sont équivalentes :*

1. *α est un entier algébrique.*
2. *$\mathbb{Z}[\alpha]$ est un groupe de type fini (engendré par un nombre fini d'éléments).*
3. *Il existe un sous-anneau B de $\mathbb{C}$ contenant $\mathbb{Z}$ et α et qui, en tant que groupe abélien, est de type fini.*

Preuve : On va montrer 1) $\Rightarrow$ 2) $\Rightarrow$ 3) $\Rightarrow$ 1). Soit α un entier algébrique. Il est donc racine d'un polynôme unitaire $P(X) = X^n+b_{n-1}X^{n-1}+\ldots+b_1X+b_0$ dans $\mathbb{Z}[X]$. Autrement dit on a

$$\alpha^n + b_{n-1}\alpha^{n-1} + \ldots + b_1\alpha + b_0 = 0$$

ce qui donne

$$\alpha^n = -(b_{n-1}\alpha^{n-1} + \ldots + b_1\alpha + b_0).$$

On peut toujours supposer que $b_0 \neq 0$ ou encore que n est minimal (sinon il suffit de simplifier par α et c'est b_1 qui devient b_0). Donc α^n appartient au sous-groupe Γ de $\mathbb{Z}[\alpha]$ engendré par $1, \alpha, \alpha^2, \ldots, \alpha^{n-1}$ et qui est un sous-groupe de type fini. Mais alors toutes les autres puissances $\alpha^{n+1}, \alpha^{n+2}, \ldots$ vont aussi appartenir à Γ. Par exemple

$$\alpha^{n+1} = \alpha.\alpha^n$$

et comme α^n est combinaison linéaire de $1, \alpha, \alpha^2, \ldots, \alpha^{n-1}$, il en est de même de α^{n+1}. Donc

$$\mathbb{Z}[\alpha] = \Gamma,$$

et $\mathbb{Z}[\alpha]$ est de type fini. Ceci montre que 1) $\Rightarrow$ 2). Pour 2) $\Rightarrow$ 3) il suffit de prendre $B = \mathbb{Z}[\alpha]$. Reste à montrer que 3) $\Rightarrow$ 1). supposons B de type fini donc de la forme

$$B = \mathbb{Z}x_1 + \ldots + \mathbb{Z}x_n.$$

Comme $x_i \in B$ pour tout i on a

$$\alpha x_i \in B$$

pour tout i (car B est un anneau). Il existe donc des $a_{ij} \in \mathbb{Z}$ tels que

$$\alpha x_i = \sum_{j=1}^{n} a_{ij}x_j.$$

Ainsi le n-uple $(x_1, \ldots, x_n)$ est solution du système d'équations linéaires

$$\sum_{j=1}^{n} (\delta_{ij}\alpha - a_{ij})X_j = 0$$

pour $i = 1, \ldots, n$ ($\delta_{ij} = 0$ si $i \neq j$ et 1 si $i = j$). Comme le système est homogène (et les $x_{i]}$ non tous nuls) son determinant doit être nul

$$det(\delta_{ij}\alpha - a_{ij}) = P(\alpha) = 0.$$

avec$(-1)^n P(X)$ le polynôme caractéristique de la matrice (a_{ij}). Donc α est racine du polynôme unitaire $P(X) \in \mathbb{Z}[X]$ ce qui montre que c'est un entier algébrique.

Définition 28 *: Soit $\alpha \in K$ un corps de nombres. Si α est un entier algébrique on dit que c'est un élément entier du corps de nombres K*

Notons O_K l'ensemble des éléments entiers de K. On a alors :

Proposition 17 *: O_K est un sous-anneau de K.*

Preuve : Il faut montrer que si $\alpha, \beta \in O_K$ alors $\alpha + \beta \in O_K$ et $\alpha\beta \in O_K$. Comme α est entier $\mathbb{Z}[\alpha]$ est de type entier :

$$\mathbb{Z}[\alpha] = \mathbb{Z}\alpha_1 + \ldots + \mathbb{Z}\alpha_n.$$

De même β étant entier on a

$$\mathbb{Z}[\beta] = \mathbb{Z}\beta_1 + \ldots + \mathbb{Z}\beta_m.$$

et donc

$$\mathbb{Z}[\alpha, \beta] = \sum_{i=1}^{n} \sum_{j=1}^{m} \mathbb{Z}\alpha_i\beta_j.$$

Ainsi le sous-anneau $B = \mathbb{Z}[\alpha, \beta]$ de $\mathbb{C}$ est lui aussi de type fini. Comme il contient $\alpha + \beta$ et $\alpha\beta$ on en déduit le résultat.
Remarque : On peut montrer facilement que $O_K \cap \mathbb{Q} = \mathbb{Z}$. En effet on a $\mathbb{Z} \subseteq O_K \cap \mathbb{Q}$ et inversement si $\beta \in O_K \cap \mathbb{Q}$ alors β est racine d'un polynôme unitaire $P(X)$ dans $\mathbb{Z}[X]$ forcément de la forme $P(X) = X - a$ avec $a \in \mathbb{Z}$ et donc $\beta \in \mathbb{Z}$. On en déduit que la trace et la norme d'un éléments entiers d'un corps de nombres sont respectivement dans $\mathbb{Z}$ et $\mathbb{Z}^*$. En effet on a $\phi_i(\beta) \in O_K$ pour tout plongement ϕ_i de K et donc $tr_{K/\mathbb{Q}}(\beta) = \sum_{i=1}^{n} \phi_i(\beta) \in O_K \cap \mathbb{Q} = \mathbb{Z}$. De même $N_{K/\mathbb{Q}}(\beta) = \prod_{i=1}^{n} \phi_i(\beta) \in O_K \cap \mathbb{Q}^* = \mathbb{Z}^*$.

3.4 Corps Quadratiques

Définition 29 *: Un corps quadratique est un corps de nombre K de degré 2 sur $\mathbb{Q}$.*

pour un corps quadratique K tout élément $\alpha \in K - \mathbb{Q}$ a pour polynôme minimal un polynôme de degré 2 et donc $K = \mathbb{Q}(\alpha)$ et $\{1, \alpha\}$ est une base de K sur $\mathbb{Q}$. Soit

$$I_\alpha(X) = X^2 + bX + c$$

le polynôme minimal de α (avec $b, c \in \mathbb{Q}$). On sait que α est racine de I_α. Donc

$$\alpha^2 + b\alpha + c = 0$$

et en tant que solution d'une équation du second degré on a

$$2\alpha = -b \pm \sqrt{b^2 - 4c}.$$

(Dans un corps $\sqrt{x}$ désigne un élément y dont le carré est x). Comme $b \in \mathbb{Q}$ on obtient

$$K = \mathbb{Q}(\alpha) = \mathbb{Q}(\sqrt{b^2 - 4c}).$$

Mais $b^2 - 4c$ est un nombre rationnel et s'écrit donc

$$b^2 - 4c = \frac{u}{v} = \frac{uv}{v^2}$$

avec $u, v \in \mathbb{Z}$ et

$$\sqrt{b^2 - 4c} = \frac{\sqrt{uv}}{v}.$$

Donc

$$K = \mathbb{Q}(\sqrt{uv})$$

et on peut supposer que $d = uv$ n'a pas de carré comme diviseur. On a donc obtenu le résultat suivant :

Proposition 18 *: Tout corps quadratique est de la forme $K = \mathbb{Q}(\sqrt{d})$ avec $d \in \mathbb{Z}$ sans diviseur carré.*

Une base de $\mathbb{Q}(\sqrt{d})$ est $\{1, \sqrt{d}\}$ et tout élément s'écrit sous la forme $a + b\sqrt{d}$ avec $a, b \in \mathbb{Q}$. Le polynôme minimal de $\sqrt{d}$ est $X^2 - d$ de racines $\sqrt{d}$ et $-\sqrt{d}$ qui sont donc conjuguées et correspondent aux deux plongements de K dans $\mathbb{C}$:

$$\phi_1 : K \hookrightarrow \mathbb{C}$$

défini par $\phi_1(a + b\sqrt{d}) = a + b\sqrt{d}$ (c'est l'identité sur K) et

$$\phi_2 : K \hookrightarrow \mathbb{C}$$

défini par $\phi_2(a + b\sqrt{d}) = a - b\sqrt{d}$.
Si $d > 0$ ces deux plongements sont réels et on a donc

$$r_1 = 2$$

$$r_2 = 0$$

et le corps est dit quadratique réel. Si par contre $d < 0$ les deux plongements sont complexes et conjugués l'un de l'autre et donc

$$r_1 = 0$$

$$r_2 = 1$$

et le corps est dit quadratique imaginaire.
Dans ce cas simple des corps quadratiques on peut déterminer complètement l'anneau des éléments entiers.

Proposition 19 *: Soit $K = \mathbb{Q}(\sqrt{d})$ un corps quadratique avec $d \in \mathbb{Z}$ sans diviseur carré (et donc d n'est pas congru à 0 modulo 4).*

1. *si $d \equiv 2 \pmod 4$ ou $d \equiv 3 \pmod 4$ alors O_K est l'ensemble des éléments de la forme $a + b\sqrt{d}$ avec $a, b \in \mathbb{Z}$. Autrement dit on a*

$$O_K = \mathbb{Z}[\sqrt{d}].$$

2. *si $d \equiv 1 \pmod 4$ alors O_K est l'ensemble des éléments de la forme $1/2(u + v\sqrt{d})$ avec $u, v \in \mathbb{Z}$ et $u \equiv v \pmod 2$.*

Preuve : Soit $x = a + b\sqrt{d} \in O_K$ (avec $a, b \in \mathbb{Q}$). La trace et la norme de x sont respectivement dans $\mathbb{Z}$ et $\mathbb{Z}^*$. Donc

$$Tr_{K/\mathbb{Q}}(x) = \phi_1(x) + \phi_2(x) = 2a \in \mathbb{Z}$$

et

$$N_{K/\mathbb{Q}}(x) = \phi_1(x).\phi_2(x) = a^2 - db^2 \in \mathbb{Z}.$$

Ainsi ces conditions sont nécéssaires pour que x soit un élément entier. Elles sont aussi suffisantes. En effet si elles sont vérifiées alors x est racine du polynôme unitaire $X^2 - 2aX + a^2 - db^2$ à coefficients dans $\mathbb{Z}$. Comme $a^2 - db^2 \in \mathbb{Z}$ on a aussi $(2a)^2 - d(2b)^2 \in \mathbb{Z}$ et donc $2b \in \mathbb{Z}$. Pour résumer cette discussion une condition nécéssaire et suffisante pour que $x = a + b\sqrt{d}$ soit entier est que

$$2a \in \mathbb{Z}$$

$$2b \in \mathbb{Z}$$

et on peut donc écrire $a = u/2$ et $b = v/2$ avec $u, v \in \mathbb{Z}$ et

$$u^2 - dv^2 \in 4\mathbb{Z}.$$

Si v est pair u l'est aussi et donc $a, b \in \mathbb{Z}$. Si v est impair alors $v^2 \equiv 1 \pmod 4$ et donc $u^2 \equiv 0 \pmod 4$ ou $u^2 \equiv 1 \pmod 4$ (puisque 0 et 1 sont les seuls carrés modulo 4). Mais si $u^2 \equiv 0 \pmod 4$ on aurait $d \equiv 0 \pmod 4$ ce qui est impossible puisque d n'a pas de diviseurs carré. Donc on a forcément $u^2 \equiv 1 \pmod 4$ et $d \equiv 1 \pmod 4$. En conclusion si v est pair alors u l'est aussi et forcément $d \equiv 2 \pmod 4$ ou $d \equiv 3 \pmod 4$. Dans ce cas $a, b \in \mathbb{Z}$ et on obtient la première partie de la proposition. Si $d \equiv 1 \pmod 4$ alors u et v doivent être de même parité et on obtient la seconde partie de la proposition.

Exemple : Si $d = -1$ alors $d \equiv 3 \pmod 4$ et on est dans le premier cas de la proposition. Le corps $\mathbb{Q}(\sqrt{-1}) = \mathbb{Q}(i)$ est quadratique imaginaire et son anneau des entiers est

$$\mathbb{Z}(\sqrt{-1}) = \mathbb{Z}(i) = \{a + ib \mid a, b \in \mathbb{Z}\}.$$

C'est l'anneau des entiers de Gauss.

Bibliographie

[1] S.Lang, Algebra, third edition, Springer, 2002.

[2] J.Calais, Extensions de Corps, Mathématiques à l'Université, Ellipses, 2006.

[3] N.Bourbaki, Eléments de Mathématiques, Algèbre, Hermann, Paris, 1965.

[4] I.Stewart, Galois Theory, Third Edition, Chapman & Hall, 2006.

[5] P.Samuel, Algebraic Number Theory, Hermann, 1970.