Master de Mathématiques, THEORIE DE GALOIS ET INTRODUCTION A LA THEORIE DES NOMBRES

==========

Jean-Luc Chabert

Programme

Extensions séparables, théorème de l'élément primitif. Extensions normales, extensions galoisiennes, groupes de Galois. Théorèmes de Galois en dimension finie. Groupe de Galois d'un polynôme et extensions par radicaux.

Anneaux d'entiers de corps de nombres. Corps quadratiques et corps cyclotomiques. Groupe des unités, théorème de Dirichlet. Décomposition d'un nombre premier.

Suggestion de bibliographie

J.-P. Escoffier, *Théorie de Galois*, Dunod

P. Samuel, *Théorie algébrique des nombres*, Hermann

Chapter 1

Extensions séparables et extensions normales

1.1 Extensions algébriques (rappels)

Sous-corps engendrés

On sait que tout homomorphisme de corps est injectif. Ainsi, si $f : K \to L$ est un homomorphisme de corps, K peut être identifié à un *sous-corps* de L ; on dit aussi que L est un *sur-corps* de K ou encore une *extension* de K. Bien sûr, les corps K et L ont alors la même caractéristique, à savoir 0 ou un nombre premier p.

On sait aussi qu'une intersection de sous-anneaux (resp. sous-corps) est un sous-anneau (resp. sous-corps). On peut donc parler de *sous-anneau* et de *sous-corps engendrés* : si A est une partie de L, le sous-anneau (resp. sous-corps) de L engendré par A est le plus petit sous-anneau (resp. sous-corps) de L contenant A.

Soit $K \subset L$ une extension de corps. Pour tout élément x de L, on note $K[x]$ le sous-anneau de L engendré par K et x. On a alors :

$$K[x] = \{P(x) \mid P \in K[X]\}$$

(ensemble des *expressions polynomiales* en x).

Pour tout élément x de L, on note $K(x)$ le sous-corps de L engendré par K et x. On a alors :

$$K(x) = \left\{ \frac{P(x)}{Q(x)} \mid P, Q \in K[X],\, Q(x) \neq 0 \right\}$$

(ensemble des *expressions rationnelles* en x).

Noter que le corps $K(x)$ est le corps des fractions de l'anneau intègre $K[x]$.

Définition. Soit $K \subset L$ une extension de corps.

1. On dit que l'extension est *monogène* s'il existe un élément $x \in L$ tel que $L = K(x)$.

2. On dit que l'extension est *de type fini* s'il existe un nombre fini d'éléments $x_1, \ldots, x_n \in L$ tels que $L = K(x_1, \ldots, x_n)$.

Eléments algébriques

Définition. Soit $K \subset L$ une extension de corps. On appelle *degré* de l'extension et on note $[L : K]$, la dimension, finie ou non, du K-espace vectoriel L. Si ce degré est fini, on dit qu'il s'agit d'une *extension finie*.

Par exemple, $[\mathbb{C} : \mathbb{R}] = 2$, $[\mathbb{R} : \mathbb{Q}] = \infty$, $[\mathbb{F}_3(T) : \mathbb{F}_3] = \infty$.

Définition. Soit $K \subset L$ une extension de corps et soit x un élément de L.

1. x est dit *algébrique* sur K s'il existe un polynôme non nul $P \in K[X]$ tel que $P(x) = 0$.

2. x est dit *transcendant* sur K s'il n'est pas algébrique sur K.

Par exemple, $\sqrt{3}$ et i sont algébriques sur $\mathbb{Q}$, tandis que e et π sont transcendants sur $\mathbb{Q}$.

Proposition 1.1.1 *Soient $K \subset L$ une extension de corps et x un élément de L. L'homomorphisme d'anneaux*

$$P \in K[X] \mapsto P(x) \in L$$

a pour image $K[x]$ et pour noyau un idéal premier de $K[X]$.

1. *Si x est transcendant sur K, le noyau est l'idéal (0) et on a :*

$$K[x] \simeq K[X],\ K(x) \simeq K(X) \text{ et } [K(x) : K] = \infty.$$

2. *Si x est algébrique sur K, le noyau est engendré par un polynôme P irréductible sur K et on a :*

$$K(x) = K[x] \simeq K[X]/(P).$$

De plus, si $\deg(P) = n$, alors $\{1, x, \ldots, x^{n-1}\}$ est une base de $K[x]$ sur K et $[K[x] : K] = n$.

Ainsi, $\mathbb{Q}[i\sqrt{5}] \simeq \mathbb{Q}[X]/(X^2+5)$ tandis que $\mathbb{Q}[\pi] \simeq \mathbb{Q}[X]$.

Définition. Pour tout élément non nul $x \in L$ algébrique sur K, on appelle *polynôme minimal* de x sur K le polynôme unitaire $P \in K[X]$ de plus petit degré tel que $P(x) = 0$.
Par suite, le polynôme minimal de x sur K est l'unique polynôme unitaire irréductible sur K tel que $P(x) = 0$.

Proposition 1.1.2 *Soit $K \subset L$ une extension de corps et soit x un élément de L. Les assertions suivantes sont équivalentes* :

1. *x est algébrique sur K,*
2. *$[K(x) : K]$ est fini,*
3. *$K[x]$ est un corps.*

Extensions algébriques

Proposition 1.1.3 *Soient $K \subset L \subset M$ des extensions finies de corps. Si $(x_i)_{1\leq i\leq n}$ est une base du K-espace vectoriel L et si $(y_j)_{1\leq j\leq m}$ est une base du L-espace vectoriel M, alors $(x_i y_j)_{1\leq i\leq n, 1\leq j\leq m}$ est une base du K-espace vectoriel M. En particulier*

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

Exercice. Si $[L : K]$ est un nombre premier, alors il n'y a pas de corps strictement compris entre K et L (noter que $[L : K] = 1$ équivaut à $L = K$).

Corollaire 1.1.4 *Soit $K \subset L$ une extension finie.*

1. *Tout élément $x \in L$ est algébrique sur K et le degré du polynôme minimal de x divise $[L : K]$.*
2. *Pour toute extension M de L, un élément $x \in M$ est algébrique sur K si et seulement si il est algébrique sur L.*

Définition. L'extension $K \subset L$ est dite *algébrique* si tout élément de L est algébrique sur K.

Si L est une extension algébrique de K, alors, pour tous $x_1, \ldots, x_n \in L$, on a $K(x_1, \ldots, x_n) = K[x_1, \ldots, x_n]$ et $[K(x_1, \ldots, x_n) : K]$ est fini.

Par exemple, pour tout $n \in \mathbb{N}^*$, $[\mathbb{Q}[e^{\frac{i\pi}{2^n}}] : \mathbb{Q}] = 2^n$, et $\cup_{n\in\mathbb{N}}\mathbb{Q}[e^{\frac{i\pi}{2^n}}]$ est une extension de $\mathbb{Q}$ qui est algébrique mais non de type fini.

1.2 Clôture algébrique

Corps de rupture

Définition. Soient K un corps et $P \in K[X]$ un polynôme irréductible sur K. On appelle *corps de rupture* du polynôme P toute extension L de K contenant un élément x tel que :

1. $P(x) = 0$,
2. $L = K[x]$.

Dans ce cas, le degré de l'extension $[K[x] : K]$ est égal au degré de P. De plus, si P est unitaire, alors P est le polynôme minimal de x.

Par exemple, $\mathbb{Q}[i]$ est un corps de rupture de $X^2 + 1$ sur $\mathbb{Q}$.

Proposition 1.2.1 *Soit $P \in K[X]$ un polynôme irréductible sur K. Le corps $K[X]/(P)$ est une extension de K. Muni de l'élément $\overline{X}$, image de X dans le quotient, c'est un corps de rupture du polynôme P, appelé* corps de rupture canonique *de P.*

Exemple. $\mathbb{C} \simeq \mathbb{R}[X]/(X^2 + 1)$ où $\overline{X}$ est classiquement noté i.

Définition. On dit que deux extensions L et M du corps K sont *K-isomorphes* s'il existe un isomorphisme de corps de L sur M qui laisse fixes les éléments de K.

Par exemple, $z \in \mathbb{C} \mapsto \overline{z} \in \mathbb{C}$ est un $\mathbb{R}$-automorphisme de $\mathbb{C}$.

Proposition 1.2.2 *Soit $P \in K[X]$ un polynôme irréductible et soit L une extension de K. Si L contient une racine de P, alors, pour toute racine y de P dans L, on a : $K[y] \simeq K[X]/(P)$. Deux corps de rupture de P sont toujours K-isomorphes.*

Exemple. *Le polynôme $X^3 - 2$ irréductible sur $\mathbb{Q}$ admet dans $\mathbb{C}$ les trois racines : $\sqrt[3]{2}$, $\sqrt[3]{2}j$, $\sqrt[3]{2}j^2$. On a :*

$$\mathbb{Q}[X]/(X^3 - 2) \simeq \mathbb{Q}[\sqrt[3]{2}] \simeq \mathbb{Q}[\sqrt[3]{2}j] \simeq \mathbb{Q}[\sqrt[3]{2}j^2].$$

Exercice. Si P est un polynôme irréductible sur K dont le degré est premier avec $[L : K]$, alors P est encore irréductible sur L.

Corps de décomposition

Définition. Soit $P = a_0 + a_1X + \ldots + a_nX^n \in K[X]$ où $a_n \neq 0$. On appelle *corps de décomposition* de P toute extension L de K contenant des éléments $x_1, \ldots x_n$ (non nécessairement distincts) tels que :

1. P s'écrive sous la forme $a_n \prod_{1 \leq i \leq n}(X - x_i)$,
2. $L = K[x_1, \ldots, x_n]$.

Exemple. $\mathbb{Q}[\sqrt[3]{2}, j] = \mathbb{Q}[\sqrt[3]{2}, \sqrt[3]{2}j]$ est un corps de décomposition de $X^3 - 2$. On a :

$$\left[\mathbb{Q}[\sqrt[3]{2}, j] : \mathbb{Q}\right] = \left[\mathbb{Q}[\sqrt[3]{2}, j] : [\mathbb{Q}[\sqrt[3]{2}]\right] \times \left[[\mathbb{Q}[\sqrt[3]{2}] : \mathbb{Q}\right] = 6.$$

Proposition 1.2.3 *Pour tout polynôme $P \in K[X]$, il existe une extension L de K qui est un corps de décomposition de P. Deux corps de décomposition de P sont K-isomorphes.*

Clôture algébrique

Définition. Un corps Ω est dit *algébriquement clos* si, pour tout sur-corps L de Ω, tout élément de L algébrique sur Ω appartient en fait à Ω.

Ω est algébriquement clos équivaut aux assertions équivalentes suivantes :
— tout polynôme irréductible $P \in \Omega[X]$ est de degré 1,
— tout polynôme non constant $P \in \Omega[X]$ se décompose en un produit de facteurs du premier degré à coefficients dans Ω (P est dit *scindé* dans Ω),
— tout polynôme non constant $P \in \Omega[X]$ a au moins une racine dans Ω.

Théorème de d'Alembert.
Le corps $\mathbb{C}$ des nombres complexes est algébriquement clos.

Remarques. 1- Un corps algébriquement clos est infini.
2- Un corps algébriquement clos ne peut être ordonné.

Définition. Une *clôture algébrique* du corps K est une extension Ω de K telle que

1. Ω soit algébrique sur K,
2. Ω soit algébriquement clos.

Par exemple, $\mathbb{C}$ est une clôture algébrique de $\mathbb{R}$.

Théorème 1.2.4 (admis) *Tout corps K possède une clôture algébrique. Deux clôtures algébriques de K sont K-isomorphes.*

Un tel énoncé nécessite l'*axiome du choix* dont on parlera plus tard.

Exemple. L'ensemble $\overline{\mathbb{Q}} = \{x \in \mathbb{C} \mid x \text{ algebrique sur } \mathbb{Q}\}$ est une clôture algébrique de $\mathbb{Q}$. C'est un corps dénombrable appelé *corps des nombres algébriques*.

Remarque. Si Ω est une clôture algébrique de K, alors, pour tout polynôme $P \in K[X]$, Ω contient un corps de décomposition et un seul de P (c'est le corps engendré sur K par les racines de P dans Ω).

1.3 Extensions séparables

Soit K un corps et soit Ω une clôture algébrique de K fixée une fois pour toutes.

Ainsi, tout élément x de Ω possède un *polynôme minimal* P sur K : polynôme unitaire, irréductible dans $K[X]$ et tel que $P(x) = 0$ et, dans $\Omega[X]$, on a :

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

où les $x_i \in \Omega$ sont les racines de P, éventuellement répétées selon leur multiplicité, on les appelle les *conjugués* de x sur K.

Au risque de nous répéter, précisons que le polynôme P possède un corps de décomposition et un seul contenu dans Ω, à savoir, le corps $K[x_1, \ldots, x_n]$ et possède au plus autant de corps de rupture dans Ω qu'il y a de conjugués de x distincts, à savoir, les corps $K[x_i]$ où x_i décrit l'ensemble de ces conjugués.

Définition. On dit qu'un polynôme $Q \in K[X]$ est *séparable* si ses racines dans Ω sont simples.

Cette notion ne dépend pas du corps K lui-même (on peut remplacer K par un sur-corps L).

Remarques. 1- *Un polynôme $Q \in K[X]$ est séparable si et seulement s'il est premier avec son polynôme dérivé*. [En effet, Q non séparable $\Leftrightarrow$ Q possède une racine multiple x (dans Ω) $\Leftrightarrow$ Q et Q' possèdent une racine commune x (dans Ω) $\Leftrightarrow$ Q et Q' sont divisibles par un même polynôme non constant $P \in K[X]$, à savoir, le polynôme minimal de x sur K.]
2- *Un polynôme irréductible P est séparable si et seulement si son polynôme dérivé n'est pas identiquement nul* ; et c'est toujours le cas en caractéristique 0. [En effet,

P non séparable $\Leftrightarrow$ P et P' ont une racine commune x dans Ω. Mais, comme P est irréductible, P est (au coefficient dominant près) le polynôme minimal de x et donc x est racine de P' si et seulement si $P' \equiv 0$.]
3- *Un polynôme irréductible $P \in K[X]$ n'est pas séparable si et seulement si il est de la forme $P(X) = Q(X^p)$ où $Q \in K[X]$* (et caractéristique de $K = p \neq 0$).

Définition. On dit qu'un élément x de Ω est *séparable* sur K si x est racine simple de son polynôme minimal.Cette notion dépend fortement du corps K.

Proposition 1.3.1 *Si la caractéristique de K est $p \neq 0$ et si tout élément de K possède une racine p-ième dans K, alors tout élément $x \in \Omega$ est séparable sur K.*

Remarque. *Si le corps K est fini de caractéristique $p \neq 0$, alors tout élément de K possède une racine p-ième dans K.* [Le morphisme de corps $x \in K \mapsto x^p \in K$ étant injectif est aussi surjectif par suite de la finitude de K.]

Proposition 1.3.2 *Si le corps K possède l'une des deux propriétés suivantes :*

1. *la caractéristique de K est 0,*
2. *K est fini,*

alors tout élément algébrique sur K est séparable sur K ou encore, de façon équivalente, tout polynôme irréductible sur K est séparable.

Contre-exemple. Le polynôme $P(X) = X^p - T$ à coefficients dans $K = \mathbb{F}_p(T)$ est irréductible dans $K[X]$, mais n'est pas séparable.

Définition. Une extension algébrique L/K est dite *séparable* lorsque tout élément de L est séparable sur K.

Soit $K \subset L \subset M \subset \Omega$. Il est immédiat que, si l'extension M/K est séparable, alors les extensions M/L et L/K sont séparables.

Proposition 1.3.3 *Si le corps K est de caractéristique 0 ou est fini, alors toute extension algébrique de K est séparable.*

Proposition 1.3.4 [**Théorème de l'élément primitif**]
Toute extension algébrique finie séparable L/K est monogène : il existe $x \in L$ tel que $L = K[x]$.

Corollaire 1.3.5 *Toute extension finie de $\mathbb{Q}$ ou de $\mathbb{F}_q$ est monogène.*

Exemples. 1. $\mathbb{Q}[i, \sqrt{2}] = \mathbb{Q}[i + \sqrt{2}]$.
2. $\mathbb{F}_{q^n} = \mathbb{F}_q[\zeta]$ où ζ est une racine primitive $(q^n - 1)$-ième de l'unité.

1.4 K-morphismes de corps

Soit $K \subset L \subset \Omega$. Un morphisme de corps $\sigma : L \to \Omega$ est toujours injectif ; sa restriction au sous-corps premier K_0 de K est nécessairement l'identité. Autrement dit, $\sigma(L) \simeq L$ et $\sigma_{|K_0} = id_{K_0}$.
On va s'intéresser aux K-*morphismes* de L, c'est-à-dire, aux morphismes de corps $\sigma : L \to \Omega$ tels que $\sigma|_K = id_K$. Lorsque σ est un K-morphisme de L, on dit que L et $\sigma(L)$ sont K-isomorphes et le corps-image $\sigma(L)$ est appelé *corps conjugué* de L sur K.
[On a déjà parlé de K-isomorphismes à propos des corps de rupture : les corps de rupture d'un polynôme P irréductible sur K sont tous K-isomorphes.]

Remarque préliminaire. Pour tout K-morphisme $\sigma : L \to \Omega$ et tout $x \in L$, $\sigma(x)$ est un conjugué de x sur K.

Proposition 1.4.1 *Soit $x \in \Omega$ et soient $x_1 = x, x_2, \ldots, x_r$ les conjugués distincts de x sur K. Il y a exactement r K-morphismes de $L = K[x]$ dans Ω, à savoir, les morphismes*

$$\sigma_i : Q(x) \in K[x] \mapsto Q(x_i) \in K[x_i] \quad (i = 1, \ldots, r).$$

Le morphisme σ_i est caractérisé par $\sigma_i(x) = x_i$.

Proposition 1.4.2 *Soit L/K une extension finie.*
1. Le nombre de K-morphismes de L dans Ω est $\leq [L : K]$.
2. Le nombre de K-morphismes de L dans Ω est égal à $[L : K]$ si et seulement si l'extension L/K est séparable.

Lemme 1.4.3 *Soit $K \subset L_1 \subset L \subset \Omega$ où l'extension L/K est finie.*
1. Si σ est un K-morphisme de L, alors la restriction $\sigma|_{L_1}$ de σ à L_1 est un K-morphisme de L_1.
2. Si τ est un K-morphisme de L_1, alors le nombre de K-morphismes σ de L tels que $\sigma|_{L_1} = \tau$ est $\leq [L : L_1]$.
3. Si L/K est séparable, il y a exactement $[L : L_1]$ prolongements σ de τ à L.

Corollaire 1.4.4 *L'extension algébrique $K[x]/K$ est séparable si et seulement si x est séparable sur K.*

Corollaire 1.4.5 *Soit $K \subset L \subset M \subset \Omega$. L'extension M/K est séparable si et seulement si les extensions M/L et L/K sont séparables.*

En particulier, l'extension $K[x_1, \ldots, x_r]$ est séparable si et seulement si $x_1, \ldots, x_r$ sont séparables sur K.

1.5 Extensions normales

Définition. Une extension algébrique L/K est dite *normale* si, pour tout $x \in L$, tous les conjugués de x sur K sont aussi dans L.

Si l'extension algébrique L/K est normale, L est stable par tout K-morphisme.

Proposition 1.5.1 *Si l'extension algébrique finie L/K est normale, alors tous les K-morphismes de L dans Ω sont des K-automorphismes de L et il y en a au plus $[L : K]$.*

Exemples. 1. Toute extension quadratique est normale.
2. Ω est une extension normale de tous ses sous-corps.
3. L'extension $\mathbb{Q}[\sqrt[3]{2}]/\mathbb{Q}$ n'est pas normale.
4. Tout corps fini de caractéristique p est extension normale de son sous-corps premier $\mathbb{F}_p$

Une intersection d'extensions normales de K est une extension normale de K. Par suite, si $K \subset L \subset \Omega$, il existe une plus petite extension normale de K contenant L et contenue dans Ω, on l'appelle *extension normale de K engendrée* par L.

Remarques. Soient $K \subset L \subset M \subset \Omega$:
— Si l'extension M/K est normale, alors l'extension M/L est normale [mais en général pas l'extension L/K].
— Les extensions M/L et L/K peuvent êre normales sans que M/K le soit.

Exemple. L'extension biquadratique $\mathbb{Q}[\sqrt[4]{2}]/\mathbb{Q}$ n'est pas normale. En effet, $\sqrt[4]{2}$ a pour polynôme minimal $X^4 - 2$ qui a aussi pour racine $i\sqrt[4]{2}$. Or, $i\sqrt[4]{2} \notin \mathbb{Q}[\sqrt[4]{2}] \subset \mathbb{R}$.

Proposition 1.5.2 *Une extension algébrique finie L/K est normale si, et seulement si, L est le corps de décomposition d'un polynôme à coefficients dans K.*

Proposition 1.5.3 *Une extension algébrique finie L/K est normale si, et seulement si, L n'a pas d'autre corps conjugué sur K que lui-même.*

Chapter 2

Théorèmes de Galois

2.1 Groupes de Galois et extensions galoisiennes

Définition. Soit L/K une extension *quelconque* de corps. On appelle *groupe de Galois* de l'extension L/K le sous-groupe du groupe des automorphismes de L formé des K-automorphismes de L. On le note $Gal(L/K)$ ou $G(L/K)$.

Exemples. 1. $G(\mathbb{C}/\mathbb{R}) \simeq \mathbb{Z}/2\mathbb{Z}$.

2. $G(\mathbb{R}/\mathbb{Q}) = \{id_{\mathbb{R}}\}$.

3. $G(\mathbb{Q}[\sqrt{2}]/\mathbb{Q}) = \{id, \sigma\}$ où, pour $a, b \in \mathbb{Q},\ \sigma(a + b\sqrt{2}) = a - b\sqrt{2}$.

4. $G(\mathbb{Q}[\sqrt[3]{2}]/\mathbb{Q}) = \{id\}$.

5. $G(\mathbb{Q}[i]/\mathbb{Q}) = \{id, \tau\}$ où τ désigne la conjugaison complexe.

Proposition 2.1.1 *Soit L/K une extension algébrique finie. Alors* :
1. $|G(L/K)| \leq [L : K]$.
2. $|G(L/K)| = [L : K]$ *si et seulement si l'extension L/K est à la fois séparable et normale.*

Définition. Une extension algébrique L/K est dite *galoisienne* si elle est à la fois séparable et normale.

Exemples. 1- Toute extension quadratique de $\mathbb{Q}$ est galoisienne.
2- Tout corps fini est extension galoisienne de n'importe lequel de ses sous-corps.

Proposition 2.1.2 *Une extension algébrique finie L/K est galoisienne si et seulement si L est corps de décomposition d'un polynôme séparable à coefficients dans K.*

Exemple. Une extension finie de $\mathbb{Q}$ est galoisienne si, et seulement si, elle est le corps de décomposition d'un polynôme à coefficients rationnels.

Proposition 2.1.3 *Pour tout corps L de caractéristique p et toute puissance q de p, l'application $x \in L \mapsto x^q \in L$ est un morphisme de corps.*

Proposition 2.1.4 *Le groupe de Galois $G(\mathbb{F}_{q^n}/\mathbb{F}_q)$ de l'extension galoisienne $\mathbb{F}_{q^n}/\mathbb{F}_q$ est cyclique d'ordre n engendré par le $\mathbb{F}_q$-automorphisme de $\mathbb{F}_{q^n}$, dit* automorphisme de Frobenius :

$$\pi_q : x \in \mathbb{F}_{q^n} \mapsto x^q \in \mathbb{F}_{q^n}.$$

Remarque. Soient $K \subset L \subset M \subset \Omega$:
— Si l'extension M/K est galoisienne, alors l'extension M/L est galoisienne [mais en général pas l'extension L/K].
— Les extensions M/L et L/K peuvent être galoisiennes sans que M/K le soit.

2.2 Théorèmes de Galois

Soit L/K une extension de corps.

Définition. Pour toute partie X de $G(L/K)$, l'ensemble

$$L^X = \{x \in L \mid \sigma(x) = x \ \ \forall \sigma \in X\}$$

est un corps compris entre K et L appelé *corps fixe* ou *corps des invariants* de X.

En fait, le corps fixe de X est aussi égal au corps fixe du sous-groupe $\langle X \rangle$ de $G(L/K)$ engendré par X. On se limitera donc à considérer des corps fixes relativement à des sous-groupes de $G(L/K)$.

Inversement, pour tout corps M compris entre K et L, l'ensemble

$$\{\sigma \in G(L/K) \mid \sigma(x) = x \ \ \forall x \in M\}$$

est un sous-groupe de $G(L/K)$. En fait, ce sous-groupe est l'ensemble de tous les M-automorphismes de L, ce que l'on a convenu de noter $G(L/M)$.
On a ainsi deux applications entre l'ensemble des sous-groupes H de $G(L/K)$ et l'ensemble des corps M compris entre K et L :

$$H \mapsto L^H \ \text{ et } \ M \mapsto G(L/M).$$

Ces deux applications renversent les inclusions. Sont-elles réciproques l'une de l'autre ?

Proposition 2.2.1 (Enoncé fondamental) *Soient L un corps, G un groupe fini d'automorphismes de L et $K = L^G$ le corps fixe de G. Alors L/K est une extension galoisienne finie de groupe de Galois G.*

Application. Soient k un corps, n un entier ≥ 1, $L = k(X_1, \ldots, X_n)$ et K le sous-corps de L formé des fractions rationnelles symétriques. Alors l'extension L/K est galoisienne, $G(L/K) \simeq \mathcal{S}_n$, $[L : K] = n!$ et $K = k(\Sigma_1, \ldots, \Sigma_n)$.
[$\mathcal{S}_n$ désigne le groupe symétrique de degré n et $\Sigma_1, \ldots, \Sigma_n$ désignent les polynômes symétriques élémentaires en les $X_1, \ldots, X_n$.]

Corollaire 2.2.2 (Premier théorème de Galois) *Soit L/K une extension galoisienne finie de groupe de Galois G. L'application $H \mapsto L^H$ de l'ensemble des sous-groupes H de G dans l'ensemble des corps M compris entre K et L est une bijection décroissante dont la bijection réciproque est $M \mapsto G(L/M)$.*

Remarque. Soit L/K une extension galoisienne finie. Si M et M' sont deux corps intermédiaires K-isomorphes, alors les sous-groupes $G(L/M)$ et $G(L/M')$ de $G(L/K)$ sont conjugués.

Proposition 2.2.3 (Deuxième théorème de Galois) *Soit L/K une extension galoisienne finie de groupe de Galois G et soit M un corps compris entre K et L. L'extension M/K est galoisienne si et seulement si le sous-groupe $H = G(L/M)$ de $G = G(L/K)$ est normal. Dans ce cas, $G(M/K) \simeq G/H$.*

2.3 Groupe de Galois d'un polynôme

Dans cette section et la suivante, K désigne un corps de caractéristique 0.
Soit toujours Ω une clôture algébrique de K.

Définition. Soit f un polynôme à coefficients dans K. On appelle *groupe de Galois sur K du polynôme f* le groupe de Galois $G(L/K)$ où L désigne le corps de décomposition de f sur K (contenu dans Ω).

Si $x_1, \ldots, x_r$ désignent les racines de f dans Ω, alors $L = K[x_1, \ldots, x_r]$ et tout $\sigma \in G(L/K)$ induit une permutation de l'ensemble $\{x_1, \ldots, x_r\}$. D'où, un morphisme injectif de groupes de $G(L/K)$ dans $\mathcal{S}_r$. En particulier $|G(L/K)|$ divise $r!$.

Extensions cyclotomiques

Soit $n \geq 3$ et soit ζ_n une racine primitive n-ième de l'unité (dans Ω). Le corps $K_n = K[\zeta_n]$ est indépendant du choix de ζ_n, c'est le corps de décomposition sur K du polynôme $X^n - 1$. On dit que K_n est une *extension cyclotomique* de K.

L'extension K_n/K est galoisienne et tout $\sigma \in G(K_n/K)$ est caractérisé par $\sigma(\zeta_n) = \zeta_n^{j_\sigma}$ où j_σ est un entier premier à n. L'application induite par j :

$$\sigma \in G(K_n/K) \mapsto \overline{j_\sigma} \in (\mathbb{Z}/n\mathbb{Z})^\times$$

est un morphisme de groupes injectif. Par suite, $G(K_n/K)$ est abélien.

En particulier, pour $K = \mathbb{Q}$, $K_n = \mathbb{Q}[\zeta_n]$ est à la fois corps de rupture et corps de décomposition du n-ième polynôme cyclotomique Φ_n, $[\mathbb{Q}[\zeta_n] : \mathbb{Q}] = \varphi(n)$ et $G(\mathbb{Q}[\zeta_n]/\mathbb{Q}) \simeq (\mathbb{Z}/n\mathbb{Z})^\times$. Notons que, pour p premier, $G(\mathbb{Q}[\zeta_p]/\mathbb{Q})$ est cyclique.

Rappel. On appelle *n-ième polynôme cyclotomique* le polynôme :

$$\Phi_n(X) = \prod_{0 \leq k \leq n-1, (k,n)=1} \left(X - exp\left(\frac{2ik\pi}{n}\right)\right).$$

On sait que $\Phi_n(X) \in \mathbb{Z}[X]$, $\Phi_n(X)$ est irréductible sur $\mathbb{Q}$, $X^n - 1 = \prod_{d|n} \Phi_d(X)$ et $n = \sum_{d|n} \varphi(d)$.

Extensions de Kummer

Soient $n \geq 2$, a un élément non nul de K et L le corps de décomposition sur K du polynôme $X^n - a$. Notons α un élément de Ω tel que $\alpha^n = a$.

— Si le corps K contient une racine primitive n-ième de l'unité ζ_n, alors $L = K[\alpha]$ et tout $\sigma \in G(L/K)$ est caractérisé par $\sigma(\alpha) = \zeta_n^{k_\sigma}\alpha$ où k_σ est un entier. L'application induite par k :

$$\sigma \in G(L/K) \mapsto \overline{k_\sigma} \in \mathbb{Z}/n\mathbb{Z}$$

est un morphisme de groupes injectif. Par suite, $G(L/K)$ est cyclique. Une telle extension est appelée *extension de Kummer*.

— Sinon, $L = K[\zeta_n, \alpha]$ où ζ_n désigne une racine primitive n-ième de l'unité. Soit $K_n = K[\zeta_n]$. On a :

$$K \subset K_n = K[\zeta_n] \subset L = K_n[\alpha].$$

Comme l'extension K_n/K est galoisienne,

$$G(L/K_n) \lhd G(L/K) \quad \text{et} \quad G(L/K)/G(L/K_n) \simeq G(K_n/K)$$

où $G(L/K_n)$ est cyclique et $G(K_n/K)$ est abélien.

2.4 Equations résolubles par radicaux

Une équation polynomiale $f(X) = 0$ à coefficients dans K est dite *résoluble par radicaux* sur K si ses racines s'expriment à partir des coefficients de f à l'aide d'additions, de multiplications et d'extractions de racines k-ièmes ($k \geq 2$).

Exemples.. 1. Les équations de degré 2 sont résolubles par radicaux.
2. Les formules de Cardan montrent que les équations de degré 3 aussi.
3. Les équations de degré 4 se ramènent à des équations de degré 3.

Définition. Un corps L est dit *extension par radicaux* du corps K s'il existe une suite d'extensions monogènes $K = K_0 \subset K_1 \subset K_2 \subset \cdots \subset K_s = L$ où, pour $0 \leq i < s$, $K_{i+1} = K_i[\alpha_i]$ et $\alpha_i^{n_i} \in K_i$ (pour certains $n_i \geq 1$).

L'équation $f = 0$ est résoluble par radicaux sur K signifie que les racines de f appartiennent à une extension par radicaux de K. On va montrer qu'il existe des équations de degré 5 qui ne sont pas résolubles par radicaux en utilisant la notion de groupe résoluble.

Définition. Un groupe G est dit *résoluble* s'il existe une suite de sous-groupes $\{e\} = G_r \subset G_{r-1} \subset G_{r-2} \subset \cdots \subset G_1 \subset G_0 = G$ telle que, pour $0 \leq i < r$, $G_{i+1} \lhd G_i$ et G_i/G_{i+1} soit abélien.

On rappelle que $D(G)$ désigne le groupe dérivé de G, c'est-à-dire, le sous-groupe de G engendré par les commutateurs des éléments de G.

Proposition 2.4.1 *Un groupe G est résoluble si et seulement s'il existe un entier r tel que $D^r(G) = \{e\}$ où $D^{k+1}(G) = D(D^k(G))$.*

Exemples. 1. Un groupe abélien est résoluble.
2. Les sous-groupes et les quotients d'un groupe résoluble sont résolubles.
3. Le groupe S_n est résoluble si et seulement si $n < 5$.

Proposition 2.4.2 *Si L est une extension de K par radicaux et si L/K est galoisienne, alors le groupe de Galois $G(L/K)$ est résoluble.*

Proposition 2.4.3 *Si L est une extension de K par radicaux, alors il existe une extension par radicaux de K contenant L et galoisienne sur K*

Théorème 2.4.4 *Si le groupe de Galois sur le corps K d'un polynôme $f(X) \in K[X]$ n'est pas un groupe résoluble, alors l'équation $f(X) = 0$ n'est pas résoluble par radicaux sur K.*

Exemple. [**abstrait**] Soit $n \geq 5$. Considérons le polynôme

$$f_n(T) = T^n + \prod_{k=1}^{n} (-1)^k \Sigma_k T^{n-k}$$

à coefficients dans $K = \mathbb{Q}(\Sigma_1, \ldots, \Sigma_n)$; il est de degré n et irréductible sur K. Son corps de décomposition est le corps $L = \mathbb{Q}(X_1, \ldots, X_n)$ et le groupe de Galois $G(L/K) \simeq S_n$ n'est pas résoluble. Donc, l'*équation générale* de degré n, $f_n(T) = 0$, n'est pas résoluble par radicaux sur le corps K.

Exemple. [**numérique**]. L'équation :

$$X^5 - 10X + 5 = 0$$

n'est pas résoluble par radicaux sur $\mathbb{Q}$. En effet, le groupe de Galois du polynôme $X^5 - 10X + 5$ est isomorphe $\mathcal{S}_5$ (car il contient un élément d'ordre 5 et une transposition).

Chapter 3

Notions de module et . . . d'élément entier sur un anneau

3.1 Modules

La notion de module sur un anneau généralise la notion d'espace vectoriel sur un corps. Elle étend aussi la notion de groupe abélien et celle d'idéal d'un anneau.

Dans tout ce chapitre, A désigne un anneau commutatif et unitaire.

Définition. Un *A-module* est un ensemble M muni :
— d'une addition qui est une loi de groupe commutatif et
— d'une multiplication par les éléments de A :

$$(a, m) \in A \times M \mapsto am \in M$$

satisfaisant aux conditions suivantes :
$\forall a, b \in A$, $\forall m, n \in M$:

$a(m + n) = am + an$
$(a + b)m = am + bm$
$(ab)m = a(bm)$
$1m = m$.

On a alors aussi :

$$a0 = 0 = 0m \text{ et } a(-m) = (-a)m = -(am).$$

Exemples.
1. Un espace vectoriel sur un corps K est un K-module (et réciproquement).
2. Un groupe abélien est un $\mathbb{Z}$-module (et réciproquement).
3. Un idéal d'un anneau A est un A-module contenant dans A (et réciproquement).
4. A^n muni des lois suivantes est un A-module :

$$(a_1, \ldots, a_n) + (b_1, \ldots, b_n) = (a_1 + b_1, \ldots, a_n + b_n)$$
$$a(a_1, \ldots, a_n) = (aa_1, \ldots, aa_n).$$

5. Une A-algèbre B, c'est-à-dire, un anneau B muni d'un morphisme d'anneaux $\varphi : A \to B$, est en particulier un A-module lorsqu'il est muni de la multiplication $ab = \varphi(a)b$. Ainsi, les anneaux $A[X]$ ou $A/\mathfrak{I}$ (où $\mathfrak{I}$ est un idéal de A) sont des A-modules.

6. L'anneau (non commutatif) $\mathcal{M}_n(A)$ des matrices carrées de taille n à coefficients dans A est un A-module.

3.2 Sous-modules

Définition. Soient A un anneau et M un A-module. Un *sous-A-module* N de M est une partie N de M qui est un sous-groupe pour l'addition et qui est stable par la multiplication par les éléments de A.

Exemples. 1. Les sous-A-modules de l'anneau A sont les idéaux de A.
2. Les sous-$\mathbb{Z}$-modules d'un groupe abélien G sont les sous-groupes de G.
3. Pour tout A-module M, $\{0\}$ et M sont des sous-A-modules de M.
4. Une intersection de sous-A-modules de M est un sous-A-module de M.

Proposition 3.2.1 *(définition) Soient M un A-module et X un partie non vide de M. L'intersection des sous-A-modules de M contenant X est un sous-A-module de M, c'est le plus petit sous-A-module de M contenant X. On l'appelle le sous-A-module de M* engendré par *X, on le note parfois $< X >$. C'est encore l'ensemble des combinaisons linéaires des éléments de X à coefficients dans A, autrement dit,*

$$< X >= \{a_1x_1 + \ldots + a_kx_k \mid k \in \mathbb{N}^*, a_i \in A, x_i \in X\}.$$

Définitions. 1. Le A-module M est dit *monogène* s'il est engendré par un élément, c'est-à-dire, s'il existe $x \in M$ tel que $M = \{ax \mid a \in A\}$.

2. Le A-module M est dit *de type fini* s'il est engendré par une partie finie, c'est-à-dire, s'il existe un nombre fini d'éléments $x_1, \ldots, x_n \in M$ tels que
$$M = \{a_1x_1 + \cdots + a_nx_n \mid a_1, \ldots, a_n \in A\}.$$

Proposition 3.2.2 *(définition) Soient M un A-module et N un sous-A-module de M. Le groupe quotient M/N muni de la multiplication*
$$a(m + N) = am + N$$
est un A-module. On l'appelle le module quotient *M/N de M par N.*

Exemple. Si $\mathfrak{I}$ est un idéal de A, le A-module $A/\mathfrak{I}$ n'est autre que le quotient des A-modules A et $\mathfrak{I}$.

3.3 Eléments entiers sur un anneau

Dans cette section A et B désignent deux anneaux quelconques tels que $A \subset B$.

Définition. Un élément x de B est dit *entier* sur A s'il est racine d'un polynôme unitaire à coefficients dans A, c'est-à-dire, s'il existe $n \in \mathbb{N}^*$ et des éléments $a_0, a_1, \ldots, a_{n-1} \in A$ tels que

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

Exemples. 1. Lorsque A est un corps, dire que x est entier sur A signifie que x est algébrique sur A.
2. Les éléments de $\mathbb{C}$ entiers sur $\mathbb{Z}$ sont appelés des *entiers algébriques*. Par exemple : $\sqrt{2}$ ou $a + ib$ avec $a, b \in \mathbb{Z}$.
3. Les entiers algébriques de $\mathbb{Q}$ sont les éléments de $\mathbb{Z}$.

Proposition 3.3.1 *Etant donné un élément x de B, les assertions suivantes sont équivalentes* :
1. l'élément x est entier sur A,
2. l'anneau $A[x]$ est un A-module de type fini,
3. il existe un anneau C, A-module de type fini, tel que $A[x] \subset C \subset B$.

Remarque. On verra plus tard que lorsque l'anneau A est principal (ou plus généralement noethérien), pour que l'élément x de B soit entier sur A, il faut et il suffit qu'il existe un A-module de type fini M (pas nécessairement un anneau) tel que $A[x] \subset M \subset B$.

Corollaire 3.3.2 *Soient $x_1, \ldots, x_r \in B$. Si $x_1, \ldots, x_r$ sont entiers sur A, alors l'anneau $A[x_1, \ldots, x_r]$ est un A-module de type fini.*

Proposition 3.3.3 *L'ensemble des éléments de B entiers sur A est un sous-anneau de B contenant A. On l'appelle* fermeture intégrale *de A dans B et on le note parfois A'_B.*

Exemple. $\mathbb{Z}'_{\mathbb{Q}[i]} = \mathbb{Z}[i]$.

Définitions. 1. L'anneau B est dit *entier* sur A si tout élément de B est entier sur A (c.-à-d., $A'_B = B$).
2. L'anneau A est dit *intégralement fermé* dans B si tout élément de B entier sur A appartient à A (c.-à-d., $A'_B = A$).

Exemple. $\mathbb{Z}[\sqrt{5}]$ est entier sur $\mathbb{Z}$, mais n'est pas intégralement fermé dans $\mathbb{Q}[\sqrt{5}]$. [Considérer $\frac{1}{2}(1 + \sqrt{5})$.]

Proposition 3.3.4 *Soient $A \subset B \subset C$ trois anneaux. Si B est entier sur A et si C est entier sur B, alors C est entier sur A.*

Proposition 3.3.5 *Supposons que B soit un anneau intègre entier sur l'anneau A. Alors, B est un corps si et seulement si A est un corps.*

3.4 Anneaux intégralement clos

Définitions. Supposons A intègre de corps des fractions K.
1. La fermeture intégrale A'_K de A dans K est appelée *clôture intégrale* de A et notée plus simplement A'.
2. L'anneau A est dit *intégralement clos* lorsqu'il est égal à sa clôture intégrale.

Proposition 3.4.1 1- *La clôture intégrale A' d'un anneau intègre A est un anneau intégralement clos.*
2- *Toute intersection d'anneaux intégralement clos est un anneau intégralement clos.*

Proposition 3.4.2 *Soit A un anneau intègre et soit S une partie multiplicative de A. Si A' désigne la clôture intégrale de A, alors la clôture intégrale de $S^{-1}A$ est $S^{-1}A'$ [autrement dit, $(S^{-1}A)' = S^{-1}(A')$].*

Proposition 3.4.3 *Un anneau principal est intégralement clos.*

Plus généralement, un anneau factoriel est intégralement clos.

Proposition 3.4.4 *Soit A un anneau intègre de corps des fractions K et soit L un corps extension de K. Un élément x de L est entier sur A si et seulement si les coefficients du polynôme minimal de x sur K sont eux-mêmes entiers sur A.*

Corollaire 3.4.5 *Si l'anneau A est intégralement clos, un élément x dans une extension du corps des fractions K de A est entier sur A si et seulement si son polynôme minimal sur K est à coefficients dans A.*

Exemple. Un élément $x = a + b\sqrt{d}$ de $\mathbb{Q}[\sqrt{d}]$ (où $a, b \in \mathbb{Q}$) est un entier algébrique si et seulement si $2a$ et $a^2 - db^2$ appartiennent $\mathbb{Z}$.

Application. *Les polynômes cyclotomiques $\Phi_n(X)$ sont irréductibles dans $\mathbb{Q}[X]$.*
On rappelle que, pour $n \geq 2$, le n-ième polynôme cyclotomique $\Phi_n(X)$ est défini par :

$$\Phi_n(X) = \prod_{1 \leq k \leq n-1,\, (k,n)=1} \left(X - e^{\frac{2ik\pi}{n}} \right).$$

On sait que $\deg \Phi_n(X) = \varphi(n)$ et que $\Phi_n(X) \in \mathbb{Z}[X]$.

3.5 L'anneau des entiers d'un corps quadratique

Définition. On appelle *corps quadratique* tout corps $K \subset \mathbb{C}$ tel que $[K : \mathbb{Q}] = 2$.

Tout corps quadratique est de la forme $\mathbb{Q}[\sqrt{d}]$ où $d \in \mathbb{Z}$ est sans "facteurs carrés" (c'est-à-dire, non divisible par le carré d'un nombre premier) et où, pour $d < 0$, on convient d'écrire $\sqrt{d}$ au lieu de $i\sqrt{-d}$.

On notera A_K la fermeture intégrale de $\mathbb{Z}$ dans K.

Proposition 3.5.1 *Soit* $K = \mathbb{Q}[\sqrt{d}]$ *:*

$$\text{Si } d \equiv 2 \text{ ou } 3 \pmod 4, \text{ alors } A_{\mathbb{Q}[\sqrt{d}]} = \{a + b\sqrt{d} \mid a, b \in \mathbb{Z}\},$$

$$\text{Si } d \equiv 1 \pmod 4, \text{ alors } A_{\mathbb{Q}[\sqrt{d}]} = \left\{ \frac{1}{2}(u + v\sqrt{d}) \mid u, v \in \mathbb{Z},\ 2|u - v \right\}.$$

Proposition 3.5.2 *Pour tout corps quadratique* $K = \mathbb{Q}[\sqrt{d}]$*, le* $\mathbb{Z}$*-module* A_K *est libre de rang* 2 *:*

$$\text{Si } d \equiv 2 \text{ ou } 3 \pmod 4, \quad A_K = \mathbb{Z} + \sqrt{d}\mathbb{Z},$$

$$\text{Si } d \equiv 1 \pmod 4, \quad A_K = \mathbb{Z} + \mathbb{Z}\frac{1 + \sqrt{d}}{2}.$$

Chapter 4

Modules libres

4.1 Morphismes de modules

Définition. Soient M et N deux A-modules. On dit que $\varphi : M \to N$ est un *morphisme* de A-modules ou encore une *application A-linéaire* si, pour tous $m, n \in M$ et $a \in A$, on a :

$$\varphi(m+n) = \varphi(m) + \varphi(n) \text{ et } \varphi(am) = a\varphi(n).$$

Lorsque φ est bijectif on parle d'*isomorphisme* de A-modules.

Proposition 4.1.1 *Soit $\varphi : M \to N$ un morphisme de A-modules.*
1- *L'image $Im(\varphi)$ et le noyau $Ker(\varphi)$ de φ sont des A-modules*
2- *On a l'isomorphisme de A-modules :*

$$M/Ker(\varphi) \simeq Im(\varphi).$$

Définitions. Soit M un A-module et soit $X = \{x_1, \ldots, x_n\} \subset M$.

1. La famille X est *génératrice* si la partie X engendre le A-module M.
2. La famille X est *libre* si, quels que soient $a_1, \ldots, a_n \in A$, la relation $\sum_{i=1}^{n} a_i x_i = 0$ implique $a_1 = \cdots = a_n = 0$.
3. La famille X est une *base* de M si elle est à la fois libre et génératrice.

Considérons l'application A-linéaire :

$$\varphi : (a_1, \ldots, a_n) \in A^n \mapsto a_1x_1 + \cdots + a_nx_n \in M.$$

L'application φ est surjective si et seulement si la famille X est *génératrice*

[c.-à-d., tout élément de M s'écrit sous la forme $\sum_{i=1}^{n} a_i x_i$].
L'application φ est injective si et seulement si la famille X est *libre* sur A
[c.-à-d., pour tous $a_1, \ldots, a_n \in A$, $(\sum_{i=1}^{n} a_i x_i = 0 \Rightarrow a_1 = \ldots = a_n = 0)$].
L'application φ est bijective si et seulement si X est une *base* du A-module M
[tout élément de M s'écrit d'une façon et d'une seule sous la forme $\sum_{i=1}^{n} a_i x_i$].

Remarques. 1. Le A-module A^n possède une base canonique et tout A-module M qui possède une base formée de n éléments est isomorphe à A^n.

2. Contrairement au cas des espaces vectoriels :
— deux éléments peuvent être liés sans être proportionnels,
— en général, un module ne possède pas de base.

3. Un A-module engendré par n éléments $x_1, \ldots, x_n$ est isomorphe à un quotient du A-module A^n par un sous-A-module (à savoir, $Ker(\varphi)$ avec les notations précédentes). En particulier, un A-module monogène engendré par un élément x est isomorphe à $A/\mathcal{I}$ où $\mathcal{I}$ est l'idéal $\mathcal{I} = \{a \in A \mid ax = 0\}$.

Les notions de famille génératrice, de famille libre et de base s'étendent sans difficultés au cas de parties infinies.

4.2 Modules libres

Définition. Un A-module M distinct de $\{0\}$ est dit *libre* s'il possède une base.

Proposition 4.2.1 *Un A-module M distinct de $\{0\}$ est libre si, et seulement si, il existe une famille $\{x_i\}_{i\in I}$ d'éléments de M telle que tout élément x de M s'écrive d'une façon et d'une seule sous la forme :*

$$x = \sum_{k=1}^{r} n_k x_{i_k} \quad \text{avec } r \in \mathbb{N}^*, i_1, \ldots, i_r \in I,\ n_1, \ldots, n_r \in \mathbb{Z}.$$

La famille $X = \{x_i\}_{i\in I}$ est alors une base *de M et le A-module M est isomorphe $A^{(I)}$.*

Proposition 4.2.2 *Si X est une base d'un A-module libre M alors, pour tout A-module N et toute application $f : X \to N$, il existe un morphisme de A-module et un seul $\varphi : M \to N$ tel que $\varphi(x) = f(x)$ pour tout $x \in X$.*

Proposition 4.2.3 *Toutes les bases d'un A-module libre ont le même cardinal.*

Définition. On appelle *rang* d'un A-module libre M le cardinal d'une base de M.

Proposition 4.2.4 *Soit M un A-module libre de rang n.*

1. *Toute famille génératrice possède au moins n éléments.*
2. *Toute famille génératrice formée de n éléments est une base.*
3. *Si $(x_1, \ldots, x_n)$ une base de M, alors la famille $(y_1, \ldots, y_n)$ où on pose $y_i = \sum_{1 \leq j \leq n} b_{i,j} x_j$ est une base de M si et seulement si le déterminant de la matrice $(b_{i,j}) \in \mathcal{M}_n(A)$ est inversible dans A.*

Une matrice carrée $B \in \mathcal{M}_n(A)$ est inversible dans $\mathcal{M}_n(A)$ si et seulement si $\det(B)$ est inversible dans A.

Remarques. 1. Une famille libre formée de n éléments n'est pas nécessairement une base.
2. Un module libre est de type fini si, et seulement si, il est de rang fini.
3. Une famille génératrice ne contient pas nécessairement une base et une famille libre ne peut pas toujours être complétée en une base.

4.3 Modules de type fini sur un anneau principal

Proposition 4.3.1 (Théorème de la base adaptée) . *Supposons l'anneau A principal. Soit M un A-module libre de rang n et soit N un sous-A-module de M. Alors, il existe un entier k tel que $0 \leq k \leq n$, des éléments $m_1, \ldots, m_n$ de M et des éléments $a_1, \ldots, a_k$ de A tels que :*

1. *$m_1, \ldots, m_n$ soit une base de M,*
2. *$a_1 m_1, \ldots, a_k m_k$ soit une base de N,*
3. *a_i divise a_{i+1} dans A pour $i = 1, \ldots, k-1$.*

Corollaire 4.3.2 *Lorsque l'anneau A est principal, tout sous-A-module d'un A-module libre de rang n est un A-module libre de rang $k \leq n$.*

Proposition 4.3.3 (Théorème de structure) . *Si l'anneau A est principal, tout A-module de type fini M est isomorphe à une somme directe de A-modules monogènes* :

$$A^r \oplus A/(d_1) \oplus A/(d_2) \oplus \cdots \oplus A/(d_s)$$

où d_{i+1} divise d_i pour $i = 1, \ldots, s-1$. De plus, l'entier r et la suite des idéaux principaux (d_i) sont uniquement déterminés.

4.4 Correspondances

V espace vectoriel sur un corps K	M module sur un anneau com. A	G groupe abélien
(K-module) sous-espace vectoriel W esp. vect. quotient V/W ss-esp. vect. engendré dimension finie dimension 1 ($V \simeq K$)	(A-module) sous-module N module quotient M/N ss-module engendré type fini monogène ($M \simeq A/I$)	($\mathbb{Z}$-module) sous-groupe H groupe quotient G/H ss-gr. engendré type fini monogène ($G \simeq \mathbb{Z}/(d)$)
module libre =		
espace vectoriel qcq dimension n $\simeq K^n$ base = famille libre et géné. famille géné. de n elts famille libre de n elts	module libre rang n $\simeq A^n$ famille libre et géné. famille géné. de n elts —	groupe abélien libre rang n $\simeq \mathbb{Z}^n$ famille libre et géné. famille géné. de n elts —

Chapter 5

Discriminants

5.1 Norme et trace (rappels)

Soit L/K une extension algébrique de degré fini n.

Définition. Pour tout $x \in L$, on appelle *trace* (resp. *norme*) de x sur K et on note $Tr_{L/K}(x)$ (resp. $N_{L/K}(x)$) la trace (resp. le déterminant) de l'application K-linéaire

$$m_x : y \in L \mapsto xy \in L.$$

L'application *trace* :

$$Tr_{L/K} : x \in L \mapsto Tr_{L/K}(x) \in K$$

est une forme linéaire sur le K-espace vectoriel L.
L'application *norme* :

$$N_{L/K} : x \in L \mapsto N_{L/K}(x) \in K$$

induit un morphisme de groupes multiplicatifs de L^* sur K^*.

En d'autres termes, pour tous $x, y \in L$ et $a \in K$, on a :

$$Tr_{L/K}(x+y) = Tr_{L/K}(x) + Tr_{L/K}(y), \quad Tr_{L/K}(ax) = aTr_{L/K}(x),$$

$$N_{L/K}(xy) = N_{L/K}(x)N_{L/K}(y), \text{ et aussi, } N_{L/K}(ax) = a^n N_{L/K}(x).$$

En particulier, si $[L : K] = n$ et $a \in K$, alors

$$Tr_{L/K}(a) = na \text{ et } N_{L/K}(a) = a^n.$$

Cas particulier : $L = K[x]$.
Soit

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

le polynôme minimal de x sur K, on a alors :

$$Tr_{K[x]/K}(x) = -a_{n-1} \quad \text{et} \quad N_{K[x]/K}(x) = (-1)^n a_0.$$

5.2 Norme et trace (nouveau)

Proposition 5.2.1 *Soit L/K un extension algébrique et soit $x \in L$.*
— Si x est séparable sur K, alors

$$Tr_{K[x]/K}(x) = x_1 + x_2 + \ldots + x_n \ \text{ et } \ N_{K[x]/K}(x) = x_1x_2 \ldots x_n$$

où $x_1 = x$, $x_2, \ldots, x_n$ désignent les racines du polynôme minimal de x sur K (les conjugués de x sur K).

— Si x n'est pas séparable sur K, alors

$$Tr_{K[x]/K}(x) = 0.$$

Proposition 5.2.2 *Soient $K \subset L \subset M$ des extensions algébriques de degrés finis. Pour tout $x \in M$, on a* :

$$Tr_{M/K}(x) = Tr_{L/K}(Tr_{M/L}(x)) \quad \text{et} \quad N_{M/K}(x) = N_{L/K}(N_{M/L}(x)).$$

En particulier, pour $x \in L$, on a :

$$Tr_{M/K}(x) = [M : L] \times Tr_{L/K}(x) \quad \text{et} \quad N_{M/K}(x) = \big(N_{L/K}(x)\big)^{[M:L]}.$$

Corollaire 5.2.3 *Soient L/K une extension algébrique finie et x un élément de L.*
— Si x est séparable sur K, alors

$$Tr_{L/K}(x) = [L : K[x]] \sum_i x_i \ \text{ et } \ N_{L/K}(x) = (\prod_i x_i)^{[L:K[x]}.$$

où les x_i désignent les conjugués de x sur K.
— Si x n'est pas séparable sur K, alors

$$Tr_{L/K}(x) = 0.$$

Proposition 5.2.4 *Supposons L/K séparable finie et soit $\mathcal{M}(L/K)$ l'ensemble des K-morphismes de L (dans une clôture algébrique Ω de L). Pour tout $x \in L$, on a :*

$$Tr_{L/K}(x) = \sum_{\sigma \in \mathcal{M}(L/K)} \sigma(x) \quad \text{et} \quad N_{L/K}(x) = \prod_{\sigma \in \mathcal{M}(L/K)} \sigma(x).$$

Corollaire 5.2.5 *Si L/K est galoisienne de groupe de Galois G, alors pour tout $x \in L$, on a :*

$$Tr_{L/K}(x) = \sum_{\sigma \in G} \sigma(x) \quad \text{et} \quad N_{L/K}(x) = \prod_{\sigma \in G} \sigma(x).$$

Application : l'anneau des entiers d'un corps cyclotomique.

On appelle *corps cyclotomique* tout corps $\mathbb{Q}[\zeta_n]$ engendré sur $\mathbb{Q}$ par un racine de l'unité ζ. On se limite ici à un cas particulier :

Proposition 5.2.6 *Considérons le corps cyclotomique $\mathbb{Q}[\zeta_p]$ où p désigne un nombre premier impair et ζ_p une racine primitive p-ième de l'unité. L'anneau des entiers $A_{\mathbb{Q}[\zeta_p]}$ est $\mathbb{Z}[\zeta_p]$. C'est donc un $\mathbb{Z}$-module libre de rang $p-1 = [\mathbb{Q}[\zeta_p] : \mathbb{Q}]$ admettant $(1, \zeta_p, \ldots, \zeta_p^{p-2})$ pour base sur $\mathbb{Z}$.*

On peut montrer que, plus généralement, quel que soit l'entier $m \geq 3$, le corps cyclotomique $\mathbb{Q}[\zeta_m]$ où ζ_m désigne une racine primitive m-ième de l'unité a pour anneau d'entiers $\mathbb{Z}[\zeta_m]$. C'est donc un $\mathbb{Z}$-module libre dont le rang est égal à $\varphi(m) = [\mathbb{Q}(\zeta_m) : \mathbb{Q}]$.

5.3 Discriminant

On suppose toujours que L/K est une extension algébrique finie de degré n.

Définition. L'application

$$(x, y) \in L \times L \mapsto Tr_{L/K}(xy) \in K$$

est une forme bilinéaire symétrique sur L. Le déterminant de la matrice de cette forme bilinéaire relativement à une base $(x_1, \ldots, x_n)$ de L sur K est appelé *discrimant* de la base $(x_1, \ldots, x_n)$:

$$D(x_1, \ldots, x_n) = \det(Tr_{L/K}(x_i x_j)).$$

Remarque. Si $(y_1, \ldots, y_n)$ est une autre base de L sur K et si on désigne par $A = (a_{i,j}) \in \mathcal{M}_n(K)$ la matrice de changement de base $(y_j = \sum_i a_{i,j} x_i)$, alors

$$D(y_1, \ldots, y_n) = (\det(A))^2 \times D(x_1, \ldots, x_n).$$

Proposition 5.3.1 *Si L/K est une extension séparable finie, alors la forme bilinéaire $(x, y) \in L \times L \mapsto Tr_{L/K}(xy) \in K$ est non dégénérée.*

Preuve par l'exemple. Soit $L = K[x]$ où x est séparable sur K. Soit F le polynôme minimal de x sur K et soit n son degré. Alors,

$$D(1, x, \ldots, x^{n-1}) = (-1)^{\frac{n(n-1)}{2}} N_{K[x]/K}(F'(x)) = \prod_{1 \leq i < j \leq n} (x_i - x_j)^2$$

où les x_i désignent les conjugués de x sur K.
Il s'agit du discriminant du polynôme F :

$$\Delta(F) = (-1)^{\frac{n(n-1)}{2}} Res(F, F').$$

Chapter 6

Anneaux d'entiers de corps de nombres

6.1 L'anneau des entiers d'un corps de nombres

Dfinitions. 1. On appelle *corps de nombres* toute extension algébrique finie de $\mathbb{Q}$.
2. On appelle *anneau des entiers* du corps de nombres K l'anneau A_K fermeture intégrale de $\mathbb{Z}$ dans K.

L'anneau A_K est donc formé des éléments x de K entiers sur $\mathbb{Z}$ (ceux pour lesquels il existe un polynôme unitaire $Q \in \mathbb{Z}[X]$ tel que $Q(x) = 0$ ou, de façon équivalente, ceux dont le polynôme minimal sur $\mathbb{Q}$ est à coefficients dans $\mathbb{Z}$).

Remarque. Soit K un corps de nombres.
1- Pour tout $x \in K$, il existe $k \in \mathbb{N}^*$ tel que kx appartienne à A_K.
2- Pour tout $x \in A_K$, les conjugués de x sur $\mathbb{Q}$ sont entiers sur $\mathbb{Z}$ et, par suite, $Tr_{K/\mathbb{Q}}(x)$ et $N_{K/\mathbb{Q}}(x)$ sont des entiers.

Proposition 6.1.1 *Pour tout corps de nombres K, le $\mathbb{Z}$-module A_K est libre de rang $n = [K : \mathbb{Q}]$.*

Corollaire 6.1.2 *Pour tout corps de nombres K, l'anneau des entiers A_K est noethérien (c.-à-d., tout idéal de A_K est de type fini).*

Définition. Les discriminants de toutes les bases du $\mathbb{Z}$-module A_K sont égaux entre eux. Cette valeur commune d_K est appelée *discriminant absolu* ou simplement *discriminant* du corps de nombres K.

Remarque. Soient $x_1, \ldots, x_n \in A_K$ tels que $(x_1, \ldots, x_n)$ soit une base de $K/\mathbb{Q}$: $(x_1, \ldots, x_n)$ est une base de $\mathbb{Z}$-module A_K si et seulement si $D(x_1, \ldots, x_n) = d_K$.

Proposition 6.1.3 *Soit $d \in \mathbb{Z}$ sans "facteurs carrés".*

1. *Si $d \equiv 2$ ou $3 \pmod 4$, alors $d_{\mathbb{Q}[\sqrt{d}]} = 4d$.*
2. *Si $d \equiv 1 \pmod 4$, alors $d_{\mathbb{Q}[\sqrt{d}]} = d$.*

Proposition 6.1.4 *Soit p un nombre premier impair et ζ_p une racine primitive p-ième de l'unité. Alors*

$$d_{\mathbb{Q}[\zeta_p]} = \pm p^{p-2}.$$

Proposition 6.1.5 *Soient K un corps de nombres et A_K son anneau d'entiers. Pour tout idéal premier non nul $\mathfrak{p}$ de A_K, on a :*

1. *$\mathfrak{p} \cap \mathbb{Z} = p\mathbb{Z}$ où p est un nombre premier,*
2. *$A_K/\mathfrak{p}$ est un $\mathbb{Z}/p\mathbb{Z}$-espace vectoriel de dimension finie,*
3. *$\mathfrak{p}$ est maximal et le quotient $A_K/\mathfrak{p}$ est un corps fini.*

6.2 Anneaux de Dedekind

Définition. Un *anneau de Dedekind* est un anneau noethérien intégralement clos dont tous les idéaux premiers non nuls sont maximaux.

Exemples. 0. Un corps est un anneau de Dedekind. (On conviendra généralement d'exclure ce cas.)
1. Un anneau principal est un anneau de Dedekind.
2. $\mathbb{Z}[i\sqrt{5}]$ est un anneau de Dedekind non factoriel.
3. Un anneau est à la fois de Dedekind et factoriel si, et seulement si, il est principal.

Théorème 6.2.1 *Les anneaux d'entiers de corps de nombres sont des anneaux de Dedekind.*

Proposition 6.2.2 *Un anneau de fractions d'un anneau de Dedekind est un anneau de Dedekind.*

Dans un anneau de Dedekind, la factorisation unique des éléments n'a pas toujours lieu (par exemple dans $\mathbb{Z}[i\sqrt{5}]$), en revanche, il y a une factorisation unique des idéaux :

Théorème 6.2.3 *Soit A un anneau de Dedekind. Tout idéal non nul $\mathfrak{I}$ de A s'écrit d'une façon et d'une seule (à l'ordre près) comme produit fini d'idéaux maximaux :*

$$\mathfrak{I} = \prod_{\mathfrak{m} \in \max(A)} m^{v_{\mathfrak{m}}(\mathfrak{I})} \quad \text{avec } v_{\mathfrak{m}}(\mathfrak{I}) \in \mathbb{N}.$$

La preuve de ce théorème utilise notamment les lemmes suivants :

Lemme 1. Dans un anneau quelconque, si un idéal premier contient un produit fini d'idéaux, alors il contient l'un d'eux.

Lemme 2. Dans un anneau noethérien intègre, tout idéal non nul contient un produit fini d'idéaux premiers non nuls.

Lemme 3. Soit A un anneau de Dedekind et soit x un élément du corps des fractions K de A. S'il existe un idéal non nul $\mathfrak{a}$ de A tel que $x\mathfrak{a} \subset \mathfrak{a}$, alors x appartient à A.

Lemme 4. Soit A un anneau de Dedekind distinct de son corps des fractions K. Pour tout idéal maximal $\mathfrak{m}$ de A, posons $(A : \mathfrak{m}) = \{x \in K \mid x\mathfrak{m} \subset A\}$. Alors

$$\mathfrak{m}.(A : \mathfrak{m}) = \left\{ \sum_k m_k n_k \mid m_k \in \mathfrak{m}, n_k \in (A : \mathfrak{m}) \right\} = A.$$

Formulaire. Soit A un anneau de Dedekind. Soient $\mathfrak{a}$ et $\mathfrak{b}$ deux idéaux non nuls de A. Notons $v_{\mathfrak{m}}(\mathfrak{a})$ l'exposant de $\mathfrak{m}$ dans la décomposition de $\mathfrak{a}$. On a :

$$\mathfrak{a} \subset \mathfrak{b} \Leftrightarrow v_{\mathfrak{m}}(\mathfrak{a}) \geq v_{\mathfrak{m}}(\mathfrak{b}) \ \forall \mathfrak{m} \in \max(A)$$

$$v_{\mathfrak{m}}(\mathfrak{ab}) = v_{\mathfrak{m}}(\mathfrak{a}) + v_{\mathfrak{m}}(\mathfrak{b})$$

$$v_{\mathfrak{m}}(\mathfrak{a} + \mathfrak{b}) = \inf\left(v_{\mathfrak{m}}(\mathfrak{a}), v_{\mathfrak{m}}(\mathfrak{b})\right)$$

$$v_{\mathfrak{m}}(\mathfrak{a} \cap \mathfrak{b}) = \sup\left(v_{\mathfrak{m}}(\mathfrak{a}), v_{\mathfrak{m}}(\mathfrak{b})\right).$$

Exemple. Dans l'anneau $\mathbb{Z}[i\sqrt{5}]$:
— les éléments 3, 7, $1 + 2i\sqrt{5}$, $1 - 2i\sqrt{5}$ sont irréductibles,
— les idéaux $\mathfrak{p}_3 = (3, 1 + 2i\sqrt{5})$, $\mathfrak{q}_3 = (3, 1 - 2i\sqrt{5})$, $\mathfrak{p}_7 = (7, 1 + 2i\sqrt{5})$, $\mathfrak{q}_7 = (7, 1 - 2i\sqrt{5})$ sont premiers.
On a les factorisations :

$$21 = 3 \times 7 = (1 + 2i\sqrt{5})(1 - 2i\sqrt{5})$$

et les décompositions uniques

$$(3) = \mathfrak{p}_3\mathfrak{q}_3 \ , \ (7) = \mathfrak{p}_7\mathfrak{q}_7 \ , \ \mathfrak{p}_3\mathfrak{p}_7 = (1 + 2i\sqrt{5}) \ , \ \mathfrak{q}_3\mathfrak{q}_7 = (1 - 2i\sqrt{5}) \ ,$$

$$\mathfrak{p}_3\mathfrak{q}_7 = (4 - i\sqrt{5}) \ , \ \mathfrak{q}_3\mathfrak{p}_7 = (4 + i\sqrt{5}) \ , \ (21) = \mathfrak{p}_3\mathfrak{q}_3\mathfrak{p}_7\mathfrak{q}_7.$$

6.3 Anneaux noethériens (rappels et compléments)

Définition. Un *anneau noethérien* est un anneau dont tous les idéaux sont de type fini.

Exemples.
1- Tout anneau principal est noethérien.
2- Un quotient d'un anneau noethérien est noethérien.
3- Un anneau de fractions d'un anneau noethérien est noethérien.
4- Un anneau de polynômes (à un nombre fini d'indéterminées) à coefficients dans un anneau noethérien est noethérien.

Proposition 6.3.1 *Soit A un anneau noethérien. Alors, toute suite croissante d'idéaux de A est stationnaire.*

Corollaire 6.3.2 *Soit A un anneau noethérien. Alors, tout famille non vide d'idéaux de A possède au moins un élément maximal relativement à la relation d'inclusion.*

C'est une conséquence immédiate de l'énoncé suivant :

Proposition 6.3.3 *Soit E un ensemble ordonné. Les assertions suivantes sont équivalentes :*
1. Toute suite croissante d'éléments de E est stationnaire.
2. Toute partie non vide de E possède un élément maximal.

Cette assertion utilise l'

Axiome du choix.

$$\forall E \quad \exists \tau : X \in \mathcal{P}(E) \setminus \{\emptyset\} \mapsto \tau(X) \in E \text{ tel que } \tau(X) \in X.$$

Une telle fonction τ s'appelle *fonction de choix* sur l'ensemble E.

L'axiome du choix est équivalent à la proposition bien connue suivante :

Proposition 6.3.4 *Soient X et Y deux ensembles. Pour qu'une application $f : X \to Y$ soit surjective il faut et il suffit qu'il existe une application $g : Y \to X$ telle que $f \circ g = id_Y$.*

Chapter 7

Groupes des unités et décomposition des nombres premiers dans les corps de nombres

Dans tout ce chapitre K désigne un corps de nombres et A_K l'anneau des entiers de K.

7.1 Groupe des unités

Définition. On appelle *unités* d'un corps de nombres K les unités, c.-à-d., les éléments inversibles de l'anneau des entiers A_K.

Le groupe des unités de K est noté U_K au lieu de $U(A_K)$ ou $A_K^\times$.

Proposition 7.1.1 *Pour qu'un élément x d'un corps de nombres K soit une unité il faut et il suffit que x soit un entier de K et que $N_{K/\mathbb{Q}}(x) = \pm 1$.*

Notations. Soit K un corps de nombres de degré n. Soient $\sigma_1, \ldots, \sigma_n$ les $\mathbb{Q}$-morphimes de K dans $\mathbb{C}$. Notons r_1 le nombre de σ_i tels que $\sigma_i(K) \subset \mathbb{R}$ et $2r_2$ le nombre de σ_i tels que $\sigma_i(K) \not\subset \mathbb{R}$. On a $r_1 + 2r_2 = n$. Posons

$$r_K = r_1 + r_2 - 1.$$

Proposition 7.1.2 (Le théorème des unités de Dirichlet) *Soient K un corps de nombres, $r_K = r_1 + r_2 - 1$ l'entier défini ci-dessus et G_K le groupe cyclique*

formé des racines de l'unité contenues dans K. Alors

$$U_K \simeq \mathbb{Z}^{r_K} \times G_K.$$

Lemme 7.1.3 *Tout sous-groupe discret non nul H de $\mathbb{R}^n$ est un groupe abélien libre de rang $r \leq n$.*

Définition. On appelle *système d'unités fondamentales* d'un corps de nombres K tout ensemble de $r = r_K$ unités $u_1, \ldots, u_r$ telle que toute unité u de K s'écrive d'une façon et d'une seule sous la forme

$$u = z u_1^{n_1} \cdots u_r^{n_r}$$

avec $n_i \in \mathbb{Z}$ et z racine de l'unité dans K.

Unités des corps quadratiques

Proposition 7.1.4 Unités des corps quadratiques imaginaires
Soit $d \in \mathbb{N}^*$ sans facteurs carrés et soit $K = \mathbb{Q}[\sqrt{-d}]$.
Le groupe des unités de K est $\{\pm 1\}$ sauf pour $d = 1$ et $d = 3$:

1. *Si $K = \mathbb{Q}[i]$, alors*
$$U_K = \{\pm 1, \pm i\}.$$
2. *Si $K = \mathbb{Q}[i\sqrt{3}]$, alors*
$$U_K = \left\{ \left(\frac{1 + i\sqrt{3}}{2} \right)^k \mid 0 \leq k \leq 5 \right\}.$$

Proposition 7.1.5 Unités des corps quadratiques réels
Soit d un entier sans facteurs carrés ≥ 2 et soit $K = \mathbb{Q}[\sqrt{d}]$. Alors

$$U_K \simeq \{\pm 1\} \times \mathbb{Z}.$$

7.2 Décomposition d'un nombre premier

Proposition 7.2.1 *Soit K un corps de nombres et soit p un nombre premier. Alors il existe un entier $g \geq 1$, des idéaux maximaux $\mathfrak{m}_1, \ldots, \mathfrak{m}_g$ de A_K et des entiers $e_1, \ldots, e_g \geq 1$ tels que*

$$pA_K = \prod_{i=1}^{g} \mathfrak{m}_i^{e_i}.$$

Les idéaux $\mathfrak{m}_i$ sont les idéaux maximaux $\mathfrak{m}$ de A_K au-dessus de p, c'est-à-dire, tels que $\mathfrak{m} \cap \mathbb{Z} = p\mathbb{Z}$.

Définitions. L'exposant e_i est appelé l'*indice de ramification* de $\mathfrak{m}_i$ et, la dimension

$$f_i = [A_K/\mathfrak{m}_i : \mathbb{F}_p]$$

du $\mathbb{F}_p$-espace vectoriel $A_K/\mathfrak{m}_i$ est appelée le *degré résiduel* de $\mathfrak{m}_i$.
On pose parfois $e_i = e(\mathfrak{m}_i/p)$ et $f_i = f(\mathfrak{m}_i/p)$.

Proposition 7.2.2 *Avec les notations précédentes, A_K/pA_K est aussi un $\mathbb{F}_p$-espace vectoriel et on a :*

$$\sum_{i=1}^{q} e_i f_i = \dim_{\mathbb{F}_p}(A_K/pA_K) = [K : \mathbb{Q}].$$

Définitions. Soient p un nombre premier et $\mathfrak{m}$ un idéal maximal de A_K au-dessus de p.
1- On dit que $\mathfrak{m}$ est *ramifié* dans l'extension $K/\mathbb{Q}$ si $e(\mathfrak{m}/p) \neq 1$.
2- On dit que p est *ramifié* dans l'extension $K/\mathbb{Q}$ si l'un des idéaux maximaux $\mathfrak{m}$ de A_K au-dessus de p est ramifié (l'un des $e_i = e(\mathfrak{m}_i, p)$ est ≥ 2).
3- On dit que p est *totalement ramifié* dans l'extension $K/\mathbb{Q}$ lorsque $e_1 = n$.
4- On dit que p est *totalement décomposé* dans l'extension $K/\mathbb{Q}$ lorsque $g = n$.

Proposition 7.2.3 *Pour qu'un nombre premier p se ramifie dans l'extension $K/\mathbb{Q}$ il faut et il suffit qu'il divise le discriminant d_K.*

7.3 Cas particuliers

Proposition 7.3.1 Cas d'un corps cyclotomique. *Soient p un nombre premier et ζ une racine primitive p-ième de l'unité. Posons*

$$A = A_{\mathbb{Q}[\zeta]} \quad \text{et} \quad \mathfrak{m} = A(\zeta - 1).$$

Alors

$$pA = \mathfrak{m}^{p-1}A \quad \text{et} \quad A/\mathfrak{m} \simeq \mathbb{Z}/p\mathbb{Z}.$$

Proposition 7.3.2 Cas d'un corps quadratique. *Soit d un entier sans facteurs carrés et soit $A = A_{\mathbb{Q}[\sqrt{d}]}$. Soit p un nombre premier. Alors*

1. *$pA = \mathfrak{m}_1\mathfrak{m}_2 \Leftrightarrow p \neq 2$ et $\overline{d}$ carré dans $\mathbb{Z}/p\mathbb{Z}$ ou $p = 2$ si $d \equiv 1 \pmod 8$.*
2. *$pA = \mathfrak{m} \Leftrightarrow p \neq 2$ et $\overline{d}$ non carré dans $\mathbb{Z}/p\mathbb{Z}$ ou $p = 2$ si $d \equiv 5 \pmod 8$.*
3. *$pA = \mathfrak{m}^2 \Leftrightarrow p \neq 2$ et $p|d$ ou $p = 2$ si $d \equiv 2, 3 \pmod 4$.*

Plus généralement,

Proposition 7.3.3 *Supposons qu'il existe $\alpha \in A_K$ tel que $A_K = \mathbb{Z}[\alpha]$ et soit $f(X)$ le polynôme minimal de α sur $\mathbb{Q}$. Fixons un nombre premier p. Considérons l'image canonique $\overline{f}$ de f dans $\mathbb{F}_p[X]$ et sa décomposition*

$$\overline{f}(X) = \prod_{i=1}^{g} g_i(X)^{e_i}$$

où les g_i sont des polynômes unitaires et irréductibles. Notons $f_i(X)$ des polynômes unitaires relevant les $g_i(X)$ dans $\mathbb{Z}[X]$. Alors, les $\mathfrak{m}_i = (p, f_i(\alpha))$ sont les idéaux maximaux de A_K au-dessus de p,

$$pA_K = \prod_{i=1}^{g} \mathfrak{m}_i^{e_i}$$

est la factorisation de pA_K en produit de puissances d'idéaux maximaux et

$$[A_K/\mathfrak{m}_i : \mathbb{F}_p] = \deg(f_i).$$

Remarque. Avec les hypothèses précédentes, si p ne divise pas le discriminant de d_K, alors les exposants e_i sont tous égaux à 1 (p est non ramifié dans l'extension).

7.4 Extensions galoisiennes

Proposition 7.4.1 *Supposons l'extension $K/\mathbb{Q}$ est galoisienne de groupe de Galois $G = G(K/\mathbb{Q})$. Alors*

1. *L'anneau A_K est stable par G, c.-à-d., pour tout $\sigma \in G$, $\sigma(A) = A$.*

2. *Le groupe G opère transitivement sur l'ensemble des idéaux maximaux $\mathfrak{m}$ de A_K au-dessus d'un même nombre premier p, autrement dit, si $\mathfrak{m}$ et $\mathfrak{m}'$ sont au-dessus de p alors il existe $\sigma \in G$ tel que $\sigma(\mathfrak{m}) = \mathfrak{m}'$.*

3. *Pour un même nombre premier p, les g idéaux maximaux $\mathfrak{m}_i$ au-dessus de p ont le même indice de ramification e et le même degré résiduel f. Par suite :*

$$pA_K = \left(\prod_{i=1}^{g} \mathfrak{m}_i\right)^{e} \quad \text{et} \quad [K : \mathbb{Q}] = efg.$$

Cas des corps cyclotomiques

Proposition 7.4.2 *Soient p un nombre premier, $r \in \mathbb{N}^*$, ζ_{p^r} une racine primitive p^r-ième de l'unité et $K = \mathbb{Q}[\zeta_{p^r}]$. Alors,*

1. *l'anneau des entiers de K est $\mathbb{Z}[\zeta_{p^r}]$,*
2. *$|d_K| = p^s$ où $s = p^{r-1}(rp - r - 1)$,*
3. *$pA_K = (1 - \zeta_{p^r})^{\varphi(p^r)}$ (p est totalement décomposé.)*

Proposition 7.4.3 *Soient $m \geq 3$, ζ_m une racine primitive m-ième de l'unité et $K = \mathbb{Q}[\zeta_m]$. Soit p un nombre premier et e_p, f_p, g_p les entiers que l'on sait correspondant. Posons $m = m_0 p^r$ où $p \not| m_0$. Alors*

1. *$e_p = \varphi(p^r)$,*
2. *f_p est le plus petit entier > 0 tel que $p^{f_p} \equiv 1 \pmod{m_0}$,*
3. *$g_p = \frac{n}{e_p f_p}$.*

Ainsi,

$$pA_K = (\mathfrak{m}_1 \cdots \mathfrak{m}_g)^{\varphi(p^r)} \quad \text{avec} \quad [A_K/\mathfrak{m}_i : \mathbb{F}_p] = f_p \quad \text{pour } i = 1, \ldots, g.$$

Corollaire 7.4.4 *Le nombre premier p est totalement décomposé dans l'extension $\mathbb{K}[\zeta_m/\mathbb{Q}]$ si et seulement si $p \equiv 1 \pmod{m}$.*

Contents