Théorie de Galois

I. El Hage

2001

Table des matières

Remerciements

Mes remerciements vont à mon collègue A. Sahili qui a bien voulu relire ce cours.

Mes remerciements iront aussi à toute personne désireuse de formuler des remarques et/ou des corrections. Ces remarques et corrections seront les biens venues. Veuillez les adresser à l'adresse suivante :

ihage@ul.edu.lb

Chapitre 1

Corps des racines

1.1 Introduction

Tous les corps considérés dans ce cours seront des corps commutatifs. Soit K un tel corps.

Définition On dit qu'un corps E est une **extension** du corps K si, et seulement si, K est un sous-corps de E.

Exemple $\mathbb{C}$ est une extension de $\mathbb{R}$ et de $\mathbb{Q}$.

Exemple $\mathbb{R}$ est une extension de $\mathbb{Q}\left(\sqrt{2}\right)$.

Exemple $\mathbb{Q}\left(\sqrt{2}\right)$ est une extension de $\mathbb{Q}$.

Exemple Le corps $K(X)$ des fractions rationnelles à une indeterminée sur le corps K est une extension de K.

Définition On appelle **équation polynomiale** sur K toute équation de la forme $P(x)=0$, où P est polynôme appartenant à $K[X]$.

Le **degré** de cette équation est le degré du polynôme. Les **solutions** de cette équation $P(x)=0$ sont les racines du polynôme P dans une extension E de K.

Exemple Une équation de degré 1 est de la forme $ax+b=0$ où $a\in K^*$ et $b\in K$.

Exemple Une équation de degré 2 est de la forme $ax^2+bx+c=0$ où $a\in K^*$, $b\in K$ et $c\in K$.

Le but de ce cours est de répondre aux deux questions suivantes :

Question 1 : Ayant une équation polynomiale de degré n sur un corps K, est-il possible de trouver une extension E de K, dans laquelle, l'équation possède une solution ?

Question 2 : Dans le cas où l'équation polynomiale $P(x) = 0$ possède une solution dans une extension E de K, sous quelles conditions cette solution s'exprime-elle, à partir des coefficients de P, à l'aide des quatre opérations et des radicaux ?

1.2 Corps des racines

Soit K un corps.

Définition une extension E de K est un **corps de rupture** pour le polynôme $f(X) \in K[X]$ sur K si, et seulement si, E contient une racine de f.

Exemple $\mathbb{R}$ est un corps de rupture pour $X^3 - 2$ sur $\mathbb{Q}$.

Théorème Si $f(X)$ est un polynôme irréductible dans $K[X]$, alors f possède un corps de rupture sur K.

Démonstration Soit M l'idéal de $K[X]$ engendré par le polynôme f. M est un idéal maximal car $K[X]$ est un anneau principal et f est irréductible. Si E désigne l'anneau quotient $K[X]/M$, alors E est un corps. On peut regarder K comme un sous-corps de E. Pour voir ça, soit $p; K[X] \longrightarrow K[X]/M$ la surjection canonique. La restriction q de p à K est un homomorphisme non nul car $p(1) = \overline{1}$. Il en résulte que cet homomorphisme est injectif car son anneau de départ est un corps. On en déduit que K est isomorphe à $q(K)$, ce qui permet d'identifier K et $q(K)$. Ainsi E devient une extension de K. Soit $\alpha = \overline{X} = p(X)$. En écrivant

$$f(X) = a_0 + a_1 X + \cdots + a_n X^n$$

nous obtenons

$$\begin{aligned} f(\alpha) &= a_0 + a_1\alpha + \cdots + a_n\alpha^n \\ &= q(a_0) + q(a_1)\, p(X) + \cdots + q(a_n)\,(p(X))^n \\ &= p(a_0) + p(a_1)\, p(X) + \cdots + p(a_n)\,(p(X))^n \\ &= p(a_0 + a_1 X + \cdots + a_n X^n) \\ &= p(f) \\ &= \overline{0} \end{aligned}$$

Donc E est une extension de K contenant la racine α de f.

Corollaire Tout polynôme $f(X) \in K[X]$ possède un corps de rupture sur K.

Démonstration En effet, tout polynôme $f \in K[X]$ se décompose en produit de polynômes irréductibles.

Définition Une extension E de K est un **corps de décomposition** pour f sur K si, et seulement si, f peut être scindé dans $E[X]$ c.d. il peut être décomposé en produit de polynômes linéaires dans $E[X]$.

Exemple Le corps $\mathbb{C}$ est un corps de décomposition sur $\mathbb{R}$ pour le polynôme X^2+1.

Exemple Le corps $\mathbb{Q}$ est un corps de décomposition sur $\mathbb{Q}$ pour le polynôme X^2-1.

Théorème Tout polynôme $f \in K[X]$ possède un corps de décomposi-tion sur K.

Démonstration On procède par récurrence sur le degré n de f. Si $n=1$, alors K est un corps de décomposition pour f sur K. Supposons le théorème vrai pour tout polynôme de degré plus petit que n et démontrons-le pour les polynômes de degré n. D'après le corollaire précédent, il existe une extension E de K contenant une racine a de f. Le polynôme $X-a$ divise $f(X)$ dans $E[X]$. Nous avons $f(X) = (X-a)\,g(X)$ dans $E[X]$, avec $\deg(g) = n-1$. L'hypothèse de récurrence nous permet de trouver un corps de décomposition F pour $g(X)$ sur E. On a $g(X) = k\prod_{i=2}^{i=n}(X-a_i)$ dans $F[X]$ et

$$f(X) = (X-a)\,g(X) = (X-a)\,k\prod_{i=2}^{i=n}(X-a_i) = k\prod_{i=1}^{i=n}(X-a_i)$$

dans $F[X]$ où $a_1 = a$. Ainsi, F est un corps de décomposition pour f sur K.

Définition Un corps de décomposition minimal pour f sur K est appelé un **corps des racines** pour f sur K.

Exemple $\mathbb{C}$ est un corps des racines sur $\mathbb{R}$ pour le polynôme X^2+1.

Exemple $\mathbb{Q}\left(\sqrt{2}\right)$ est un corps de décomposition sur $\mathbb{Q}$ pour le polynôme X^2-2.

1.3 Adjonction

Définition Soit A est une partie d'une extension E de K. Le sous-corps de E engendré par $K\cup A$ est appelé le **corps engendré par A sur K** ou le corps obtenu par l'**adjonction** de A à K. On dira alors que A est un **système de générateurs** de $K(A)$ sur K.

Notation Le corps engendré par A sur K sera désigné par $K(A)$. Si A est fini et si $a_1,\ldots,a_n$ sont ses éléments, alors nous écrirons $K(a_1,\ldots,a_n)$ à la place de $K(A)$.

Exemple Si $A=\emptyset$, alors $K(A)=K$.

Exemple $\mathbb{C}=\mathbb{R}(i)$.

Remarque Une extension E de K peut avoir plusieurs système de générateurs sur K : ainsi $\mathbb{R}(i)=\mathbb{C}=\mathbb{R}(1+i)$.

Théorème Si A et B sont deux parties d'une extension E de K, alors $K(A\cup B)=K(A)(B)$.

Démonstration Tout sous-corps de E qui contient K,A et B contient $K(A)$ et B. Réciproquement, tout sous-corps de de E qui contient $K(A)$ et B contient K,A et B.Il en résulte que la famille de tous les sous-corps de E contenant K, A et B est égale à celle de tous les sous-corps de E qui contiennent $K(A)$ et B. Ceci prouve que $K(A\cup B)$, qui est le plus petit élément de la première famille, est égal à $K(A)(B)$, qui est le plus petit élément de la seconde.

Corollaire $K(a_1,\ldots,a_n)=K(a_1,\ldots,a_{n-1})(a_n)$.

Théorème Tout polynôme $f\in K[X]$, possède un corps des racines sur K.

Démonstration Soit E un corps de décomposition pour f sur K. Ce polynôme s'écrit sous la forme

$$f(X)=k\prod_{i=1}^{i=n}(X-a_i)$$

dans $E[X]$. Soit $S = K(a_1,...,a_n)$. Il est facile de voir que S est un corps de décomposition pour f sur K. Ce corps de décomposition est minimal car, si R est un corps de décomposition pour f sur K contenu dans S, alors f s'écrit

$$f(X) = k' \prod_{i=1}^{i=n} (X - b_i)$$

dans $R[X]$. Mais $R[X] \subseteq S[X]$. Il en résulte que f s'écrit de deux manières comme produit de polynômes linéaires qui sont irréductibles. L'unicité d'une telle décomposition implique $k = k'$ et $\{a_1,...,a_n\} = \{b_1,...,b_n\}$. D'où

$$R \subseteq S = K(a_1,...,a_n) = K(b_1,...,b_n) \subseteq R$$

ce qui prouve $R = S$. S est un corps des racines pour f sur K.

Théorème Si E est un corps de décomposition sur K pour le polynôme $f(X) \in K[X]$, alors E contient un corps de racines unique pour f sur K.

Démonstration Si

$$f(X) = k \prod_{i=1}^{i=n} (X - a_i) \in E[X]$$

est la décomposition de f comme produit de facteurs linéaires dans $E[X]$, alors $a_1,a_2,...,a_n$ sont les racines de f dans E et $R = K(a_1,a_2,...,a_n)$ est un corps de racines pour f sur K comme nous l'avons vu. Si T est un autre corps de racines pour f sur K, alors f s'écrit

$$f(X) = k' \prod_{i=1}^{i=n} (X - b_i) \in T[X]$$

Il en résulte

$$f(X) = k \prod_{i=1}^{i=n} (X - a_i) = k' \prod_{i=1}^{i=n} (X - b_i) \in E[X]$$

L'unicité d'une telle décomposition implique $k = k'$ et

$$\{a_1,...,a_n\} = \{b_1,...,b_n\}$$

. Ainsi $R \subseteq T$ et $R = T$ car T est un corps de décomposition minimal pour f sur K.

1.4 Degré d'une extension

Soit E une extension de K. E peut être muni d'une structure de K-espace vectoriel en définissant la multiplication par un scalaire par

$$(\alpha,x) \mapsto \alpha x$$

Définition On appelle **degré** de l'extension E, la dimension de E en tant que K-espace vectoriel. Ce degré sera noté $[E:K]$.

Exemple $[\mathbb{C}:\mathbb{R}]=2$, $\left[\mathbb{Q}\left(\sqrt{2}\right):\mathbb{Q}\right]=2$, $[\mathbb{R}:\mathbb{Q}]$ est infini.

Exemple $[K:K]=1$.

Une extension E de K sera dite **finie** si, et seulement si, $[E:K]$ est fini. Elle sera dite **infinie** dans le cas contraire.

Théorème Si E est une extension de K et L est un corps intermédiaire entre K et L, alors

$$[E:K]=[E:L]\,[L:K].$$

Démonstration Soit $(x_i)_{i\in I}$ une base du L-espace vectoriel E et $\left(y_j\right)_{j\in J}$ une base du K-espace vectoriel L. Nous allons prouver que $\left(x_iy_j\right)_{(i,j)\in I\times J}$ est une base du K-espace vectoriel E.

C'est un système de générateurs : tout $x\in E$ s'écrit $x=\sum\limits_{i\in I}a_ix_i$ où $a_i\in L$ pour tout $i\in I$. Or tout a_i peut s'écrire $a_i=\sum\limits_{j\in J}b_{ij}y_j$. Nous obtenons

$$x=\sum_{i\in I}a_ix_i=\sum_{i\in I}\left(\sum_{j\in J}b_{ij}y_j\right)x_i=\sum_{(i,j)\in I\times J}b_{ij}x_iy_j$$

C'est un système libre : Si $\sum\limits_{(i,j)\in I\times J}b_{ij}x_iy_j=0$ alors

$$\sum_{i\in I}\left(\sum_{j\in J}b_{ij}y_j\right)x_i=0$$

ce qui implique $\sum\limits_{j\in J}b_{ij}y_j=0$ pour tout $i\in I$ car $(x_i)_{i\in I}$ est une base du L-espace vectoriel E. Mais $\left(y_j\right)_{j\in J}$ est une base du K-espace vectoriel L, d'où $b_{ij}=0$ pour tout $(i,j)\in I\times J$.

La famille $\left(x_i y_j\right)_{(i,j)\in I\times J}$ étant une base du K-espace vectoriel E, nous avons

$$\begin{aligned}[E:K] &= \dim_K(E) = Card(I\times J) = Card(I)\times Card(J)\\ &= \dim_L(E)\times\dim_K(L) = [E:L][L:K].\end{aligned}$$

Corollaire Si $K = E_0 \subseteq E_1 \subseteq .... \subseteq E_n = E$ alors

$$[E:K] = [E_n : E_0] = \prod_{i=1}^{i=n} [E_i : E_{i-1}]$$

Démonstration Par une simple récurrence.

Chapitre 2

Extensions simples

2.1 Extensions simples

Définition Une extension E de K est **simple** si, et seulement si, il existe $a \in E$ tel que $E = K(a)$.

Exemple $\mathbb{C} = \mathbb{R}(i)$ est une extension simple de $\mathbb{R}$, $K(X)$ est une extension simple de K.

L'importance des extensions simples provient du fait que leurs structures peuvent être parfaitement déterminées d'une part et que la majorité des extensions que nous allons rencontrer sont en réalité des extensions simples. Nous allons déterminer la structure d'une extension simple.

Théorème Soit $E = K(a)$ une extension de K. Il existe un homomorphisme d'anneaux et un seul

$$\sigma; K[X] \longrightarrow E$$

qui vérifie $\sigma(X) = a$ et $\sigma(k) = k$ pour tout $k \in K$.

Démonstration Soit $\sigma; K[X] \longrightarrow E$ l'application définie par $\sigma(P) = P(a)$ pour tout $P \in K[X]$. Il est facile de vérifier que σ satisfait les conditions du théorème. Il nous reste à prouver l'unicité de σ. Si τ est une autre solution, alors nous avons pour tout $P = \sum_{i=0}^{i=n} b_i X^i$ dans $K[X]$

$$\tau(P) = \tau\left(\sum_{i=0}^{i=n} b_i X^i\right) = \sum_{i=0}^{i=n} \tau(b_i)\,\tau(X)^i = \sum_{i=0}^{i=n} b_i a^i = P(a) = \sigma(P)$$

D'où $\tau = \sigma$.

Notation Le sous-anneau de E engendré par $K\cup\{a\}$ sera noté $K[a]$ alors que $K(a)$ désigne le sous-corps de E engendré $K\cup\{a\}$.

Théorème $\mathrm{Im}(\sigma)$ est le sous-anneau $K[a]$ de E engendré par $K\cup\{a\}$.

Démonstration $\mathrm{Im}(\sigma)$ est un sous-anneau de E. Il contient $K=\sigma(K)$ et $a=\sigma(X)$. Si L est un sous-anneau de E contenant $K\cup\{a\}$ alors $\mathrm{Im}(\sigma)\subseteq L$ car tout élément c de $\mathrm{Im}(\sigma)$ s'écrit $c=P(a)=\sum_{i=0}^{i=n} b_i a^i\in L$.

Considérons le noyau de σ. C'est un idéal de $K[X]$. Deux cas sont possibles : $Ker(\sigma)=(0)$ ou $Ker(\sigma)\neq(0)$. Dans le premier cas, l'élément a de E sera dit **transcendant** sur K, et dans le second, a sera dit **algébrique** sur K.

Exemple $\sqrt{2}$ est algébrique sur $\mathbb{Q}$ alors que π est transcendant sur $\mathbb{Q}$.

Exemple $X\in K(X)$ est transcendant sur K.

2.1.1 Cas où a est algébrique sur K

$I(a)=Ker(\sigma)$, est un idéal non nul de $K[X]$. Mais $K[X]$ est un anneau principal. Donc $Ker(\sigma)$ est principal. D'un autre côté, deux générateurs de $I(a)$ sont tels que l'un d'eux est le produit de l'autre par un élément de K^*, il en résulte que cet idéal possède un générateur unitaire et un seul.

Définition Le générateur unitaire de $I(a)$ sera noté $Irr(a,K)$ et appelé le **polynôme minimal** de a sur K.

Exemple i est algébrique sur $\mathbb{R}$ et $Irr(i,\mathbb{R})=X^2+1$.

Exemple $\sqrt{2}$ est algébrique sur $\mathbb{Q}$ et $Irr(i,\mathbb{Q})=X^2-2$.

Théorème Le polynôme $Irr(a,K)$ est irréductible dans $K[X]$.

Démonstration Sinon, on pourra l'écrire sous la forme $Irr(a,K)=gh$ où g et h sont deux polynômes de degré inférieur au degré n de $Irr(a,K)$. Mais, nous avons

$$g(a)h(a)=(gh)(a)=Irr(a,K)(a)=0$$

qui implique $g(a)=0$ ou $h(a)=0$. Dans le premier cas, nous aurons $g\in I(a)$ et $Irr(a,K)$ divise g, et dans le second cas, $h\in I(a)$ et $Irr(a,K)$ divise h ce qui est impossible vu les degrés de ces polynômes.

Remarque Nous avons

$$[f(a)=0] \Longleftrightarrow [f \in I(a)] \Longleftrightarrow [Irr(a,K) \text{ divise } f]$$

Le théorème précédent justifie la notation $Irr(a,K)$ pour le polynôme minimal de a sur K.

Théorème Si $K \subseteq L \subseteq E = K(a)$, alors $E = L(a)$ et $Irr(a,L)$ divise $Irr(a,K)$ dans $L[X]$.

Démonstration E est un sous-corps de E contenant $L \cup \{a\}$. Si H est un sous-corps de E contenant $L \cup \{a\}$, alors H contient $K \cup \{a\}$ et $E \subseteq H$ car E est le plus petit sous-corps de E contenant $K \cup \{a\}$. Donc E est le plus petit sous-corps de E contenant $L \cup \{a\}$, ce qui prouve $E = L(a)$. Le polynôme $Irr(a,K)$ appartient à $L[X]$ et vérifie $Irr(a,K)(a) = 0$. Il en résulte que $Irr(a,L)$ divise $Irr(a,K)$ dans $L[X]$.

Théorème Si a est algébrique sur K, alors

$$K(a) = K[a] \approx K[X]/I(a).$$

Démonstration Considérons l'homomorphisme σ défini par $\sigma(P) = P(a)$ pour tout $P \in K[X]$. Nous avons

$$K[a] = \text{Im}(\sigma) \approx K[X]/Ker(\sigma) \approx K[X]/I(a).$$

Il en résulte que $K[a]$ est un corps car l'idéal $I(a)$ est maximal. Ceci prouve $K(a) = K[a]$ et par suite $K(a) = K[a] \approx K[X]/I(a)$.

Théorème Si $n = deg(Irr(a,K))$, alors $E = K(a)$ est une extension de degré n et $\left\{1,a,a^2,\ldots,a^{n-1}\right\}$ est une base du K-espace vectoriel E.

Démonstration Les éléments $1,a,a^2,\ldots,a^{n-1}$ sont linéairement indépendants car sinon, on peut trouver un polynôme non nul de degré inférieur ou égal à $n-1$ dont a est une racine. Ce polynôme appartiendrait à $I(a)$ ce qui est impossible car $I(a)$ est engendré par un polynôme de degré n. Pour prouver que ces éléments forment un système de générateurs du K-espace vectoriel E, il suffit de démontrer que

$$a^m \in Vect\left(1,a,a^2,\ldots,a^{n-1}\right)$$

pour tout $m \in \mathbb{N}$ car tout élément de $K(a) = K[a]$ s'écrit sous la forme $x = \alpha_0 + \alpha_1 a + \cdots + \alpha_q a^q$. Ceci est vrai pour $m \leq n-1$. Si $m \geq n$, alors m s'écrit $m = n+r$. Nous allons démontrer $a^m \in Vect\left(1,a,a^2,...,a^{n-1}\right)$ par récurrence sur r. Si $r = 0$, alors $m = n$. En écrivant $Irr(a,K)$ sous la forme

$$Irr(a,K) = b_0 + b_1 X + \cdots + b_{n-1}X^{n-1} + X^n,$$

on obtient

$$b_0 + b_1 a + \cdots + b_{n-1}a^{n-1} + a^n = 0$$

et

$$a^n = c_0 + c_1 a + \cdots + c_{n-1}a^{n-1} \in Vect\left(1,a,a^2,...,a^{n-1}\right)$$

où $c_i = -b_i$ pour $1 = 0,1,...,n-1$.

Supposons que

$$a^{n+r} = t_0 + t_1 a + \cdots + t_{n-1}a^{n-1} \in Vect\left(1,a,a^2,...,a^{n-1}\right)$$

alors nous avons

$$a^{n+r+1} = aa^{n+r} = at_0 + t_1 a^2 + \cdots + t_{n-1}a^n \in Vect\left(1,a,a^2,...,a^{n-1}\right)$$

car

$$at_0 + t_1 a^2 + \cdots + t_{n-2}a^{n-1} \in Vect\left(1,a,a^2,...,a^{n-1}\right)$$

et

$$t_{n-1}a^n \in Vect\left(1,a,a^2,...,a^{n-1}\right)$$

Il en résulte $a^m \in Vect\left(1,a,a^2,...,a^{n-1}\right)$ pour tout $m \in \mathbb{N}$. Ceci prouve $[E:K] = \dim_K(E) = n$.

2.1.2 Cas où a est transcendant sur K

Dans ce cas, l'homomorphisme σ est injectif. Ceci prouve que $K[X]$ est isomorphe à $K[a]$. Mais ces deux anneaux possèdent des corps de fractions, et σ peut être prolongé en un homomorphisme du corps de fractions $Q(K[X]) = K(X)$ de $K[X]$ au corps de fractions $Q(K[a]) = K(a) = E$ de $K[a]$. Il en résulte :

Théorème Si a est transcendant sur K, alors $E = K(a)$ est isomorphe à $K(X)$.

2.2 Extensions algébriques

Définition Une extension E de K sera dite **algébrique** si, et seulement si, tout élément a de E est algébrique sur K. Elle sera dite **transcendante** dans le cas contraire.

Exemple $\mathbb{C}$ est une extension algébrique de $\mathbb{R}$, mais $\mathbb{R}$ est une extension transcendante de $\mathbb{Q}$.

Théorème Toute extension finie E de K est algébrique.

Démonstration Soit a un élément de E et $n = [E : K]$. Les éléments $1,a,a^2,\ldots,a^n$ sont linéairement dépendants car $\dim_K(E) = n$. Il existe des scalaires (éléments de K) $b_0,b_1,\ldots,b_n$, non tous nuls, tels que

$$b_0 + b_1 a + \cdots + b_{n-1}a^{n-1} + b_n a^n = 0.$$

Si

$$P = b_0 + b_1 X + \cdots + b_{n-1}X^{n-1} + b_n X^n,$$

alors $P \neq 0$ et $P(a) = 0$ ce qui prouve que a est algébrique sur K. Il en résulte que E est une extension algébrique de K.

Théorème Une extension simple $E = K(a)$ est algébrique si, et seulement si, a est algébrique sur K.

Démonstration Si a est algébrique sur K, alors E est une extension finie de K ce qui prouve que cette extension est algébrique. Réciproquement, si l'extension E est algébrique, alors a, élément de E, est algébrique sur K.

Théorème Si $K \subseteq L \subseteq E$, alors si $a \in E$ est algébrique sur K, alors il est algébrique sur L.

Démonstration Si a est algébrique sur K, alors a est une racine d'un polynôme $f \in K[X]$. Mais $f \in L[X]$ car $K \subseteq L$. Il en résulte que a est algébrique sur L.

Théorème L'extension $E = K(a_1,a_2,\ldots,a_n)$ de K est algébrique si, et seulement si, les éléments $a_1,a_2,\ldots,a_n$ sont tous algébriques sur K.

Démonstration Si E algébrique sur K, alors les éléments $a_1,a_2,\ldots,a_n$ de E sont tous algébriques sur K. Réciproquement, nous allons démontrer que si les

éléments $a_1,a_2,...,a_n$ sont tous algébriques sur K, alors l'extension E de K est finie. Posons

$$K_0 = K \text{ et } K_i = K(a_1,a_2,...,a_i) \text{ pour } i = 1,2,..,n$$

Nous avons $K_i = K_{i-1}(a_i)$. D'un autre côté, a_i est algébrique sur K_{i-1} car a_i est algébrique sur K et $K \subseteq K_{i-1} \subseteq K_i$. Ceci implique que le degré $[K_i : K_{i-1}]$ est fini pour tout i et $[E : K] = [K_n : K_0] = \prod_{i=1}^{i=n} [K_i : K_{i-1}]$ est fini. Ainsi, l'extension E de K est finie. Elle est algébrique.

Corollaire Si R est un corps des racines pour $P(X) \in K[X]$ sur K, alors R est une extension algébrique de K.

Démonstration Nous avons $R = K(a_1,a_2,...,a_n)$ où $a_1,a_2,...,a_n$ sont les racines de P dans R. Comme chaque a_i est algébrique sur K (il est racine de P), R est une extension algébrique de K.

2.3 Simplicité d'une extension

Le but de ce paragraphe est de prouver qu'une extension finie E de K est simple si, et seulement si, l'ensemble des corps intermédiaires entre K et E est fini. Ceci découlera des théorèmes suivants :

Théorème Si $E = K(a)$, où a est algébrique sur K, et si L est un corps intermédiaire entre K et E, alors $Irr(a,L)$ divise $Irr(a,K)$ et $L = K(a_1,a_2,...,a_{n-1})$ où $a_1,a_2,...,a_{n-1}$ sont les coefficients de $Irr(a,L)$.

Démonstration Soit $H = K(a_1,a_2,...,a_{n-1})$. Nous avons

$$K \subseteq H \subseteq L \subseteq E = K(a) \,.Irr(a,L)$$

appartient à $H[X]$ et est irréductible dans $H[X]$ car il est irréductible dans $L[X]$ ($H[X] \subseteq L[X]$). Il en résulte

$$Irr(a,H) = irr(a,L) \text{ et } H(a) = E = L(a).$$

Ce qui précède implique

$$[E : H] = \deg(Irr(a,H)) = \deg(Irr(a,L)) = [E : L]$$

et

$$[L : H] = \frac{[E : H]}{[E : L]} = 1.$$

D'où $H = L$.

Théorème Si $E = K(a)$ est une extension simple, alors l'ensemble des corps intermédiaires entre K et E est fini.

Démonstration Soit φ l'application de l'ensemble des corps intermédiaires dans celui des facteurs de $Irr(a,K)$ qui associe à L le facteur $Irr(a,L)$. Cette application est injective, car si $Irr(a,L) = Irr(a,L')$, alors L et L' sont tous les deux égaux au corps engendré sur K par les coefficients du polynôme $Irr(a,L) = Irr(a,L')$. On en déduit que l'ensemble des corps intermédiaires est fini car l'ensemble des facteurs de $Irr(a,K)$ est fini.

Pour prouver la réciproque, nous distingons deux cas :

2.3.1 Cas où K est fini

Théorème Si K est un corps fini et E est une extension finie de K, alors E est une extension simple de K.

Démonstration Si $Card(K) = q$ et $[E : K] = n$, alors $Card(E) = q^n$ car le K-espace vectoriel E est isomorphe à K^n. Il en résulte que E est un corps fini. Nous prouverons par la suite que le groupe multiplicatif d'un corps fini est cyclique. On en déduit que si a est un générateur du groupe E^*, alors $E = K(a)$.

2.3.2 Cas où K est infini

Théorème Si l'ensemble des corps intermédiaires entre K et E est fini et si $E = K(a_1,a_2)$, alors E est une extension simple de K.

Démonstration Considérons l'ensemble des corps intermédiaires de la forme $K(a_1 + ta_2)$ où $t \in K$. Cet ensemble est fini. Comme K est infini, il existe deux éléments distincts t et u tels que

$$K(a_1 + ta_2) = K(a_1 + ua_2) = L.$$

Nous avons

$$(t-u)\,a_2 = (a_1 + ta_2) - (a_1 + ua_2) \in L$$

et $a_2 \in L$ car $t - u \neq 0$. Nous avons aussi $a_1 = (a_1 + ta_2) - ta_2 \in L$. Il en résulte

$$L = K(a_1 + ta_2) = K(a_1,a_2) = E.$$

Théorème Toute extension finie E de K est engendrée sur K par un nombre fini d'éléments c.à.d. elle est de la forme $E = K(a_1,a_2,...,a_n)$.

Démonstration Nous allons démontrer ce théorème par récurrence sur le degré $p = [E : K]$. Si $p = 2$ et $a \in E - K$, alors $K \neq K(a) \subseteq E$ et

$$1 < [K(a) : K] \leq [E : K] = 2.$$

Il en résulte $[K(a) : K] = [E : K] = 2$ et $E = K(a)$. Si le théorème est vrai pour les extensions de degrés $\leq p-1$, il est aussi vrai pour les extensions de degré p. En effet, si $a_1 \in E - K$, alors $[E : K(a_1)] \leq p-1$. Il en résulte que E s'écrit $E = K(a_1)(a_2,...,a_n) = K(a_1,...,a_n)$.

Théorème Si l'ensemble des corps intermédiaires entre K et E est fini, alors E est une extension simple de K.

Démonstration Comme E est une extension finie de K, E est de la forme

$$E = K(a_1,a_2,...,a_n).$$

Nous allons prouver le théorème par récurrence sur n. Pour $n = 2$, le théorème est vrai comme nous l'avons démontré ci-haut. Supposons le théorème vrai pour $n-1$. L'extension $E = K(a_1,a_2,...,a_{n-1})$ est telle que l'ensemble des corps intermédiaires est fini. C'est donc une extension simple $K(b)$ de K. Nous obtenons

$$E = K(a_1,a_2,...,a_n) = K(a_1,a_2,...,a_{n-1})(a_n) = K(b,a_1).$$

Mais cette extension est simple d'après ce qui a été démontré. Donc E est une extension simple de K.

Théorème Une extension finie E de K est simple si, seulement si, l'ensemble des corps intermédiaires entre K et E est fini.

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

Définition On appelle **élément primitif** d'une extension finie E de K, tout élément a de E tel que $E = K(a)$.

Exemple i est un élément primitif de l'extension $\mathbb{C}$ de $\mathbb{R}$. $\sqrt{2}+\sqrt{3}$ est un élément primitif de l'extension $\mathbb{Q}\left(\sqrt{2},\sqrt{3}\right)$ de $\mathbb{Q}$.

Chapitre 3

Prolongement d'isomorphismes

3.1 Isomorphisme

Nous rappelons qu'un homomorphisme de corps est un homomorphisme d'anneaux qui conserve l'élément neutre de la multiplication.

Théorème Tout homomorphisme de corps est injectif.

Démonstration Soit $\sigma; K \longrightarrow L$ un homomorphisme de corps. $Ker(\sigma)$ est un idéal de K. $Ker(\sigma) \neq K$ car $\sigma(1) = 1$. Il en résulte $Ker(\sigma) = (0)$ et par suite σ est injectif.

Un homomorphisme de corps $\sigma; K \longrightarrow L$, étant injectif, sera dit un **isomorphisme** de K dans L. Le but de ce chapitre est de répondre à la question suivante :

Question : Ayant un isomorphisme $\sigma; K \longrightarrow K'$, une extension simple E de K et une extension E' de K', est-il possible de prolonger σ en un isomorphisme $\overline{\sigma}$ de E dans E' ?

Définition Soit E et F deux extensions du même corps K. Un isomorphisme $\sigma; E \longrightarrow F$ de E dans F sera appelé un **K-isomorphisme** si, et seulement si, il laisse fixe tout élément de K c.à.d. $\sigma(k) = k$ pour tout $k \in K$.

Exemple L'application $\varphi; \mathbb{C} \longrightarrow \mathbb{C}$ définie par $\varphi(u) = \overline{u}$ (le conjugué de u) est un $\mathbb{R}$-isomorphisme de $\mathbb{C}$ dans $\mathbb{C}$.

Théorème Soit E et F deux extensions du même corps K et $\sigma; E \longrightarrow F$ un K-isomorphisme. σ est une application K-linéaire.

Démonstration Nous avons

$$\sigma(ax) = \sigma(a)\sigma(x) = a\sigma(x) \text{ pour tout } (a,x) \in K \times E.$$

Théorème Soit $\sigma; K \longrightarrow K'$ un isomorphisme de K sur K', E une extension de K, E' une extension de K' et $\overline{\sigma}; E \longrightarrow E'$ un isomorphisme qui prolonge σ. Nous avons $[\overline{\sigma}(E) : K'] = [E : K]$.

Démonstration Soit $b = \{e_1,...,e_n\}$ une base du K-espace vectoriel E et soit $f_i = \overline{\sigma}(e_i)$ pour $i = 1,2,...,n$. La famille $\{f_1,...,f_n\}$ est une base du K'-espace vectoriel $\overline{\sigma}(E)$. En effet, tout élément $y = \overline{\sigma}(x) \in \overline{\sigma}(E)$ peut s'écrire sous la forme

$$\begin{aligned} y = \overline{\sigma}(x) &= \overline{\sigma}(x_1 e_1 + \cdots + x_n e_n) \\ &= \overline{\sigma}(x_1)\overline{\sigma}(e_1) + \cdots + \overline{\sigma}(x_n)\overline{\sigma}(e_n) \\ &= \sigma(x_1) f_1 + \cdots + \sigma(x_n) f_n \end{aligned}$$

ce qui prouve que $\{f_1,...,f_n\}$ est une famille génératrice du K'-espace vectoriel $\overline{\sigma}(E)$. Les f_i sont linéairement indépendants : Supposons avoir

$$b_1 f_1 + \cdots + b_n f_n = 0.$$

Comme σ est une application surjective, il existe, pour $i = 1,2,...,n$, $a_i \in K$ tel que $b_i = \sigma(a_i)$. Nous obtenons

$$\begin{aligned} &\overline{\sigma}(a_1 e_1 + \cdots + a_n e_n) = \overline{\sigma}(a_1)\overline{\sigma}(e_1) + \cdots + \overline{\sigma}(a_n)\overline{\sigma}(e_n) \\ &= b_1 f_1 + \cdots + b_n f_n = 0. \end{aligned}$$

Cette relation implique $a_1 e_1 + \cdots + a_n e_n = 0$ et $a_i = 0$ pour $i = 1,2,..,n$. D'où $b_i = 0$ pour $i = 1,2,..,n$ ce qui achève la démonstration.

3.2 Prolongement d'isomorphismes

Soit $\sigma; K \longrightarrow K'$ un isomorphisme de K sur K' , $E = K(a)$ une extension simple de K et E' une extension de K'. Nous allons étudier la question du prolongement de σ en un isomorphisme de E dans E'.

3.2.1 Cas où a est transcendant sur K

Théorème σ peut être prolongé d'une manière unique en un isomorphime

$$\widehat{\sigma}; K[X] \longrightarrow K'[X]$$

qui transforme X en X.

Démonstration Soit $\widehat{\sigma}; K[X] \longrightarrow K'[X]$ l'application définie par

$$\widehat{\sigma}(a_0 + a_1X + \cdots + a_nX^n) = \sigma(a_0) + \sigma(a_1)X + \cdots + \sigma(a_n)X^n.$$

C'est un simple exercice de prouver que $\widehat{\sigma}$ est un homomorphisme d'anneaux vérifiant $\widehat{\sigma}(X) = X$ et $\widehat{\sigma}(k) = \sigma(k)$ pour tout $k \in K$. $\widehat{\sigma}$ est injective, car si nous avons

$$\widehat{\sigma}(P) = \widehat{\sigma}(a_0 + a_1X + \cdots + a_nX^n) = 0$$

alors $\sigma(a_i) = 0$ pour $i = 0,1,...,n$. Il en résulte $a_i = 0$ pour $i = 0,1,...,n$ et $P = 0$. $\widehat{\sigma}$ est l'unique isomorphisme qui vérifie $\widehat{\sigma}(X) = X$ et $\widehat{\sigma}(k) = \sigma(k)$ pour tout $k \in K$ car, si τ est une autre solution, alors nous avons

$$\begin{aligned}\tau(a_0 + a_1X + \cdots + a_nX^n) &= \tau(a_0) + \tau(a_1) + \cdots + \tau(a_n)X^n \\ &= \sigma(a_0) + \sigma(a_1)X + \cdots + \sigma(a_n)X^n \\ &= \widehat{\sigma}(P).\end{aligned}$$

pour tout $P \in K[X]$.

Théorème Si E' contient un élément a' transcendant sur K', alors on peut prolonger σ d'une manière unique en un isomorphisme qui transforme a en a'.

Démonstration Soit $F' = K'(a')$. F'est une extension de K' isomorphe à $K'(X)$ car a' est transcendant sur K'. On peut pronlonger σ en un isomorphisme $\widehat{\sigma}; K[X] \longrightarrow K'[X]$ par

$$\widehat{\sigma}(a_0 + a_1X + \cdots + a_nX^n) = \sigma(a_0) + \sigma(a_1X) + \cdots + \sigma(a_n)X^n.$$

$\widehat{\sigma}$ est l'unique prolongement de σ qui vérifie $\widehat{\sigma}(X) = X$ et $\widehat{\sigma}(k) = \sigma(k)$ pour tout $k \in K$. Cet isomorphisme $\widehat{\sigma}$ peut être prolongé, d'une manière unique, en un isomorphisme σ' de $K(X)$, corps des fractions de $K[X]$, dans $K'(X)$, corps des fractions de $K'[X]$, tel que $\sigma'(X) = X$ et $\sigma'(k) = \sigma(k)$ pour tout $k \in K$. Finalement, soit u l'unique isomorphisme de $K(a)$ sur $K(X)$ tel que $u(a) = X$ et u' l'unique isomorphisme de $K'(X)$ sur $K'(a')$ tel que $u'(X) = a'$. Nous avons

$$\begin{array}{ccccccc} & & K & \xrightarrow{\sigma} & K' & & \\ & & \downarrow & & \downarrow & & \\ & & K[X] & \xrightarrow{\widehat{\sigma}} & K'[X] & & \\ & & \downarrow & & \downarrow & & \\ K(a) & \xrightarrow{u} & K(X) & \xrightarrow{\sigma'} & K'(X) & \xrightarrow{u'} & K'(a') \end{array}$$

où les flêches verticales sont les injections canoniques. Posons $\overline{\sigma} = u' \circ \sigma' \circ u$. $\overline{\sigma}$ est un isomorphisme et il vérifie

$$\overline{\sigma}(a) = \left(u' \circ \sigma' \circ u\right)(a) = u'\left(\sigma'\left(u(a)\right)\right) = u'\left(\sigma'(X)\right) = u'(X) = a'$$

et

$$\overline{\sigma}(k) = \left(u' \circ \sigma' \circ u\right)(k) = u'\left(\sigma'\left(u(k)\right)\right) = u'\left(\sigma'(k)\right) = u'(\sigma(k)) = \sigma(k)$$

$\overline{\sigma}$ est unique, car $\widehat{\sigma}$,σ',u et u' sont tous uniques.

Remarque Si $E' = K'(a')$ alors $\overline{\sigma}$ est bijectif.

Théorème Si σ peut être prolongé en un isomorphisme $\overline{\sigma}$, alors $a' = \overline{\sigma}(a)$ est transcendant sur K'.

Démonstration Sinon, il existe des éléments b'_0,b'_1,...,b'_n, non tous nuls, tels que

$$b'_0 + b'_1 a' + \cdots + b'_n \left(a'\right)^n = 0.$$

Mais chaque b'_i peut s'écrire sous la forme $b'_i = \sigma(b_i)$, il en résulte

$$\begin{aligned}\overline{\sigma}(b_0 + b_1 a + \cdots + b_n a^n) &= \overline{\sigma}(b_0) + \overline{\sigma}(b_1)\, a' + \cdots + \overline{\sigma}(b_n)\,(a^n) \\ &= b'_0 + b'_1 a' + \cdots + b'_n \left(a'\right)^n = 0\end{aligned}$$

qui implique $b_0 + b_1 a + \cdots + b_n a^n = 0$, avec les b_i non tous nuls, qui prouve que a est algébrique sur K en contradiction l'hypothèse que a est transcendant sur K.

Ce qui précède permet d'énoncer :

Théorème σ peut être prolongé en un isomorphisme $\overline{\sigma}$ de $E = K(a)$ dans E' si, et seulement si, E' contient un élément a' transcendant sur K'.

3.2.2 Cas où a est algébrique sur K

Théorème Si E' contient un élément a' algébrique sur K' tel que

$$\widehat{\sigma}\left(Irr(a,K)\right) = Irr\left(a',K'\right),$$

alors on peut prolonger σ d'une manière unique en un isomorphisme qui transforme a en a'..

Démonstration Soit $I(a)$ (resp. $I(a')$) l'idéal de $K[X]$ (resp. de $K'[X]$) engendré par $Irr(a,K)$ (resp. par $Irr(a',K')$), u (resp. u') l'unique isomorphisme de $K(a)$ (resp. $K'[X]/I(a')$) sur $K[X]/I(a)$ (resp. $K'(a')$) tel que $u(a)=\overline{X}$ (resp. $u'\left(\overline{X}\right)=a'$). Comme dans le cas où a est transcendant sur K, σ peut être prolongé en $\widehat{\sigma}$. $\widehat{\sigma}$ peut être prolongé en un isomorphisme σ' de $K[X]/I(a)$ sur $K'[X]/I(a')$ car, nous avons $\widehat{\sigma}(I(a))\subseteq I(a',K')$ du fait que $\widehat{\sigma}(Irr(a,K))=Irr(a',K')$. Nous obtenons

$$\begin{array}{ccccccc} & & K & \xrightarrow{\sigma} & K' & & \\ & & \downarrow & & \downarrow & & \\ & & K[X] & \xrightarrow{\widehat{\sigma}} & K'[X] & & \\ & & \downarrow & & \downarrow & & \\ K(a) & \xrightarrow{u} & K[X]/I(a) & \xrightarrow{\sigma'} & K'[X]/I(a') & \xrightarrow{u'} & K'(a') \end{array}$$

où les flêches verticales du premier niveau sont les injections canoniques et celles du second niveau sont les surjections canoniques. Posons $\overline{\sigma}=u'\circ\sigma'\circ u$. $\overline{\sigma}$ est un isomorphisme et il vérifie

$$\overline{\sigma}(a)=\left(u'\circ\sigma'\circ u\right)(a)=u'\left(\sigma'\left(u(a)\right)\right)=u'\left(\sigma'\left(\overline{X}\right)\right)=u'\left(\overline{X}\right)=a'$$

et

$$\overline{\sigma}(k)=\left(u'\circ\sigma'\circ u\right)(k)=u'\left(\sigma'\left(u(k)\right)\right)=u'\left(\sigma'(k)\right)=u'(\sigma(k))=\sigma(k)$$

$\overline{\sigma}$ est unique car $\widehat{\sigma}$,σ',u et u' sont tous uniques.

Remarque Si $E'=K'(a')$, alors $\overline{\sigma}$ est bijectif.

Théorème Si σ peut être prolongé en un isomorphisme $\overline{\sigma}$, alors $a'=\overline{\sigma}(a)$ est algébrique sur K' et $\widehat{\sigma}(Irr(a,K))=Irr(a',K')$.

Démonstration Soit $P=b_0+b_1X+\cdots+X^n$ le polynôme minimal de a sur K. Nous avons

$$b_0+b_1a+\cdots+b_na^n=0$$

et

$$0=\overline{\sigma}(b_0+b_1a+\cdots+a^n)=\overline{\sigma}(b_0)+\overline{\sigma}(b_1)a'+\cdots+\overline{\sigma}\left(a'\right)^n$$

qui prouve que a' est algébrique sur K'. Le polynôme

$$P'=b'_0+b'_1X+\cdots+X^n$$

où $b'_i=\overline{\sigma}(b_i)=\sigma(b_i)$ est irréductible dans $K'[X]$ car $\widehat{\sigma}$ est un isomorphisme et P est irréductible dans $K[X]$. D'où

$$Irr(a',K')=P'=\widehat{\sigma}(P)=\widehat{\sigma}(Irr(a,K)).$$

Ce qui précède nous permet d'énoncer :

Théorème σ peut être prolongé en un isomorphism $\overline{\sigma}$ de $E = K(a)$ dans E' si, et seulement si, E' contient un élément a' algébrique sur K' tel que $\widehat{\sigma}(Irr(a,K)) = Irr(a',K')$

Les théorèmes précédents peuvent être résumés en :

Théorème Si $\sigma; K \longrightarrow K'$, $E = K(a)$ est une extension simple de K et $E' = K'(a')$ une extension simple de K', alors il est possible de prolonger σ en un isomorphisme $\overline{\sigma}$ de E dans E' tel que $\overline{\sigma}(a) = a'$ si, et seulement si, une des deux conditions suivantes est vérifiée :

- a est transcendant sur K et a' est transcendant sur K'.
- a est algébrique sur K, a' est algébrique sur K' et

$$\widehat{\sigma}(Irr(a,K)) = Irr\left(a',K'\right).$$

Théorème Si $E = K(a)$ et $E' = K(a')$ sont deux extensions simples du même corps K, alors il existe un K-isomorphisme $\overline{\sigma}$ de E sur E' tel que $\overline{\sigma}(a) = a'$ si, et seulement si, une des deux conditions suivantes est vérifiée :

- a et a' sont tous les deux transcendants sur K.
- a et a' sont tous les deux algébriques sur K et $Irr(a,K) = Irr(a',K)$.

3.3 Unicité du corps des racines

Soit $\sigma; K \longrightarrow K'$ un isomorphisme de corps, $P \in K[X]$, $P' = \widehat{\sigma}(P)$, R un corps des racines pour P sur K et R' un corps des racines pour P' sur K'. R s'écrit $R = K(a_1,\ldots,a_n)$ où $a_1,\ldots,a_n$ sont les racines de P dans R. Nous avons aussi $R' = K'(a'_1,\ldots,a'_n)$ où $a'_1,\ldots,a'_n$ sont les racines de P' dans R'. Soit $R_i = K(a_1,\ldots,a_i)$ pour $i = 1,2,..,n$.

Théorème Il est possible de prolonger σ en un isomorphisme de R sur R'.

Démonstration Nous allons prouver par récurrence sur i, que σ peut être prolongé en un isomorphisme σ_i de R_i dans R'. Pour $i=1$, le résultat est vrai. En effet, $Irr(a_1,K)$ est un facteur irréductible de P. Ainsi, le polynôme $\widehat{\sigma}(Irr(a_1,K))$ est un facteur irréductible de P'. Un des éléments $a'_1,\ldots,a'_n$, soit a'_1, est une racine de ce facteur. On peut alors prolonger σ en un isomorphisme σ_1 de R_1 dans R'. Supposons σ prolongé en un isomorphisme σ_i de R_i dans R'. Or $R_{i+1}=R_i(a_i)$. En raisonnant comme avant, on peut prolonger σ_i en un isomorphisme σ_{i+1} de R_{i+1} dans R'. Pour $i=n$, nous avons un isomorphisme σ_n de $R_n=R$ dans R' qui prolonge σ. D'où

$$[R:K]=\left[\sigma_n(R):K'\right]\leq\left[R':K'\right].$$

D'une manière similaire, nous avons $[R':K']\leq[R:K]$ et par suite,

$$[R:K]=\left[\sigma_n(R):K'\right]=\left[R':K'\right].$$

Ceci prouve $\sigma_n(R)=R'$.

Corollaire Deux corps des racines pour le polynôme $P\in K[X]$ sur K sont K-isomorphes.

Chapitre 4

Racines de l'unité

4.1 Racines de l'unité

Soit K un corps et n un entier naturel non nul.

Définition Un élément $a \in K$ est une **racine n$^{\text{ème}}$ de l'unité** si, et seulement si, $a^n = 1$.

Il résulte de cette définition que $a \in K$ est une racine $n^{ème}$ de l'unité si, et seulement si, a est une racine du polynôme $U(X) = X^n - 1 \in K[X]$.

Exemple $1 \in K$ est une racine $n^{ème}$ de l'unité pour tout $n \in \mathbb{N}^*$. i est une racine $4^{ème}$ de l'unité dans $\mathbb{C}$. $j = \dfrac{1}{2} + i\dfrac{\sqrt{3}}{2}$ est une racine cubique de l'unité dans $\mathbb{C}$.

Soit $S_n(K)$ l'ensemble de toutes les racines $n^{ème}$ de l'unité dans K. Cet ensemble est non vide car $1 \in S_n(K)$.

Théorème Si m divise n, alors $S_m(K) \subseteq S_n(K)$.

Démonstration Si m divise n, alors n s'écrit $n = pm$ où $p \in \mathbb{N}^*$. Il en résulte

$$[a \in S_m(K)] \Longrightarrow [a^m = 1] \Longrightarrow [a^n = a^{mp} = (a^m)^p = 1] \Longrightarrow [a \in S_n(K)]$$

Théorème $S_n(K)$ est un groupe multiplicatif.

Démonstration $S_n(K) \neq \emptyset$ comme nous l'avons vu. D'un autre côté, si a et b sont des racines $n^{ème}$ de l'unité, alors a et b sont non nuls et vérifient

$$\left(ab^{-1}\right)^n = a^n \left(b^{-1}\right)^n = a^n (b^n)^{-1} = 1$$

ce qui prouve le théorème.

Définition On appelle **corps premier** d'un corps K le plus petit sous-corps de K.

Théorème Le corps premier de K est le sous-corps de K engendré par 1.

Démonstration En effet, 1 appartient à tous les sous-corps de K . Il en résulte que le sous-corps de K engendré par 1 est le plus petit sous-corps de K c.d. son corps premier.

Théorème Le corps premier de K est l'intersection de tous les sous-corps de K.

Démonstration Facile à vérifier.

Théorème Le corps premier d'un corps K est isomorphe à $\mathbb{Q}$ si sa caractéristique est nulle, et à $\mathbb{Z}/(p)$ si cette caractéristique est $p \neq 0$.

Démonstration Soit u l'application de $\mathbb{Z}$ dans K définie par $u(n) = n.1$. Il est facile de vérifier que u est un homomorphisme d'anneaux et que $\mathrm{Im}(u)$ est le sous-anneau de K engendré par 1. $Ker(u)$ est un idéal de $\mathbb{Z}$. Il est engendré par un élément p de $\mathbb{Z}$. p est la caractéristique de K. Si $p = 0$, alors $\mathbb{Z}$ est isomorphe à $\mathrm{Im}(u)$ et le corps des fractions de $\mathbb{Z}$ (c.à.d. $\mathbb{Q}$) au corps des fractions de $\mathrm{Im}(u)$. Mais ce corps est le plus petit sous corps de K contenant 1. Il est le corps premier de K. Donc, si K est de caratéristique nulle, son corps premier est isomorphe à $\mathbb{Q}$. Si $p \neq 0$, alors $\mathrm{Im}(u)$ est isomorphe à $\mathbb{Z}/Ker(u) = \mathbb{Z}/(p)$ qui est un corps (p est premier). Ce sous-corps de K est le sous-corps engendré par 1. Donc, si K est de caractéristique $p \neq 0$, son corps premier est isomorphe à $\mathbb{Z}/(p)$.

Exemple $\mathbb{Q}$ est le corps premier de $\mathbb{R}$ et de $\mathbb{C}$. $\mathbb{Z}/(p)$ est égal à son corps premier.

Soit P le corps premier de K. Nous avons $U(X) = X^n - 1 \in P[X]$. Soit R le corps des racines de U sur P.

Théorème Si la caractéristique p de K est nulle ou si elle ne divise pas n, alors R contient n racines $n^{ème}$ de l'unité distinctes.

Démonstration Il suffit de prouver que les racines du polynôme U sont toutes simples. Sinon, U et son polynôme dérivé $U' = nX^{n-1}$ ont une racine commune. Or zéro est la seule racine de U' car $p = 0$ ou n est non divisible par p. Comme

0 n'est pas une racine de U, toutes les racines de U sont simples et R en contient n.

Pour démontrer que $S_n(K)$ est un groupe cyclique, nous avons besoin d'un théorème de la théorie de groupes.

Lemme Soient a et b deux éléments d'un groupe abélien multiplicatif G. Si $p = Ord(a)$ et $q = Ord(b)$ sont premiers entre eux, alors $Ord(ab) = pq$.

Démonstration Tout d'abord, $gr(a) \cap gr(b)$ est réduit à $\{e\}$ car si x est un élément de cette intersection, alors l'ordre r de x est un diviseur commun de p et q. Cet ordre est donc égal à 1 (p et q sont premiers entre eux) et $x = e$. D'un autre côté, $(ab)^{pq} = a^p b^q = ee = e$. Enfin, si d est l'ordre de ab, alors $(ab)^d = a^d b^d$. Il en résulte $a^d = \left(b^{-1}\right)^d \in gr(a) \cap gr(b) = \{e\}$ et par suite $a^d = e = b^d$. On en déduit que d est donc un multiple commun de p et q, donc de leur produit car ils sont premier entre eux. Ainsi pq est l'ordre de ab.

Lemme Soient $a_1,\ldots,a_n$ des élément d'un groupe abélien multiplicatif G. Si les ordres des $a_1,\ldots,a_n$ sont premiers deux à deux, l'ordre de leur produit est égal au produit des ordres de ces éléments.

Démonstration Par récurrence.

Théorème Si la caractéristique p de K est nulle ou si elle ne divise pas n, alors $S_n(K)$ est un groupe cyclique.

Démonstration Soit $n = p_1^{n_1} \ldots p_t^{n_t}$ la décomposition de n comme produit de nombres premiers. Pour tout $i = 1,2,\ldots,t$ il existe au plus $\dfrac{n}{p_i}$ éléments a qui vérifient $a^{\frac{n}{p_i}} = 1$, car le polynôme $X^{\frac{n}{p_i}} - 1$ possède au plus $\dfrac{n}{p_i}$ racines. Soit, pour $i = 1,2,\ldots,t$, $a_i \in S_n(K)$ tel que $a_i^{\frac{n}{p_i}} \neq 1$. Considérons $m_i = \dfrac{n}{p_i^{n_i}}$ et $b_i = a_i^{m_i}$. Les éléments b_i sont d'ordre $p_i^{n_i}$ car leurs $p_i^{n_i}$ puissances sont égaux à 1 et leurs $p_i^{n_i-1}th$ puissances sont différents de 1. Le produit $b = b_1 \ldots b_t$ est le produit d'éléments dont les ordres sont premiers entre eux, il en résulte que l'ordre de b est le produits des ordres des b_i. Ainsi b est d'ordre n. Il engendre $S_n(K)$.

Corollaire $S_n(K)$ est isomorphe à $\mathbb{Z}/(n)$.

Définition On dit qu'une racine $n^{ème}$ de l'unité est une **racine $n^{ème}$ primitive de l'unité** si, et seulement si, cette racine engendre le groupe $S_n(K)$.

Si $z \in S_n(K)$ est une racine $n^{ème}$ primitive de l'unité, alors

$$S_n(K) = \left\{1, z, z^2, \ldots, z^{n-1}\right\}$$

Le nombre de ces racines primitives est celui des générateurs du groupe cyclique $S_n(K)$. Nous savons, d'après la théorie des groupes, que ces générateurs sont les z^q où $q \in \{1,2,\ldots,n-1\}$ et q est premier avec n. Leur nombre est noté $\varphi(n)$.

Exemple Les racine $12^{ème}$ primitives de l'unité dans $\mathbb{C}$ sont $\omega, \omega^5, \omega^7$ et ω^{11} où $\omega = \exp\left(\frac{i\pi}{6}\right)$.

4.2 Corps finis

Les exemples les plus simples de corps finis sont les corps $\mathbb{Z}/(p)$ où p est un nombre premier. Soit K un corps fini.

Théorème La caractéristique de K est non nulle.

Démonstration Car sinon, le corps premier de K serait isomorphe à $\mathbb{Q}$.

Théorème Si $Card(K) = q$, alors K est le corps des racines du polynôme $X^q - X$ le corps premier P de K.

Démonstration Soit a un élément de K. Si $a = 0$, alors $a^q - a = 0$. Si $a \neq 0$, alors a appartient au groupe multiplicatif de K qui est un groupe fini d'ordre $q-1$. Il en résulte $a^{q-1} = 1$ et $a^q - a = 0$. Ce qui précède prouve que K est un corps de décomposition pour $X^q - X$ sur P. Il est un corps des racines pour $X^q - X$ sur P car tout corps de décomposition pour pour ce polynôme sur P doit contenir tous les éléments de K.

Théorème Si $Card(K) = q$, alors q est une puissance de la caratéristique p de K.

Démonstration K est un P-espace vectoriel. Si $[K:P] = n$, alors $q = Card(K) = (Card(P))^n = p^n$.

Corollaire Deux corps finis de même cardinal ont la même caractéris-tique.

Démonstration Soient q, q' les cardinaux et p, p' les caractéristiques des deux corps. Nous avons

$$p^n = q = q' = \left(p'\right)^m$$

ce qui implique $p = p'$ car ces deux entiers sont des nombres premiers.

Théorème Deux corps finis de même cardinal sont isomorphes.

Démonstration Soit K et K' de même cardinal q. Soient P le corps premier de K et P' celui de K'. P et P' sont isomorphes car ils sont isomorphes chacun à $\mathbb{Z}/(p)$. Soit σ un isomorphisme entre K et K'. Le corps K est le corps des racines pour $X^q - X$ sur P. Il est isomorphe à K', corps des racines pour $X^q - X = \widehat{\sigma}(X^q - X)$ sur P'.

Théorème Pour tout nombre premier p et tout entier $n \geq 1$, il existe un corps fini, unique à un isomorphisme près, de cardinal $q = p^n$.

Démonstration Il suffit de prendre le corps des racines pour $X^q - X$ sur $P = \mathbb{Z}/(p)$.

Théorème Le groupe multiplicatif K^* d'un corps fini K est cyclique.

Démonstration Nous avons $K^* = S_n(K)$ où $n = Card(K) - 1$.

Chapitre 5

Extensions normales

Soit E une extension algébrique d'un corps K. E peut être un corps de rupture sur K pour un polynôme $f(X) \in K[X]$ sans être un corps de décomposition come le montre l'exemple suivant :

Exemple $\mathbb{R}$ est un corps de rupture pour X^3-2 sur $\mathbb{Q}$ sans être un corps de décomposition car nous avons :

$$X^3-2=\left(X-\sqrt[3]{2}\right)\left(X^2+\sqrt[3]{2}X+\sqrt[3]{4}\right)$$

et $X^2+\sqrt[3]{2}X+\sqrt[3]{4}$ est irréductible dans $\mathbb{R}[X]$.

Définition Une extension algébrique E de K sera dite **normale** si, et seulement si, chaque fois que E est un corps de rupture pour un polynôme irréductible $f(X) \in K[X]$ sur K, il est un corps de décomposition pour f sur K.

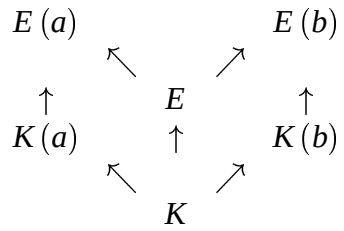
Ainsi, E est une extension normale de K si, et seulement si, chaque fois qu'un polynôme irréductible $f(X) \in K[X]$ possède une racine dans E, alors il se décompose en produit de facteurs linéaires dans $E[X]$. Parfois on exprime ceci en disant que E est une extension normale de K si, et seulement si, chaque fois qu'un polynôme irréductible $f(X) \in K[X]$ possède une racine dans E, alors il possède toutes ses racines dans E.

Exemple $\mathbb{C}$ est une extension normale de $\mathbb{R}$ car les polynôme irréductible dans $\mathbb{R}[X]$ sont de degré 1 ou 2.

Exemple L'extension $E=\mathbb{Q}\left(\sqrt[3]{2}\right)$ de $\mathbb{Q}$ n'est pas normale car le polynôme $X^3-2 \in \mathbb{Q}[X]$ possède une racine dans E sans se décomposer en produit de facteurs linéaires dans $E[X]$.

Théorème Soit E un corps des racines pour le polynôme $Q(X) \in K[X]$ sur K. Soit $f \in K[X]$ un polynôme irréductible, a et b deux racines de f. Nous avons $[E(a) : E] = [E(b) : E]$.

Démonstration Considérons le diagramme



Si $a_1,\ldots,a_n$ sont les racines de Q dans E, alors nous avons

- $E = K(a_1,\ldots,a_n)$.
- $E(a) = K(a_1,\ldots,a_n,a) = K(a)(a_1,\ldots,a_n)$ est le corps des racines de Q sur $K(a)$.
- $E(b)$ est le corps des racines de Q sur $K(b)$.
- Il existe un K-isomorphisme σ de $K(a)$ sur $K(b)$ tel que $\sigma(a) = b$, car a et b sont deux racines du même polynôme irréductible f (donc $Irr(a,K) = Irr(b,K)$).
- $\widehat{\sigma}(Q) = Q$ car $Q \in K[X]$. Il en résulte que $E(b)$ est le corps des racines de $\widehat{\sigma}(Q)$ sur $K(b)$.
- Le K-isomorphisme σ peut être prolongé en un isomorphisme de $E(a)$ sur $E(b)$.
- On en déduit $[E(a) : K(a)] = [E(b) : K(b)]$ et

$$\begin{aligned}[E(a) : E] &= \frac{[E(a) : K]}{[E : K]} = \frac{[E(a) : K(a)][K(a) : K]}{[E : K]} \\ &= \frac{[E(b) : K(b)][K(b) : K]}{[E : K]} = \frac{[E(b) : K]}{[E : K]} \\ &= [E(b) : E]\end{aligned}$$

,

Théorème Une extension finie E de K est normale si, et seulement si, elle est le corps des racines sur K pour un polynôme $f(X) \in K[X]$.

Démonstration Si l'extension E de K est finie, alors elle est algébrique et est de la forme $E = K(a_1,...,a_n)$. Soit $P_i(X) = Irr(a_i,K)$ pour $i = 1,2,...,n$ et soit $P(X) = \prod_{i=1}^{i=n} P_i(X)$. Nous allons prouver que E est le corps des racines de P sur K. Tout d'abord, chaque $P_i(X)$ se décompose en produit de facteurs linéaires dans $E[X]$ car il est irréductible, il possède une racine dans E et E est normale sur K. Il en résulte que P se décompose en produit de facteurs linéaires dans $E[X]$ et E est un corps de décomposition pour P sur K. Ensuite, E est un corps de décomposition minimal pour P sur K car si F est un corps de décomposition pour P sur K contenu dans E, alors F doit contenir tous les a_i ce qui prouve $F = E$.

Réciproquement, supposons que E est le corps des racines pour un polynôme $Q \in K[X]$ sur K et soit $f \in K[X]$ un polynôme irréductible ayant une racine a dans E. Soit M le corps des racines de fQ sur K. M s'écrit $M = K(a_1,...,a_n,b_1,...,b_m)$ où $a_1,...,a_n$ sont les racines de Q dans M et $b_1,...,b_m$ sont celles de f. Nous avons, par le théorème précédent,

$$[E(b_1) : E] = [E(b_i) : E] \text{ pour } i = 2,3,...,m.$$

Si $b_1 \in E$, alors $[E(b_1) : E] = 1 = [E(b_i) : E]$ ce qui prouve $b_i \in E$ pour $i = 2,3,...,m$. Il en résulte $E = M$ et E est un corps de décomposition pour f sur K.

Définition Soit E une extension de K. Une **clôture normale** de E est une extension normale de K qui satisfait les deux contions suivantes :

1. $K \subseteq E \subseteq N$.
2. Si M est une extension normale de K vérifiant $K \subseteq E \subseteq M \subseteq N$, alors $M = N$.

En d'autre termes, la clôture normale de E est une extension normale minimale de K contenant E.

Exemple $\mathbb{C}$ est une clôture normale de l'extension $\mathbb{R}$ de $\mathbb{Q}$.

Théorème Toute extension finie E de K possède une clôture normale.

Démonstration E, étant une extension finie K, elle est algébrique et elle s'écrit $E = K(a_1,...,a_n)$. Les éléments a_i sont tous algébrique sur K. Soit

$$P_i(X) = Irr(a_i,K) \text{ et } P = P_1...P_n.$$

Soit N un corps des racines pour P sur K. N est une extension normale de K contenant E. D'un autre côté, si M est une extension normale de K vérifiant

$K \subseteq E \subseteq M \subseteq N$, alors M est un corps de décomposition pour chaque P_i car elle contient une racine pour ce polynôme irréductible. Ainsi, M est un corps de décomposition pour P sur K contenu dans N. Or N est un corps de racines pour P sur K, d'où $M = N$.

Théorème Deux clôtures normales d'une extension finie E de K sont K-isomorphes.

Démonstration D'après ce qui précède, ces deux extensions de K sont deux corps de racines pour le polynôme $P = \prod_{i=1}^{i=n} Irr(a,K)$ sur K. Elles sont K-isomorphes.

Théorème Soit E une extension normale finie de K et F une extension algébrique de K contenant E. Tout K-isomorphisme σ de E dans F est un K-automorphisme de E.

Démonstration E étant une extension normale finie de K, elle est le corps des racines d'un polynôme $P \in K[X]$ et elle s'écrit $E = K(a_1,\ldots,a_n)$ où $a_1,\ldots,a_n$ sont les racines du polynôme P. Il suffit de prouver $\sigma(E) \subseteq E$, car E est un K-espace vectoriel de dimension finie et σ est un endomorphisme injectif de cet espace vectoriel. Or $\sigma(a_i)$ est une racine de P pour $i = 1,2,..,n$. Il en résulte $\sigma(a_i) \in E$ pour $i = 1,2,..,n$. et par suite $\sigma(E) \subseteq E$.

Théorème Soit E une extension normale finie de K et F un corps intermédiaire entre K et E. Tout K-isomorphisme σ de F dans E peut être prolongé en un K-automorphisme de E.

Démonstration E est le corps des racines d'un polynôme $P \in K[X]$ sur K. Il est aussi le corps des racines pour P sur F et sur $\sigma(F)$. Ainsi, le K-isomorphisme σ de F sur $\sigma(F)$ peut être prolongé en un K-isomorphisme de E dans E. Ce prolongement de σ est, en réalité, un K-automorphisme, car E est un K-espace vectoriel de dimension finie.

Chapitre 6

Extensions séparables

6.1 Degré de Galois d'une extension

Toutes les extensions considérées dans ce chapitre seront finies. Soit E une extension de K, N et N' deux clôtures normales de E, I l'ensemble des K-isomorphismes de E dans N et I' celui des K-isomorphismes de E dans N'.

Théorème $Card(I) = Card(I')$.

Démonstration N et N' sont deux clôtures normales de E. Il existe un K-isomorphisme σ de N sur N'. Soit $\varphi; I \longrightarrow I'$ l'application définie par $\varphi(u) = \sigma \circ u$. Il est facile de prouver que l'application φ est bijective. Donc $Card(I) = Card(I\prime)$.

Définition On appelle **degré galoisien** d'une extension E de K, le cardinal de l'ensemble des K-isomorphismes de E dans une clôture normale de E.

La définition du degré galoisien ne dépend pas du choix de la clôture normale de E d'après le théorème précédent. Le degré galoisien de l'extension E de K sera noté $\overline{[E : K]}$.

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

Théorème Soit L une extension normale de K contenant une clôture normale de E. Le degré galoisien $\overline{[E : K]}$ est égal au cardinal de l'ensemble des K-isomorphismes de E dans L.

Démonstration Soit J l'ensemble des K-isomorphismes de E dans L. Nous avons $I \subseteq J$. Réciproquement, tout $\sigma \in J$ peut être prolongé en un K-automorphisme $\overline{\sigma}$ de L, car L est une extension normale de K. La restriction de $\overline{\sigma}$ à N est un K-automorphisme de N car N est une extension normale de K.

Nous avons $\sigma(E) \subseteq \overline{\sigma}(E) \subseteq \overline{\sigma}(N) = N$. Il en résulte que, σ est, en réalité, un K-isomorphisme de E dans N c.à.d. $\sigma \in I$. D'où $I = J$.

Théorème Soit E' une extension de K'. Si $\overline{\sigma}$ est un isomorphisme de E sur E' tel que sa restriction σ à K est un isomorphisme de K sur K', alors $\overline{[E:K]} = \overline{[E':K']}$.

Démonstration Soit N une clôture normale de E et N' une clôture normale de E'. L'isomorphisme $\overline{\sigma}$ peut être prolongé en un isomorphisme σ' de N sur N'. L'application φ qui associe à chaque K-isomorphisme u de E dans N, le K'-isomorphisme $u' = \sigma \circ u \circ \sigma^{-1}$ de E' dans N' est bijective. Il en résulte $\overline{[E:K]} = \overline{[E':K']}$.

Théorème Si nous avons $K \subseteq L \subseteq E$, alors $\overline{[E:K]} = \overline{[E:L]} \times \overline{[L:K]}$.

Démonstration Soit N une clôture normale de E. Pour tout K-isomorphisme σ de L dans N, on note J_σ l'ensemble de tous les K-isomorphismes de E dans N qui prolongent σ. Si $\overline{\sigma} \in J_\sigma$, alors $\overline{\sigma}(E)$ est un corps intermédiaire entre $\sigma(L)$ et N. Soit I_σ l'ensemble des tous les $\sigma(L)$-isomorphismes de $\overline{\sigma}(E)$ dans N. Nous allons prouver que I_σ et J_σ ont le même cardinal. Considérons l'application $f; I_\sigma \longrightarrow J_\sigma$ définie par $f(u) = u \circ \overline{\sigma}$. Il est facile de voir que f est injective. Elle est aussi surjective; car si $u' \in J_\sigma$, u' peut s'écrire sous la forme $u' = f\left(u' \circ \overline{\sigma}^{-1}\right)$, car $\overline{\sigma}$ peut être regardé comme un isomorphisme de E sur $\overline{\sigma}(E)$. Or, nous avons $Card\,(I_\sigma) = \overline{[\overline{\sigma}(E):\sigma(L)]}$ et, d'après le théorème précédent, $\overline{[\overline{\sigma}(E):\sigma(L)]} = \overline{[E:L]}$. D'où $Card\,(I_\sigma) = \overline{[E:L]}$. Pour terminer la démonstration, remarquons que (J_σ) est une partition de l'ensemble J des tous les K-isomorphismes de E dans N. Ainsi, nous avons

$$\begin{aligned}\overline{[E:K]} &= Card\,(J) = \sum_\sigma Card\,(J_\sigma) = \sum_\sigma Card\,(I_\sigma) \\ &= \sum_\sigma \overline{[E:L]} = \overline{[E:L]} \times \overline{[L:K]}\end{aligned}$$

Théorème Si $E = K(a)$, alors $\overline{[E:K]}$ est le nombre des racines distinctes de $Irr\,(a,K)$.

Démonstration Soit N une clôture normale de E, I l'ensemble des tous les K-isomorphismes de E dans N et A l'ensemble des racines distinctes de $Irr\,(a,K)$ dans N. L'application de I dans A qui associe σ à $\sigma(a)$ est bijective. D'où $\overline{[E:K]} = Card\,(I) = Card\,(A)$.

Corollaire Si $E = K(a)$, alors $\overline{[E:K]} \leq [E:K]$.

Théorème Si E est une extension finie de K, alors $\overline{[E:K]} \leq [E:K]$.

Démonstration Comme E est une extension finie de K, elle s'écrit $E = K(a_1,...,a_n)$. Si $K_i = K(a_1,...,a_i)$, alors $K_i = K_{i-1}(a_i)$. Démontrons par récurrence sur i que $\overline{[K_i:K]} \leq [K_i:K]$. Pour $i = 1$, la propriété est vraie car nous avons

$$\overline{[K_1:K]} = \overline{[K(a_1):K]} \leq [K(a_1):K] = [K_1:K]$$

Supposons le propriété vraie pour i et démontrons-la pour $i+1$. Nous avons

$$\overline{[K_{i+1}:K]} = \overline{[K_{i+1}:K_i]} \times \overline{[K_i:K]} \leq [K_{i+1}:K_i] \times [K_i:K] = [K_{i+1}:K]$$

Par récurrence, nous obtenons

$$\overline{[E:K]} = \overline{[K_n:K]} \leq [K_n:K] = [E:K]$$

6.2 Extensions Séparables

Soit E une extension de K.

Définition L'extension E de K sera dite **séparable** si, et seulement si, $\overline{[E:K]} = [E:K]$.

Exemple $\mathbb{C}$ est une extension séparable de $\mathbb{R}$.

Définition Un élément a d'une extension E de K sera dit séparable sur K si, et seulement si, toutes les racines de $Irr(a,K)$ sont simples.

Exemple i est séparable sur $\mathbb{R}$. $\sqrt{2}$ séparable sur $\mathbb{Q}$.

Théorème Une extension simple $E = K(a)$ est séparable si, et seulement si, a est séparable sur K.

Démonstration Soit $[E:K]=n=\deg(Irr(a,k))$. Nous avons

$$\begin{aligned}[E \text{ est séparable sur } K] &\Longleftrightarrow \left[\overline{[E:K]}=[E:K]\right]\\ &\Longleftrightarrow [Irr(a,K) \text{ possède } n \text{ racines distinctes}]\\ &\Longleftrightarrow [\text{toute racine de } Irr(a,K) \text{ est simple}]\\ &\Longleftrightarrow [a \text{ est séparable sur } K]\end{aligned}$$

Théorème Une extension finie E de K est séparable si, et seulement si, tout élément a de E est séparable sur K.

Démonstration Si E est séparable sur K, Alors nous avons

$$\begin{aligned}\overline{[E:K(a)]}\times\overline{[K(a):K]}&=\overline{[E:K]}=[E:K]\\ &=[E:K(a)]\times[K(a):K]\end{aligned}$$

Or

$$\overline{[E:K(a)]}\leq[E:K(a)] \text{ et } \overline{[K(a):K]}\leq[K(a):K]$$

D'où

$$\overline{[E:K(a)]}=[E:K(a)] \text{ et } \overline{[K(a):K]}=[K(a):K]$$

et a est séparable sur K. Réciproquement, E s'écrit $E=K(a_1,...,a_n)$ car elle est une extension finie de K. Posons $K_i=K(a_1,...,a_i)$. Nous avons $K_i=K_{i-1}(a_i)$, $Irr(a_i,K_{i-1})$ divise $Irr(a_i,K)$ et a_i est séparable sur K. Il en résulte que a_i est séparable sur K_{i-1} et $\overline{[K_i:K_{i-1}]}=[K_i:K_{i-1}]$ pour $i=1,2,...,n$. Il en résulte

$$\overline{[E:K]}=\prod_{i=1}^{i=n}[K_i:K_{i-1}]=[E:K]$$

ce qui prouve que E est séparable sur K.

Théorème de l'élément primitif Toute extension séparable finie E de K est simple.

Démonstration Il suffit de prouver que l'ensemble des corps intermédiaires entre K et E est fini. Soit $\mathcal{F}$ cet ensemble et I l'ensemble des tous les K-isomorphismes de E dans une clôture normale N. Soit $h;\mathcal{F}\longrightarrow P(I)$ l'application qui associe à $L\in\mathcal{F}$ le sous-ensemble de I défini par

$$\{\sigma\in I \quad / \quad \sigma(a)=a \text{ pour tout } a\in L\}.$$

Cette application est injective; car si $L \neq L'$, et si $a \in L - L'$, alors a est séparable sur K, ce qui prouve que a est séparable sur L'. D'où

$$\overline{[L'(a) : L']} = \left[L'(a) : L'\right] > 1.$$

Ce qui précède montre qu'il existe un L'-isomorphisme σ de $L'(a)$ dans N tel que $\sigma(a) \neq a$. Or σ peut être prolongé en un K-automorphisme $\overline{\sigma}$ de N car N est une clôture normale. La restriction σ^* de $\overline{\sigma}$ à E est un K-isomorphisme de E dans N qui vérifie $\sigma^*(a) = \overline{\sigma}(a) = \sigma(a) \neq a$. Il en résulte $\sigma^* \in h(L')$ et $\sigma^* \notin h(L)$ qui prouve $h(L) \neq h(L')$. Pour finir la démonstration, notons que l'ensemble $P(I)$ des parties de I est fini car I est fini.

Chapitre 7

Les correspondances de Galois

7.1 Groupe de Galois

Soit E une extension normale finie d'un corps K. L'ensemble des K-automorphismes de E forment un groupe pour la composition d'application.

Définition Le groupe de tous les K-automorphismes de E sera appelé le groupe de Galois de l'extension E de K.

Exemple $\mathbb{C}$ est une extension normale finie de $\mathbb{R}$. Son groupe de Galois possède deux éléments : l'identité et le $\mathbb{R}$-automorphisme σ qui associe à chaque nombre complexe z son conjugué $\overline{z}$.

Le groupe de Galois d'une extension E de K sera noté $G(E/K)$.

Théorème $G(E/K)$ est un groupe fini dont l'ordre est le degré galoisien $\overline{[E:K]}$ de l'extension.

Démonstration $G(E/K)$ est l'ensemble I de tous les K-isomorphismes de E dans une clôture normale de E. Or E est sa propre clôture normale car elle est une extension normale de K. D'où $G(E/K) = I$.

Corollaire $Ord\,(G(E/K)) \leq [E:K]$.

7.2 Les correspondance de Galois

Sot E une extension finie de K.

Définition L'extension E de K sera dite une **extension galoisienne** si, et seulement si, E est une extension normale et séparable de K.

Exemple $\mathbb{C}$ est une extension galoisienn de $\mathbb{R}$.

Théorème Si E est une extension galoisienne de K, alors

$$Ord\left(G\left(E/K\right)\right) = \left[E : K\right].$$

Démonstration Nous avons $Ord\left(G\left(E/K\right)\right) = \overline{\left[E : K\right]} = \left[E : K\right]$.

Soit $G\left(E/K\right)$ le groupe de Galois d'une extension galoisienne finie E de K, $\mathcal{C}$ l'ensemble des corps intermédiaires entre K et E et $\mathcal{H}$ l'ensemble des sous-groupes de $G\left(E/K\right)$. Pour tout $L \in \mathcal{C}$, on pose

$$S\left(L\right) = \left\{u \in G\left(E/K\right) \quad / \quad \left(\forall x \in L\right)\left[u\left(x\right) = x\right]\right\}$$

et pour tout $H \in \mathcal{H}$

$$I\left(H\right) = \left\{x \in E \quad / \quad \left(\forall u \in H\right)\left[u\left(x\right) = x\right]\right\}$$

Il est facile de prouver que $S(L)$ est un sous-groupe de $G\left(E/K\right)$ et $I(H)$ est un corps intermédiaire entre K et E. Ainsi, nous avons deux applications $S; \mathcal{C} \longrightarrow \mathcal{H}$ et $I; \mathcal{H} \longrightarrow \mathcal{C}$. Ces deux applications sont visiblement décroissantes.

Théorème Pour tout $L \in \mathcal{C}$, E est une extension galoisienne finie de L et $G\left(E/L\right) = S\left(L\right)$.

Démonstration E, étant une extension normale de K, elle est le corps des racines pour un polynôme $P \in K\left[X\right]$ sur K. E est aussi un corps des racines pour P sur L. Donc, E est une extension normale de L. D'un autre côté, tout élément $a \in E$ est séparable sur K. Ceci prouve que toutes les racines de $Irr\left(a,K\right)$ sont simples. Il en résulte que $Irr\left(a,L\right)$ (qui divise $Irr\left(a,K\right)$) possède la même propriété. On en déduit que E est une extension séparable de L et par suite une extension galoisienne de L. Enfin, $G\left(E/L\right)$ est l'ensemble des L-automorphismes de E.

Théorème $S \circ I = id_{\mathcal{H}}$.

Démonstration Nous avons à prouver $\left(S \circ I\right)\left(H\right) = S\left(I\left(H\right)\right) = H$ pour tout $H \in \mathcal{H}$. Soit $L = I\left(H\right)$ et $H' = S\left(L\right) = \left(S \circ I\right)\left(H\right)$. Alors $H' = G\left(E/L\right)$ et $H \subseteq H'$. D'un autre côté, soit $H = \left\{\sigma_1,\ldots,\sigma_n\right\}$ et a un élément primitif de l'extension E de K. Nous avons $E = K\left(a\right) = L\left(a\right)$. Le polynôme $P = \prod_{i=1}^{i=n}\left(X - \sigma_i\left(a\right)\right)$ appartient à

$L[X]$, en effet

$$\widehat{\sigma}(P)=\prod_{i=1}^{i=n}(X-(\sigma\circ\sigma_i)(a))=P$$

pour tout $\sigma\in H$, car $\{\sigma_1,\ldots,\sigma_n\}=H=\{\sigma\circ\sigma_1,\ldots,\sigma\circ\sigma_n\}$ (H est un groupe). Nous avons

$$\begin{aligned}[P(a)=0]&\Longrightarrow[Irr(a,L)/P]\\&\Longrightarrow\left[\begin{array}{c}Ord(H')=[E:L]=\deg(Irr(a,L))\\\leq\deg(P)=n=Ord(H)\end{array}\right]\end{aligned}$$

Or H est un sous-groupe du groupe fini H'. D'où $Ord(H)\leq Ord(H')$ et par suite $H=H'$, car H' est un groupe fini.

Théorème $I\circ S=id_{\mathcal{C}}$.

Démonstration Soit L un élément de $\mathcal{C}$. Posons $H=S(L)$ et $L'=I(H)=(I\circ S)(L)$. Nous avons $L\subseteq L'$. D'un autre côté, si $b\in L'$, alors b est laissé fixe par tout élément de $H=S(L)=G(E/L)$. Toutes les racines de $Irr(b,L)$ sont simples, car $Irr(b,L)$ divise $Irr(b,K)$ et b est séparable sur K. Or, si b' est une autre racine de $Irr(b,L)$, il existe un L-isomorphisme de $L(b)$ dans E qui transforme b en b'. Ce L-isomorphisme peut être prolongé en un L-automorphisme σ de E. On en déduit qu'il existe $\sigma\in G(E/L)=H$ tel que $\sigma(b)=b'\neq b$ ce qui prouve $b\notin L'$ en contradiction avec le choix de b. Il en résulte que b est l'unique racine de $Irr(b,L)$ et par suite $b\in L$. Donc $L=L'$.

Corollaire L'application de $\mathcal{C}$ dans $\mathcal{H}$ qui associe à L l'élément $G(E/L)$ est une bijection décroissante.

Théorème Si $K\subseteq L\subseteq E$, alors nous avons : L est une extension normale de K si, et seulement si, $G(E/L)$ est un sous-groupe distingué de $G(E/K)$.

Démonstration Soit $\sigma\in G(E/K)$. Nous avons $\sigma(x)\in L$ pour tout $x\in L$ car L est une extension normale de K. Il en résulte

$$\left(\sigma^{-1}\circ\tau\circ\sigma\right)(x)=\sigma^{-1}(\tau(\sigma(x)))=\sigma^{-1}(\sigma(x))=x$$

pour tout $\tau\in G(E/L)$. Ainsi, $\sigma^{-1}\circ\tau\circ\sigma\in G(E/L)$ pour tout $\tau\in G(E/L)$, ce qui prouve que ce sous-groupe de $G(E/K)$ est distingué. Réciproquement, si $G(E/L)$ est un sous-groupe distingué de $G(E/K)$, alors tout K-isomorphisme τ de L dans E est un K-automorphisme de L : τ peut être prolongé en un K-automorphisme $\overline{\tau}$ de E et $\overline{\tau}^{-1}\circ\sigma\circ\overline{\tau}\in G(E/L)$ pour tout $\sigma\in G(E/L)$. Si $x\in L$,

alors $x=\left(\overline{\tau}^{-1}\circ\sigma\circ\overline{\tau}\right)(x)$ et $\overline{\tau}(x)=(\sigma\circ\overline{\tau})(x)$ pour tout $\sigma\in G(E/L)$. Il en résulte que $\overline{\tau}(x)\in L$ et $\tau(x)\in L$. D'où $\tau(L)\subseteq L$ et τ est un K-automorphisme de L ce qui prouve que L est une extension normale de K.

Théorème Soit L un corps intermédiaire, extension normale de K. Le groupe $G(L/K)$ est isomorphe au groupe quotient $G(E/K)/G(E/L)$.

Démonstration $G(E/L)$ est un sous-groupe distingué de $G(E/K)$, car L est une extension normale de K. Soit φ l'application de $G(E/K)$ dans $G(L/K)$ qui associe à σ sa restriction à L. C'est une application de $G(E/K)$ dans $G(L/K)$ car la restriction de σ à L est un K-isomorphisme de L dans E et par suite un K-automorphisme de L, car L est une extension normale de K. L'application φ est surjective, car tout $\alpha\in G(L/K)$, étant un K-isomorphisme de L dans E, peut être prolongé en un K-automorphisme $\overline{\sigma}$ de E. Finalement, φ est un homomorphisme de groupes et son noyau est $G(L/K)$, d'où $G(E/K)/G(E/L)\approx G(L/K)$.

7.3 EXEMPLE

Soit R le corps des racine du polynôme $X^4-2\in\mathbb{Q}[X]$ sur $\mathbb{Q}$. Nous avons $R=\mathbb{Q}\left(i,\sqrt[4]{2}\right)$.

Degré de R sur $\mathbb{Q}$: Nous avons $[R:\mathbb{Q}]=\left[R:\mathbb{Q}\left(\sqrt[4]{2}\right)\right]\left[\mathbb{Q}\left(\sqrt[4]{2}\right):\mathbb{Q}\right].\left[\mathbb{Q}\left(\sqrt{2}\right):\mathbb{Q}\right]=4$, car X^4-2 est irréductible dans $\mathbb{Q}[X]$. $\left[R:\mathbb{Q}\left(\sqrt[4]{2}\right)\right]=2$, car $Irr\left(i,\mathbb{Q}\left(\sqrt[4]{2}\right)\right)=X^2+1$. D'où $[R:\mathbb{Q}]=8$.

Groupe $G(R/\mathbb{Q})$: Si $\sigma\in G(R/\mathbb{Q})$, alors

- $\sigma(i)$ est une racine de X^2+1. Donc $\sigma(i)=\pm i$.
- $\sigma\left(\sqrt[4]{2}\right)$ est une racine de X^4-2. Donc

$$\sigma\left(\sqrt[4]{2}\right)=\pm\sqrt[4]{2}$$

ou

$$\sigma\left(\sqrt[4]{2}\right)=\pm i\sqrt[4]{2}$$

.

Or σ est complètement déterminé par son action sur i et $\sqrt[4]{2}$ car ces éléments engendrent R sur $\mathbb{Q}$. Il en résulte que le groupe de Galois de l'extension R de $\mathbb{Q}$

est

Groupe de Galois de l'extension de $R/\mathbb{Q}$

	σ_1	σ_2	σ_3	σ_4	σ_5	σ_6	σ_7	σ_8
$\sigma(i)$	i	i	i	i	$-i$	$-i$	$-i$	$-i$
$\sigma\left(\sqrt[4]{2}\right)$	$\sqrt[4]{2}$	$-\sqrt[4]{2}$	$i\sqrt[4]{2}$	$-i\sqrt[4]{2}$	$\sqrt[4]{2}$	$-\sqrt[4]{2}$	$i\sqrt[4]{2}$	$-i\sqrt[4]{2}$

La loi de composition de ce groupe est définie par le tableau suivant

$\circ$	σ_1	σ_2	σ_3	σ_4	σ_5	σ_6	σ_7	σ_8
σ_1	σ_1	σ_2	σ_3	σ_4	σ_5	σ_6	σ_7	σ_8
σ_2	σ_2	σ_1	σ_4	σ_3	σ_6	σ_5	σ_8	σ_7
σ_3	σ_3	σ_4	σ_2	σ_1	σ_7	σ_8	σ_6	σ_5
σ_4	σ_4	σ_3	σ_1	σ_2	σ_8	σ_7	σ_5	σ_6
σ_5	σ_5	σ_6	σ_8	σ_7	σ_1	σ_2	σ_4	σ_3
σ_6	σ_6	σ_5	σ_7	σ_8	σ_2	σ_1	σ_3	σ_4
σ_7	σ_7	σ_8	σ_5	σ_6	σ_3	σ_4	σ_1	σ_2
σ_8	σ_8	σ_7	σ_6	σ_5	σ_4	σ_3	σ_2	σ_1

Sous-groupes de $G(R/\mathbb{Q})$:

- Sous-groupe d'ordre 1 : $\{\sigma_1\}$
- Sous-groupe d'ordre 2 : $A = \{\sigma_1,\sigma_2\}$, $B = \{\sigma_1,\sigma_5\}$, $C = \{\sigma_1,\sigma_6\}$, $D = \{\sigma_1,\sigma_7\}$ et $E = \{\sigma_1,\sigma_8\}$.
- Sous-groupe d'ordre 4 : $F = \{\sigma_1,\sigma_2,\sigma_3,\sigma_4\}$, $G = \{\sigma_1,\sigma_2,\sigma_5,\sigma_6\}$ et $H = \{\sigma_1,\sigma_2,\sigma_7,\sigma_8\}$.
- Sous-groupe d'ordre : $G(R/\mathbb{Q})$.

Diagramme des sous-groupes :

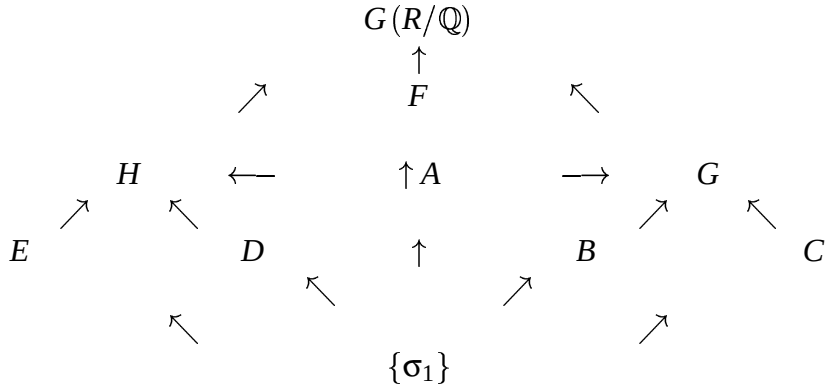
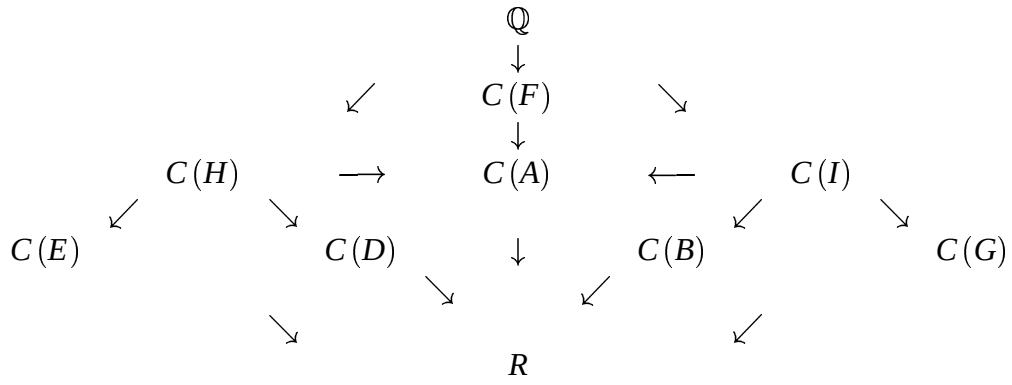


Diagramme des corps intermédiaires :



où $C(M)$ est le corps intermédiaire associé au sous-groupe M de $G(R/\mathbb{Q})$. Pour déterminer ces corps intermédiaires, on considère une base du $\mathbb{Q}$-espace vectoriel R exprimée en termes de i et $\sqrt[4]{2}$. Nous avons la base

$$\left\{1,\sqrt[4]{2},\left(\sqrt[4]{2}\right)^2,\left(\sqrt[4]{2}\right)^3,i,i\sqrt[4]{2},i\left(\sqrt[4]{2}\right)^2,i\left(\sqrt[4]{2}\right)^3\right\}$$

obtenue en multipliant terme à terme la base $\left\{1,\sqrt[4]{2},\left(\sqrt[4]{2}\right)^2,\left(\sqrt[4]{2}\right)^3\right\}$ de l'extension $\mathbb{Q}\left(\sqrt[4]{2}\right)$ de $\mathbb{Q}$ et la base $\{1,i\}$ de l'extension R de $\mathbb{Q}\left(\sqrt[4]{2}\right)$. Un élément $x\in R$ s'écrit, d'une manière unique, sous la forme

$$x=b_0+b_1\sqrt[4]{2}+b_2\left(\sqrt[4]{2}\right)^2+b_3\left(\sqrt[4]{2}\right)^3c_0i+c_1i\sqrt[4]{2}+c_2i\left(\sqrt[4]{2}\right)^2+c_3i\left(\sqrt[4]{2}\right)^3$$

Pour déterminer $C(A)$, on utilise l'équivalence

$$[x\in C(A)]\Longleftrightarrow[\sigma_2(x)=x]$$

Or

$$\sigma_2(x)=b_0-b_1\sqrt[4]{2}+b_2\left(\sqrt[4]{2}\right)^2-b_3\left(\sqrt[4]{2}\right)^3c_0i-c_1i\sqrt[4]{2}+c_2i\left(\sqrt[4]{2}\right)^2-c_3i\left(\sqrt[4]{2}\right)^3$$

Donc

$$\begin{aligned}[x\in C(A)]&\Longleftrightarrow[\sigma_2(x)=x]\Longleftrightarrow[b_1=b_3=c_1=c_3=0]\\&\Longleftrightarrow\left[x\in\mathbb{Q}\left(i,\left(\sqrt[4]{2}\right)^2\right)\right]\end{aligned}$$

et $C(A)=\mathbb{Q}\left(i,\left(\sqrt[4]{2}\right)^2\right)=\mathbb{Q}\left(i,\sqrt{2}\right)$. D'une manière analogue, on détermine les autres corps intermédiaires Les résultats sont résumés dans le tableau suivant :

Sous-groupe	Corps intermédiaire associé
A	$\mathbb{Q}\left(i,\sqrt{2}\right)$
B	$\mathbb{Q}\left(\sqrt[4]{2}\right)$
C	$\mathbb{Q}\left(i\sqrt[4]{2}\right)$
D	$\mathbb{Q}\left((1+i)\sqrt[4]{2}\right)$
E	$\mathbb{Q}\left((1-i)\sqrt[2]{2}\right)$
F	$\mathbb{Q}(i)$
H	$\mathbb{Q}\left(i\sqrt{2}\right)$
I	$\mathbb{Q}\left(\sqrt{2}\right)$

Sous-groupes distingués de $G(R/\mathbb{Q})$: Les sous-groupes d'ordre 4 sont distingués. A est la seule sous-groupe distingué d'ordre 2.

Extensions normale de $\mathbb{Q}$: Les corps intermédiaires qui sont des extensions normales de $\mathbb{Q}$ sont ceux associés aux sous-groupes distingués de $G(R/\mathbb{Q})$. Ces corps sont : $\mathbb{Q}(i)$, $\mathbb{Q}\left(\sqrt{2}\right)$, $\mathbb{Q}\left(i\sqrt{2}\right)$ and $\mathbb{Q}\left(i,\sqrt{2}\right)$.

Chapitre 8

Compléments sur les groupes

8.1 Quelques théorèmes

Soit $f; G \longrightarrow G'$ un homomorphisme de groupes surjectif. Nous allons désigner par $S(G')$ l'ensemble des sous-groupes de G' et par $S_f(G)$ celui des sous-groupes de G contenant $Ker(f)$.

Théorème Il existe une bijection de $S(G')$ sur $S_f(G)$.

Démonstration Soit φ l'application de $S(G')$ dans $S_f(G)$ qui associe à H' le sous-groupe $f^{-1}(H')$ de G. φ est injective, car nous avons

$$\begin{aligned}\left[\varphi(H') = \varphi(K')\right] &\Longrightarrow \left[f^{-1}(H') = f^{-1}(K')\right] \\ &\Longrightarrow \left[f\left(f^{-1}(H')\right) = f\left(f^{-1}(K')\right)\right] \\ &\Longrightarrow \left[H' = K'\right]\end{aligned}$$

vu que f est surjective. D'un autre côté, si $H \in S_f(G)$, alors

$$H' = f(H) \in S(G') \text{ et } \varphi(H') = f^{-1}(H') = H$$

car nous avons

$$\begin{aligned}\left[x \in f^{-1}(f(H))\right] &\Longrightarrow \left[f(x) \in f(H)\right] \\ &\Longrightarrow (\exists y \in H)\left[f(x) = f(y)\right] \\ &\Longrightarrow \left[x - y \in Ker(f) \subseteq H\right] \\ &\Longrightarrow \left[x \in H\right]\end{aligned}$$

D'où $f^{-1}(f(H)) \subseteq H$. L'autre inclusion est évidente. Ainsi φ est surjective.

Théorème La bijection φ est croissante.

Démonstration Si $H' \subseteq K'$, alors

$$\begin{aligned}\left[x \in \varphi\left(H'\right)\right] &\Longrightarrow \left[x \in f^{-1}\left(H'\right)\right] \\ &\Longrightarrow \left[f(x) \in H'\right] \\ &\Longrightarrow \left[f(x) \in K'\right] \\ &\Longrightarrow \left[x \in f^{-1}\left(K'\right) = \varphi\left(K'\right)\right]\end{aligned}$$

D'où $\varphi(H') \subseteq \varphi(K')$.

Théorème H' est un sous-groupe distingué de G' si, et seulement si, le sous-groupe $H = \varphi(H')$ de G est distingué.

Démonstration Si H' est un sous-groupe distingué de G', alors nous avons

$$\begin{aligned}[x \in G, y \in H] &\Longrightarrow \left[f(x) \in G',\ f(y) \in H'\right] \\ &\Longrightarrow \left[f\left(x^{-1}yx\right) = f(x)^{-1} f(y) f(x) \in H'\right] \\ &\Longrightarrow \left[x^{-1}yx \in f^{-1}\left(H'\right) = H\right]\end{aligned}$$

Réciproquement, si le sous-groupe H de G est distingué, alors H' est un sous-groupe distingué de G'. En effet, si $x' \in G'$ et $y' \in H'$, alors il existe $x \in G$ et $y \in H$ tels que $x' = f(x)$ et $y' = f(y)$ ($H' = f\left(f^{-1}(H')\right) = f(H)$ car f est surjective). Nous avons

$$\left(x'\right)^{-1} y' x' = f(x)^{-1} f(y) f(x) = f\left(x^{-1}yx\right) \in f(H) = H'$$

car $x^{-1}yx \in H$.

Théorème Si H' est distingué dans G' et $H = \varphi(H')$, alors G'/H' est isomorphe à G/H.

Démonstration L'application

$$g; G \xrightarrow{f} G' \xrightarrow{p'} G'/H'$$

où p' est la surjection canonique qui est un homomorphisme de groupes. Il est surjectif et son noyau est H car

$$[x \in Ker(g)] \Longleftrightarrow \left[p'(f(x)) = g(x) = \overline{e'}\right] \Longleftrightarrow \left[f(x) \in H'\right] \Longleftrightarrow [x \in H]$$

D'où $G'/H' = \mathrm{Im}(g) \simeq G/H$.

8.2 Chaînes normales

Soient G_1 et G_2 deux sous-groupes de G tels que $G_1 \subseteq G_2$.

Définition On appelle **chaîne normale** de G entre G_2 et G_1 toute chaîne de sous-groupes de G

$$G_1 = H_0 \subseteq H_1 \subseteq \cdots \subseteq H_n = G_2$$

telle que chaque H_i soit un sous-groupe distingué de son successeur H_{i+1}.

Les groupes quotients $F_i = H_{i+1}/H_i$ pour $i = 0,1,...,n-1$ sont appelés les **facteurs** de la chaîne.

Définition On appelle **chaîne normale** du groupe G toute chaîne normale de G entre $\{e\}$ et G.

Exemple Soit S_3 le groupe des permutations de l'ensemble $\{1,2,3\}$ et A_3 le groupe alterné d'ordre 3. La chaîne

$$\{i\} \subseteq A_3 \subseteq S_3$$

est une chaîne normale du groupe S_3.

Théorème Si $f; G \longrightarrow G'$ est un homomorphisme surjectif, alors f transforme toute chaîne normale

$$\{e\} = H_0 \subseteq H_1 \subseteq \cdots \subseteq H_n = G$$

de G en une chaîne normale

$$\left\{e'\right\} = H'_0 \subseteq H'_1 \subseteq \cdots \subseteq H'_n = G'$$

de G' et il existe un homomorphisme surjectif u_i du facteur $F_i = H_{i+1}/H_i$ sur le facteur $F'_i = H'_{i+1}/H'_i$ pour $i = 0,1,...,n-1$.

Démonstration L'homomorphisme f transforme la chaîne

$$\{e\} = H_0 \subseteq H_1 \subseteq \cdots \subseteq H_n = G$$

en la chaîne

$$\left\{e'\right\} = H'_0 \subseteq H'_1 \subseteq \cdots \subseteq H'_n = G'$$

où $H'_i = f(H_i)$ pour $i = 0,1,...,n-1$. Cette chaîne est normale, car l'image d'un sous-groupe distingué par un homomorphisme surjectif est un sous-groupe distingué. D'un autre côté, L'application u_i définie par

$$u_i(p_i(x)) = p'_i(f(x))$$

est bien définie, car nous avons

$$\begin{aligned}[p_i(x)=p_i(y)] &\Longrightarrow \left[xy^{-1}\in H_i\right]\\ &\Longrightarrow \left[f(x)\,f(y)^{-1}=f\left(xy^{-1}\right)\in f(H_i)=H_i'\right]\\ &\Longrightarrow \left[p_i'(f(x))=p_i'(f(y))\right]\end{aligned}$$

où p_i et p_i' sont les surjections canoniques. Il est facile de vérifier que u_i est un homomorphisme de groupes surjectif.

Théorème Si $f;G\longrightarrow G'$ est un homomorphisme injectif, alors toute chaîne normale

$$\left\{e'\right\}=H_0'\subseteq H_1'\subseteq\cdots\subseteq H_n'=G'$$

de G' est transformée par f^{-1} en une chaîne normale

$$\{e\}=H_0\subseteq H_1\subseteq\cdots\subseteq H_n=f^{-1}(G)=G$$

de $f^{-1}(G)$ et il existe un homomorphisme injectif v_i du facteur $F_i=H_{i+1}/H_i$ dans le facteur $F_i'=H_{i+1}'/H_i'$ pour $i=0,1,...,n-1$.

Démonstration Soit $H_i=f^{-1}(H_i')$ pour $i=0,1,...,n-1$. Les sous-groupes H_i de G forment une chaîne

$$\{e\}=H_0\subseteq H_1\subseteq\cdots\subseteq H_n=f^{-1}(G)=G$$

où $H_0=f^{-1}\left(H_0'\right)=f^{-1}(e')=Ker(f)=\{e\}$. Cette chaîne est normale car nous avons

$$\begin{aligned}[x\in H_{i+1},\,y\in H_i] &\Longrightarrow \left[f(x)\in H_{i+1}',\,f(y)\in H_i'\right]\\ &\Longrightarrow \left[f\left(x^{-1}yx\right)=f(x)^{-1}f(y)\,f(x)\in H_i'\right]\\ &\Longrightarrow \left[x^{-1}yx\in H_i\right]\end{aligned}$$

L'application v_i est définie comme l'application u_i du théorème précédent. C'est un homomorphisme de groupes. Il est injectif car nous avons

$$\begin{aligned}\left[v_i(p_i(x))=\overline{e'}\right] &\Longrightarrow \left[p_i'(f(x))=\overline{e'}\right]\\ &\Longrightarrow \left[f(x)\in H_i'\right]\\ &\Longrightarrow \left[x\in f^{-1}\left(H_i'\right)=H_i\right]\\ &\Longrightarrow \left[p_i(x)=\overline{e}\right]\end{aligned}$$

Théorème Si chaque facteur d'une chaîne normale de G possède une chaîne normale, alors nous obtenons une chaîne normale de G en concaténant les différentes chaînes des facteurs. Les facteurs de la nouvelle chaîne sont isomorphes aux facteurs des chaînes des différents facteurs.

Démonstration Soit

$$\{e\} = H_0 \subseteq H_1 \subseteq \cdots \subseteq H_n = G$$

une chaîne normale de G et soit

$$\{\overline{e}\} = K_{i,0} \subseteq K_{i,1} \subseteq \cdots \subseteq K_{i,n_i} = F_i$$

une chaîne normale du facteur F_i pour $i = 1,2,\ldots,n-1$. La surjection canonique $p_i; H_{i+1} \longrightarrow F_i$ transforme cette chaîne en une chaîne normale de G entre H_i et H_{i+1}

$$H_i = L_{i,0} \subseteq L_{i,1} \subseteq \cdots \subseteq L_{i,n_i} = H_{i+1}$$

où $L_{ij} = p_i^{-1}\left(K_{ij}\right)\ L_{i,j}/H_i \approx K_{i,j}$. Il en résulte que la chaîne

$$\begin{aligned}\{e\} = H_0 = L_{0,0} \subseteq L_{0,1} \subseteq \cdots \subseteq L_{0,n_0} = H_1 \subseteq \cdots \subseteq H_{n-1} \\ = L_{n-1,0} \subseteq L_{n-1,1} \subseteq \cdots \subseteq L_{n-1,n_i} = H_n = G\end{aligned}$$

est une chaîne normale de G. Il nous reste à prouver que le facteur $L_{i,j+1}/L_{i,j}$ est isomorphe au facteur $K_{i,j+1}/K_{i,j}$ et ceci pour $j = 0,1,\ldots,n_i-1$ et pour $i = 0,1,\ldots,n-1$. La restriction de p_i à $L_{i,j+1}$ est un homomorphisme surjectif de $L_{i,j+1}$ sur $K_{i,j+1}$. Le dernier théorème de la section précédente nous donne l'isomorphisme recherché (prendre $G' = K_{i,j+1}$, $H' = K_{i,j}$ et $H = L_{i,j}$).

8.3 Groupes résolubles

Définition On dit qu'un groupe G est résoluble si, et seulement si, il possède une chaîne normale dont les facteurs sont abéliens.

Exemple Le groupe S_3 est résoluble.

Théorème tout groupe abélien est résoluble.

Démonstration Il suffit de prendre la chaîne $\{e\} \subseteq G$.

Théorème Tout groupe cyclique est résoluble.

Démonstration Car un groupe cyclique est abélien.

Théorème Toute image par un homomorphisme d'un groupe résoluble est un groupe résoluble.

Démonstration Si G' est une image homomorphe du groupe résoluble G, alors il existe un homomorphisme surjectif $f; G \longrightarrow G'$. Si

$$\{e\} = H_0 \subseteq H_1 \subseteq \cdots \subseteq H_n = G$$

est une chaîne normale de G à facteurs abéliens, alors la chaîne

$$\left\{e'\right\} = H'_0 \subseteq H'_1 \subseteq \cdots \subseteq H'_n = G'$$

où $H'_i = f(H_i)$ pour $i = 0,1,...,n-1$ est normale et ses facteurs sont des images homomorphes de ceux de la chaîne de G (par l'homomorphisme u_i). Il en résulte que la chaîne G' est une chaîne normale à facteurs abélien. Ceci prouve que G' est résoluble.

Corollaire Tout groupe quotient d'un groupe résoluble est un groupe résoluble.

Démonstration En effet, un groupe quotient de G est une image homomorphe de G par la surjection canonique.

Théorème Si $f; G \longrightarrow G'$ est un homomorphisme injectif et si G' est résoluble, alors G est résoluble.

Démonstration Si G' est résoluble, alors il possède une chaîne normale

$$\left\{e'\right\} = H'_0 \subseteq H'_1 \subseteq \cdots \subseteq H'_n = G'$$

à facteurs abéliens. La chaîne

$$\{e\} = H_0 \subseteq H_1 \subseteq \cdots \subseteq H_n = G$$

où $H_i = f^{-1}(H'_i)$ pour $i = 0,1,...,n$ est une chaîne normale et il existe homomorphisme injectif $v_i; H_{i+1}/H_i \longrightarrow H'_{i+1}/H'_i$. Il en résulte que les facteurs de la chaîne

de G sont tous abéliens, ce qui prouve que G est résoluble.

Corollaire Tout sous-groupe K d'un groupe résoluble est un groupe résoluble.

Démonstration Il suffit d'appliquer le théorème précédent à l'injection canonique.

Théorème Si G possède une chaîne normale dont les facteurs sont des groupes résolubles, alors G est résoluble.

Démonstration Soit

$$\{e\} = H_0 \subseteq H_1 \subseteq \cdots \subseteq H_n = G$$

une chaîne normale de G telle que tous les facteurs $F_i = H_{i+1}/H_i$ sont résolubles. Nous avons démontré que l'on peut utiliser ces chaînes normales des facteurs pour construire une chaîne normale de G dont les facteurs sont isomorphes aux facteurs des différentes chaînes normales des facteurs. Mais les chaînes des F_i peuvent être choisies à facteurs abéliens, il en résulte que les facteurs de la chaîne concaténée sont tous abéliens et G est résoluble.

Théorème Soit H un sous-groupe distingué de G. G est résoluble si, et seulement si, H et G/H sont résolubles.

Démonstration Si G est résoluble, alors H et G/H sont résolubles comme nous l'avons vu. Réciproquement, si H et G/H sont résolubles, alors

$$\{e\} \subseteq H \subseteq G$$

est une chaîne normale de G dont les facteurs $F_1 = H/\{e\} \approx H$ et $F_2 = G/H$ sont résolubles. Il en résulte que G est résoluble.

Dans la suite, nous allons prouver que G est résoluble si, et seulement si, G possède une chaîne normale dont les facteurs sont des groupes cycliques d'ordres premiers. Il est clair que si G satisfait cette condition, alors G est résoluble. Pour démontrer la réciproque, nous démontrons les théorèmes préliminaires suivants :

Théorème Si p est un facteur premier de l'ordre d'un groupe cyclique fini G, alors G possède un élément d'ordre p.

Démonstration Si a est un générateur de G, alors l'élément $b = a^{\frac{n}{p}}$ est d'ordre p, car $b^p = e$ et p est premier.

Théorème Si p est un facteur premier de l'ordre d'un groupe abélien fini G, alors G possède un élément d'ordre p.

Démonstration Par récurrence sur l'ordre n de G. Si $n = 1$, le théorème est vrai. Supposons le théorème vrai pour tous les groupes finis d'ordre $< n$ et démontrons-le pour les groupes finis d'ordre n. Soit G un tel groupe. Si G est cyclique, alors on est ramené au théorème précédent. Sinon, G possède un élément h d'ordre m tel que $1 < m < n$. Soit $H = gr(h)$. Le groupe quotient G/H est d'un ordre $< n$. Deux cas sont possibles :

1. p divise m : dans ce cas, p divise l'ordre du groupe H qui est d'ordre $m < n$. Ainsi H contient un élément d'ordre p.
2. p ne divise pas m : p divise l'ordre de G/H car $n = m \times ord(G/H)$ et p est premier. Il existe $\overline{y} \in G/H$ d'ordre p. L'élément $x = y^m$ vérife $x \neq e$ (sinon $\overline{y}^m = \overline{e}$ et p divise $m = Ord(\overline{y})$) et $x^p = (y^m)^p = (y^p)^m = e$ car $y^p \in H$ ($\overline{y}^p = \overline{e}$) et m est l'ordre de H. On en déduit que p est l'ordre de x car p est premier.

Corollaire Si G est un groupe abélien fini d'ordre non premier, alors G possède un sous-groupe propre.

Démonstration Si p est un facteur premier de l'ordre de G, alors G possède un élément d'ordre p. Le sous-groupe $H = gr(a)$ est un sous-groupe propre de G.

Théorème Si G est un groupe résoluble, alors G possède une chaîne normale dont les facteurs sont des groupes cycliques d'ordres premiers.

Démonstration Soit

$$\{e\} = H_0 \subseteq H_1 \subseteq \cdots \subseteq H_n = G$$

une chaîne normale à facteurs abéliens. Nous supposons que cette chaîne est la plus longue des chaînes normales de G à facteurs abéliens. Si un facteur F_i n'était pas un groupe cyclique d'ordre premier, alors F_i possède un sous-groupe propre et G possède un sous-groupe H tel que $H_i \subseteq H \subseteq H_{i+1}$. H est distingué dans H_{i+1}, car si $x \in H_{i+1}$ et $y \in H$, alors $\overline{x}^{-1}\overline{yx} = \overline{y}$ (F_i est abélien). Il en résulte $x^{-1}yxy^{-1} \in H_i \subseteq H$ et $x^{-1}yx = \left(x^{-1}yxy^{-1}\right)y \in H$. D'un autre côté, H/H_i est abélien (sous-groupe de F_i) et H_{i+1}/H est abélien car nous avons

$$H_{i+1}/H \simeq (H_{i+1}/H_i) / (H/H_i)$$

et $(H_{i+1}/H_i)\,/\,(H/H_i)$ est abélien car c'est un quotient du groupe abélien F_i. Ainsi, si nous insérons H entre H_i et H_{i+1} nous obtenons une chaîne normale à facteurs abéliens plus longue que la plus longue des telles chaînes.

8.4 Groupe dérivé

Soit G un groupe distinct de $\{e\}$. Pour tout $(a,b) \in G \times G$, l'élément $a^{-1}b^{-1}ab$ sera noté $[a,b]$ et appelé le **commutateur** de a et b.

Théorème Les propriétés suivantes sont vraies :

1. $[G$ est abélien$] \Longleftrightarrow [[ab] = e$ pour tout $(a,b) \in G \times G]$.
2. L'inverse d'un commutateur est un commutateur.
3. Si c est un commutateur, alors $x^{-1}cx$ est un commutateur pour tout $x \in G$.

Démonstration Ces propriétés sont faciles à vérifier.

Définition Le sous-groupe de G engendré par tous les commutateurs $[a,b]$, $(a,b) \in G \times G$, sera appelé **groupe dérivé** du groupe G. Il sera noté G'.

Théorème Le groupe dérivé G' de G est l'ensemble des produits finis de commutateurs.

Démonstration Soit H l'ensemble des produits finis de commutateurs. H est un sous-groupe de G et il contient tous les commutateurs. Il est le plus petit sous-groupe de G qui contient tous les commutateurs car si un sous-groupe K de G contient tous les commutateurs, alors K contient tous les produits finie de commutateurs. Ainsi $H \subseteq K$ et $H = G'$.

Théorème Le groupe dérivé G' de G est un sous-groupe distingué de G.

Démonstration Car, si $y \in G'$, alors y est un produit fini de commutateurs, soit $y = c_1 \cdots c_t$. Il en résulte

$$x^{-1}yx = x^{-1}c_1 \cdots c_t x = \left(x^{-1}c_1x\right)\left(x^{-1}c_2x\right)\cdots\left(x^{-1}c_tx\right) \in G'$$

car le conjugué d'un commutateur est un commutateur.

Théorème Si H est un sous-groupe distingué de G, alors G/H est abélien si, et seulement si, $G' \subseteq H$.

Démonstration Si $c = a^{-1}b^{-1}ab$ est un commutateur, alors

$$\overline{c} = \overline{a^{-1}b^{-1}}\overline{a}\overline{b} = \overline{a}^{-1}\overline{b}^{-1}\overline{a}\overline{b} = \overline{e}.$$

Il en résulte $c \in H$ qui prouve $G' \subseteq H$. Réciproquement, si $G' \subseteq H$, alors nous avons pour tout $\left(\overline{a},\overline{b}\right) \in G/H \times G/H$

$$\overline{a}^{-1}\overline{b}^{-1}\overline{a}\overline{b} = \overline{a^{-1}b^{-1}}\overline{a}\overline{b} = \overline{a^{-1}b^{-1}ab} = \overline{e}$$

et par suite G/H est abélien.

Corollaire G/G' est abélien.

On définit, par récurrence, le **groupe dérivé d'ordre** i comme étant le groupe dérivé du groupe $G^{(i-1)}$: $G^{(i)} = \left(G^{(i-1)}\right)'$. On définit $G^{(0)}$ comme étant le grouep G. Nous avons :

Théorème Si G est un groupe résoluble, et si

$$G = G_0 \supseteq G_1 \supseteq \cdots \supseteq G_n = \{e\}$$

est une chaîne normale à facteurs abéliens, alors $G^{(i)} \subseteq G_i$ pour $i = 0,1,\ldots,n$.

Démonstration Par récurrence . Si $i = 0$, nous avons $G_0 = G = G^{(0)}$. Supposons avoir $G^{(i)} \subseteq G_i$. Nous avons $G^{(i+1)} = \left(G^{(i)}\right)' \subseteq G_i'$. Comme G_i/G_{i+1} est abélien, on a $G_i' \subseteq G_{i+1}$ et par suite

$$G^{(i+1)} = \left(G^{(i)}\right)' \subseteq G_i' \subseteq G_{i+1}.$$

Théorème G est résoluble si, et seulement si, $G^{(n)} = \{e\}$ pour certains n.

Démonstration Si G est résoluble et si

$$G = G_0 \supseteq G_1 \supseteq \cdots \supseteq G_n = \{e\}$$

est une chaîne normale à facteurs abéliens, alors $G^{(n)} \subseteq G_n = \{e\}$, d'où $G^{(n)} = \{e\}$. Réciproquement, si $G^{(n)} = \{e\}$ pour un entier naturel n, alors la chaîne

$$G = G^{(0)} \supseteq G' = G^{(1)} \supseteq \cdots \supseteq G^{(n)} = \{e\}$$

est une chaîne normale à facteurs abéliens car $G^{(i)}/G^{(i+1)}$ est abélien car $G^{(i+1)} = \left(G^{(i)}\right)'$. Ainsi G est résoluble.

Théorème Le groupe alterné A_n n'est pas résoluble pour $n \geq 5$.

Démonstration Nous allons démontrer que A_n' contient tous les cycles de longueur 3. Si (abc) est un tel cycle, alors

$$(abc) = (adc)(bec)(acd)(bce) = (acd)^{-1}(bce)^{-1}(acd)(bce) \in A_n'$$

où d et e des éléments distincts et distinct de a,b,c ($n \geq 5$). Il en résulte que A_n, engendré par les cycles de longueur 3, est égal à son groupe dérivé A_n'. Ceci prouve que A_n n'est pas résoluble pour $n \geq 5$, car son groupe dérivé de n'importe quel ordre est distinct de $\{i\}$.

Corollaire S_n n'est pas résoluble pour $n \geq 5$.

Démonstration Sinon, A_n serait résoluble.

Théorème S_n est résoluble pour $n \in \{1,2,3,4\}$.

Démonstration Ceci est claire pour $n = 1,2,3$. Pour $n = 4$, nous avons la chaîne

$$\{i\} \subseteq W \subseteq V \subseteq A_4 \subseteq S_4$$

où V est le groupe

$$V = \{i, (12)(34), (13)(24), (14)(23)\}$$

et W est un sous-groupe d'ordre 2 de V. Cette chaîne est normale. La seule vérification à faire est que V est un sous-groupe distingué de A_4. Mais V est distingué dans S_4. Ainsi la chaîne est normale. Les facteurs sont tous d'ordre 2 ou 3, ils sont abéliens. Il en résulte que S_4 est résoluble.

Chapitre 9

Résolubilité par des radicaux

9.1 Groupe de Galois d'un polynôme

Dans ce chapitre, tous corps considérés sont de caractéristique nulle. Soient K une corps et f un polynôme dans $K[X]$.

Définition On appelle **groupe de Galois** de f sur K le groupe de Galois $G(E/K)$ où E est un corps des racines pour f sur K. Il sera noté $G_K(f)$.

Lemme Soit $f \in K[X]$ et M une extension de K. Le groupe $G_M(f)$ est isomorphe à une sous-groupe de $G_K(f)$.

Démonstration Soit N un corps des racines pour f sur M. On a $N = M(a_1,\ldots,a_n)$ où $a_1,\ldots,a_n$ sont les racines de f dans N. Le corps $E = K(a_1,\ldots,a_n)$ est un corps de racines pour f sur K. Si $\sigma \in G(N/M)$, alors sa restriction à E est un $K-$automorphisme de E car E est une extension normale de K. Soit $\varphi; G(N/M) \longrightarrow G(E/K)$ l'application qui associe à chaque $\sigma \in G(N/M)$ sa restriction à E. φ est un homomorphisme de groupes. Il est injectif car si $\varphi(\sigma) = id_E$, alors $\sigma(a_i) = a_i$ pour tout i. Il en résulte $\sigma = id_M$. Ainsi $G(N/M)$ est isomorphe à $\mathrm{Im}(\varphi)$ qui est un sous-groupe de $G(E/K)$.

Soit $f \in K[X]$ et $L = K(a_1,\ldots,a_n)$ un corps des racines pour f sur K, où $a_1,\ldots,a_n$ sont les racines de f dans L. Tout $\sigma \in G(L/K)$ permute les racines de f. D'un autre côté, deux $K-$automorphismes σ et τ de L sont égaux si, et seulement si, $\sigma(a_i) = \tau(a_i)$ pour tout i. Ainsi le groupe de Galois de f peut être regardé comme un sous-groupe de du groupe des permutations de ses racines. Nous avons alors

Lemme Soit $f \in K[X]$. Le groupe de Galois de f sur K est isomorphe à un sous-groupe de S_n où n est le nombre des racines distinctes de f.

9.2 Polynômes résolubles et leurs groupes de Galois

Définition On dit qu'un polynôme $f \in K[X]$ est **résoluble par des radicaux** si, et seulement si, les racines de f dans un corps des racines peuvent être construites à partir des coefficients en un nombre fini d'étapes faisant intervenir les quatre opérations et l'extraction de racines $n^{ièmes}$ pour des entiers naturels appropriés n.

Il découle de cette définition, qu'un polynôme $f \in K[X]$ est résoluble par des radicaux si, et seulement si, il existe des corps K_0,K_1,...,K_m tels que $K_0 = K$, le polynôme f est scindé dans $K_m[X]$ et pour tout entier i entre1et m, le corps K_i est obtenu à partir du corps K_{i-1}, par l'adjonction d'un élément $\alpha_i \in K_i$ qui vérifie $\alpha_i^{p_i} \in K_{i-1}$ pour un certain entiers positif p_i. En plus, nous pouvons supposer les p_i premiers car si $n = p_1 p_2 \ldots p_{k-1} p_k$, où les p_i sont premiers, et si α est une racine $n^{ième}$ de a, on adjoint α en adjoignant successivement $\alpha^{p_1}, (\alpha^{p_1})^{p_2}, \ldots, (((\alpha^{p_1}))\ldots)^{p_k} = \alpha$.

On se propose de démontrer le résultat fondamental suivant

f est résoluble par radicaux si, et seulement si, son groupe de Galois $G_K(f)$ est résoluble.

Soit L un corps et p un nombre premier. Supposons le polynôme $X^p - 1$ scindé dans $L[X]$. Ce polynôme ne possède que des racines simples car aucune de ses racines n'est une racine commune avec le polynôme dérivé pX^{p-1}. Un élément $\omega \in L$ est une **racine $p^{ième}$ primitive** de l'unité si, et seulement si, $\omega \neq 1$ et est une racine du polynôme $X^p - 1$. Les racines $p^{ièmes}$ primitives de l'unité sont donc les racines du polynôme

$$X^{p-1} + X^{p-1} + \cdots + X + 1$$

De même, le groupe des racines $p^{ièmes}$ primitives de l'unité dans L forment un groupe cyclique engendré par n'importe laquelle de ces racines.

Lemme Soit K un corps et p un nombre premier. Si ω est une racine $p^{ième}$ primitive de l'unité dans une extension de K, alors le groupe de Galois de l'extension $K(\omega)$ de K est abélien.

Démonstration Soit $L = K(\omega)$ et soient σ,$\tau \in G(L/K)$. $\sigma(\omega)$ et $\tau(\omega)$ sont des racines du polynôme $X^p - 1$. Il existe deux entiers a et b tels que $\sigma(\omega) = \omega^a$

et $\tau(\omega)=\omega^b$. Il en résulte

$$\begin{aligned}(\sigma\circ\tau)(\omega)&=\sigma(\tau(\omega))=\sigma\left(\omega^b\right)=(\sigma(\omega))^b=(\omega^a)^b=\omega^{ab}\\&=\left(\omega^b\right)^a=(\tau(\omega))^a=\tau(\omega^a)=\tau(\sigma(a))=(\tau\circ\sigma)(a)\end{aligned}$$

ce qui prouve $\sigma\circ\tau=\tau\circ\sigma$ car $L=K(\omega)$.

Lemme Soit K un corps et M un corps des racines sur K pour le polynôme $X^p-c\in K[X]$ où p est un nombre premier. Le groupe de Galois de l'extension M de K est résoluble.

Démonstration Le résultat est trivial si c est nul. Supposons c non nul. Les racines du polynôme X^p-c sont toutes non nulles et distinctes car la seule racine de son polynôme dérivé est nulle. Si α est une racine de ce polynôme et si ω est une racine $p^{ième}$ primitive de l'unité, alors les racines de X^p-c sont $\alpha,\omega\alpha,\omega^2\alpha,...,\omega^{p-1}\alpha$. On a alors $M=K(\alpha,\omega)$. Le corps $K(\omega)$ est un corps intermédiaire et est une extension normale de K car c'est un corps de racines pour X^p-1 sur K. Il en résulte que le groupe $G(M/K(\omega))$ est un sous-groupe distingué du groupe $G(M/K)$ et que le groupe quotient $G(M/K)/G(M/K(\omega))$ est isomorphe à $G(K(\omega)/K)$. Or ce dernier est un groupe abelien, il suffit alors de prouver que le groupe $G(M/K(\omega))$ est abelien car, dans ce cas, la chaîne

$$\{i\}\subseteq G(M/K(\omega))\subseteq G(M/K)$$

serait une chaîne normale à facteurs abélien de $G(M/K)$.

M est obtenu à partir de $K(\omega)$ par l'adjonction d'un élément α vérifiant $\alpha^p=c\in K$. Ainsi, tout $\sigma\in G(M/K(\omega))$ est parfaitement déterminé par son action sur α. En plus $\sigma(\alpha)$ est une racine de X^p-c. Il en résulte qu'il existe un entier a tel $\sigma(\alpha)=\alpha\omega^a$. De même, si $\tau\in G(M/K(\omega))$, il existe un entier b tel que $\tau(\alpha)=\alpha\omega^b$. On a alors

$$\begin{aligned}(\sigma\circ\tau)(\alpha)&=\sigma(\tau(\alpha))=\sigma\left(\alpha\omega^b\right)\\&=\sigma(\alpha)\sigma\left(\omega^b\right)=\sigma(\alpha)\sigma(\omega)^b=c\omega^a\omega^b=\alpha\omega^{ab}\\(\tau\circ\sigma)(\alpha)&=\tau(\sigma(\alpha))=\tau(\alpha\omega^a)\\&=\tau(\alpha)\tau(\omega^a)=\tau(\alpha)\tau(\omega)^a=c\omega^b\omega^a=\alpha\omega^{ab}\end{aligned}$$

ce qui prouve $\sigma\circ\tau=\tau\circ\sigma$ et $G(M/K(\omega))$ est abelien.

Lemme Soit $f \in K[X]$ et soit $K' = K(\alpha)$ où $\alpha^p \in K$ pour un nombre premier p. Le groupe $G_K(f)$ est résoluble si, et seulement si, le groupe $G_{K'}(f)$ est résoluble.

Démonstration Soit N un corps des racines pour le polynôme $f(X)(X^p - c)$ sur K, où $c = \alpha^p \in K$. N contient un corps des racines L pour f sur K et un corps de racines M pour $X^p - c$ sur K. Les extensions N de K, L de K et M de K sont toutes galoisiennes. Les groupes $G(N/M)$ et $G(N/L)$ sont des sous-groupes distingués de $G(N/K)$. En plus le groupe $G(L/K)$ est isomorphe au groupe quotient $G(N/K)/G(N/L)$ et le groupe $G(M/K)$ est isomorphe au groupe quotient $G(N/K)/G(N/M)$. M et N sont des corps des racines pour le polynôme $X^p - c$ sur K et L respectivement. Il résulte du lemme précédent que $G(M/K)$ et $G(N/L)$ sont résolubles. Or nous savons que si H est un sous-groupe distingué d'un groupe G, alors G est résoluble si, et seulement si H et G/H le sont. Ainsi $G(N/K)$ est résoluble si, et seulement si, $G(N/M)$ est résoluble. De même, $G(N/K)$ est résoluble si, et seulement si, $G(L/K)$ est résoluble. Mais $G(N/M) \approx G_M(f)$ et $G(L/K) \approx G_K(f)$.Il en résulte que $G_M(f)$ est résoluble si, et seulement si, $G_K(f)$ est résoluble.

Maintenant M est aussi un corps des racines pour le polynôme $X^p - c$ sur K', car $K' = K(\alpha)$ où α est une racine de ce polynôme. Ainsi, le groupe $G_M(f)$ est résoluble si, et seulement si, le groupe $G_{K'}(f)$ est résoluble. Il en résulte que le groupe $G_K(f)$ est résoluble si, et seulement si, le groupe $G_{K'}(f)$ est résoluble.

Théorème Soit $f \in K[X]$. Si f est résoluble par des radicaux, alors son groupe de Galois $G_K(f)$ est résoluble.

Démonstration Si f est résoluble par des radicaux, alors il existe une suite K_0,K_1,...,K_m de corps tel que $K_0 = K$, f est scindé dans $K_m[X]$ et, pour i entre 1 et m, $K_i = K_{i-1}(\alpha_i)$ avec $\alpha_i^{p_i} \in K_{i-1}$ pour un nombre premier p_i. Le groupe $G_{K_m}(f)$ est résoluble car c'est le groupe réduit à l'identité de K_m. D'un autre côté, le lemme précédent montre que le groupe $G_{K_i}(f)$ est résoluble si, et seulement si, le groupe $G_{K_{i-1}}(f)$ est résoluble, et ce pour tout $i > 0$. Il en résulte que $G_K(f) = G_{K_0}(f)$ est résoluble.

Lemme Soit p un nombre premier, K un corps et L une extension galoisienne de degré p de K. On suppose que K contient une racine $p^{ième}$ primitive de l'unité. Alors il existe $\alpha \in L$ tel que $L = K(\alpha)$ et $\alpha^p \in K$.

Démonstration Le groupe $G(L/K)$ est un groupe cyclique car son ordre est un nombre premier. Soient σ un générateur de ce groupe et ω une racine $p^{ième}$

primitive de l'unité. Soit $b \in L-K$ et soit, pour $i = 0,1,...,p-1$,

$$\alpha_j = b + \omega^j \sigma(b) + \omega^{2j}\sigma^2(b) + \cdots + \omega^{(p-1)j}\sigma^{p-1}(b)$$

Cet élément est parfois appelé la **résolvante de Lagrange**. Nous avons $\sigma\left(\alpha_j\right) = \omega^{-j}\alpha_j$ pour $j = 0,1,...,p-1$, car $\sigma(\omega) = \omega$, $\sigma\left(\sigma^{p-1}(b)\right) = b$ et $\omega^p = 1$ Il en résulte $\sigma\left(\alpha_j^p\right) = \alpha_j^p$ et par suite $\alpha_j^p \in K$ pour $j = 0,1,...,p-1$. Mais

$$\alpha_0 + \alpha_1 + \cdots + \alpha_{p-1} = pb$$

car ω^j est une racine du polynôme $X^{p-1} + X^{p-2} + \cdots + X + 1$ pour tous les j non divisibles par p. Or $pb \in L-K$ car $b \in L-K$ et $p \neq 0$ dans K. Il en résulte qu'un des éléments $\alpha_0,\alpha_1,...,\alpha_{p-1}$ appartient à $L-K$. Soit $\alpha = \alpha_i$ un tel élément. $[K(\alpha):K]$ divise $[L:K] = p$. On en déduite $[K(\alpha):K] = p$ car p est premier et $\alpha \notin K$. Ainsi $L = K(\alpha)$ avec $\alpha^p \in K$.

Théorème Soit $f \in K[X]$ où K est un corps de caractéristique nulle. Si le groupe $G_K(f)$ est résoluble, alors f est résoluble par des radicaux.

Démonstration Soit ω une racine $p^{ième}$ primitive de l'unité où p est un nombre premier. Le groupe $G_{K(\omega)}(f)$ est isomorphe à un sous-groupe de $G_K(f)$ et est par suite résoluble. D'un autre côté, f est résoluble par des radicaux sur K si, et seulement si, f est résoluble par des radicaux sur $K(\omega)$ car $K(\omega)$ est obtenue à partir de K par adjonction d'un élément ω qui vérifie $\omega^p = 1 \in K$. Dès lors, on peut supposer que le corps K contient une racine $p^{ième}$ primitive de l'unité pour tous les diviseurs premiers de $n = Ord(G_K(f))$.

Le résultat est trivialement vrai pour $n = 1$ car dans ce cas f est scindé dans $K[X]$. Supposons la propriété vraie pour les extensions dont l'ordre du groupe de Galois est inférieur à n. Soit L un corps des racines pour f sur K. L est une extension galoisienne de K et $G(L/K) \approx G_K(f)$. Le groupe résoluble $G(L/K)$ possède un sous-groupe distingué H tel que le groupe quotient $G(L/K)/H$ soit cyclique d'ordre un nombre premier diviseur de $n = Ord(G_K(f))$. Soit M le corps des invariants de H. On a $H = G(L/M)$ et $G(M/K) \approx G(L/K)/H$. D'où $[M:K] = Ord(G(L/K)/H) = p$. Il en résulte que M est de la forme $M = K(\alpha)$ pour un $\alpha \in M$ qui vérifie $\alpha^p \in K$. Comme $G_M(f) \approx H$ et H est résoluble, alors $G_M(f) = G(L/M)$ est résoluble. L'hypothèse de récurrence montre que f est résoluble par des radicaux sur M. Les racines de f se trouvent donc, dans une extension de M obtenue par adjonction successive de radicaux. Or M est obtenue à partir de K par l'adjonction du radical α, donc les racines de f se trouvent dans une extension de K obtenue par adjonction successive de radicaux. f est alors résoluble par des radicaux.

Chapitre 10

Equation générale de degré n

10.1 Equation de degrée n

Tous les corps considérés dans ce chapitre seront de caractéristique nulle. Soit $b_1,\ldots,b_s$ des éléments d'une extension d'un corps K.

Définition On dira que les éléments $b_1,\ldots,b_s$ sont **algébriquement indépendants** sur K si, et seulement si, ces éléments ne satisfont aucune relation de la forme

$$\sum \alpha_{i_1 i_2 \ldots i_s} b_1^{i_1} \ldots b_s^{i_s} = 0$$

à coefficients non nuls.

Autrement dit, $b_1,\ldots,b_s$ sont algébriquement indépendants si, et seulement si, ils n'annulent aucun polynôme non nul $P(X_1,\ldots,X_s) \in K[X_1,\ldots,X_s]$ à n indéterminées.

Exemple Si a est transcendant sur K et b est transcendant sur $K(a)$, alors a,b sont algébriquement indépendants sur K, car si nous avons

$$\sum_{i,j} \alpha_{i,j} a^i b^j = 0$$

alors

$$\sum_j \left(\sum_i \alpha_{ij} a^i \right) b^j = 0$$

Mais b est transcendant sur $K(a)$, d'où

$$\sum_i \alpha_{ij} a^i = 0 \text{ pour tout } j$$

a est aussi transcendant sur K. Les relations précédentes impliquent $\alpha_{ij} = 0$ pour tout i et tout j ce qui prouve l'indépendance algébrique de a et b sur K.

L'**équation générale de degré** n sur un corps K est une équation de la forme

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

où les coefficients $a_0,a_1,\ldots,a_{n-1}$ sont algébriquement indépendants sur K. Soit $F = K(a_0,a_1,\ldots,a_{n-1})$ et $f(X) = X^n + a_{n-1}X^{n-1} + \cdots + a_1X + a_0$. Nous avons $f(X) \in F[X]$ et $F \simeq K(Y_1,\ldots,Y_n)$ corps des fractions rationnelles en n idéterminées $Y_1,\ldots,Y_n$ et à coefficients dans K. Soit $u_1,u_2,\ldots,u_n$ les racines de f dans un corps des racines $F(u_0,u_1,\ldots,u_{n-1})$ pour f sur F.

Théorème $u_1,u_2,\ldots,u_n$ sont algébriquement indépendants sur K.

Démonstration Sinon, soit

$$\sum \alpha_{i_1i_2\ldots i_n} u_1^{i_1}\ldots u_n^{i_n} = 0$$

une relation de dépendance algébrique sur K. Posons

$$P(X_1,\ldots,X_n) = \sum \alpha_{i_1i_2\ldots i_n} X_1^{i_1}\ldots X_n^{i_n}$$

Ce polynôme non nul satisfait $P(u_1,u_2,\ldots,u_n) = 0$. Considérons le polynôme

$$H(X_1,\ldots,X_n) = \prod_{\sigma\in S_n} P\left(X_{\sigma(1)},\ldots,X_{\sigma(n)}\right)$$

Le polynôme H est visiblement symétrique. La théorie des polynômes symétriques nous apprend qu'il existe un polynôme unique $Q(X_1,\ldots,X_n)$ dans $K[X_1,\ldots,X_n]$ tel que

$$H(X_1,\ldots,X_n) = Q(\Sigma_1,\ldots,\Sigma_n)$$

où $\Sigma_1,\Sigma_2,\ldots,\Sigma_n$ sont les polynômes symétriques élémentaires

$$\begin{aligned}
\Sigma_1 &= X_1 + X_2 + \cdots + X_n \\
\Sigma_2 &= X_1X_2 + X_1X_3 + \cdots + X_{n-1}X_n \\
\Sigma_3 &= X_1X_2X_3 + \cdots + X_{n-2}X_{n-1}X_n \\
&\vdots \\
\Sigma_n &= X_1X_2\cdots X_n
\end{aligned}$$

La relation $P(u_1,u_2,\ldots,u_n) = 0$ implique $H(u_1,u_2,\ldots,u_n) = 0$ et par suite $Q(\Sigma'_1,\ldots,\Sigma'_n) = 0$ où $\Sigma'_i = \Sigma_i(u_1,u_2,\ldots,u_n)$. Or $\Sigma'_i = (-1)^i a_{n-i}$. Il en résulte

$$Q(-a_{n-1},a_{n-2},-a_{n-3},\ldots,(-1)^n a_0) = 0$$

Mais, les éléments $a_0,\ldots,a_{n-1}$ sont algébriquement indépendants sur K. Ceci implique $Q=0$ et par suite $H=0$ et $P=0$.

Corollaire Les racines $u_1,u_2,\ldots,u_n$ sont distinctes.

Démonstration Car si $u_i=u_j$, alors $u_i-u_j=0$ est une relation de dépendence algébrique sur K satisfaites par les éléments $u_1,u_2,\ldots,u_n$.

Théorème $K(u_1,u_2,\ldots,u_n)=F(u_1,u_2,\ldots,u_n)$

Démonstration Nous avons

$$\begin{aligned} F(u_1,u_2,\ldots,u_n) &= K(a_0,\ldots,a_{n-1})(u_1,u_2,\ldots,u_n) \\ &= K(a_0,\ldots,a_{n-1},u_1,u_2,\ldots,u_n) \\ &= K(u_1,u_2,\ldots,u_n) \end{aligned}$$

car les coefficients a_i peuvent s'exprimer en fonction des racines $u_1,\ldots,u_n$ par l'intermédiaire des polynômes symétriques élémentaires.

Théorème Le groupe de Galois G du polynôme f est isomorphe à S_n.

Démonstration Il suffit de prouver que G est le groupe $S(A)$ de toute les permutations de l'ensemble $A=\{u_1,u_2,\ldots,u_n\}$ des racines de f car ce groupe de permutations est isomorphe au groupe S_n. Soit $\sigma\in G$. $\sigma\in S(A)$ car elle permute les racines $u_1,u_2,\ldots,u_n$ de f. Réciproquement, soit t une permutation de $A=\{u_1,u_2,\ldots,u_n\}$ et soit

$$\sigma;K[u_1,u_2,\ldots,u_n]\longrightarrow K[u_1,u_2,\ldots,u_n]$$

l'application définie par

$$\sigma(g(u_1,u_2,\ldots,u_n))=g(t(u_1),\ldots,t(u_n))$$

σ est bien définie car tout élément de $K[u_1,u_2,\ldots,u_n]$ s'écrit d'une manière unique sous la forme $g(u_1,u_2,\ldots,u_n)$. Il est aisé de prouver que σ est un K-automorphisme de l'anneau $K[u_1,u_2,\ldots,u_n]$. Il peut être prolongé en un K-automorphisme τ du corps $K(u_1,u_2,\ldots,u_n)$, corps des fractions de l'anneau $K[u_1,u_2,\ldots,u_n]$. Il nous reste à prouver que τ est un F-automorphisme de $K(u_1,u_2,\ldots,u_n)$. Mais τ laisse fixe tout élément a_i car a_i est une fonction symétrique des racines $u_1,u_2,\ldots,u_n$. Ainsi, τ appartient au groupe de Galois G de f sur F.

Corollaire L'équation générale de degré n n'est pas résoluble par des radicaux pour $n \geq 5$.

Démonstration Pour $n \geq 5$, le groupe de Galois de l'équation générale de degré n est isomorphe à S_n qui est non résoluble.

10.2 Discriminant

Soit

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

l'équation générale de degré n sur un corps K. Soit $P = K(a_0,a_1,\ldots,a_{n-1})$ et R un corps des racines sur P pour le polynôme

$$f(X) = X^n + a_{n-1}X^{n-1} + \cdots + a_1 X + a_0$$

Le groupe de Galois de f est isomorphe à S_n. Soit $u_1,u_2,\ldots,u_n$ les racines de f dans R.

Définition On appelle **discriminant** de f l'élément $D = \Delta^2$ où Δ est l'élément $\prod_{i<j}(u_i - u_j) \in R$.

Exemple Le discriminant de l'équation générale de degré 2 sur K est

$$D = \Delta^2 = (u_0 - u_1)^2 = a_1^2 - 4a_0$$

Théorème $\sigma(\Delta) = \pm\Delta$ pour tout $\sigma \in G(R/P)$.

Démonstration Nous avons

$$\sigma(\Delta) = \sigma\left(\prod_{i<j}(u_i - u_j)\right) = \prod_{i<j}\left(\sigma(u_i) - \sigma(u_j)\right) = \varepsilon(\sigma)\Delta = \pm\Delta$$

où $\varepsilon(\sigma)$ est la signature de la permutation σ.

Corollaire $\Delta^2 \in P$.

Démonstration Car $\sigma(\Delta^2) = \sigma(\Delta)^2 = \Delta^2$ pour tout $\sigma \in G(R/P)$.

Théorème Le corps des éléments laissés fixe par le groupe alterné A_n est $P(\Delta)$.

Démonstration Soit L le corps des éléments laissés fixes par A_n. Nous avons $A_n = G(R/L)$. L'extension L de P est normale, car $A_n = G(R/L)$ est un sous-groupe distingué de $S_n = G(R/P)$. En plus, le groupe de Galois $G(L/P)$ est isomorphe au groupe quotient S_n/A_n qui est un groupe d'ordre 2. Ainsi $[L:P] = 2$. L'élément Δ est invariant par chaque élément de A_n car $\sigma(\Delta) = \pm\Delta$. Il en résulte $\Delta \in L$ et $[P(\Delta):P] = 2$. D'où $L = P(\Delta)$.

10.3 Equation de degré 2

Cette équation est de la forme

$$x^2 + bx + c = 0$$

Nous avons $u_0 - u_1 = \Delta$ et $u_0 + u_1 = b$. En résolvant le système linéaire

$$\begin{cases} u_0 - u_1 = \Delta \\ u_0 + u_1 = b \end{cases}$$

nous obtenons

$$u_0 = \frac{-b+\Delta}{2} \text{ et } u_1 = \frac{-b-\Delta}{2}$$

10.4 Equation de degré 3

Cette équation est de la forme

$$x^3 + a_2x^2 + a_1x + a_0 = 0$$

En posant $y = x - \dfrac{a_2}{3}$, nous obtenons

$$x^3 + px + q = 0$$

Le discriminant de cette équation est

$$\Delta = -4p^3 - 27q^2$$

Son groupe de Galois, identifié à S_3, est résoluble et

$$S_3 \supseteq A_3 \supseteq \{e\}$$

est une chaîne normale à facteurs abéliens de S_3. Il correspond à cette chaîne par la correspondance de Galois, la chaîne suivante de corps intermédiaires

$$P \subseteq P(\Delta) \subseteq R$$

Le groupe de Galois de l'extension R de $P(\Delta)$ est A_3. Mais A_3 est un groupe cyclique d'ordre 3. Il est engendré par le cycle (123). Il en résulte que le groupe de Galois $G(R/P(\Delta))$ est engendré par le $P(\Delta)$-automorphisme σ de R qui vérifie

$$\sigma(u_1) = u_2,\ \sigma(u_2) = u_3 \text{ et } \sigma(u_3) = u_1$$

Ainsi, $[P(\Delta)(u_1) : P(\Delta)] = 3$ et $R = P(\Delta)(u_1) = P(\Delta,u_1)$.

On applique la méthode de la résolvante de Lagrange. Nous avons

$$\begin{aligned}
\beta_1 &= u_1 + z\sigma(u_1) + z^2\sigma^2(u_1) = u_1 + zu_2 + z^2u_3 \\
\beta_2 &= u_1 + z^2u_2 + zu_3 \\
\beta_3 &= u_1 + u_2 + u_3
\end{aligned}$$

Un calcul assez complexe nous donne

$$\begin{aligned}
\beta_1^3 &= \left(u_1 + zu_2 + z^2u_3\right)^3 = -\frac{27}{2}q + \frac{3}{2}\sqrt{-3}\Delta \\
\beta_2^3 &= -\frac{27}{2}q - \frac{3}{2}\sqrt{-3}\Delta \\
\beta_1\beta_2 &= -3p
\end{aligned}$$

Donc, u_1,u_2,u_3 forment une solution du système linéaire suivant

$$\begin{cases} u_1 + u_2 + u_3 = 0 \\ u_1 + zu_2 + z^2u_3 = \beta_1 \\ u_1 + z^2u_2 + zu_3 = \beta_2 \end{cases}$$

Pour résoudre ce système, nous devons calculer β_1 et β_2. Parmi les solutions possibles, on choisit celle qui vérifie $\beta_1\beta_2 = -3p$. La résolution du système linéaire nous donne alors

$$u_0 = \frac{\beta_1 + \beta_2}{3},\ u_1 = \frac{z^2\beta_1 + z\beta_2}{3} \text{ et } u_2 = \frac{z\beta_1 + z^2\beta_2}{3}$$

Exemple Pour résoudre l'équation de degré 3 suivante

$$x^3 - 5x^2 + 19x + 25 = 0$$

on pose $y = x - \frac{5}{3}$. Nous obtenons l'équation suivante

$$x^3 + \frac{32}{3}x + \frac{1280}{27} = 0$$

Le discriminant de cette équation est

$$\Delta^2 = -4p^3 - 27q^2 = -4\left(\frac{32}{3}\right)^3 - 27\left(\frac{1280}{27}\right)^2 = -65536$$

D'où

$$\beta_1^3 = \left(4\left(\sqrt{3}+1\right)\right)^3 \text{ et } \beta_2^3 = \left(-4\left(\sqrt{3}-1\right)\right)^3$$

et $\beta_1\beta_2 = -3p = -32$. On en déduit

$$\beta_1 = 4\left(\sqrt{3}-1\right) \text{ et } \beta_2 = -4\left(\sqrt{3}+1\right)$$

ce qui donne

$$\begin{aligned} u_0 &= \frac{\beta_1+\beta_2}{3} = -\frac{8}{3} \\ u_1 &= \frac{z^2\beta_1+z\beta_2}{3} = \frac{4}{3} - i \\ u_2 &= \frac{z\beta_1+z^2\beta_2}{3} = \frac{4}{3} + i \end{aligned}$$

et

$$\begin{aligned} x_0 &= u_0 + \frac{5}{3} = -1 \\ x_1 &= u_1 + \frac{5}{3} = 3 - 4i \\ x_2 &= u_2 + \frac{5}{3} = 3 + 4i \end{aligned}$$

10.5 Equation de degré 4

Cette équation est de la forme suivante

$$x^4 + a_3x^3 + a_2x^2 + a_1x + a_0 = 0$$

En posant $y = x - \dfrac{a_3}{4}$, nous obtenons

$$x^4 + px^2 + qx + r = 0$$

Le discriminant de cette équation est

$$\Delta = 16p^4r - 4p^3q^3 - 128p^2r^2 + 144pq^2r - 27q^4 + 256r^3$$

Le groupe de Galois de cette équation, identifié à S_4, est résoluble et

$$S_4 \supseteq A_4 \supseteq V \supseteq W \supseteq \{e\}$$

Où

$$V = \{e, u = (12)(34), v = (13)(24), t = (14)(23)\}, W = \{e, u\}$$

est une chaîne normale à facteurs abéliens de S_4. Il lui correspond, par la correspondance de Galois, la chaîne suivante de corps intermédiaires

$$P \subseteq P(\Delta) \subseteq L_1 \subseteq L_2 \subseteq R$$

Nous avons

$$G(R/P(\Delta)) \simeq A_4,\ G(R/L_1) \simeq V,\ G(R/L_2) \simeq W$$

et

$$[R:P] = 24,\ [R:P(\Delta)] = 12,\ [R:L_1] = 4,\ [R:L_2] = 2$$
$$[L_2:L_1] = 2, [L_2:P(\Delta)] = 6, [L_1:P(\Delta)] = 3 \text{ et } [P(\Delta):P] = 2$$

L_1 est engendré sur $P(\Delta)$ par un élément invariant par tous les $\sigma \in V$. Mais cet élément est modifié par au moins un élément de A_4. Considérons l'élément $\theta = (u_0+u_1)(u_2+u_3)$. Cet élément vérifie

$$u(\theta) = (u_1+u_0)(u_3+u_2) = \theta$$
$$v(\theta) = (u_2+u_3)(u_0+u_1) = \theta$$
$$t(\theta) = (u_3+u_2)(u_1+u_0) = \theta$$

Donc $\theta \in L_1$. d'un autre côté, $\sigma = (123) \in A_4$ et $\sigma(\theta) \neq \theta$ ce qui prouve $\theta \notin P(\Delta)$. D'où $L_1 = P(\Delta)(\theta) = P(\Delta,\theta)$. Le polynôme minimal de θ sur $P(\Delta)$ est le polynôme ayant comme racines les $\sigma(\theta)$ pour tout élément σ de $A_4 = G(R/P(\Delta))$. Mais

$$A_4 = \left\{ \begin{array}{c} e, (123), (124), (134), (234), (132), (142), (143), \\ (243), (13)(24), (14)(23), (12)(34) \end{array} \right\}$$

Calculant ces image de θ, nous obtenons

$$\begin{aligned}\theta_1 &= \theta\\ \theta_2 &= (u_0+u_2)(u_1+u_3)\\ \theta_3 &= (u_0+u_3)(u_1+u_2)\end{aligned}$$

Or ces images sont les racines de l'équation

$$(x-\theta_1)(x-\theta_2)(x-\theta_3) = x^3 - b_1x^2 + b_2x - b_3 = 0$$

avec

$$\begin{aligned}b_1 &= \theta_1+\theta_2+\theta_3 = 2p\\ b_2 &= \theta_1\theta_2+\theta_1\theta_3+\theta_2\theta_3 = p^2-4r\\ b_3 &= \theta_1\theta_2\theta_3 = -q^2\end{aligned}$$

Cette équation de degré 3 est appelée **la résolvante cubique** de l'équation de degré 4. Le polynôme minimal de θ sur $P(\Delta)$ est donc le polynôme $X^3 - b_1X^2 + b_2X - b_3$. θ_1 et θ_2 appartiennent à L_1 car ils sont invariants par tous les éléments de $V = G(R/L_1)$.

L_2 est engendré sur L_1 par un élément de degré 2. Si $\lambda = u_1+u_2$, alors λ est invariant par tous les éléments de W mais transformé par l'élément v de V car nous avons

$$v(\lambda) = u_3+u_4 \neq \lambda \quad (u_1+u_2+u_3+u_4 = 0)$$

Donc $\lambda \in L_1$ et $\lambda \notin L_2$. Il en résulte $L_2 = L_1(\lambda)$ et la chaîne des corps intermédiaires devient

$$P \subseteq P(\Delta) \subseteq P(\Delta,\theta) \subseteq P(\Delta,\theta,\lambda) \subseteq R$$

Pour calculer les racines u_1,u_2,u_3,u_4 en fonction de $\theta_1,\theta_2,\theta_3$, nous avons

$$\begin{cases}(u_1+u_2)(u_3+u_4) = \theta_1\\ u_1+u_2+u_3+u_4 = 0\end{cases}$$

Ces deux équations nous donnent

$$\begin{cases}u_1+u_2 = \sqrt{-\theta_1}\\ u_3+u_4 = -\sqrt{-\theta_1}\end{cases}$$

De même, nous avons

$$\begin{cases}u_1+u_3 = \sqrt{-\theta_2}\\ u_2+u_4 = -\sqrt{-\theta_2}\end{cases}$$

et

$$\begin{cases}u_1+u_4 = \sqrt{-\theta_3}\\ u_2+u_3 = -\sqrt{-\theta_3}\end{cases}$$

Le choix de $\sqrt{-\theta_1},\sqrt{-\theta_2},\sqrt{-\theta_3}$ doit satisfaire

$$\left(\sqrt{-\theta_1}\right)\left(\sqrt{-\theta_2}\right)\left(\sqrt{-\theta_3}\right)=(u_1+u_2)(u_1+u_3)(u_1+u_4)=-q$$

Nous obtenons

$$\begin{aligned}u_1&=\frac{1}{2}\left(\sqrt{-\theta_1}+\sqrt{-\theta_2}+\sqrt{-\theta_3}\right)\\ u_2&=\frac{1}{2}\left(\sqrt{-\theta_1}-\sqrt{-\theta_2}-\sqrt{-\theta_3}\right)\\ u_3&=\frac{1}{2}\left(\sqrt{-\theta_1}+\sqrt{-\theta_2}-\sqrt{-\theta_3}\right)\\ u_4&=\frac{1}{2}\left(\sqrt{-\theta_1}-\sqrt{-\theta_2}+\sqrt{-\theta_3}\right)\end{aligned}$$

Exemple Soit à résoudre l'équation de degré 4 suivante

$$x^4-2x^3+4x^2+2x-5=0$$

En posant $y=x-\frac{1}{2}$, nous obtenons

$$y^4+\frac{5}{2}y^2+5y-\frac{51}{16}=0$$

La résolvante cubique est

$$x^3-5x^2+19x+25=0$$

Les racines de cette équation de degré 3 sont

$$\theta_1=-1,\theta_2=3-4i \text{ et } \theta_3=3+4i.$$

Nous avons

$$\begin{aligned}\sqrt{-\theta_1}&=\pm 1\\ \sqrt{-\theta_2}&=\sqrt{4i-3}=\pm(1+2i)\\ \sqrt{-\theta_3}&=\sqrt{-3-4i}=\pm(1-2i)\end{aligned}$$

La condition

$$\left(\sqrt{-\theta_1}\right)\left(\sqrt{-\theta_2}\right)\left(\sqrt{-\theta_3}\right)=(u_1+u_2)(u_1+u_3)(u_1+u_4)=-q=-5$$

nous donne $\sqrt{-\theta_1}=1,\sqrt{-\theta_2}=1+2i$ et $\sqrt{-\theta_3}=2i-1$. Les racines de l'équation en y sont

$$y_0=\frac{1}{2}+2i,y_1=\frac{1}{2}-2i,y_2=\frac{1}{2} \text{ et } y_3=-\frac{3}{2}$$

On en déduit les racines de l'équation initiale en x. Ces racines sont

$$x_0=1+2i,x_1=1-2i,x_2=1 \text{ et } x_3=-1$$