THEORIE DES CORPS

Cours de mathématiques pour Licence L3 et Master M1

Cours et Exercices corrigés [1]

Michel Goze, Elisabeth Remm

1. Edité par Ramm Algebra Center

Introduction

Ce cours s'adresse aux étudiants de troisième année de Licence mathématiques ou de première année de Master

Table des matières

Chapitre 1

Corps. Généralités

1.1 Définition d'un corps

1.1.1 Définition

Définition 1 *Un corps $\mathbb{K}$ est un ensemble non vide muni de deux lois de composition (deux opérations), notées $+$ et $\times$ vérifiant les conditions suivantes :*

1. *La loi de composition $+$ vérifie :*
   (a) *Elle est associative $(x+y)+z = x+(y+z)$, $\forall x, y, z \in \mathbb{K}$,*
   (b) *Elle est commutative : $x+y = y+x$, $\forall x, y \in \mathbb{K}$,*
   (c) *$\mathbb{K}$ possède un élément neutre 0 : $x+0 = x$, $\forall x \in \mathbb{K}$,*
   (d) *Tout élément x de $\mathbb{K}$ possède un symétrique $(-x)$ par rapport à 0 : $x+(-x) = 0$, $\forall x \in \mathbb{K}$.*
2. *La loi de composition $\times$ vérifie :*
   (a) *Elle est associative $(x \times y) \times z = x \times (y \times z)$, $\forall x, y, z \in \mathbb{K}$,*
   (b) *Elle est distributive par rapport à la loi $+$: $x \times (y+z) = x \times y + x \times z$, $\forall x, y, z \in \mathbb{K}$,*
   (c) *$\mathbb{K}$ possède un élément neutre e pour $\times$: $x \times e = e \times x = x$, $\forall x \in \mathbb{K}$,*
   (d) *Tout élément $x \neq 0$ de $\mathbb{K}$ possède un inverse (x^{-1}) par rapport à e : $x \times (x^{-1}) = (x^{-1}) \times x = e$, $\forall x \in \mathbb{K}$.*

Autrement dit, un corps est un anneau unitaire non réduit à 0 dans lequel tout élément $x \neq 0$ possède un inverse. Le groupe des unités du corps $\mathbb{K}$, c'est-à-dire le groupe des éléments inversibles pour la multiplication $\times$ est égal à $\mathbb{K}^* = \mathbb{K} - \{0\}$. Pour simplifier les écritures, nous écrirons xy à la place de $x \times y$.

Une propriété caractéristique d'un corps est la suivante : Dans un corps $\mathbb{K}$, quel que soit $a \in \mathbb{K}$ tel que $a \neq 0$ et quel que soit $b \in \mathbb{K}$, les équations

$$\begin{cases} ax = b, \\ ya = b \end{cases}$$

ont, chacune, une solution et une seule

$$\begin{cases} x = a^{-1}b, \\ y = ba^{-1}. \end{cases}$$

Définition 2 *Un corps dont la multiplication est commutative est dit commutatif.*

Dans les ouvrages anglo-saxons, le mot corps se traduit par *field*. Mais on prendra garde que ce vocable *field* sous-entend toujours que le corps soit commutatif. Lorsque le corps n'est pas commutatif, on utilise parfois les notions d'anneau à division (division ring or skew field).

Proposition 1 *Soit A un anneau unitaire commutatif non réduit à $\{0\}$. Alors A est un corps (commutatif) si et seulement si les seuls idéaux de A sont A et $\{0\}$.*

Démonstration. Supposons que tous les seuls idéaux de A soient A et $\{0\}$. Comme A est non nul, il existe $a \in A,\ a \neq 0$. Soit $aA = \{ax, x \in A\}$ l'idéal principal engendré par a. Comme il est non nul, on a $aA = A$. Il existe donc $x \in A$ tel que $ax = e$, e étant l'élément neutre de A. Ainsi a est inversible et A est un corps. Inversement, si A est un corps et I un idéal non nul de A, alors pour tout $a \in I$ on a $aa^{-1} = e \in I$ et tout idéal contenant e coïncide avec A. D'où la proposition.

1.1.2 Exemples de corps

1. L'ensemble des nombres rationnels $\mathbb{Q}$, l'ensemble des nombres réels $\mathbb{R}$ et l'ensemble des nombres complexes $\mathbb{C}$ sont des corps commutatifs.
2. Le corps des Quaternions. On considère l'ensemble $\mathbb{H}$ des matrices de la forme

$$\begin{pmatrix} a & -b \\ \overline{b} & \overline{a} \end{pmatrix}$$

avec $a, b \in \mathbb{C}$ et où $\overline{a}$ désigne le conjugué de a.

Proposition 2 *L'ensemble $\mathbb{H}$ est muni d'une structure de corps non commutatif.*

Démonstration. Il est clair que $\mathbb{H}$ est un sous-anneau de l'anneau $\mathcal{M}_2(\mathbb{C})$ des matrices carrées complexes. Il nous suffit donc de montrer que tout élément non nul est inversible. Soit

$$A = \begin{pmatrix} a & -b \\ \overline{b} & \overline{a} \end{pmatrix}$$

une matrice de $\mathbb{H}$. Son déterminant est égal à

$$\det A = a\overline{a} + b\overline{b} = |a|^2 + |b|^2.$$

Ainsi $\det A \neq 0$ si et seulement si A n'est pas la matrice nulle. Ainsi A est inversible dans $\mathcal{M}_2(\mathbb{C})$. Montrons que son inverse est dans $\mathbb{H}$. On a

$$A^{-1} = \begin{pmatrix} \dfrac{\overline{a}}{|a|^2+|b|^2} & \dfrac{b}{|a|^2+|b|^2} \\ \dfrac{-\overline{b}}{|a|^2+|b|^2} & \dfrac{a}{|a|^2+|b|^2} \end{pmatrix} = \begin{pmatrix} \alpha & -\beta \\ \overline{\beta} & \overline{\alpha} \end{pmatrix}$$

et $A^{-1} \in \mathbb{H}$ et $\mathbb{H}$ est un corps. Montrons qu'il n'est pas commutatif. On a

$$\begin{pmatrix} i & 0 \\ 0 & \bar{i} \end{pmatrix} \cdot \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} 0 & -i \\ -i & 0 \end{pmatrix}$$

et

$$\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \cdot \begin{pmatrix} i & 0 \\ 0 & \bar{i} \end{pmatrix} = \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix}.$$

Ceci montre la non commutativité du produit.

3. Soit p un nombre premier. L'anneau $\mathbb{Z}/p\mathbb{Z}$ des entiers modulo p est un corps fini contenant p éléments .

1.1.3 Sous-corps. Sous-corps premier

Définition 3 *On appelle sous-corps d'un corps $\mathbb{K}$ un sous-ensemble de $\mathbb{K}$ qui est lui même un corps par rapport à l'addition et à la multiplication de $\mathbb{K}$.*

Ainsi un sous-ensemble $\mathbb{L}$ de $\mathbb{K}$ est un sous-corps si $\mathbb{L}$ est un sous-groupe additif de $\mathbb{K}$ (pour l'addition de $\mathbb{K}$) et si $\mathbb{L}^* = \mathbb{L} - \{0\}$ est un sous-groupe multiplicatif de $\mathbb{K}^*$. Si $\mathbb{L}$ est un sous-corps de $\mathbb{K}$, on dit que $\mathbb{K}$ est un surcorps de $\mathbb{L}$.

Lemme 1 *Toute intersection de sous-corps du corps $\mathbb{K}$ est un sous-corps de $\mathbb{K}$.*

Démonstration. Comme cette propriété est déjà vraie pour les anneaux unitaires, l'intersection des sous-corps de $\mathbb{K}$ est un sous-anneau unitaire de $\mathbb{K}$. Soit x un élément non nul de cette intersection. Dans chacun des sous-corps, cet élément est inversible dont l'inverse correspond à x^{-1}, l'inverse de x dans $\mathbb{K}$. Ainsi x^{-1} est dans chacun des sous-corps et x est inversible dans l'intersection qui est donc un sous-corps de $\mathbb{K}$.

Notons $\Pi(\mathbb{K})$ l'intersection des sous-corps de $\mathbb{K}$. Il n'admet aucun sous-corps autre que lui même.

Définition 4 *On appelle sous-corps premier du corps $\mathbb{K}$ le sous-corps $\Pi(\mathbb{K})$ obtenu comme l'intersection des sous-corps de $\mathbb{K}$. On dit qu'un corps Π est un corps premier, s'il est le sous-corps premier d'un corps.*

Etant donnée une partie X de $\mathbb{K}$, on peut définir le plus petit sous-corps $\Pi_X(\mathbb{K})$ de $\mathbb{K}$ contenant X. C'est l'intersection de tous les sous-corps de $\mathbb{K}$ contenant X. En particulier, si $X = \{e\}$, l'élément neutre pour la multiplication de $\mathbb{K}$, le sous-corps $\Pi_e\mathbb{K}$ est contenu dans tous les sous-corps de $\mathbb{K}$. Il coïncide avec le sous-corps premier $\Pi(\mathbb{K})$. Dans le paragraphe suivant, nous déterminerons la structure de tous les corps isomorphes à un sous-corps premier d'un corps.

1.1.4 Homomorphismes de corps

Définition 5 *Soient $\mathbb{K}_1$ et $\mathbb{K}_2$ deux corps. Une application $f : \mathbb{K}_1 \to \mathbb{K}_2$ est un homomorphisme de corps si elle vérifie*

1. *f(x+y)=f(x)+f(y) ,*
2. *f(xy)=f(x)f(y)*

pour tout $x, y \in \mathbb{K}_1$.

Ainsi f est un homomorphisme des groupes additifs et un homomorphisme des groupes multiplicatifs $\mathbb{K}_1^*$ et $\mathbb{K}_2^*$. On en déduit $f(0) = 0,\ f(-x) = -f(x)$ et, si f est non nul, $f(e) = e'$ où e et e' désignent respectivement les éléments neutres pour la multiplication de $\mathbb{K}_1$ et $\mathbb{K}_2$ et $f(x^{-1}) = (f(x))^{-1}$. L'homomorphisme f est donc un homomorphisme d'anneau unitaire. Son noyau

$$\ker f = \{x \in \mathbb{K}_1,\ f(x) = 0\}$$

est un idéal de $\mathbb{K}_1$. Il est donc réduit à $\{0\}$ et f est injectif.

Proposition 3 *Tout homéomorphisme de corps non nul est injectif.*

1.2 Caractéristique d'un corps

1.2.1 Définition

Considérons le sous-groupe additif $(e) = \{ne, n \in \mathbb{Z}\}$ engendré par l'élément neutre e du corps. C'est un sous-groupe du groupe additif de $\mathbb{K}$. Si ce sous-groupe est fini, (e) est un sous-groupe cyclique d'ordre fini n_e. Ainsi on a

$$n_e e = 0.$$

et l'équation $ne = 0$ est vérifiée si et seulement si n est nul ou est un multiple de n_e. Si le groupe monogène (e) est infini, l'équation $ne = 0$ avec $n \in \mathbb{Z}$ implique $n = 0$.

Définition 6 *Soit $\mathbb{K}$ un corps et soit (e) le groupe monogène engendré par l'élément neutre de $\mathbb{K}$ noté e. Alors si le sous-groupe (e) est cyclique d'ordre fini n_e on dit que $\mathbb{K}$ est de caractéristique n_e sinon $\mathbb{K}$ est dit de caractéristique* 0.

Proposition 4 *Soit $\mathbb{K}$ un corps de caractéristique p avec $p \neq 0$. Alors p est un nombre premier.*

Démonstration. Par hypothèse p est le plus petit entier positif non nul tel que $pe = 0$. Si p n'est pas premier, il existe deux entiers positifs non nuls et différents de 1 tel que $p_1 p_2 = p$. Donc $p_1 p_2 e = 0$. Ainsi $(p_1 e)(p_2 e) = p_1 p_2 e^2 = pe = 0$ et comme $\mathbb{K}$ est un corps, il n'admet pas de diviseurs de zéro ce qui implique que $p_1 e = 0$ ou $p_2 e = 0$ ce qui est contraire à la définition de p.

Proposition 5 *Soit $\mathbb{K}$ un corps.*

1. *Si $\mathbb{K}$ est de caractéristique $p \neq 0$, le sous-corps premier de $\mathbb{K}$ est isomorphe à $\mathbb{Z}/p\mathbb{Z}$.*
2. *Si $\mathbb{K}$ est de caractéristique 0 alors le sous-corps premier de $\mathbb{K}$ est isomorphe au corps des rationnels $\mathbb{Q}$.*

Démonstration. Soit $\varphi : \mathbb{Z} \to \mathbb{K}$ l'homomorphisme d'anneaux unitaires défini par $\varphi(n) = ne$. On a

$$\mathrm{Im}(\varphi) = (e)$$

et son noyau est soit nul, soit égal à $p\mathbb{Z}$ par définition de la caractéristique p. Supposons $p \neq 0$, le sous-groupe additif $(e) = \{0, e, \cdots, (p-1)e\}$ muni de la multiplication induite par celle de $\mathbb{K}$ est un sous-anneau commutatif isomorphe à $\mathbb{Z}/p\mathbb{Z}$ et comme p est premier, c'est aussi un corps. Comme ce sous-corps ne contient pas de sous-corps propre, on en déduit que c'est le sous-corps premier de $\mathbb{K}$. Si la caractéristique est nulle, le groupe monogène (e) est infini et isomorphe à $\mathbb{Z}$. C'est donc un sous-anneau commutatif intègre et le corps premier de $\mathbb{K}$ est isomorphe au corps des fractions de $\mathbb{Z}$ c'est à dire $\mathbb{Q}$. Nous reverrons explicitement la construction de $\mathbb{Q}$ au paragraphe suivant.

Corollaire 1 *Tout corps fini $\mathbb{K}$ est de caractéristique $p \neq 0$ et sa cardinalité est une puissance de p.*

Démonstration. En effet, si $\mathbb{K}$ est fini son corps premier ne peut être isomorphe à $\mathbb{Q}$ et donc sa caractéristique p est différente de zéro. On a donc $pe = 0$ et pour tout x de $\mathbb{K}$, $px = p(ex) = (pe)x = 0$.

1.2.2 L'homomorphisme de Frobenius

Proposition 6 *Soit $\mathbb{K}$ un corps de caractéristique p, $p \neq 0$. L'application*

$$F : \mathbb{K} \to \mathbb{K}$$

définie par

$$F(x) = x^p$$

est un homomorphisme de corps. Il est appelé l'homomorphisme de Frobenius.

Démonstration. Rappelons la formule du binôme

$$(x+y)^p = x^p + px^{p-1}y + \cdots + C_p^k x^{p-k}y^k + \cdots + y^p$$

où $C_p^k = \dfrac{p!}{k!(p-k)!}$. Mais pour tout k, $1 \leq k \leq p-1$, p divise C_p^k. Comme p est la caractéristique de $\mathbb{K}$, on en déduit que pour tout k, $1 \leq k \leq p-1$, $C_p^k = 0$. Ainsi

$$(x+y)^p = x^p + y^p.$$

Mais $F(x+y) = (x+y)^p$. Ainsi $F(x+y) = F(x) + F(y)$ pour tout $x, y \in \mathbb{K}$. De même, on a $F(xy) = (xy)^p = x^p y^p = F(x)F(y)$ et F est un homomorphisme du corps $\mathbb{K}$.

1.3 Quelques constructions de corps

1.3.1 Le corps des fractions d'un anneau intègre

Soit A un anneau intègre, c'est-à-dire commutatif unitaire dont l'unité 1_A est différente de 0 et sans diviseur de 0. Notons par A^* l'ensemble $A - \{0\}$. Considérons dans $A \times A^*$ la relation :

$$(a,b)\mathcal{R}(c,d) \text{ si et seulement si } ad = bc.$$

Cette relation est d'équivalence car elle est
— réflexive $(a,b)\mathcal{R}(a,b)$,
— symétrique $(a,b)\mathcal{R}(c,d)$ implique $(c,d)\mathcal{R}(a,b)$,
— transitive $(a,b)\mathcal{R}(c,d)$ et $(c,d)\mathcal{R}(e,f)$ impliquent $(a,b)\mathcal{R}(e,f)$.

Les deux premières affirmations se démontre facilement. Montrons la transitivité. Comme $(a,b)\mathcal{R}(c,d)$ et $(c,d)\mathcal{R}(e,f)$, on a $ad = bc$ et $cf = de$. On en déduit $adf = bcf$ et $cfb = deb$. Ainsi $adf = deb$ soit $d(af - eb) = 0$. Comme l'anneau est intègre et comme $d \neq 0$, on déduit $af = eb$ ce qui implique $(a,b)\mathcal{R}(e,f)$. La relation est bien transitive. Ceci étant, soit $A \times A^*/\mathcal{R}$ l'ensemble quotient. Notons par $\frac{a}{b}$ la classe d'équivalence de (a,b) :

$$\frac{a}{b} = \{(c,d) \in A \times A^*,\ ad - bc = 0\}.$$

Définissons dans $A \times A^*/\mathcal{R}$ les opérations, l'addition et la multiplication, suivantes :

$$\frac{a}{b} + \frac{c}{d} = \frac{ad + bc}{bd}$$

et

$$\frac{a}{b}\frac{c}{d} = \frac{ac}{bd}.$$

Ces opérations sont bien définies car le résultat de chacune d'elle ne dépend pas du choix des représentants des classes d'équivalence. En effet, supposons que $(a',b') \in \frac{a}{b}$ et $(c',d') \in \frac{c}{d}$. On a donc $ab' = ba'$ et $cd' = dc'$. Montrons que

$$\frac{ad + bc}{bd} = \frac{a'd' + b'c'}{b'd'}.$$

On a

$$(ab' - ba')dd' = 0,\ (cd' - dc')bb' = 0.$$

Ainsi

$$ab'dd' + cd'bb' = ba'dd' + c'dbb'$$

et

$$b'd'(ad + cb) = bd(a'd' + b'c').$$

Ainsi

$$\frac{ad + bc}{bd} = \frac{a'd' + b'c'}{b'd'}.$$

L'addition est bien définie. Montrons maintenant que $\frac{ac}{bd} = \frac{a'c'}{b'd'}$. On a

$$(ab' - ba')cd' = 0,\ (cd' - dc')a'b = 0.$$

Ainsi

$$ab'cd' - a'bcd' = -cd'a'b + a'bc'd$$

soit

$$ab'cd' = a'bc'd$$

et

$$(ac, bd)\mathcal{R}(a'c', b'd').$$

La multiplication est aussi bien définie. Montrons que, muni de cette addition et cette multiplication, l'ensemble quotient $A \times A^*/\mathcal{R}$ a une structure de corps.

— $(A \times A^*/\mathcal{R}, +)$ est un groupe abélien. L'addition est commutative et associative car $(A, +)$ est un groupe commutatif. L'élément neutre est $\frac{0}{1}$. En effet $\frac{a}{b} + \frac{0}{1} = \frac{a}{b}$. Notons que $\frac{0}{1} = \frac{0}{b}$ pour tout $b \neq 0$. L'opposé de $\frac{a}{b}$ est $\frac{-a}{b}$.

— La multiplication est commutative, associative, distributive par rapport à l'addition. L'élément neutre est $\frac{1}{1}$ et le symétrique de $\frac{a}{b}$ avec $a \neq 0$ est $\frac{b}{a}$.

On a bien muni l'ensemble quotient d'une structure de corps. Ce corps est appelé le corps des fractions de A. En particulier, si nous prenons pour A l'anneau $\mathbb{Z}$, son corps des fractions est le corps $\mathbb{Q}$ des nombres rationnels.

1.3.2 Le quotient d'un anneau par un idéal maximal

Soient A un anneau commutatif et I un idéal de A. Notons par $\pi : A \to A/I$ la projection canonique. Rappelons que A/I est l'anneau quotient correspondant à la relation d'équivalence dans A :

$$x\mathcal{R}y \Longleftrightarrow x - y \in I.$$

L'idéal I est dit maximal si $I \neq A$ et s'il est maximal pour l'inclusion, c'est-à-dire si J est un idéal de A vérifiant $A \neq J$ et $I \subseteq J$, alors $J = I$. Rappelons que le lemme de Krull précise que tout idéal I de A, tel que $I \neq A$ est contenu dans un idéal maximal.

Proposition 7 *Soit A un anneau et I un idéal de A. Alors l'anneau quotient A/I est un corps si et seulement si I est un idéal maximal de A.*

Démonstration. Supposons que A/I soit un corps et considérons un idéal J tel que $I \subset J \subseteq A$. Il existe $a \in J$ tel que $a \notin I$. Soit $aA = \{ax,\ x \in A\}$ l'idéal de A engendré par a. Il est clair que $aA \subseteq J$ et $\pi(aA) \neq 0$. Montrons que $\pi(aA)$ est un idéal de A/I. On a pour tout $x, y \in A$,

$$\pi(ax)\pi(y) = \pi(axy)$$

et donc $\pi(ax)\pi(y) \in \pi(aA)$ pour tout $y \in A$. Donc $\pi(aA)$ est un idéal de A/I. Mais par hypothèse A/I est un corps, ses seuls idéaux sont donc $\{0\}$ et A/I. Si $\pi(aA) = \{0\}$, alors $aA \subset I$ ce qui est n'est pas possible. Donc $\pi(aA) = A/I$ et $J = A$ ce qui montre que I est maximal. Inversement, supposons que I soit un idéal maximal de A. Soit $\overline{J}$ un idéal non nul de A/I et soit J le sous-ensemble de A constitué des éléments $x \in A$ tels que $\pi(x) \in J$. Si $J = A$ alors $\overline{J} = A/I$. Sinon, soit $x \in J$ et $y \in A$. Alors $\pi(xy) = \pi(x)\pi(y) \in \overline{J}$ car $\pi(x) \in \overline{J}$ qui est un idéal de A/I. Ainsi $xy \in J$ et J est un idéal de A vérifiant $J \neq A$. Or J contient I car tout $x \in I$ vérifie $\pi(x) = 0 \in \overline{J}$. Comme I est maximal, alors $J = I$ et $\overline{J} = \{0\}$. On en déduit que tout idéal de A/I est soit nul, soit égal à A/I. D'après la Proposition 1, A/I est un corps.

1.3.3 Les corps de rupture d'un polynôme

Soient $\mathbb{K}$ un corps commutatif et $\mathbb{K}[X]$ l'anneau des polynômes à une indéterminée et à coefficients dans $\mathbb{K}$. Cet anneau est commutatif, unitaire et euclidien. Il est donc principal et intègre. Soit I un idéal de $\mathbb{K}[X]$. Comme les idéaux sont principaux, il existe un élément m_I de $\mathbb{K}[X]$ tel que $I = \{Pm_I, P \in \mathbb{K}[X]\}$. Ce polynôme m_I est de degré minimal dans I. Si on le suppose unitaire, le coefficient de plus haut degré est égal à 1, alors un tel générateur de I est unique.

Lemme 2 *Les éléments inversibles de $\mathbb{K}[X]$ sont les polynômes non nuls de degré 0.*

Démonstration. Il est clair que tout élément non nul de $\mathbb{K}$ considéré comme un polynôme de $\mathbb{K}[X]$ de degré 0 est inversible dans $\mathbb{K}[X]$. Soit $P \in \mathbb{K}[X]$ de degré n, $n \geq 1$. Si P est inversible, il existe $Q \in \mathbb{K}[X]$ tel que $PQ = e$. Si m est le degré de Q, on a donc $nm = 0$ et donc $m = 0$. Mais ceci implique que P, qui est l'inverse de Q soit aussi de degré 0.

Définition 7 *Un polynôme $P \in \mathbb{K}[X]$ est dit irréductible si*

1. *Son degré est supérieur ou égal à 1,*
2. *Ses seuls diviseurs non constants dans $\mathbb{K}[X]$ sont les polynômes aP avec $a \in \mathbb{K}$, $a \neq 0$.*

Soit $P \in \mathbb{K}[X]$. Notons par (P) l'idéal principal de $\mathbb{K}[X]$ engendré par P.

Proposition 8 *Si P est un polynôme irréductible de $\mathbb{K}[X]$, alors l'idéal (P) est maximal.*

Démonstration. En effet, si (P) n'est pas maximal, il est contenu dans un idéal I tel que $I \neq \mathbb{K}[X]$. Comme l'anneau $\mathbb{K}[X]$ est principal, I est un idéal principal. Il existe donc $Q \in \mathbb{K}[X]$ tel que $I = (Q)$. Comme $(P) \subset (Q)$, alors $P \in (Q)$, et il existe un polynôme R tel que $P = QR$. Si l'inclusion $(P) \subset (Q)$ est stricte, le polynôme R est de degré au moins égal à 1 est P n'est pas irréductible, ce qui est contraire à l'hypothèse.

Conséquence. Si P est un polynôme irréductible de $\mathbb{K}[X]$, alors l'anneau quotient $\mathbb{K}[X]/(P)$ est un corps.

Soit $\pi : \mathbb{K}[X] \to \mathbb{K}[X]/(P)$ la projection canonique. C'est un homomorphisme d'anneaux surjectif. Le corps $\mathbb{K}$ considéré comme l'ensemble des polynômes de $\mathbb{K}[X]$ de degré 0 est un sous-anneau de $\mathbb{K}[X]$. La restriction de π à $\mathbb{K}$ est injective. En effet, soient $\alpha, \beta \in \mathbb{K}$. Si $\pi(\alpha) = \pi(\beta)$, alors $\pi(\alpha - \beta) = 0$ et $\alpha - \beta \in (P)$. Comme P est de degré au moins égal à 1, on en déduit $\alpha - \beta = 0$ et cette restriction est injective. On peut donc considérer $\mathbb{K}$ comme un sous-corps de $\mathbb{K}[X]/(P)$. Le corps $\mathbb{K}[X]/(P)$ contenant $\mathbb{K}$ est appelé un corps de rupture du polynôme irréductible P. Nous étudierons en détail ce corps dans les chapitres qui suivent.

1.4 Quelques corps particuliers

1.4.1 Corps ordonnés

Définition 8 *Soit $\mathbb{K}$ un corps commutatif et soit $\leq$ une relation d'ordre sur $\mathbb{K}$. On dit que $(\mathbb{K}, \leq)$ est un corps ordonné si*

1. *Le groupe additif $(\mathbb{K}, +)$ est un groupe ordonné pour $\leq$, c'est-à-dire pour tout $a, b, c \in \mathbb{K}$, on a*

$$a \leq b \Rightarrow a + c \leq b + c,$$

2. *La relation d'ordre est compatible avec la multiplication, c'est-à-dire, pour tout $a, b \in \mathbb{K}$, on a*

$$a \geq 0,\ b \geq 0 \Longrightarrow ab \geq 0.$$

Par exemple, le corps des nombres réels $\mathbb{R}$ est un corps ordonné pour la relation d'ordre usuelle. Un corps ordonné est nécessairement de caractéristique 0. En effet tous les éléments $0, e, e + e, e + e + e, \cdots$ sont distincts. En particulier, un corps ordonné est infini.

Proposition 9 *Tout sous-corps d'un corps ordonné est aussi ordonné pour la relation d'ordre induite. En particulier, le sous-corps premier d'un corps ordonné est isomorphe à $\mathbb{Q}$.*

Démonstration. La première partie est évidente. Comme tout corps ordonné est infini et donc de caractéristique 0, son corps premier est isomorphe à $\mathbb{Q}$ qui est donc aussi ordonné.

Proposition 10 *Dans un corps ordonné, tous les carrés sont positifs, c'est-à-dire*

$$a^2 \geq 0$$

pour tout $a \in \mathbb{K}$.

Démonstration. Montrons tout d'abord que e est positif ($e \geq 0$). En effet, si $e \leq 0$, alors $-e \geq 0$ et $e(-e) = -e \leq 0$ ce qui contredit notre hypothèse. Ainsi $e \geq 0$. Considérons à présent $a \in \mathbb{K}$. Si $a \geq 0$, alors $aa = a^2 \geq 0$. Si $a \leq 0$, alors $-a \geq 0$ et $a^2 = (-a)(-a) \geq 0$. Ainsi $a^2 \geq 0$ pour tout $a \in \mathbb{K}$.

Définition 9 *Un corps ordonné $\mathbb{K}$ est dit archimédien si pour tout $a \in \mathbb{K}$, il existe deux éléments m et n du sous-corps premier $\mathbb{Q}$ de $\mathbb{K}$ tels que*

$$m \leq a \leq n.$$

Un corps qui ne vérifie pas cette propriété est dit non archimédien.

1.4.2 Corps algébriquement clos

Soit $\mathbb{K}$ un corps commutatif et soit $\mathbb{K}[X]$ l'anneau des polynômes à une indéterminée à coefficients dans $\mathbb{K}$. Si $P = a_0 + a_1X + \cdots + a_nX^n$ est un élément de $\mathbb{K}[X]$ et si $\alpha \in \mathbb{K}$, on note par $P(\alpha)$ le scalaire

$$P(\alpha) = a_0 + a_1\alpha + \cdots + a_n\alpha^n.$$

Définition 10 *Le scalaire $\alpha \in \mathbb{K}$ est appelé racine du polynôme P s'il vérifie $P(\alpha) = 0$.*

Exemples

1. Tout polynôme du premier degré $P = a_0 + a_1X$, avec $a_1 \neq 0$, admet une racine $\alpha = -a_0a_1^{-1}$.
2. Un polynôme réel $P = a_0 + a_1X + a_2X^2 \in \mathbb{R}[X]$ de degré 2 admet une racine si et seulement si son discriminant
$$\Delta = a_1^2 - 4a_0a_2$$
vérifie
$$\Delta \geq 0.$$
3. Tout polynôme $P \in \mathbb{R}[X]$ de degré impair admet une racine.

Définition 11 *Un corps commutatif $\mathbb{K}$ est dit algébriquement clos si tout polynôme $P \in \mathbb{K}[X]$ non constant admet au moins une racine dans $\mathbb{K}$.*

D'après les exemples ci-dessus, les corps $\mathbb{R}$ ou $\mathbb{Q}$ ne sont pas algébriquement clos.

Théorème 1 *(Théorème de d'Alembert). Le corps $\mathbb{C}$ des nombres complexes est algébriquement clos.*

Démonstration. Il existe plusieurs démonstration de ce théorème, également appelé Théorème Fondamental de l'Algèbre. La démonstration la plus simple est probablement celle basée sur le théorème de Liouville dans la théorie des fonctions d'une variable complexe. Soit $P \in \mathbb{C}[X]$. Supposons que P n'ait pas de racine dans $\mathbb{C}$. Alors, pour tout $z \in \mathbb{C}$, $P(z) \neq 0$ et la fonction $g(z) = 1/P(z)$ est une fonction entière bornée non constante. Or toute fonction entière bornée est constante. D'où la contradiction.

1.5 Les corps de nombres

1.5.1 Le corps $\mathbb{Q}$ des nombres rationnels

Par définition, le corps $\mathbb{Q}$ des nombres rationnels est le corps des fractions de l'anneau $\mathbb{Z}$. Nous avons vu qu'il est isomorphe à tout sous-corps premier d'un corps de caractéristique 0. Il n'est pas algébriquement clos. Considérons par exemple le polynôme rationnel $1 + X^2$. S'il admettait une racine rationnelle $\alpha = \dfrac{p}{q}$ avec $p, q \in \mathbb{Z}$ et $q \neq 0$, alors $\alpha^2 + 1 = 0$ donnerait $p^2 + q^2 = 0$ soit $p = q = 0$ ce qui est impossible. C'est aussi un corps totalement ordonné archimédien, la relation d'ordre total prolongeant la relation d'ordre

naturel de $\mathbb{Z}$. Notons enfin qu'il existe dans $\mathbb{Q}$ des parties majorées non vide ne possédant pas de borne supérieure. Prenons par exemple la partie $A = \{a \leq 0 \in \mathbb{Q},\ a^2 < 2\}$. Cette partie de $\mathbb{Q}$ est non vide et majorée, par exemple, par 2. Elle ne possède pas de borne supérieure. Rappelons qu'une borne supérieure d'une partie A est un élément de $\mathbb{Q}$ qui est le plus petit des majorants. Si cette borne supérieure existe, elle est unique. Si cette borne supérieure est dans A, c'est le plus grand élément de A. Supposons que $A = \{a \leq 0 \in \mathbb{Q},\ a^2 < 2\}$ possède une borne supérieure α. Montrons dans un premier temps que A ne possède pas de plus grand élément. En effet si β est un tel élément, alors il vérifie $\beta^2 < 2$. Il existe un entier n tel que $2 - \beta^2 > 10^{-n}$. Posons $b = \beta + 10^{-n-1}$. Cet élément vérifie $b > \beta$. Comme $\beta < 2$, alors

$$b^2 = \beta^2 + 2\beta.10^{-n-1} + 10^{-2n-2} < \beta^2 + 2\beta.10^{-n-1} + 10^{-n-1} < \beta^2 + 5.10^{-n-1} < \beta^2 + 10^{-n} < 2.$$

Donc $b \in A$. Mais nous avons vu que $b > \beta$ et β est le plus grand élément de A. On a donc une contradiction et A n'a pas de plus grand élément . Comme A ne possède pas de plus grand élément, $\alpha^2 > 2$. Il existe un entier n tel que $\alpha^2 - 2 > 10^{-n}$. On pose $z = \alpha - 10^{-n-1}$. On remarque que $z^2 < 2$. Si $x \geq z$, alors

$$x^2 \geq z^2 = \alpha^2 - 2\alpha.10^{-n-1} + 10^{-2n-2} > \alpha^2 - 2\alpha.10^{-n-1} > \alpha^2 - 10^{-n} > 2$$

et $x \notin A$. Ainsi tout élément de A est inférieur à est inférieur à z . Donc z est un majorant de A. Mais par hypothèse, $z < \alpha$ Ceci contredit la définition de α. Ainsi la partie A n'a pas de borne supérieure.

1.5.2 Le corps $\mathbb{R}$ des nombres réels

Le corps des réels se définit à partir de $\mathbb{Q}$ mais par des approches plutôt reliées à l'analyse qu'à l'algèbre. En effet, un des défauts majeurs de $\mathbb{Q}$ pour faire de l'analyse (étude des fonctions d'une variable rationnelle, suites et séries rationnelles) est du au fait que $\mathbb{Q}$ n'est pas complet pour la distance usuelle. D'où l'idée de "grossir" $\mathbb{Q}$ de manière minimale afin d'obtenir un corps complet dans lequel $\mathbb{Q}$ se plonge naturellement. Il existe donc plusieurs voies de construction du corps des réels. La première est de construire le plus petit corps contenant $\mathbb{Q}$ contenant toutes les limites des suites de Cauchy. On préfère ici une approche plus algébrique basée sur les coupures de Dedekind.

Définition 12 *On appelle coupure de $\mathbb{Q}$, toute partition (A_1, A_2) de l'ensemble des nombres rationnels en deux sous-ensembles tels que tout élément de A_1 soit strictement inférieur à tout élément de A_2.*

Exemples

1. Tout nombre rationnel r permet de définir une coupure : $A_1 = \{s \in \mathbb{Q},\ s \leq r\}$, $A_2 = \{s \in \mathbb{Q},\ s \geq r\}$ et (A_1, A_2) est une coupure de $\mathbb{Q}$. Notons que dans ce cas, A_1 admet r comme plus grand élément.
2. L'existence d'un plus grand élément dans A_1 pour une coupure quelconque (A_1, A_2) n'est pas en général assurée. Prenons par exemple la coupure suivante donnée par $A_2 = \{s \in \mathbb{Q}, s > 0,\ s^2 \leq 2\}$, et $A_1 = \mathbb{Q} - A_2$ son complémentaire. D'après le paragraphe précédent, A_1 n'a pas de plus grand élément .

Remarque Considérons une coupure (A_1, A_2) de $\mathbb{Q}$. Le sous-ensemble A_1, que l'on peut supposer non vide et non égal à $\mathbb{Q}$, vérifie

— Soit $r \in A_1$. Si $s \in \mathbb{Q}$ vérifie $s < r$, alors $s \in A_1$. En effet, si $s \in A_2$, tout élément de A_1 doit être inférieur à s, ce qui est contraire à notre hypothèse.

— Si $r \in A_1$, il existe $s \in A_1$ tel que $s < r$. En effet, dans le cas contraire, tout élément s vérifiant $s < r$ serait dans A_2 ce qui est impossible.

Inversement, tout sous-ensemble A_1 vérifiant les propriétés ci-dessus définit une coupure $(A_1, \mathbb{Q} - A_1)$.

Notons par $\mathbb{R}$ l'ensemble des coupures de $\mathbb{Q}$.

Définition d'une addition dans $\mathbb{R}$. Soient (A_1, A_2) et (B_1, B_2) deux coupures de $\mathbb{Q}$. Posons

$$(A_1, A_2) + (B_1, B_2) = (C_1, C_2)$$

avec

$$C_1 = \{r + s,\ r \in A_1, s \in B_1\}$$

et $C_2 = \mathbb{Q} - C_1$. Le couple (C_1, C_2) définit une coupure de $\mathbb{Q}$. En effet, supposons qu'il existe $t_2 \in C_2$ inférieur à un élément $r + s$ de C_1. On a alors $t_2 - s < r$ ce qui implique $t_2 - s \in A_1$. D'où $t_2 = (t_2 - s) + s \in C_1$ ce qui est impossible. L'addition est bien une opération interne dans $\mathbb{R}$. Vérifions que cette addition munit $\mathbb{R}$ d'une structure de groupe abélien.

— L'addition est associative et commutative. Ceci se déduit des propriétés de l'addition dans $\mathbb{Q}$.

— Soit $(\overline{0}, \mathbb{Q} - \overline{0})$ la coupure associée au rationnel $0 \in \mathbb{Q}$. rappelons que

$$\overline{0} = \{s \in \mathbb{Q},\ s < 0\}.$$

Alors $(\overline{0}, \mathbb{Q} - \overline{0})$ est élément neutre de l'addition dans $\mathbb{R}$. En effet, soit $r + s$ un rationnel tel que $r \in A_1$ et $s \in \overline{0}$.

— Tout élément $(A_1, A_2) \in \mathbb{R}$ admet un opposé. Considérons le sous-ensemble, noté $-A_1$ définit par

$$-A_1 = \{s \in \mathbb{Q}, s + r < 0, \forall r \in A_1\}.$$

Ce sous-ensemble définit une coupure $(-A_1, \mathbb{Q} - (-A_1))$ de $\mathbb{Q}$. En effet A_1 est non vide car si $u \in A_2$, alors $u > r$ pour tout $r \in A_1$ et donc $r - u < 0$ et $(-u) \in -A_1$. Soit $t \notin -A_1$. Il existe $r \in A_1$ tel que $t + r \geq 0$. Ainsi $t + r \geq 0 > r + s$ pour tout $s \in -A_1$ et donc $t > s$ pour tout $s \in -A_1$ On a donc bien une coupure. Elle vérifie

$$(A_1, A_2) + (-A_1, \mathbb{Q} - (-A_1)) = (\overline{0}, \mathbb{Q} - \overline{0}).$$

En effet, si $r \in A_1$ et $s \in -A_1$ alors, par définition de $-A_1$, $r + s < 0$ et donc $r + s \in \overline{0}$).

Définition d'une multiplication dans $\mathbb{R}$. Considérons, dans un premier temps, deux coupures (A_1, A_2), (B_1, B_2), les sous-ensembles A_1, B_1 vérifiant les conditions de la Remarque (1.5.2), telles qu'il existe $a, b \in \mathbb{Q}$, $a > 0$, $b > 0$ et $a \in A_1$ et $b \in B_1$. On pose alors, dans ce cas

$$(A_1, A_2).(B_1, B_2) = (C_1, C_2)$$

avec

$$C_1 = \{x \in \mathbb{Q}, \exists a > 0 \in A_1, \exists b > 0 \in B_1, x \leq ab\}.$$

On vérifie sans peine que C_1 vérifie les conditions de la Remarque (1.5.2) et donc (C_1, C_2) est bien une coupure de $\mathbb{Q}$. Posons également

$$(A_1, A_2).(\overline{0}, \mathbb{Q} - \overline{0}) = (\overline{0}, \mathbb{Q} - \overline{0}).(A_1, A_2) = (\overline{0}, \mathbb{Q} - \overline{0}).$$

Etendons la définition de ce produit à toutes les coupures de la façon suivante :

— $(-(A_1, A_2)).(B_1, B_2) = (A_1, A_2).(-(B_1, B_2)) = -((A_1, A_2).(B_1, B_2))$,

— $(-(A_1, A_2)).(-(B_1, B_2)) = (-(A_1, A_2)).(-(B_1, B_2)) = (A_1, A_2).(B_1, B_2)$

où $-(A_1, A_2)$ désigne l'opposé de la coupure (A_1, A_2).

Cette multiplication vérifie les propriétés suivantes :

— Elle est commutative.

— La coupure $(\overline{1}, \mathbb{Q} - \overline{1})$ est élément neutre.
— Toute coupure différente de $(\overline{0}, \mathbb{Q} - \overline{0})$ admet un inverse. En effet, supposons dans un premier temps que (A_1, A_2) est une coupure telle que A_1 contienne un élément $a > 0$. Considérons le sous-ensemble

$$B_1 = \{x \in \mathbb{Q},\ xa \leq 1\ \forall a > 0 \in A_1\}.$$

Il vérifie les conditions de la Remarque (1.5.2) et $(B_1, B_2 = \mathbb{Q} - B_1)$ est une coupure. Par définition de B_1, on a bien $(A_1, A_2).(B_1, B_2) = (\overline{1}, \mathbb{Q} - \overline{1})$. On la note dans ce cas, $(A_1, A_2)^{-1}$. Si A_1 ne contient aucun élément positif, alors on pose

$$(A_1, A_2)^{-1} = -(-A_1, A_2)^{-1}.$$

— La multiplication est distributive par rapport à l'addition. On vérifie cette identité sur les coupures (A, A') telles que A contienne un élément positif. En effet, dans ce cas $(A_1, A_2).((B_1, B_2)+(C_1, C_2)) = (D_1, D_2)$ avec $D_1 = \{x \in \mathbb{Q}, \exists a > 0 \in A_1, b > 0 \in B_1, c > 0 \in C_1, x \leq a(b+c)\}$. Mais $a(b+c) = ab+ac$. Ainsi (D_1, D_2) correspond à la coupure $(A_1, A_2).(B_1, B_2) + (A_1, A_2).(C_1, C_2)$. Les autres cas s'en déduisent.

Conséquence. $\mathbb{R}$ *est un corps commutatif.*

Nous pouvons munir $\mathbb{R}$ d'une relation d'ordre compatible avec la structure de corps en posant

$$(A_1, A_2) \leq (B_1, B_2) \Longleftrightarrow A_1 \subset B_1.$$

Pour cette relation d'ordre total, la propriété d'Archimède est vérifiée.

Conséquence. $\mathbb{R}$ *est un corps commutatif totalement ordonné archimédien.*

Proposition 11 *Toute partie non vide et majorée de* $\mathbb{R}$ *admet un plus petit majorant.*

Cette proposition fondamentale est assi connue sous le nom de l'axiome de la borne supérieure. Soient E un ensemble ordonné et A une partie de E non vide et majorée. Si l'ensemble des majorants de A admet un élément minimum m, alors m est appelé borne supérieure de A. On dit que E satisfait l'axiome de la borne supérieure, si toute partie non vide majorée de E admet une borne supérieure. La proposition précédente précise que $\mathbb{R}$, comme corps totalement ordonné, vérifie cette propriété.

Démonstration. Tout d'abord, pour simplifier les notations, nous désignerons par une simple lettre (grecque par exemple) les éléments de $\mathbb{R}$, ainsi $\alpha \in \mathbb{R}$ désignera une coupure (A, B) de $\mathbb{Q}$, en supposant de plus que A qui est non vide et distinct de $\mathbb{Q}$ vérifie les conditions :

1. Si $r \in A$ et si $s \in \mathbb{Q}$ est tel que $s < r$, alors $s \in A$,
2. pour tout $s \in A$, il existe $r \in A$ tel que $s < r$.

La relation d'ordre s'interprète ainsi. Soient $\alpha, \beta \in \mathbb{R}$ tels que $\alpha \neq \beta$. Alors $\alpha < \beta$ si et seulement si les coupures correspondantes (A, B) et (A', B') vérifient $A \subset A'$. Montrons que R vérifie la propriété de la borne supérieure. Soit X une partie non vide majorée de $\mathbb{R}$. Soit $\beta = \bigcup_{\alpha \in A} \alpha$. Alors β correspond à une coupure non vide car elle contient A. Si γ est un majorant de A, alors $\beta < \gamma$ ce qui implique que la coupure correspondant à β n'est pas égale à $\mathbb{Q}$. Ainsi tout majorant de A est supérieur à γ et donc γ est une borne supérieure.

Théorème 2 *$\mathbb{R}$ est un corps commutatif, totalement ordonné, archimédien et satisfaisant la propriété de la borne supérieure.*

Il existe une autre construction du corps des réels à partir de celui des rationnels. La construction précédente est essentiellement basée sur le fait que $\mathbb{Q}$ ne possède pas la propriété de la borne supérieure, son extension $\mathbb{R}$ possède les propriétés basiques de $\mathbb{Q}$, relation d'ordre adaptée, Archimède, mais, c'est le point fondamental, vérifie la propriété de la borne supérieure. La deuxième construction part du constat qu'il existe sur $\mathbb{Q}$ des suites de Cauchy qui ne convergent pas. L'idée est donc de construire une extension de $\mathbb{Q}$ dans laquelle toutes les suites de Cauchy, en particulier celles de $\mathbb{Q}$, convergent.

Définition 13 *On appelle suite de Cauchy dans $\mathbb{Q}$ toute suite (u_n) telle que*

$$\forall \varepsilon \in \mathbb{Q}, \varepsilon > 0, \exists n_0 \in \mathbb{N},\ \forall p, q \in \mathbb{N}, p, q > n_0 \longrightarrow |u_p - u_q| < \varepsilon.$$

Par exemple, toute suite dans $\mathbb{Q}$ qui est convergente est une suite de Cauchy. Ceci est en général démontré dans le cours d'analyse de première année. Mais la réciproque est fausse. Considérons, par exemple, la suite des rationnels construite ainsi : u_n est le plus grand rationnel positif comportant n chiffres après la virgule et tel que son carré soit strictement inférieur à 2. Cette suite ne converge pas, en effet sa limite devrait vérifier $l^2 = 2$ et il n'existe aucun rationnel vérifiant cette égalité. Par contre, on montre que cette suite est de Cauchy. Il existe donc des suites de Cauchy dans $\mathbb{Q}$ qui ne converge pas. Notons, toutefois, que toute suite de Cauchy est bornée.

Considérons l'ensemble E des suites de Cauchy dans $\mathbb{Q}$. Cet ensemble est non vide et muni de l'addition et de la multiplication terme à terme des suites, E est un anneau commutatif unitaire. Soit I le sous-ensemble de E constitué des suites de Cauchy qui convergent vers 0. C'est un sous-anneau de E. Soit $u \in E$ et $v \in I$. Comme u est une suite de Cauchy, elle est bornée et le produit des suites u et v, comme v tend vers 0, tend aussi vers 0. Ainsi $uv \in I$ et I est un idéal de E.

Lemme 3 *I est un idéal maximal de E.*

Démonstration. Soit J un idéal de E contenant strictement I. Il existe une suite $u = (u_n) \in J$ qui ne converge pas vers 0. Nous allons montrer que la suite v définie par $v_n = u_n^{-1}$ est bien définie et appartient à E. Comme la suite u ne tend pas vers 0, à partir d'un certain rang, les termes u_n sont non nuls et donc u_n^{-1} est bien défini. On a

$$\left|\frac{1}{u_p} - \frac{1}{u_q}\right| = \left|\frac{u_q - u_p}{u_p u_q}\right|.$$

Or, soit ϵ_1 donné. Il existe n_1 tel que pour tout $n > n_1$, on ait $|u_n| > \epsilon_1$. De même, comme u est de Cauchy, pour ϵ_2 donné, il existe n_2 tel que pour tout $p, q > n_2$ on ait $|u_q - u_p| < \epsilon_2$. Ainsi, pour tout $p, q > Max(n_1, n_2)$, on a

$$\left|\frac{1}{u_p} - \frac{1}{u_q}\right| < \frac{\epsilon_2}{\epsilon_1^2}.$$

Prenons $\epsilon_2 = \epsilon_1^3$. On en déduit

$$\left|\frac{1}{u_p} - \frac{1}{u_q}\right| < \epsilon_1$$

et la suite $\frac{1}{u_n}$ est de Cauchy. Comme J est un idéal, le produit des suites (u_n) et (u_n^{-1}) est dans J. Ainsi J contient l'élément neutre donnée par la suite constante (1). Donc $J = E$. Ceci montre que I est maximal.

Conséquence. L'anneau quotient E/I est un corps. Par construction, il est commutatif. On démontre, mais nous ne le ferons pas dans l'immédiat, que ce corps est totalement ordonné, archimédien et complet. De là, on en déduit, non sans difficulté, qu'il vérifie la propriété de la borne supérieure. Ainsi ce corps est isomorphe à $\mathbb{R}$.

1.5.3 Le corps des nombres complexes

Considérons sur $\mathbb{R}^2$, la structure de groupe abélien additif associé à l'addition

$$(x, y) + (x', y') = (x + x', y + y').$$

Si nous considérons comme multiplication, le produit composantes par composantes, c'est-à-dire

$$(x, y) * (x', y') = (xx', yy')$$

le triplet $(\mathbb{R}^2, +, *)$ est un anneau unitaire, mais n'est pas un corps, l'élément $(1, 0)$, par exemple, n'a pas d'inverse. Par contre, si nous définissons le produit par

$$(x, y) \cdot (x', y') = (xx' - yy', xy' + x'y)$$

alors le triplet, noté $\mathbb{C}$, est un corps commutatif. En effet, on montre aisément que le produit est associatif, distributif par rapport à l'addition et l'inverse de $(x, y) \neq (0, 0)$ est $\left(\frac{x}{x^2+y^2}, -\frac{y}{x^2+y^2}\right)$. Le sous-ensemble constitué des paires $(x, 0)$ avec $x \in \mathbb{R}$ est un sous-corps isomorphe à $\mathbb{R}$.

Pour retrouver les notations classiques, nous poserons $i = (0, 1)$ et par abus, on écrira, pour tout $x \in \mathbb{R}$, $x = (x, 0)$. Ainsi le nombre complexe (tout élément de $\mathbb{C}$) $z = (x, y)$ s'écrit

$$z = x + iy$$

et x est appelée la partie réelle de z et y sa partie imaginaire. Notons que i vérifie

$$i^2 = (-1, 0) = -1.$$

Ainsi, dans le corps des complexes, le polynôme $X^2 + 1$ a au moins une racine et n'est pas irréductible. Rappelons, toutefois, que $X^2 + 1$ est irréductible en tant que polynôme réel.

Proposition 12 *Le corps $\mathbb{C}$ des nombres complexes est isomorphe au corps de rupture $\mathbb{R}[X]/(X^2+1)$ du polynôme irréductible $X^2 + 1$.*

Démonstration. Considérons le corps de rupture $\mathbb{R}[X]/(X^2 + 1)$ du polynôme réel irréductible $X^2 + 1$. Notons par I la classe, dans ce quotient, du polynôme X. Chaque élément de $\mathbb{R}[X]/(X^2 + 1)$ s'écrit de manière unique $a + bI$ avec $a, b \in \mathbb{R}$. L'addition et la multiplication sont données par

$$\begin{cases} (a + bI) + (c + dI) = (a + c) + (b + d)I, \\ (a + bI)(c + dI) = (ac - bd) + (ad + bc)I. \end{cases}$$

On en déduit que l'application

$$f : \mathbb{C} \to \mathbb{R}[X]/(X^2 + 1)$$

définie par $f(a + ib) = a + bI$ est un isomorphisme de corps.

1.5.4 Le corps des quaternions

Considérons sur $\mathbb{R}^4$, la structure de groupe abélien additif associé à l'addition

$$(x_1, x_2, x_3, x_4) + (x'_1, x'_2, x'_3, x'_4) = (x_1 + x'_1, x_2 + x'_2, x_3 + x'_3, x_4 + x'_4).$$

Définissons la multiplication par

$$(x_1, x_2, x_3, x_4) \cdot (x'_1, x'_2, x'_3, x'_4) = (y_1, y_2, y_3, y_4)$$

avec

$$\begin{cases} y_1 &= x_1x'_1 - x_2x'_2 - x_3x'_3 - x_4x'_4, \\ y_2 &= x_1x'_2 + x_2x'_1 + x_3x'_4 - x_4x'_3, \\ y_3 &= x_1x'_3 + x_3x'_1 - x_2x'_4 + x_4x'_2, \\ y_4 &= x_1x'_4 + x_4x'_1 + x_2x'_3 - x_3x'_2. \end{cases}$$

Alors le triplet $(\mathbb{R}^4, +, \cdot)$, noté $\mathbb{H}$, est un corps non commutatif. Nous laissons le lecteur vérifier que cette multiplication est associative. Comme ce produit est défini par une application bilinéaire à valeurs dans $\mathbb{R}^4$, le produit est distributif par rapport à l'addition. Son élément neutre est $e = (1, 0, 0, 0)$. L'inverse de (x_1, x_2, x_3, x_4), supposé non nul, est l'élément (y_1, y_2, y_3, y_4) donné par

$$\begin{cases} y_1 = \dfrac{x_1}{x_1^2 + x_2^2 + x_3^2 + x_4^2}, \\ y_2 = \dfrac{-x_2}{x_1^2 + x_2^2 + x_3^2 + x_4^2}, \\ y_3 = \dfrac{-x_3}{x_1^2 + x_2^2 + x_3^2 + x_4^2}, \\ y_4 = \dfrac{-x_4}{x_1^2 + x_2^2 + x_3^2 + x_4^2}. \end{cases}$$

Ainsi $\mathbb{H}$ est un corps. Posons

$$1 = (1, 0, 0, 0),\ i = (0, 1, 0, 0),\ j = (0, 0, 1, 0),\ k = (0, 0, 0, 1).$$

Tout élément de $\mathbb{H}$, appelé nombre quaternion, s'écrit donc

$$z = x_1 1 + x_2 i + x_3 j + x_4 k.$$

Comme $ij = k,\ jk = i,\ ki = j$ et $ji = -k,\ kj = -ji\ ik = -j$, ce corps n'est pas commutatif.

Proposition 13 *Le corps des quaternions $\mathbb{H}$ contient un sous-corps isomorphe à $\mathbb{C}$.*

Démonstration. Soit K l'ensemble des quaternions de la forme $(x_1, x_2, 0, 0)$. Alors K est un sous-corps de $\mathbb{H}$ isomorphe à $\mathbb{C}$. En effet, si $(x_1, x_2, 0, 0), (x'_1, x'_2, 0, 0)$ sont des éléments de K, alors

- $(x_1, x_2, 0, 0) - (x'_1, x'_2, 0, 0) = (x_1 - x'_1, x_2 - x'_2, 0, 0) \in K$,
- $(x_1, x_2, 0, 0).(x'_1, x'_2, 0, 0) = (x_1x'_1 - x_2 - x'_2, x_1x'_2 + x_2x'_1, 0, 0) \in K$,
- L'inverse de $(x_1, x_2, 0, 0)$ est $\left(\dfrac{x_1}{x_1^2 + x_2^2}, \dfrac{-x_2}{x_1^2 + x_2^2}, 0, 0\right)$. Il appartient aussi à K

Donc $(K, +, \cdot)$ est un sous-corps de $\mathbb{H}$. Soit l'application

$$f : \mathbb{C} \to K$$

définie par

$$f(x_1 + ix_2) = (x_1, x_2, 0, 0).$$

Cette application est bijective et vérifie

$$f(z + z') = f(z) + f(z'),\ f(zz') = f(z)f(z')$$

pour tout $z, z' \in \mathbb{C}$. Donc f est un isomorphisme de corps de $(\mathbb{C}, +, \cdot)$ sur $(K, +, \cdot)$.

Remarques

1. On appelle algèbre sur un corps commutatif $\mathbb{K}$ un espace vectoriel A muni d'une multiplication distributive par rapport à l'addition. Si cette multiplication est associative, on parlera d'algèbre associative. Pour une étude approfondie des algèbres, on pourra se référer à l'ouvrage

   ALGEBRE MULTILINEAIRE
   http ://ramm-algebra-center.monsite-orange.fr/index.html
   ou
   http ://www.livres-mathematiques.fr/accueil.html

   En particulier, si A est une algèbre associative, alors A est un anneau pour l'addition et la multiplication. On peut donc s'intéresser aux structures d'algèbres associatives sur l'espace vectoriel $\mathbb{R}^n$. En particulier, parmi ces structures d'algèbres associatives sur $\mathbb{R}^n$, en existe-t-il dont l'anneau A soit un corps. La réponse est positive, déjà pour $n = 1$, $\mathbb{R}$ est un $\mathbb{R}$-espace vectoriel de dimension 1 qui est aussi un corps. Nous avons vu que $\mathbb{R}^2$ muni de la multiplication des nombres complexes est aussi un corps commutatif. Enfin, $\mathbb{R}^4$ muni de la multiplication des quaternions, est aussi un corps. En fait, ce sont les seuls cas possibles.
2. On appelle algèbre de composition sur un corps commutatif $\mathbb{K}$, une algèbre A non nécessairement associative vérifiant
   (a) La multiplication est unitaire. On notera 1 cet élément neutre.
   (b) Il existe une forme quadratique non dégénérée q sur l'espace vectoriel sous-jacent à A telle que $q(1) = 1$ et telle que, quels que soient les éléments $x, y \in A$,

   $$q(xy) = q(x)q(y).$$

   Pour une telle algèbre de composition, on note pour tout $x, y \in A$,

   $$N(x) = q(x),\ T(x) = N(x + 1) - N(x) - 1$$

   Les applications N et T sont en général appelées respectivement norme et trace et T est une forme linéaire non nulle sur A. On vérifie l'identité, pour tout élément $x \in A$, on a

   $$x^2 - T(x)x + N(x) = 0.$$

   On a le résultat suivant

   Proposition 14 *Toute algèbre de composition associative sur* $\mathbb{R}$ *est de dimension* $1, 2$ *ou* 4 *et est isomorphe soit à* $\mathbb{R}$*, soit à* $\mathbb{C}$ *soit à* $\mathbb{H}$*.*

   On retrouve donc le résultat de la remarque précédente.

1.5.5 Le corps des nombres p-adiques

Soit p un nombre premier fixé dans tout ce paragraphe. L'anneau $\mathbb{Z}/p\mathbb{Z}$ est un corps. Soit $n \in \mathbb{N}$ un entier non nul. Dès que $n > 1$, l'anneau $\mathbb{Z}/p^n\mathbb{Z}$ n'est pas intègre et n'est pas un corps. Notons par $\overline{r}^{(n)}$ la classe de l'élément $r \in \mathbb{Z}$ dans $\mathbb{Z}/p^n\mathbb{Z}$. Considérons l'application

$$\varphi_n : Z/p^n\mathbb{Z} \to Z/p^{n-1}\mathbb{Z}$$

définie par

$$\varphi_n(\overline{r}^{(n)}) = \overline{r}^{(n-1)}.$$

Cette application est bien définie car si $s \in \overline{r}^{(n)}$, alors il existe un entier k tel que $s = r + kp^n$. On a donc $s = r + kpp^{n-1}$ et donc $s \in \overline{r}^{(n-1)}$. L'application φ_n est un homomorphisme d'anneau surjectif. Son noyau est l'ensemble des classes $\overline{r}^{(n)}$ telles que $\overline{r}^{(n-1)} = 0$, c'est-à-dire $r = kp^{n-1}$.

Exemple. Prenons $p = 3$. Alors

$$\varphi_2 : Z/9\mathbb{Z} \to Z/3\mathbb{Z}$$

vérifie $\varphi_2(\overline{0}^{(2)}) = \varphi_2(\overline{3}^{(2)}) = \varphi_2(\overline{6}^{(2)}) = \overline{0}^{(1)}$, $\varphi_2(\overline{1}^{(2)}) = \varphi_2(\overline{4}^{(2)}) = \varphi_2(\overline{7}^{(2)}) = \overline{1}^{(1)}$ et $\varphi_2(\overline{2}^{(2)}) = \varphi_2(\overline{5}^{(2)}) = \varphi_2(\overline{8}^{(2)}) = \overline{2}^{(1)}$.

Définition 14 *On appelle anneau des entiers p-adiques, l'anneau noté $\mathbb{Z}_p$ et constitué des suites*

$$x = (\cdots, x_n, \cdots, x_1)$$

telles que

$$\begin{cases} x_n \in \mathbb{Z}/p^n\mathbb{Z}, \\ \varphi_n(x_n) = x_{n-1}, \ n \geq 2, \end{cases}$$

L'addition et la multiplication de cet anneau sont définies composantes par composantes.

Par exemple, pour $p = 3$, la suite $(\cdots, \overline{1}^{(n)}, \overline{1}^{(n-1)}, \cdots, \overline{1}^{(2)}, \overline{1}^{(1)})$ est un entier 3-adique.

Proposition 15 *Un élément $x = (\cdots, x_n, \cdots, x_1)$ de $\mathbb{Z}_p$ est inversible si et seulement si aucune des composantes x_n n'est divisible par p.*

Démonstration. Déterminons les éléments inversibles de $\mathbb{Z}/p^n\mathbb{Z}$. Soit $x \in \mathbb{Z}/p^n\mathbb{Z}$. Notons encore par x un représentant dans $\mathbb{Z}$ vérifiant $0 \leq x \leq p^{n-1}$. Ecrivons ce nombre en base p. Il existe des entiers $x_0, x_1, \cdots, x_{n-1}$ tels que pour tout $i = 0, \cdots, n-1$ on ait $0 \leq x_i \leq p-1$ et

$$x = x_0 + x_1 p + x_2 p^2 + \cdots + x_{n-1} p^{n-1}.$$

Ainsi $x \in Z/p^n\mathbb{Z}$ est inversible si et seulement si $x_0 \neq 0$. Ceci est équivalent à dire que x n'appartient pas à l'idéal principal (p) engendré par p dans $\mathbb{Z}/p^n\mathbb{Z}$. Soit

$$\pi_0 : Z/p^n\mathbb{Z} \to Z/p\mathbb{Z}$$

la surjection canonique. Alors x est inversible dans $Z/p^n\mathbb{Z}$ si et seulement si $\pi_0(x)$ est inversible dans $Z/p\mathbb{Z}$. Considérons à présent un entier p-adique $x \in \mathbb{Z}_p$. Il s'écrit $x = (\cdots, x_n, \cdots, x_1)$ et x est inversible si et seulement si chacune des composantes x_n est inversible soit, d'après ci-dessus $x_n \notin (p)$.

Corollaire 2 *Soit U le groupe des éléments inversibles de $\mathbb{Z}_p$. Tout élément $x \in \mathbb{Z}_p$ non nul s'écrit de manière unique $x = p^n u$ avec $u \in U$.*

Démonstration. Considérons la surjection

$$\epsilon_n : \mathbb{Z}_p \to \mathbb{Z}/p^n\mathbb{Z}$$

qui à x fait correspondre sa composante $x_n \in \mathbb{Z}/p^n\mathbb{Z}$. Il est clair que tout élément x tel que $x_n \in (p^n)$ vérifie $\epsilon_n(x) = 0$ Mais ceci implique $x_i = 0$ pour $i < n$ et $x_i \in (p^n)$ pour tout $i > n$. Ainsi le noyau de ϵ_n contient tous les entiers p-adiques dont les composantes sont dans les idéaux (p^n) de chaque $\mathbb{Z}/p^k\mathbb{Z}$. Inversement, supposons que chaque composante x_i soit dans (p^n). On a donc $x_i = p^n y_i$ avec $y_i = 0$ pour $i < n$. Posons $y_i = z_{i-p}$ pour $i \geq n$. Alors $x_i = p^n z_{i-n}$ et la suite (z_i) définie un entier p-adique qui est inversible. D'où la proposition.

Remarque. L'anneau $\mathbb{Z}_p$ est intègre.

Définition 15 *On appelle corps des nombres p-adiques, et on le note $\mathbb{Q}_p$, le corps des fractions de l'anneau $\mathbb{Z}_p$ des entiers p-adiques.*

Pour tout entier p-adique x non nul, il existe $n \in \mathbb{N}$ et un entier p-adique inversible u tel que $x = p^n u$. Posons

$$v_p(x) = n.$$

et $v_p(0) = +\infty$. Cette application v_p vérifie

$$\begin{cases} v_p(xy) = v_p(x)v_p(y) \\ v_p(x+y) \geq Inf(v_p(x), v_p(y)). \end{cases}$$

On dit que v_p est une valuation. Ceci permet de définir une distance sur $\mathbb{Z}_p$ par

$$d(x, y) = e^{v_p(x-y)}.$$

Il est aisé d'étendre cette distance à $\mathbb{Q}_p$. En effet, tout élément non nul de $\mathbb{Q}_p$ s'écrit de manière unique $p^n u$ avec $u \in U$ et $p \in \mathbb{Z}$. On pose également $v_p(x) = n$. Cette application est à valeurs dans $\mathbb{Z}$ et $v_p(x) \geq 0$ si et seulement si x est un entier p-adique. On posera également dans $\mathbb{Q}_p$:

$$d(x, y) = e^{v_p(x-y)}.$$

Muni de cette distance $\mathbb{Q}_p$ est un corps complet dans lequel $\mathbb{Q}$ est dense.

1.6 EXERCICES

Exercice 1. Soit A un anneau unitaire tel que $A^* = A - \{0\}$ soit un groupe multiplicatif. Montrer que A est un corps.

Exercice 2. Montrer qu'un anneau A est un corps si et seulement si il a au moins deux éléments et pour tout $a \in A^*$ et tout $b \in A$, chacune des équations

$$\begin{cases} ax = b, \\ ya = b \end{cases}$$

possède au moins une solution dans A.

Exercice 3. Montrer que tout anneau intègre ayant un nombre fini d'éléments est un corps.

Exercice 4.

1. Montrer que tout élément A du corps des quaternions $\mathbb{H}$ s'écrit de manière unique :

   $$A = a1 + bI + cJ + dK$$

   avec $a, b, c, d \in \mathbb{R}$ où

   $$1 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix},\ I = \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix},\ J = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix},\ K = \begin{pmatrix} 0 & -i \\ -i & 0 \end{pmatrix}.$$

2. Etablir la table de multiplication concernant les éléments $1, I, J, K$.
3. Soit $A = a1 + bI + cJ + dK$ un élément de $\mathbb{H}$. On pose $\overline{A} = a1 - bI - cJ - dK$. Démontrer quelques propriétés de l'application $A \to \overline{A}$, appelée conjugaison.
4. On considère $\mathbb{H}$ comme un espace vectoriel rsel de dimension 4. Montrer que l'application

   $$A \to \sqrt{A\overline{A}}$$

   est bien définie et est une norme.

Exercice 5. On désigne par $\mathbb{Q}(\sqrt{2})$ l'ensemble des nombres réels de la forme

$$a + b\sqrt{2}$$

avec $a, b \in \mathbb{Q}$. Montrer que $\mathbb{Q}(\sqrt{2})$ est un sous-corps de $\mathbb{R}$ contenant $\mathbb{Q}$.

Exercice 6. Soient $\mathbb{K}_1$ et $\mathbb{K}_2$ deux corps. Soit f $K_1 \to \mathbb{K}_2$ un homomorphisme non nul de corps.

1. Montrer que f est injectif.
2. On suppose maintenant $\mathbb{K}_1 = \mathbb{K}_2$ et que ce corps soit fini. Montrer alors que f est bijectif.

Exercice 7. Déterminer à isomorphisme près tous les corps de cardinalité 2 ou 3 ou 6.

Exercice 8. Soient A un anneau intègre unitaire et $\mathbb{K}$ un corps commutatif. Soit $f : A \to \mathbb{K}$ un homomorphisme d'anneau unitaire. Montrer que f se prolonge de manière unique en un homomorphisme de corps

$$f^* : \mathbb{K}_A \to \mathbb{K}$$

où $\mathbb{K}_A$ est le corps des fractions de A.

Exercice 9. Soit $\mathbb{K}$ un corps fini. Montrer que l'homomorphisme de Frobenius est un automorphisme. Déterminer cet automorphisme lorsque $\mathbb{K} = \mathbb{Z}/p\mathbb{Z}$, p étant premier.

Exercice 10. Montrer que le polynôme $P = X^2 + X + 1$ est irréductible dans $\mathbb{Z}/2\mathbb{Z}$. Posons $\theta = \pi(X)$ où $\pi : \mathbb{K}[X] \to \mathbb{K}[X]/(P)$ est la surjection canonique. Déterminer en fonction de θ les éléments du corps de rupture de P. Ecrire les tables d'addition et de multiplication de ce corps.

Exercice 11. Soit $\mathbb{K}$ un corps commutatif ordonné. Montrer que tout élément $a \in \mathbb{K}$ vérifie $a \geq 0$ ou $-a \geq 0$. Montrer que si a et b sont des éléments non nuls, alors

$$a \leq b, a \geq 0, b \geq 0 \Longrightarrow b^{-1} \leq a^{-1}.$$

Exercice 12. Montrer que le corps $\mathbb{C}$ des nombres complexes n'est pas ordonné.

Exercice 13. Montrer qu'un corps fini n'est jamais algébriquement clos.

Exercice 14. Décomposer comme somme d'inverses distincts d'entiers naturels le nombre rationnel $\frac{5}{7}$. Montrer que, plus généralement, tout nombre rationnel positif peut s'exprimer comme somme d'inverses distincts d'entiers naturels.

Exercice 15. Montrer que le polynôme $P = 2 + X^2$ est n'a pas de racines rationnelles.

Exercice 16.

1. Déterminer toutes les multiplications sur le groupe additif $\mathbb{R}^2$ munissant $\mathbb{R}^2$ d'une structure de corps. Les structures de corps obtenues sont-elles isomorphes à $\mathbb{C}$?
2. Peut-on munir le groupe abélien $(\mathbb{R}^3, +)$ d'une structure de corps ?

Exercice 17. Soit $\mathbb{H}$ le corps des quaternions. On appelle centre de $\mathbb{H}$ l'ensemble

$$Z(\mathbb{H}) = \{q \in \mathbb{H},\ q \cdot u = u \cdot q,\ \forall u \in \mathbb{H}\}.$$

Montrer que $Z(\mathbb{H})$ est un sous-corps commutatif de $\mathbb{H}$ isomorphe à $\mathbb{R}$.

Chapitre 2

Les corps finis

Dans tout ce chapitre, les corps considérés seront toujours supposés commutatifs.

2.1 Quelques généralités

2.1.1 Caractéristique d'un corps fini

Soit $\mathbb{K}$ un corps fini, c'est-à-dire contenant un nombre fini d'éléments. Son sous-corps premier est donc fini. Il existe un nombre premier p tel que ce sous-corps premier soit isomorphe à $\mathbb{Z}/p\mathbb{Z}$. On en déduit que $\mathbb{K}$ est de caractéristique p.

Proposition 16 *Soit $\mathbb{K}$ un corps fini. Alors sa caractéristique est non nulle.*

Exemples de corps finis

— Pour tout entier p premier, $\mathbb{Z}/p\mathbb{Z}$ est un corps à p éléments de caractéristique p. On le note $\mathbb{F}_p$.

— Soit A un anneau intègre fini contenant au moins 2 éléments. Alors A est un corps. *Démonstration.* Soit $a \in A, a \neq 0$. L'application

$$L_a : A \to A$$

définie par $L_a(x) = ax$ est un homomorphisme de groupe additif injectif. En effet $L_a(x + y) = L_a(x)+L_a(y)$ et $La(x) = 0$ implique $ax = 0$. Comme A est intègre, alors $x = 0$ et L_a est injective. Mais A est un ensemble fini. Toute application injective de A à valeurs dans A est surjective donc bijective. Il existe donc un élément a_0 tel que $L_a(a_0) = a$. On a également $L_a(a_0x) = a(a_0x) = ax = L_a(x)$ et comme L_a est injective $a_0x = x$ et ceci pour tout x. Calculons à présent xa_0. On a

$$(xa_0 - x)a = (xa_0)a - xa = x(a_0) - xa = 0$$

et donc, comme A est intègre, $xa_0 = x$. Ainsi a_0 vérifie

$$xa_0 = a_0x = x \text{ pour tout } x \in A$$

et a_0 est un élément neutre pour la multiplication de A et A est donc un anneau intègre fini unitaire. Comme L_a est bijective, il existe $b \in A$ tel que $L_a(b) = ab = a_0$ et b est l'inverse à droite de a. Mais

$$L_a(ba) = a(ba) = (ab)a = a_0a = a = L_a(a_0)$$

montre que $ba = a_0$ et b est l'inverse de a. Comme a a été choisi quelconque non nul dans A, on en déduit que tout élément non nul est inversible et A est un corps.

2.1.2 Cardinalité d'un corps fini

Théorème 3 *Soit $\mathbb{K}$ un corps fini de caractéristique p. Il existe un entier $n \neq 0$ tel que le cardinal de $\mathbb{K}$, $|\mathbb{K}|$, soit égale à p^n.*

Démonstration. Le sous-corps premier de $\mathbb{K}$ est (isomorphe à) $\mathbb{F}_p$. On en déduit que $\mathbb{K}$ est un $\mathbb{F}_p$ espace vectoriel (cette technique sera largement développée dans le paragraphe suivant). Comme $\mathbb{K}$ est fini, cet espace vectoriel est de dimension fini sur $\mathbb{F}_p$. Il est donc isomorphe à $(\mathbb{F}_p)^n$ si $n = \dim_{\mathbb{F}_p} \mathbb{K}$. Comme $(\mathbb{F}_p)^n$ contient p^n éléments, on en déduit le théorème. Ainsi, il peut exister des corps contenant $2, 3, 4 = 2^2, 5, 7, 8, 9 \cdots$ éléments mais il n'existe pas de corps à 6 éléments, 10 éléments $\cdots$

2.1.3 L'homomorphisme de Frobenius sur un corps fini

Proposition 17 *Soit $\mathbb{K}$ un corps fini de caractéristique p. Alors l'homomorphisme de Frobenius*

$$\mathcal{F} : \mathbb{K} \to \mathbb{K}$$

donné par $\mathcal{F}(x) = x^p$ est un automorphisme.

Démonstration. Nous avons vu au chapitre précédent que $\mathcal{F}$ est un homomorphisme de corps. Il est donc injectif. Comme $\mathbb{K}$ est fini, il est aussi surjectif et donc bijectif.

Notons par $Aut(\mathbb{K})$ le groupe pour composition des automorphismes du corps $\mathbb{K}$. Alors si $\mathbb{K}$ est fini de caractéristique p, on a $\mathcal{F} \in Aut(\mathbb{K})$.

Remarque. Si $\mathbb{K} = \mathbb{Z}/p\mathbb{Z} = \mathbb{F}_p$, alors $\mathcal{F} = id$. En effet, soit $x \in \mathbb{F}_p, x \neq 0$. Le groupe $\mathcal{F}_p^*$ des éléments inversibles (ou non nuls) est de cardinalité $p - 1$. On en déduit $x^{p-1} = 1$ et donc $x^p = x$. Ainsi $\mathcal{F}(x) = x$ pour tout $x \in \mathbb{F}_p$ et $\mathcal{F} = id$.

2.2 Le théorème de Wedderburn

2.2.1 Le théorème de Wedderburn

Théorème 4 *Tout corps fini est commutatif*

Démonstration. Soit $\mathbb{K}$ un corps fini. Son centre

$$Z(\mathbb{Z}) = \{x \in \mathbb{K}/xy = yx, \forall y \in \mathbb{K}\}$$

est un sous-corps de $\mathbb{K}$. Supposons $\mathbb{K}$ non commutatif. On a en particulier $Z(\mathbb{K}) \subsetneq \mathbb{K}$. Posons $p = |Z(\mathbb{K})|$. Comme $\mathbb{K}$ est un $Z(\mathbb{K})$-espace vectoriel, alors il existe n tel que $|\mathbb{K}| = q^n$ car il est de dimension finie et isomorphe à $Z(\mathbb{K})^n$. Considérons à présent le groupe, non abélien par hypothèse, $\mathbb{K}^*$. Il est d'ordre $q^n - 1$. Le groupe $\mathbb{K}^*$ opère sur lui-même par automorphisme intérieur. Si $x \in \mathbb{K}^*$, on note $\mathcal{O}(x)$ son orbite relative à cette action

$$\mathcal{O}(x) = \{yxy^{-1}, y \in \mathbb{K}^*\}$$

et $\mathbb{K}^*$ est une réunion disjointe d'orbites. Considérons le stabilisateur de x :

$$S(x) = \{y \in \mathbb{K}^*/yx = xy\}.$$

C'est le groupe multiplicatif de $\tilde{S}(x) = \{y \in \mathbb{K}/yx = xy\}$. Il est clair que $\tilde{S}(x)$ est un sous-corps de $\mathbb{K}$ contenant $Z(\mathbb{K})$, c'est-à-dire qu'on a les inclusions de corps

$$Z(\mathbb{K}) \subset \tilde{S}(x) \subset \mathbb{K}.$$

Ainsi $\tilde{S}(x)$ est aussi un $Z(\mathbb{K})$-espace-vectoriel, on en déduit qu'il existe un entier $m(x)$, $1 \leq m(x) < n$ tel que

$$|\tilde{S}(x)| = q^{m(x)}$$

et donc $|S(x)| = q^{m(x)} - 1$. On en déduit $|\theta(x)| = \dfrac{|\mathbb{K}^*|}{|S(x)|} = \dfrac{q^n - 1}{q^{m(x)} - 1}$.

Rappelons brièvement l'équation des classes, vue dans le cours sur la théorie des groupes :

"Soit G un groupe fini et $Z(G)$ son centre. Soit Ω l'ensemble des classes d'équivalence pour la conjugaison, non réduite à un singleton. Alors

$$|G| = |Z(G)| + \sum_{c \in \Omega} |c|$$

et si $x \in c$, alors

$$|c| = \frac{|G|}{|S(x)|}.$$

Notons toujours par Ω l'ensemble des classes d'équivalence dans $\mathbb{K}^*$. On a donc, en choisissant pour chaque classe $c \in \Omega$ un élément $x_c \in \mathbb{K}^*$. L'équation des classes s'écrit dans ce cas :

$$|\mathbb{K}^*| = q^n - 1 = q - 1 + \sum_{c \in \Omega} \frac{q^n - 1}{q^{m(x_c)} - 1}.$$

Comme $S(x)$ est un sous-groupe de $\mathbb{K}^*$, $q^{m(x_c)} - 1$ divise $q^n - 1$ et donc $m(x_c)$ divise n. La contradiction va reposer sur les factorisations du polynôme $X^n - 1$ par des polynômes cyclotomiques :

$$X^n - 1 = \Pi_{d/n} \Phi_d(X)$$

où d/n désigne les diviseurs de n. La notion de polynômes cyclotomiques sera vue en détail au chapitre 5. Donnons toutefois brièvement leur définition. On considère pour un entier $n > 1$ fixé les racines complexes $n$ième de l'unité :

$$\xi_k = e^{\frac{2ki\pi}{n}}, \ k = 0, \cdots, n-1.$$

La racine ξ_k est dite primitive si k est premier avec n. Notons A_n l'ensemble de ces racines n-ième primitive de l'unité. Par définition le polynôme cyclotomique $\Phi_n(X)$ est :

$$\Phi_n(X) = \Pi_{\xi \in A_n}(X - \xi).$$

L'équation des classes concernant $\mathbb{K}^*$ nous conduit à considérer les polynômes X^{n-1} et $X^{m(x_c)-1}$. Leur factorisation par les polynômes cyclotomiques donne

$$X^n - 1 = \Pi_{d/n}\Phi_d(X), \quad X^{m(x_c)} - 1 = \Pi_{d/m(x_c)}\Phi_d(X).$$

Ainsi on a

$$\frac{X^n - 1}{X^{m(x_c)} - 1} = \Pi_{d \in D}\Phi_d(X)$$

où D désigne les diviseurs de n qui ne divise par $m(x_c)$. Donc

$$q^{n-1} = q - 1 + \Pi_{d \in D}\Phi_d(q).$$

Comme $\Phi_n(q)$ divise $q^n - 1$ et $\Pi_{d \in D}\Phi_d(q)$ il divise donc $q - 1$. On en déduit en particulier que

$$|\Phi_n(q)| \leq q - 1.$$

Mais par définition $\Phi_n(q) = (q - \xi_1) \cdots (q - \xi_l)$, chaque ξ_k étant une racine primitive de l'unité. Elle vérifie en particulier $|\xi_k| = 1$ et $\xi_k \neq 1$. On en déduit immédiatement

$$|q - \xi_k| > q - 1$$

pour chacune des racines primitives ξ_k. Ceci implique

$$|\Phi_n(q)| > (q - 1)^n > q - 1.$$

Ceci contredit le résultat précédent et donc notre hypothèse de départ sur la non commutativité de $\mathbb{K}$.

2.2.2 Le groupe $\mathbb{K}^*$

Proposition 18 *Soit $\mathbb{K}$ un corps fini. Alors le groupe $\mathbb{K}^*$ des éléments inversibles est cyclique.*

Démonstration. D'après le théorème de Weddedrburn, $\mathbb{K}$ est un corps commutatif. Le groupe $\mathbb{K}^*$ est donc un groupe abélien fini.C'est un produit de groupes cycliques. Pour montrer qu'il est cyclique nous utiliserons le résultat suivant (voir le cours sur les groupes)

"Soit G un groupe fini d'ordre n tel que pour chaque diviseur d de n l'équation $x^d = 1$ a au plus d racines distinctes dans G. Alors G est cyclique."

Supposons $|\mathbb{K}^*| = n$ (si $\mathbb{K}$ est de caractéristique p, alors n est du type $p^m - 1$). Pour tout diviseur d de n, l'équation $X^d = 1$ dans $\mathbb{K}$ admet au plus d racines distinctes dans $\mathbb{K}^*$. Ainsi $\mathbb{K}^*$ est cyclique.

Exemples

1. $\mathbb{K} = \mathbb{Z}/3\mathbb{Z} = \mathbb{F}_3$. Alors $\mathbb{K}^* = \{\overline{1}, \overline{2}\}$ où $\overline{k}$ désigne la classe de $k \in \mathbb{Z}$ modulo 3. La table de ce groupe s'écrit

	$\overline{1}$	$\overline{2}$
$\overline{1}$	$\overline{1}$	$\overline{2}$
$\overline{2}$	$\overline{2}$	$\overline{1}$

   Il est cyclique : $\mathbb{K}^* =< 2 >$. Il est isomorphisme au groupe (additif) $\mathbb{Z}/2\mathbb{Z}$.

2. $\mathbb{K} = \mathbb{Z}/p\mathbb{Z} = \mathbb{F}_p$ avec p premier. Alors $\mathbb{K}^*$ est cyclique et engendré par $p-1$. Il est isomorphe à $\mathbb{Z}/(p-1)\mathbb{Z}$.

Ces exemples se généralisent aisément et on a

Proposition 19 *Soit $\mathbb{K}$ un corps fini de cardinalité q. Alors le groupe multiplicatif $\mathbb{K}^*$ est isomorphe au groupe $\mathbb{Z}/(q-1)\mathbb{Z}$.*

2.2.3 Corps finis algébriquement clos

Soit $\mathbb{K}$ un corps fini de cardinalité q. Soit $x \in \mathbb{K}^*$. Comme le groupe $\mathbb{K}^*$ est cyclique et d'ordre $q-1$, x vérifie l'équation

$$x^{q-1} = 1.$$

Ainsi tous les éléments de $\mathbb{K}$ vérifient $x^q = x$ et sont racines du polynôme $X^q - X$. On en déduit que le polynôme

$$X^q - X - 1$$

n'a pas de racine dans $\mathbb{K}$. On a donc

Proposition 20 *Un corps fini n'est jamais algébriquement clos*

Rappelons qu'un corps est algébriquement clos si tout polynôme à coefficients dans ce corps admet au moins une racine.

2.3 Existence et unicité des corps finis

Théorème 5 *Soit p un nombre premier et soit n un entier supérieur ou égal à 1. Il existe alors un corps fini de caractéristique p et de cardinalité p^n. De plus si $\mathbb{K}_1$ et $\mathbb{K}_2$ sont deux corps de caractéristique p et de cardinalité p^n, ils sont isomorphes.*

Ce théorème montre qu'il existe, à isomorphisme de corps près, un et un seul corps de cardinalité p^n. On notera ce corps $\mathbb{F}_{p^n}$.

Démonstration.

2.4 EXERCICES

Exercice 1. Ecrire la table d'addition et de multiplication d'un corps à 4 éléments

Exercice 2. Soit le polynôme $P = 1 + X + X^2 \in \mathbb{F}_2[X]$.

1. Montrer que P est irréductible dans $\mathbb{F}_2$.
2. Déterminer le corps $\mathbb{K}$ de décomposition de P.
3. Montrer que $\mathbb{K}$ est un corps fini contenant 4 éléments.

Exercice 3.

1. Montrer que si $\mathbb{K}$ est un corps fini, tout sous-groupe du groupe multiplicatif $\mathbb{K}^*$ est cyclique.
2. Déterminer les groupes multiplicatifs $\mathbb{K}^*$ lorsque $\mathbb{K} = \mathbb{F}_p$ pour $p = 2, 3, 5, 7, 11$. Trouver dans chaque cas un générateur de $\mathbb{K}^*$.

Exercice 4. On considère le corps fini $\mathbb{F}_{2^n}$ contenant 2^n éléments. On pose $\mathbb{F}_{2^n}^2 = \{x \in \mathbb{F}_{2^n} / y \in \mathbb{F}_{2^n}$ vrifiant $x = y^2\}$ l'ensemble des carrés de $\mathbb{F}_{2^n}^2 = \mathbb{F}_{2^n}$.

Exercice 5. On considère les corps finis $\mathbb{F}_{p^n}$ pou $p > 2$. Notons $\mathbb{F}_{p^n}^2$ l'ensemble des carrés de $\mathbb{F}_{p^n}$ (voir exercice 4).

1. Déterminer $\mathbb{F}_5^2, \mathbb{F}_7^2$.
2. Montrer que $|\mathbb{F}_{p^n}^2| = \frac{p^n+1}{2}$ et $|(\mathbb{F}_{p^n}^*)^2| = \frac{p^n-1}{2}$ où $(\mathbb{F}_{p^n}^*)^2 = \mathbb{F}_{p^n}^2 \cap \mathbb{F}_{p^n}^*$
3. Montrer que $x \in (\mathbb{F}_{p^n}^*)^2$ si et seulement si

$$x^{\frac{p^n-1}{2}} = 1$$

Retrouver les résultats de la question 1.

Exercice 6. Soit $\mathbb{K}$ un corps fini de caractéristique p. Montrer que sa clôture algébrique coïncide avec celle de son sous-corps premier.

Chapitre 3

Extensions de corps et nombres algébriques

Dans tout ce chapitre, les corps considérés seront toujours supposés commutatifs.

3.1 Extension de corps

3.1.1 Définition

Soient $\Bbbk$ et $\mathbb{K}$ des corps commutatifs. On dit que $\mathbb{K}$ est une extension de corps (ou plus brièvement une extension) de $\Bbbk$ si $\Bbbk$ est un sous-corps de $\mathbb{K}$.

Par exemple $\mathbb{C}$ est une extension de $\mathbb{R}$, $\mathbb{R}$ est une extension de $\mathbb{Q}$. Plus généralement, tout corps commutatif est une extension de son corps premier. C'est donc une extension de $\mathbb{Q}$ s'il est de caractéristique 0 ou une extension de $\mathbb{Z}/p\mathbb{Z}$ s'il est de caractéristique p.

Remarque. On pourrait définir la notion d'extension de $\Bbbk$ par la donnée d'un corps commutatif $\mathbb{K}$ et d'un homomorphisme de corps

$$\varphi : \Bbbk \to \mathbb{K}$$

Mais tout homomorphisme de corps est injectif. Ainsi l'image $\varphi(\Bbbk)$ de $\Bbbk$ dans $\mathbb{K}$ est un sous-corps de $\mathbb{K}$ isomorphe au corps $\Bbbk$. Le corps $\mathbb{K}$ est donc une extension de $\varphi(\Bbbk)$. Modulo cet isomorphisme, on retrouve la définition précédente.

3.1.2 Technique vectorielle

Proposition 21 *Soit $\mathbb{K}$ une extension de $\Bbbk$. Alors $\mathbb{K}$ est un $\Bbbk$-espace vectoriel.*

Démonstration. Définissons la multiplication externe sur $\mathbb{K}$ par

$$(\alpha, v) \in \Bbbk \times \mathbb{K} \to \alpha v.$$

Comme $\Bbbk \subset \mathbb{K}$, ceci est bien défini et vérifie les axiomes d'espaces vectoriels. Ainsi $\mathbb{K}$ est un $\Bbbk$-espace vectoriel.

Rappelons que l'on appelle $\Bbbk$-algèbre A un $\Bbbk$-espace vectoriel muni d'une multiplication interne

$$\begin{array}{ccc} A \times A & \to & A \\ (u, v) & \mapsto & uv \end{array}$$

distributive par rapport à l'addition

$$\begin{cases} u(v+w) = uv + uw \\ (u+v)w = uw + vw \end{cases}$$

pour tous $u, v, w \in A$.

Si cette multiplication est associative, l'algèbre est dite associative, si elle est commutative, l'algèbre est dite commutative, si elle admet un élément neutre, elle est dite unitaire. Si A est une $\Bbbk$-espace vectoriel de dimension finie n on dit que A est une $\Bbbk$-algèbre de dimension n.

Si $\mathbb{K}$ est une extension de $\Bbbk$, alors $\mathbb{K}$ est une $\Bbbk$-algèbre associative unitaire. La réciproque est fausse. Considérons par exemple $\Bbbk = \mathbb{C}$ et la $\mathbb{C}$-algèbre associative de dimension 2 définie dans une base $\{e_1, e_2\}$ par le produit

$$\begin{cases} e_1 e_1 = e_1, \\ e_1 e_2 = e_2 e_1 = e_2, \\ e_2 e_2 = e_2. \end{cases}$$

L'application $\varphi(u, v) = uv$ étant bilinéaire, la donnée des produits $e_i e_j$ détermine entièrement φ. On vérifie aisément que ce produit est associatif.

$$(e_i e_j) e_k = e_i (e_j e_k)$$

pour tout $i, j, k \in \{1, 2\}$ et unitaire. Soit $u = x_1 e_1 + x_2 e_2$. Il est inversible si et seulement s'il existe $v = y_1 e_1 + y_2 e_2$ tel que $uv = e_1$. Ceci est équivalent à

$$x_1 y_1 e_1 + (x_1 y_2 + x_2 y_1 + x_2 y_2) e_2 = e_1$$

soit

$$\begin{cases} x_1 y_1 = 1, \\ x_1 y_2 + x_2 y_1 + x_2 y_2 = 0. \\ e_2 e_2 = e_2. \end{cases}$$

Si $x_1 = 0$, alors $u = x_2 e_2$ n'est pas inversible et, munie de ce produit, l'algèbre A donnée n'est pas un corps.

Définition 16 *On appelle tour d'extension de $\Bbbk$, toute suite finie croissante de corps*

$$\Bbbk \subset \mathbb{K}_1 \subset \cdots \subset \mathbb{K}_p$$

Dans ce cas, chacun des corps $\mathbb{K}_i$ est une extension de $\mathbb{K}_j$ pour tout $1 \leq j \leq i-1$ et de $\Bbbk$.

3.1.3 Degré d'une extension

Soit $\mathbb{K}$ une extension de corps de $\Bbbk$. Alors $\mathbb{K}$ est un $\Bbbk$-espace vectoriel de dimension finie ou non.

Définition 17 *Soit $\mathbb{K}$ une extension de corps de $\Bbbk$. On appelle degré de cette extension, que l'on note $[\mathbb{K}, \Bbbk]$, la dimension du $\Bbbk$-espace vectoriel $\mathbb{K}$*

Exemples

1. $[\mathbb{C}, \mathbb{R}] = 2$; $[\mathbb{R}, \mathbb{Q}] = \infty$.
2. Considérons un corps commutatif $\Bbbk$ et le corps $\mathbb{K} = \Bbbk(X)$ des fractions rationnelle à coefficients dans $\Bbbk$. Il est clair que $\Bbbk$ s'injecte naturellement dans $\Bbbk(X)$ et donc $\Bbbk(X)$ est une extension de degré infini de $\Bbbk$.

Soit E un espace vectoriel sur $\Bbbk$ de dimension finie ou infinie. On appelle base toute famille $\mathcal{B} = \{e_i\}_{i\in I}$ de vecteurs de E libre et génératrice. Si $\mathcal{B} = \{e_i\}_{i\in I}$ est une base de E, tout vecteur $u \in E$ se décompose de manière unique

$$u = \sum_{i\in I_0} x_i e_i$$

où I_0 est une partie finie de I. L'espace vectoriel E est de dimension finie s'il existe une base $\mathcal{B}$ finie. Dans ce cas, toute les autres bases ont le même nombre d'éléments, la dimension de E, et de telles bases existent. Ceci est un condensé du cours d'algèbre linéaire de L1. Qu'en est-il si E n'est pas de dimension finie ? (on dit que E est de dimension infinie). On a toujours le résultat " Tout espace vectoriel admet une base". Pour une démonstration dans le cas de la dimension quelconque, on pourra se reporter au

Cours algèbre multilinéaire chapitre 1.

édité sur le site

http ://ramm-algebra-center.monsite-orange.fr/

Théorème 6 *(dit de la base télescopique)*
Soit $\Bbbk \subset \mathbb{K}_1 \subset \mathbb{K}_2$ une tour d'extension de longueur 2. Soit $\{e_i\}_{i\in I}$ une base du $\Bbbk$-espace vectoriel $\mathbb{K}_1$ et $\{f_j\}_{j\in J}$ une base du $\mathbb{K}_1$-espace vectoriel $\mathbb{K}_2$. Alors $\{e_i f_j\}_{i\in I, j\in J}$ une base du $\Bbbk$-espace vectoriel $\mathbb{K}_2$.

Démonstration. Tout vecteur $u \in \mathbb{K}_1$ s'écrit de manière unique

$$u = \sum_{i\in I_0} x_i e_i, \quad x_i \in \Bbbk$$

où I_0 et une partie finie de I. Tout vecteur $v \in \mathbb{K}_2$ s'écrit de manière unique

$$v = \sum_{j\in J_0} y_j f_j, \quad y_j \in \mathbb{K}_1$$

où J_0 et une partie finie de J. Comme $y_j \in \mathbb{K}_1$, ce vecteur se décompose de manière unique

$$y_j = \sum_{i\in I_j} x_{ij} e_i, \quad x_{ij} \in \Bbbk$$

où I_j est une partie finie de I. D'où

$$v = \sum_{j\in J_0} (\sum_{i\in I_j} x_{ij} e_i) f_j = \sum_{(i,j)\in I_j \times J_0} x_{ij} e_i f_j, \quad x_{ij} \in \Bbbk.$$

Cette décomposition étant unique, on en déduit que $\{e_i f_j\}_{(i,j)\in I\times J}$ est une base du $\Bbbk$-espace vectoriel $\mathbb{K}_2$.

Application. Soient $\mathbb{K}_1$ une extension de degré finie d_1 de $\Bbbk$ et $\mathbb{K}_2$ une extension de degré finie d_2 de $\mathbb{K}_1$. Alors $\mathbb{K}_2$ est une extension de $\Bbbk$ de degré fini d avec

$$d = d_1 d_2.$$

3.2 Eléments algébriques, éléments transcendants

3.2.1 Extensions monogènes

Soit $\mathbb{K}$ une extension de $\Bbbk$. On suppose $\mathbb{K} \neq \Bbbk$. Soit α un élément de $\mathbb{K}$ n'appartenant pas à $\Bbbk$. Notons par $\Bbbk(\alpha)$ le plus petit sous-corps de $\mathbb{K}$ contenant $\Bbbk$ et α. Les éléments de $\Bbbk(\alpha)$ s'écrivent

$$\frac{P(\alpha)}{Q(\alpha)}$$

avec $P, Q \in \Bbbk[X]$ l'anneau des polynômes à coefficients dans $\Bbbk$ et avec $Q(\alpha) \neq 0$.

On a donc en général $\Bbbk \subset \Bbbk(\alpha) \subset \mathbb{K}$ et $\Bbbk(\alpha)$ est une extension de $\Bbbk$ dite extension monogène ou simple.

Proposition 22 *Soit $\Bbbk[X]$ le sous-anneau de $\mathbb{K}$ contenant $\Bbbk$ et α. Alors $\Bbbk(\alpha)$ est le corps des fractions de $\Bbbk[\alpha]$.*

Démonstration. Les éléments de $\Bbbk[\alpha]$ s'écrivent

$$a_0 + a_1\alpha + \cdots + a_n\alpha^n$$

avec $a_i \in \Bbbk$, , c'est à dire

$$\Bbbk[\alpha] = \{P(\alpha)/P \in \Bbbk[X]\}.$$

Il est clair que $l\Bbbk[\alpha]$ est un anneau intègre contenu dans $\Bbbk(\alpha)$. Son corps des fractions est l'ensemble des classes des couples $(P(\alpha), Q(\alpha)$ avec $P, Q \in \Bbbk[X]$ et $Q(\alpha) \neq 0$. C'est donc bien $\Bbbk(\alpha)$.

Remarques.

1. Nous aurions pu définir $\Bbbk(\alpha)$ comme le plus petit corps contenu dans $\mathbb{K}$ et contenant $\Bbbk$ et α c'est-à-dire comme l'intersection de tous les sous-corps de $\mathbb{K}$ vérifiant cette propriété.
2. On prendra bien garde aux notations $\Bbbk[\alpha]$ et $\Bbbk(\alpha)$ désignant l'une un anneau et l'autre son corps des fractions.

Exemple. Soit l'extension $\mathbb{Q} \subset \mathbb{R}$. Nous savons que $\sqrt{2} \in \mathbb{R}$ et n'appartient pas à $\mathbb{Q}$. Ainsi

$$\mathbb{Q}(\sqrt{2}) = \left\{ \frac{P(\sqrt{2})}{Q(\sqrt{2})}, P, Q \in \mathbb{Q}[X] \text{ et } \mathbb{Q}(\sqrt{2}) \neq 0 \right\},$$

$$\mathbb{Q}[\sqrt{2}] = \left\{ P(\sqrt{2}), P \in \mathbb{Q}[X] \right\}.$$

Mais comme $(\sqrt{2})^2 = 2$, toute expression $P(\sqrt{2})$ pour $P \in \mathbb{Q}[X]$ se réduit à

$$a_0 + a_1\sqrt{2}$$

avec $a_0, a_1 \in \mathbb{Q}$. Ainsi

$$\mathbb{Q}(\sqrt{2}) = \left\{ \frac{a_0 + a_1\sqrt{2}}{b_0 + b_1\sqrt{2}}, a_0, a_1, b_0, b_1 \in \mathbb{Q} \text{ et } \mathrm{b}_0 \text{ ou } \mathrm{b}_1 \neq 0 \right\},$$

Mais $\dfrac{a_0+a_1\sqrt{2}}{b_0+b_1\sqrt{2}} = \dfrac{(a_0+a_1\sqrt{2})(b_0-b_1\sqrt{2})}{b_0^2-2b_1^2} = \left(\dfrac{a_0b_0-2a_1b_1}{b_0^2-2b_1^2}\right) + \left(\dfrac{-a_0b_1+a_1b_0}{b_0^2-2b_1^2}\right)\sqrt{2}$ et donc

$$\frac{a_0+a_1\sqrt{2}}{b_0+b_1\sqrt{2}} \in \mathbb{Q}[\sqrt{2}].$$

On en déduit que $\mathbb{Q}(\sqrt{2}) \subset \mathbb{Q}[\sqrt{2}]$ et donc, dans ce cas particulier

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

Proposition 23 *Soit $\Bbbk \subset \mathbb{K}$ une extension de corps de degré fini. Il existe une tour d'extension*

$$\Bbbk = \mathbb{K}_0 \subset \mathbb{K}_1 \subset \cdots \subset \mathbb{K}_p = \mathbb{K}$$

telle que pour tout $i = 1, \cdots, p$, le corps $\mathbb{K}_i$ soit une extension monogène de $\mathbb{K}_{i-1}$.

Démonstration. Supposons que $[\mathbb{K}, \Bbbk] = n$. Si $n = 1$ alors $\mathbb{K} = \Bbbk = \mathbb{K}_1$. Sinon, si $n > 1$, il existe un élément $\alpha \in \mathbb{K}$ tel que $\alpha \notin \Bbbk$. Considérons l'extension monogène $\Bbbk(\alpha)$. On a $[\Bbbk(\alpha), \Bbbk] > 1$. Comme $\Bbbk(\alpha)$ est un sous-corps de $\mathbb{K}$, $[\Bbbk(\alpha), \Bbbk]$ est fini et $[\mathbb{K}, \Bbbk(\alpha)] < [\mathbb{K}, \Bbbk]$. Si $\mathbb{K} = \Bbbk(\alpha)$, alors la propriété est vérifiée. Sinon on recommence le processus avec l'extension de degré fini $\Bbbk(\alpha) \subset \mathbb{K}$. Comme $[\mathbb{K}, \Bbbk(\alpha)] < n$, ce processus s'arrête au bout d'un nombre fini d'étapes.

3.2.2 Eléments algébriques

Définition 18 *Soit $\Bbbk \subset \mathbb{K}$ une extension de corps et soit $\alpha \in \mathbb{K}$, $\alpha \notin \Bbbk$. On dit que α est algébrique sur $\Bbbk$ si*

$$\Bbbk[\alpha] = \Bbbk(\alpha).$$

Par exemple $\sqrt{2}$ est algébrique sur $\mathbb{Q}$.

Considérons l'application

$$\begin{array}{rccc} \varphi : \Bbbk[X] & \to & \mathbb{K} \\ P & \mapsto & P(\alpha). \end{array}$$

C'est un homomorphisme d'anneaux (et non de corps). Son noyau est l'ensemble des polynômes $P \in \Bbbk[X]$ tels que $P(\alpha) = 0$. Supposons que φ soit injectif. Alors pour tout $P \neq 0$ appartenant à $\Bbbk[X]$ on a $P(\alpha) \neq 0$. Dans ce cas φ est un homomorphisme d'anneaux bijectif.

Proposition 24 *Soit $\Bbbk \subset \mathbb{K}$ une extension de corps. Un élément $\alpha \in \mathbb{K}$ est algébrique sur $\Bbbk$ si et seulement s'il existe un polynôme non nul $P \in \Bbbk[X]$ tel que $P(\alpha) = 0$*

Nous avons vu que α est algébrique si et seulement si le noyau de φ est non trivial. Or ce noyau est un idéal de l'anneau $\Bbbk[X]$ qui est principal. Il existe donc un unique polynôme non nul unitaire irréductible engendrant cet idéal.

Définition 19 *Soit α un élément algébrique sur $\Bbbk$. Le polynôme minimal de α est le polynôme unitaire irréductible générateur de l'idéal $\{P \in \Bbbk[X]/P(\alpha) = 0\}$.*

Supposons que α soit algébrique sur $\Bbbk$. Alors $\Bbbk[\alpha] = \Bbbk(\alpha)$ et $\Bbbk[\alpha]$ est une extension de $\Bbbk$:

$$\Bbbk \subset \Bbbk[\alpha] = \Bbbk(\alpha) \subset \mathbb{K}.$$

L'anneau $\Bbbk[\alpha]$ est donc muni d'une structure d'espace vectoriel sur $\Bbbk$. Soit P_α le polynôme minimal de α Posons $P_\alpha(X) = a_0 + a_1X + \cdots + a_nX^n$. On a donc $P_\alpha(\alpha) = a_0 + a_1\alpha + \cdots + a_n\alpha^n = 0$ et les éléments $\{1, \alpha, \cdots, \alpha^n\}$ de $\Bbbk[\alpha]$ sont linéairement dépendants dans le $\Bbbk$-espace vectoriel $\Bbbk[\alpha]$. Comme P_α et minimal, pour tout $P \in \Bbbk[X]$ tel que $d(P) < d(P)_\alpha = n$ on a $P(\alpha) \neq 0$. Ainsi tout combinaison triviale $b_0 + b_1\alpha + \cdots + b_p\alpha^p = 0$ avec $p < n$ n'est possible que pour $b_0 = b_1 = \cdots = b_p = 0$. On en déduit que la famille $\{1, \alpha, \cdots, \alpha^{n-1}\}$ de $\Bbbk[\alpha]$ est libre dans $\Bbbk[\alpha]$. Si $P \in \Bbbk[X], P \neq 0$ tel que $d(P) \geq n$ alors la division euclidienne s'écrit

$$P = P_\alpha Q + R$$

avec $d(R) < d(P_\alpha)$. D'où $P(\alpha) = P_\alpha(\alpha)Q(\alpha) + R(\alpha) = R(\alpha)$ et donc $P(\alpha) = R(\alpha)$ s'exprime sous la forme

$$b_0 + \cdots + b_p\alpha^p \text{ avec } p < n.$$

Ainsi $P(\alpha)$ se décompose dans la famille $\{1, \alpha, \cdots, \alpha^{n-1}\}$. On en déduit que cette famille est une base.

Théorème 7 *Soit $\Bbbk \subset \mathbb{K}$ une extension de corps. Un élément $\alpha \in \Bbbk$ est algébrique sur $\Bbbk$si et seulement si le $\Bbbk$-espace vectoriel $\Bbbk[\alpha]$ est de dimension finie. Dans ce cas, si $dim_{\Bbbk}\Bbbk[\alpha]$ désigne la dimension de cet espace vectoriel, on a*

$$dim_{\Bbbk}\Bbbk[\alpha] = d(P_\alpha)$$

où P_α est le polynôme minimal de α et $d(P_\alpha)$ son degré.

Démonstration. Il nous reste à établir la réciproque. Supposons que $dim_{\Bbbk}\Bbbk[\alpha] = n < \infty$. La famille de $(n+1)$ éléments $\{1, \alpha, \cdots, \alpha^n\}$ de $\Bbbk[\alpha]$ es donc liée et il existe une combinaison linéaire

$$b_0 + b_1\alpha + \cdots + b_n\alpha^n = 0$$

avec les b_i non tous nuls. Ainsi le polynôme

$$P = b_0 + b_1X + \cdots + b_nX^n \in \Bbbk[X]$$

vérifie $P(\alpha) = 0$ et donc α est algébrique sur $\Bbbk$.

Définition 20 *On appelle degré d'un élément algébrique $\alpha \in \mathbb{K}$ sur $\Bbbk$ le degré de son polynôme minimal.*

Définition 21 *Soit $\Bbbk \subset \mathbb{K}$ une extension de corps. Un élément $\zeta \in \mathbb{K}$ est dit transcendant sur $\Bbbk$ s'il n'est pas algébrique.*

Théorème 8 *Il existe des éléments de $\mathbb{C}$ qui sont transcendants dans $\mathbb{Q}$.*

Démonstration. Considérons l'application

$$\bigcup_{n\geq 0} \mathbb{Q}^{n+1} \to \mathbb{Q}[X]$$

qui à la suite finie $(a_i)_{i=0,\cdots,n}$ associe le polynôme $P = \sum a_i X^i$. Cette application est surjective. Ainsi $\mathbb{Q}[X]$ est un ensemble dénombrable (Rappelons que $\mathbb{Q}$ et donc $\mathbb{Q}^n$ sont dénombrables). Si $r(P)$ désigne l'ensemble fini des racines complexes du polynôme P, on a

$$\bigcup_{P\in\mathbb{Q}[X]} r(P) \subset \mathbb{C}.$$

Mais $\bigcup_{P\in\mathbb{Q}[X]} r(P)$ est dénombrable, car $r(P)$ est fini et $\mathbb{Q}[X]$ dénombrable. Comme $\mathbb{C}$ ne l'est pas, l'inclusion est stricte. Il existe donc des nombres complexes qui ne sont pas racines du polynômes rationnels. D'où le théorème

Exemples.

1. e est transcendant (résultat de Hermite)
2. π est transcendant (résultat de Lindermann)
3. Si d est un réel algébrique sur $\mathbb{Q}$ et β un réel non rationnel algébrique sur $\mathbb{Q}$, alors α^β est transcendant.

Ces exemples seront traités en exercice.

Théorème 9 *Soit $\Bbbk \subset \mathbb{K}$ une extension de corps. Posons*

$$\mathbb{A}_{\Bbbk,\mathbb{K}} = \{\alpha \in \mathbb{K} / \ \alpha \text{ algebrique sur } \Bbbk\}.$$

Alors $\mathbb{A}_{\Bbbk,\mathbb{K}}$ est un sous-corps de $\mathbb{K}$ contenant $\Bbbk$.

Démonstration. Soient $\alpha, \beta \in \mathbb{A}_{\Bbbk,\mathbb{K}}$. Pour montrer que $\alpha+\beta$ et $\alpha\beta$ sont algébriques sur $\Bbbk$, il suffit de montrer, d'après le théorème 7 que $\Bbbk[\alpha+\beta]$ et $\Bbbk[\alpha\beta]$ sont des extensions de degré fini. Considérons l'anneau $\Bbbk[\alpha,\beta]$, sous-anneau de $\mathbb{K}$ engendré par $\Bbbk$ et la partie $\{\alpha,\beta\}$. Les éléments de $\Bbbk[\alpha,\beta]$ s'écrivent

$$\sum_{i=0} P_i(\alpha)\beta^i$$

avec $P_i \in \Bbbk[X]$ et donc $\Bbbk[\alpha,\beta] = \Bbbk[\alpha][\beta]$ avec $P_i \in \Bbbk[X]$. Comme α est algébrique sur $\Bbbk$, on a $\Bbbk[\alpha] = \Bbbk(\alpha)$ et $\Bbbk[\alpha]$ est un sous-corps de $\mathbb{K}$. Mais β est algébrique sur $\Bbbk$ donc aussi sur $\Bbbk[\alpha]$. On en déduit que $[\Bbbk[\alpha][\beta], \Bbbk[\alpha]] < +\infty$. Ainsi

$$[\Bbbk[\alpha][\beta], \Bbbk] = [\Bbbk[\alpha][\beta], \Bbbk[\alpha]] \cdot [\Bbbk[\alpha], \Bbbk] < +\infty$$

et $\Bbbk[\alpha][\beta]$ est une extension de degré fini de $\Bbbk$. Mais $\Bbbk[\alpha+\beta]$ et $\Bbbk[\alpha\beta]$ sont des extensions de $\Bbbk$ contenus dans $\Bbbk[\alpha,\beta]$. On en déduit que $\Bbbk[\alpha+\beta]$ et $\Bbbk[\alpha\beta]$ sont des extensions monogènes de degré fini, donc $\alpha+\beta$ et $\alpha\beta$ sont algébriques.

Remarques.

1. Dans la démonstration ci-dessus on utilise le fait que si une extension d'anneau monogène $\Bbbk[\alpha]$ est un espace vectoriel de dimension finie sur $\Bbbk$, alors α est algébrique et $\Bbbk[\alpha] = \Bbbk(\alpha)$. Notons que ceci n'implique pas que toute extension de degré fini de $\Bbbk$ soit du type $\Bbbk(\alpha)$ avec α algébrique.
2. Soit l'extension $\mathbb{Q} \subset \mathbb{C}$. L'ensemble

$$\mathbb{A}_{\mathbb{Q},\mathbb{C}} = \{\alpha \in \mathbb{C} \ / \alpha \text{ algebrique sur } \mathbb{Q}\}$$

est un corps et on a la tour d'extension

$$\mathbb{Q} \subset \mathbb{A}_{\mathbb{Q},\mathbb{C}} \subset \mathbb{C}.$$

L'extension $\mathbb{Q} \subset \mathbb{A}_{\mathbb{Q},\mathbb{C}}$ n'est pas de degré fini. En effet pour tout entier n, il existe $\alpha \in \mathbb{A}_{\mathbb{Q},\mathbb{C}}$ tel que $[\mathbb{Q}(\alpha), \mathbb{Q}] = n$. Prenons par exemple $2^{\frac{1}{n}}$. Ainsi pour tout $n \in \mathbb{N}^*, \mathbb{A}_{\mathbb{Q},\mathbb{C}}$ contient un sous-espace de dimension n. On en déduit

$$dim_{\mathbb{Q}}\mathbb{A}_{\mathbb{Q},\mathbb{C}} = [\mathbb{A}_{\mathbb{Q},\mathbb{C}}, \mathbb{Q}] = \infty.$$

3. Exemples de nombres réels algébriques sur $\mathbb{Q}$: les réels constructibles
Considérons le plan euclidien $\mathbb{R}^2$ et les points $O = (0,0)$ et $I = (1,0)$. A partir de ces deux points nous pouvons construire
• la droite affine (OI)
• le cercle centré en O de rayon OI
• le cercle centré en I de rayon IO. Ces figures déterminent 4 nouveaux points dits constructibles à la règle et au compas à partir de la famille $\mathcal{F}_1 = \{O, I\}$. On détermine ainsi une nouvelle famille $\mathcal{F}_2 = \{O, I, A_1, A_2, A_3, A_4\}$ formée des points de $\mathcal{F}_1$ et des intersections des figures que nous avons définies. A partir de la famille $\mathcal{F}_2$, nous recommençons ce procédé que nous pouvons décrire ainsi. Soit $\mathcal{F}$ une famille de points de $\mathbb{R}^2$. Considérons les figures construites ainsi
• les droites affines (PQ) avec $P, Q \in \mathcal{F}$ et $P \neq Q$
• les cercles de centre P et de rayon PQ avec $P, Q \in \mathcal{F}, P \neq Q$
• les cercles de centre P et de rayon égal à la longueur QR avec $P, Q, R \in \mathcal{F}$ et $Q \neq R$.

Définition 22 *Soit $\mathcal{F}$ une partie de $\mathbb{R}^2$. Le point $M \in \mathbb{R}^2$ est constructible à la règle et au compas en un pas s'il est déterminé par l'intersection de deux figures construites à partir de $\mathcal{F}$.*

A partir de la famille $\mathcal{F}_1 = \{O, I\}$, on construit une suite de familles (finie de points) $\mathcal{F}_1 \subset \mathcal{F}_2 \subset \cdots \subset \mathcal{F}_n \cdots$ où $\mathcal{F}_i$ est la famille de points constitués des points de $\mathcal{F}_{i-1}$ et des points constructibles en un pas à partir de $\mathcal{F}_{i-1}$.

Définition 23 *Un point $M \in \mathbb{R}^2$ est constructible à la règle et au compas s'il existe i tel que M soit constructible en un pas à partir de $\mathcal{F}_{i-1}$.*
Un réel x est dit constructible si le point $M = (x, 0)$ l'est.

Théorème 10 *Tout réel constructible est algébrique sur $\mathbb{Q}$ et il existe $n \in \mathbb{N}$ tel que*

$$[\mathbb{Q}[x], \mathbb{Q}] = 2^n$$

Pour la démonstration, voir l'annexe de cet ouvrage.

Application : Problème de la duplication du cube. Il s'agit de savoir s'il existe un réel a constructible tel que $a^3 = 2$. Il est clair que si $a \in \mathbb{R}$ vérifie $a^3 = 2$, il est algébrique sur $\mathbb{Q}$. Son polynôme minimal est '$X^3 - 2$ car ce polynôme est irréductible sur $\mathbb{Q}$, d'après le critère d'Eisenstein. Mais

$$[\mathbb{Q}(\sqrt[3]{2}), \mathbb{Q}] = d(X^3 - 2) = 3$$

qui n'est pas une puissance de 2. Donc $\sqrt[3]{2}$ n'est pas constructible.

3.2.3 Eléments primitifs, éléments conjugués

Soit $\mathbb{K} = \Bbbk[\alpha]$ une extension algébrique monogène du corps $\Bbbk$. Considérons par exemple l'extension $\mathbb{Q}[j]$ de $\mathbb{Q}$ où j est une racine troisième de l'unité dans $\mathbb{C}$. Le polynôme minimal de j est $X^2 + X + 1$. Il admet comme racine $j, j^2 = -1 - j$. On en déduit que l'extension $\mathbb{Q}[j^2]$ coïncide avec l'extension $\mathbb{Q}[j]$. Ceci montre que si $\mathbb{K}$ est une extension monogène algébrique de $\Bbbk$, il n'y a pas unicité du nombre algébrique α tel que $\mathbb{K} = \Bbbk[\alpha]$.

Définition 24 *Soit $\mathbb{K}$ est une extension monogène algébrique de $\Bbbk$. Tout élément α tel que $\mathbb{K} = \Bbbk[\alpha]$ est appelé un élément primitif de l'extension $\Bbbk \subset \mathbb{K}$.*

Considérons maintenant une extension $\Bbbk \subset \mathbb{K}$ de $\Bbbk$ et soient α, β deux éléments de $\mathbb{K}$ algébriques sur $\Bbbk$. Comparons les extensions monogènes $\Bbbk[\alpha]$ et $\Bbbk[\beta]$.

Proposition 25 *Soient une extension $\Bbbk \subset \mathbb{K}$ de $\Bbbk$ et α, β deux éléments de $\mathbb{K}$ algébriques sur $\Bbbk$. Alors les propriétés suivantes sont équivalentes :*

1. *Les polynômes minimaux P_α et P_β de α et β sont égaux.*
2. *Il existe un isomorphisme de corps*
$$f : \Bbbk[\alpha] \to \Bbbk[\beta]$$
tel que f soit l'identité sur $\Bbbk$ et tel que $f(\alpha) = \beta$.

Démonstration. Montrons que $1 \Rightarrow 2$. Rappelons que si $\alpha \in \mathbb{K}$ est algébrique sur $\Bbbk$ alors le corps $\Bbbk[\alpha]$ est isomorphe au corps de rupture du polynôme minimal P_α. Comme par hypothèse $P_\alpha = P_\beta$ les corps $\Bbbk[\alpha]$ et $\Bbbk[\beta]$ sont isomorphes au corps de rupture de P_α. Cet isomorphisme f est défini par :

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

où $P_\alpha = P_\beta = a_0 + a_1X + \cdots + a_nX^n$.

Réciproquement montrons que $1 \Rightarrow 2$. Soit f un isomorphisme de $\Bbbk[\alpha]$ sur $\Bbbk[\beta]$ tel que $f(a) = a$ pour tout $a \in \Bbbk$ et $f(\alpha) = \beta$. On a

$$0 = P_\beta(\beta) = P_\beta(f(\alpha) = f(P_\beta(\alpha)).$$

Donc comme f est un isomorphisme on en déduit $P_\beta(\alpha) = 0$ et donc P_β est un polynôme annotateur de β. Par conséquent le polynôme P_α divise P_β mais P_α et P_β sont des polynômes irréductibles et unitaires donc $P_\alpha = P_\beta$.

Définition 25 *Soit une extension $\Bbbk \subset \mathbb{K}$ de $\Bbbk$. Deux éléments α, β de $\mathbb{K}$ algébriques sur $\Bbbk$ sont dits congugés sur $\Bbbk$ si les polynômes minimaux P_α et P_β sont égaux.*

3.3 Polynômes irréductibles

Si α est un nombre algébrique sur $\Bbbk$, le degré de l'extension $\Bbbk[\alpha]$ de $\Bbbk$ est donné par le degré du polynôme minimal $P_\alpha \in \Bbbk[X]$. Ce polynôme admet α comme racine et est irréductible dans $\Bbbk[X]$. L'irréductibité est en général une propriété difficile à prouver. Nous allons toutefois montrer comment traiter ceci lorsque $\Bbbk = \mathbb{Q}$ ou lorsque $\Bbbk$ est un corps fini.

3.3.1 Polynômes irréductibles sur $\mathbb{Q}$

Soit $\Bbbk \subset \mathbb{K}$ un extension de corps et soit α un élément de $\mathbb{K}$ algébrique sur $\Bbbk$. Son polynôme minimal P_α est irréductible sur $\mathbb{K}$, c'est-à-dire n'est pas le produit de deux polynômes de $\mathbb{K}[X]$ non constants. Une caractérisation des polynômes irréductibles n'est bien connue que pour $\mathbb{K} = \mathbb{R}$ ou $\mathbb{C}$:

— Tout polynôme irréductible de $\mathbb{C}[X]$ est de degré 1.
— Tout polynôme irréductible de $\mathbb{R}[X]$ est soit de degré 1, soit de degré 2 à discriminant strictement négatif.

Dans les autres cas, nous n'avons pas de résultats aussi précis. Dans ce paragraphe, nous allons préciser quelques critères concernant l'irréductibilité des polynômes de $\mathbb{Q}[X]$.

Première réduction : passage de $\mathbb{Q}[X]$ à $\mathbb{Z}[X]$. Soit $P \in \mathbb{Q}[X]$ un polynôme à coefficients rationnels. La réduction au même dénominateur des coefficients de ce polynôme montre qu'il existe un entier $m \in \mathbb{Z}$ tel que $mP \in \mathbb{Z}[X]$. Or l'irréductibilité de P dans $\mathbb{Q}[X]$ est équivalente à celle de mP toujours dans $\mathbb{Q}[X]$. ceci permet de réduire notre étude à celle de l'irréductibilité dans $\mathbb{Q}[X]$ des polynômes de $\mathbb{Z}[X]$.

Proposition 26 Racines rationnelles d'un polynômes de $\mathbb{Z}[X]$. *Soit $P(X) = a_0 + a_1 X + \cdots + a_n X^n$ un polynôme à coefficients entiers tel que $a_0 a_n \neq 0$. Soit $\alpha = p/q \in \mathbb{Q}$ une racine rationnelle de P. On suppose que les entiers p et q sont premiers entre eux. Alors p divise a_0 et q divise a_n.*

Démonstration. En effet

$$P(\alpha) = a_0 + a_1 \frac{p}{q} + \cdots + a_n \frac{p^n}{q^n} = 0.$$

Ainsi

$$q^n a_0 + q^{n-1} a_1 p + \cdots + q a_{n-1} p^{n-1} + a_n p^n = 0$$

soit

$$q^n a_0 = -p(q^{n-1} a_1 + \cdots + q a_{n-1} p^{n-2} + a_n p^{n-1}).$$

Ainsi p divise $q^n a_0$. Comme il est premier avec q, il divise a_0. De même q divise $q^{n-1} a_1 + \cdots + q a_{n-1} p^{n-2} + a_n p^{n-1}$ et donc divise $a_n p^{n-1}$. Comme il est premier avec p, il divise a_n.

Proposition 27 Equivalence entre irréductibilité dans $\mathbb{Z}[X]$ et dans $\mathbb{Q}[X]$ *Soit $P(X) = a_0 + a_1X + \cdots + a_nX^n$ un polynôme à coefficients entiers de degré supérieur ou égal à 1. Soit $\gamma(P)$ le PGCD des coefficients $(a_0, \cdots, a_n)$. Alors P est irréductible dans $\mathbb{Z}[X]$ si et seulement si P est irréductible dans $\mathbb{Q}[X]$ et $\gamma(P) = 1$.*

Démonstration. Supposons P irréductible dans $\mathbb{Q}[X]$ avec $\gamma(P) = 1$. Posons $P = Q_1Q_2$ avec $Q_1, Q_2 \in \mathbb{Z}[X]$. Les polynômes Q_1 et Q_2 appartiennent également à $\mathbb{Q}[X]$ et donc, par hypothèse, l'un des deux, par exemple Q_1 est de degré 0. Posons $Q_1 = a \in \mathbb{Z}$. Alors $P = aQ_2$. On en déduit que $\gamma(P)$ est un multiple de a. Donc $a = 1$ et P est irréductible dans $\mathbb{Z}[X]$.

Inversement, supposons que P soit irréductible dans $\mathbb{Z}[X]$ mais s'écrive $P = Q_1Q_2$ dans $\mathbb{Q}[X]$ avec Q_1 et Q_2 des polynômes de $\mathbb{Q}[X]$ de degré supérieur ou égal à 1. Soit $a \in \mathbb{Z}$ un multiple commun aux dénominateurs des coefficients de Q_1 et Q_2. Ainsi les polynômes aQ_1 et aQ_2 sont dans $\mathbb{Z}[X]$ et $aQ_1aQ_2 = a^2P$. Soit γ_i le PGCD des coefficients de aQ_i.

Lemme 4 *Si P et Q sont des polynômes non nuls dans $\mathbb{Z}[X]$, alors $\gamma(PQ) = \gamma(P)\gamma(Q)$.*

On démontrera ce lemme en exercice. On a donc

$$a^2\gamma(P) = \gamma_1\gamma_2.$$

Posons $R_i = \frac{1}{\gamma_i}aQ_i$ pour $i = 1, 2$. On a $\gamma(R_i) = 1$ et

$$a^2P = \gamma_1\gamma_2R_1R_2 = a^2\gamma(P)R_1R_2$$

d'où

$$a^2P = a^2\gamma(P)R_1R_2$$

et comme $a \neq 0$,

$$P = \gamma(P)R_1R_2.$$

Ceci contredit l'irréductibilité de P dans $\mathbb{Z}[X]$.

Proposition 28 Irréductibilité dans $\mathbb{Z}[X]$. Critère d'Eisenstein *Soit $P = a_0 + \cdots + a_nX^n$ un polynôme de $\mathbb{Z}[X]$ avec $a_0a_n \neq 0$. Supposons qu'il existe un nombre premier p tel que*

1. *p divise tous les coefficients a_i sauf a_n,*
2. *p^2 ne divise pas a_0.*

Alors P est irréductible dans $\mathbb{Z}[X]$.

Démonstration. Soit $P = a_0 + \cdots + a_nX^n$ un polynôme de $\mathbb{Z}[X]$. S'il n'est pas irréductible, il existe $Q, R \in \mathbb{Z}[X]$ de degré au moins 1 tel que $P = QR$. Posons $Q = b_0 + \cdots + b_qX^q$ et $R = c_0 + \cdots + c_rX^r$ avec $b_0, \cdots, b_q, c_0, \cdots, c_r \in \mathbb{Z}$ et $0 < q, r < n$. Soit p un nombre premier. Alors $\mathbb{Z}/p\mathbb{Z} = \mathbb{F}_p$ est un corps. Soit $\overline{P}$, $\overline{Q}$ et $\overline{R}$ les polynômes de $\mathbb{F}_p[X]$ définis par

$$\overline{P} = \overline{a_0} + \cdots + \overline{a_n}X^n,\ \overline{Q} = \overline{b_0} + \cdots + \overline{b_q}X^q,\ \overline{R} = \overline{c_0} + \cdots + \overline{c_r}X^r$$

où $\overline{a}$ désigne la classe de l'entier a dans $\mathbb{F}_p$. Si p vérifie les conditions 1 et 2, alors

$$\overline{P} = \overline{a_n}X^n$$

avec $\overline{a_n} \neq 0$. Comme $P = QR$, alors $\overline{P} = \overline{QR}$ et donc

$$\overline{P} = (\overline{b_0} + \cdots + \overline{b_q}X^q)(\overline{c_0} + \cdots + \overline{c_r}X^r).$$

On en déduit $\overline{b_q}\overline{c_r} = \overline{a_n} \neq 0$. De plus $\overline{b_0}\overline{c_0} = 0$ Donc p divise b_0 et c_0. Ainsi p^2 divise $b_0c_0 = a_0$ ce qui est contraire à l'hypothèse.

Proposition 29 Irréductibilité dans $\mathbb{F}_p[X]$ et dans $\mathbb{Q}[X]$. *Soit $P = a_0 + \cdots + a_nX^n \in \mathbb{Z}[X]$ et soit p un nombre premier. Notons par $\overline{P} = \overline{a_0} + \cdots + \overline{a_n}X^n$ sa réduction modulo p, c'est-à-dire dont les coefficients $\overline{a_i}$ sont les classes dans $\mathbb{F}_p$ des coefficients a_i de P. Supposons $\overline{a_n} \neq 0$. Alors si $\overline{P}$ est irréductible dans $\mathbb{F}_p[X]$, le polynôme P est irréductible dans $\mathbb{Q}[X]$.*

Démonstration. Supposons que l'on ait $P = QR$ dans $\mathbb{Z}[X]$. Si $Q = b_0 + \cdots + b_qX^q$ et $R = c_0 + \cdots + c_rX^r$, alors

$$\overline{P} = (\overline{b_0} + \cdots + \overline{b_q}X^q)(\overline{c_0} + \cdots + \overline{c_r}X^r)$$

et

$$\overline{a_n} = \overline{b_q}\overline{c_r}$$

et $\overline{b_q}, \overline{c_r} \neq 0$. Mais, par hypothèse $\overline{P}$ est irréductible dans $\mathbb{F}_p[X]$. L'un des polynômes $\overline{Q}$ ou $\overline{R}$ est donc de degré 0 ce qui contredit $\overline{b_q}, \overline{c_r} \neq 0$. Ainsi P est irréductible dans $\mathbb{Q}[X]$. Notons que l'on n'a pas nécessairement l'irréductibleilité de P dans $\mathbb{Z}[X]$ car si par exemple Q est de degré 0, il s'écrit $Q = b_0$ et $P = b_0R$ n'est pas irréductible dans $\mathbb{Z}[X]$.

3.3.2 Polynômes irréductibles dans un corps fini

Soit $\mathbb{K}$ un corps fini de caractéristique p. Il existe un entier n non nul tel que $\mathbb{K}$ soit de cardinalité p^n. Un tel corps de cardinalité p^n est unique à isomorphisme près. Nous l'avons noté $\mathbb{F}_{p^n}$. Soit P un polynôme irréductible de degré n sur $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$. Son corps de rupture $\mathbb{F}_p[X]/(P)$ est une extension algébrique monogène degré n de $\mathbb{F}_p$. Ce corps est de cardinal p^n. Il coïncide donc avec $\mathbb{K} = \mathbb{F}_{p^n}$.

Proposition 30 *Soit p un nombre premier. Pour tout entier $n \geq 1$ il existe un polynôme irréductible de degré n dans $\mathbb{F}_p[X]$.*

Démonstration. Considérons le corps $\mathbb{F}_{p^n}$. Le groupe $\mathbb{F}_{p^n}^*$ des éléments inversibles est cyclique et de cardinalité p^n-1. Soit ξ un générateur de ce groupe. Alors $\mathbb{F}_{p^n}^* = \{1, \xi, \cdots, \xi^{p^n-2}\}$ et donc $\mathbb{F}_{p^n} = \{0, 1, \xi, \cdots, \xi^{p^n-2}\}$. Ceci implique que $\mathbb{F}_{p^n} = \mathbb{F}_p[\xi]$. En effet tout élément $u \in \mathbb{F}_p[\xi]$ s'écrit $u = \sum a_i\xi^i$ avec $a_i \in \mathbb{F}_p$ et comme $\xi^{p^n} = \xi$ on en déduit que $u = \sum_{i \leq p^n-2} b_i\xi^i$. Comme $\mathbb{F}_{p^n}$ est un $\mathbb{F}_p$-espace vectoriel on a $u \in \mathbb{F}_{p^n}$ et donc $\mathbb{F}_p[\xi]$ est un sous-corps de $\mathbb{F}_{p^n}$. Réciproquement considérons une base $\{\xi^{i_1}, \cdots, \xi^{i_n}\}$ du $\mathbb{F}_p$-espace vectoriel $\mathbb{F}_{p^n}$ alors tout élément $v \in \mathbb{F}_{p^n}$ s'écrit $v = \sum_{k=1}^n b_k\xi^{i_k}$ et donc $v \in \mathbb{F}_p[\xi]$. Ainsi $\mathbb{F}_p[\xi] = \mathbb{F}_{p^n}$ et $\mathbb{F}_p[\xi]$ est un $\mathbb{F}_p$ espace vectoriel de dimension n. On en déduit que le polynôme minimal P_ξ de ξ est un polynôme irréductible de degré n.

Proposition 31 *Soit P un polynôme irréductible de degré n sur $\mathbb{F}_p$. Alors P divise $X^{p^n} - X$.*

Démonstration. En effet le corps de rupture de P est un corps de cardinalité $\mathbb{F}_{p^n}$. Il est donc isomorphe à $\mathbb{F}_{p^n}$. Donc d'après la démonstration précédente, il est donc égal à $\mathbb{F}_p[\xi]$ où ξ est un générateur du groupe cyclique $F_p[\xi]^*$. Ainsi $X^{p^n} - X$ est un polynôme annulateur de ξ et P qui coïncide avec le polynôme minimal de ξ divise le polynôme P.

3.4 Extensions algébriques

3.4.1 Définition

Définition 26 *Une extension $\Bbbk \subset \mathbb{K}$ de corps $\Bbbk$ est dite algébrique si tout élément $\alpha \in \mathbb{K}$ est algébrique sur $\Bbbk$.*

Exemple. Le corps $\mathbb{C}$ est une extension algébrique de $\mathbb{R}$. En effet soit $z = a + ib$ un nombre complexe. Le polynôme $P = (X - z)(X - \overline{z})$ est à coefficients réels.

$$P = (X - z)(X - \overline{z}) = (X - a - ib)(X - a + ib) = X^2 - 2abX + a^2 + b^2.$$

Ainsi $P \in \mathbb{R}[X]$ et $P(z) = 0$. Donc z est algébrique sur $\mathbb{R}$.

Considérons une extension $\Bbbk \in \mathbb{K}$. Soit $\mathbb{A}_{\Bbbk,\mathbb{K}}$ l'ensemble des éléments de $\mathbb{K}$ algébriques sur $\Bbbk$. Nous avons vu que $\mathbb{A}_{\Bbbk,\mathbb{K}}$ est un corps et $\Bbbk \subset \mathbb{A}_{\Bbbk,\mathbb{K}} \subset \mathbb{K}$ est une tour d'extension.

Proposition 32 *Le corps $\mathbb{K}$ est une extension algébrique de $\Bbbk$ si $\mathbb{K} \subset \mathbb{A}_{\Bbbk,\mathbb{K}}$.*

Ceci découle directement de la définition d'une extension algébrique. On appelle le corps $\mathbb{A}_{\Bbbk,\mathbb{K}}$ la clôture algébrique de $\Bbbk$ dans $\mathbb{K}$. Lorsque $\mathbb{A}_{\Bbbk,\mathbb{K}} = \Bbbk$, alors $\Bbbk$ est dit algébriquement fermé dans $\mathbb{K}$. Ne pas confondre cette définition avec celle des corps algébriquement clos :

Proposition 33 *Un corps $\Bbbk$ est algébriquement clos si et seulement si pour toute extension algébrique de $\Bbbk \subset \mathbb{K}$ on a $\Bbbk = \mathbb{K}$.*

En effet $\Bbbk$ est algébriquement clos si tout polynôme $P \in \Bbbk[X]$ admet une racine dans $\Bbbk$. Dans ce cas toutes les racines de P sont dans $\Bbbk$ et P est un produit de polynôme de degré 1. Si $\Bbbk \subset \mathbb{K}$ est une extension algébrique, tout élément $\alpha \in \mathbb{K}$ est racine d'un polynôme $Q \in \Bbbk[X]$. Comme $\Bbbk$ est algébriquement clos, $\alpha \in \Bbbk$ et $\mathbb{K} = \Bbbk$. Inversement soit $P \in \Bbbk[X]$ un polynôme irréductible. Soit $\mathbb{K} = \frac{\Bbbk[X]}{(P)}$ son corps de rupture (cf chapitre 1). L'application $s : \Bbbk \to \Bbbk[X]$ définie par $s(a) = a$ considérée comme polynôme de degré 0 est un morphisme d'anneau injectif. Composons s avec la surjection canonique $\pi : \Bbbk[X] \to \mathbb{K} = \frac{\Bbbk[X]}{(P)}$. Alors $\pi \circ s : \Bbbk \to \mathbb{K}$ est un homomorphisme injectif de corps et $\mathbb{K}$ est une extension de $\Bbbk$. Soit $\alpha = \pi(X) \in \mathbb{K}$. Si $\beta \in \mathbb{K}$, il existe $R = \sum a_i X^i$ avec $a_i \in \Bbbk$. Alors $\pi(R) = \sum a_i \alpha_i \overline{X}^i$ car π est un morphisme d'anneaux. On en déduit $\pi(R) = \sum a_i \alpha^i$ et donc $\beta = \sum a_i \alpha^i \in \Bbbk[\alpha]$. On en déduit que $\mathbb{K} = \Bbbk[\alpha]$ et donc par hypothèse $\Bbbk[X]/(P)$ (ou plus précisément $\pi \circ s(\Bbbk)$). Ceci implique que P est de degré 1 et que $\Bbbk$ est algébriquement clos.

Exemples.

1. $\mathbb{C}$ est algébriquement clos.
2. Considérons l'extension $\mathbb{Q} \subset \mathbb{C}$ et soit $\mathbb{A}_{\mathbb{Q},\mathbb{C}}$ le corps des nombres complexes algébriques sur $\mathbb{Q}$. Alors $\mathbb{A}_{\mathbb{Q},\mathbb{C}}$ est algébriquement clos.

3.4.2 Extensions de degré fini

Définition 27 *Une extension $\Bbbk \subset \mathbb{K}$ est dite de degré fini si*

$$[\mathbb{K};\Bbbk] < \infty$$

Théorème 11 *Toute extension $\Bbbk \subset \mathbb{K}$ de degré fini n est algébrique. De plus tout élément $\alpha \in \mathbb{K}$, qui est algébrique sur $\Bbbk$, est de degré d_α tel que $d_\alpha \leq n$.*

Démonstration. Soit $\Bbbk \subset \mathbb{K}$ une extension de degré n. Rappelons que $n = dim_{\Bbbk}\mathbb{K}$. Pour tout $\alpha \in \mathbb{K}$, la famille $\{1, \alpha, \cdots, \alpha^n\}$ est donc liée car elle contient $n+1$ éléments. $P(\alpha) = a_0 + a_1\alpha + \cdots + a_n\alpha^n = 0$. Comme $P \in \Bbbk[X]$ et admet pour racine α,α est algébrique sur $\Bbbk$ et $\mathbb{K}$ est une extension algébrique de $\Bbbk$. Ceci montre également qu'il existe un polynôme P de degré n ayant α pour racine. Comme le polynôme minimal P_α divise P, on en déduit que d $P_\alpha \neq n$ et donc d_α qui est le degré de P_α est inférieur à n.

Remarque. La réciproque de ce théorème est fausse. En effet considérons l'extension $\mathbb{Q} \subset \mathbb{A}_{\mathbb{Q},\mathbb{C}} \subset \mathbb{C}$. Elle n'est pas de degré fini. En effet pour tout $n \in \mathbb{N}$ fixé, il existe $\alpha \in \mathbb{A}_{\mathbb{Q},\mathbb{C}}$ de degré supérieur à n. Considéons par exemple $\alpha = 2^{\frac{1}{n+1}}$. Le polynôme $X^{n+1} - 2$ est dans $\mathbb{Q}[X]$ et vérifie $P(\alpha) = 0$. D'après le critère d'Einsenstein, il est irréductible dans $\mathbb{Q}$, donc $P = P_\alpha$. On en déduit $d_\alpha = n+1$. Donc pour tout n, $\mathbb{A}_{\mathbb{Q},\mathbb{C}}$ contient un sous-espace vectoriel de dimension supérieur à n. Il est donc de dimension infinie.

3.4.3 Les extensions $\Bbbk(\alpha_1, \cdots, \alpha_n)$

Soit $\Bbbk \subset \mathbb{K}$ une extension de $\Bbbk$. Considérons n éléments $\alpha_1, \cdots, \alpha_n \in \mathbb{K}$. On note pour $\Bbbk[\alpha_1, \cdots, \alpha_n] = \{P(\alpha_1, \cdots, \alpha_n) \,/\, P \in \Bbbk[X_1, \cdots, X_n]\}$ où $\Bbbk[X_1, \cdots, X_n]$ désigne l'anneau des polynômes à coefficients dans $\Bbbk$à n indéterminées.

On note par $\Bbbk(\alpha_1, \cdots, \alpha_n)$ le corps des fractions de $\Bbbk[\alpha_1, \cdots, \alpha_n]$ c'est-à-dire

$$\Bbbk(\alpha_1, \cdots, \alpha_n) = \left\{ \frac{P(\alpha_1, \cdots, \alpha_n)}{Q(\alpha_1, \cdots, \alpha_n)}, P, Q \in \Bbbk[X_1, \cdots, X_n], Q(\alpha_1, \cdots, \alpha_n) \neq 0 \right\}.$$

Le corps $\Bbbk$ s'identifie à un sous-corps de $\Bbbk(\alpha_1, \cdots, \alpha_n)$ et on déduit la tour d'extension

$$\Bbbk \subset \Bbbk(\alpha_1, \cdots, \alpha_n) \subset \mathbb{K}.$$

Proposition 34 *Soient $\alpha_1, \cdots, \alpha_n \in \mathbb{K}$ des éléments algébriques sur $\Bbbk$. Alors l'extension $\Bbbk(\alpha_1, \cdots, \alpha_n)$ est algébrique sur $\Bbbk$ et de degré fini. De plus $\Bbbk(\alpha_1, \cdots, \alpha_n) = \Bbbk[\alpha_1, \cdots, \alpha_n]$.*

Démonstration. Construisons une tour d'extension algébrique associée à $\alpha_1, \cdots, \alpha_n$. Posons $\mathbb{K}_0 = \mathbb{k}, \mathbb{K}_1 = \mathbb{k}(\alpha_1) = \mathbb{k}[\alpha_1]$. On a l'extension

$$\mathbb{k} = \mathbb{K}_0 \subset \mathbb{K}_1.$$

algébrique de degré fini d_1.

Soit $\mathbb{K}_2 = \mathbb{K}_1[\alpha_2] = \mathbb{k}(\alpha_1)[\alpha_2]$. Mais α_2 est algébrique sur $\mathbb{k}$ donc sur $\mathbb{k}(\alpha_1)$. Ainsi $\mathbb{K}_2 = \mathbb{K}_1(\alpha_2) = \mathbb{k}(\alpha_1)(\alpha_2)$. Comme tout polynôme $P \in \mathbb{k}[X_1, X_2]$ peut se mettre sous la forme

$$P(X_1, X_2) = \sum_{i=0}^{l} P_i(X_1) X_2^i$$

avec $P_i \in \mathbb{k}[X_1]$, donc $\mathbb{k}[X_1, X_2] \subset \mathbb{k}(X_1)[X_2] = \mathbb{k}[X_1][X_2]$ on réciproquement on peut montrer que en déduit que $\mathbb{k}[X_1][X_2] \subset \mathbb{k}[X_1, X_2]$. On a alors

$$\mathbb{K}_2 = \mathbb{k}(\alpha_1)(\alpha_2) = \mathbb{k}[\alpha_1][\alpha_2] = \mathbb{k}[\alpha_1, \alpha_2].$$

Ainsi $\mathbb{k}[\alpha_1, \alpha_2]$ est un corps et est égal à son corps des fractions et on a $\mathbb{k}(\alpha_1, \alpha_2) = \mathbb{k}[\alpha_1, \alpha_2] = \mathbb{K}_2$. Comme $\dim_{\mathbb{k}} \mathbb{K}_2 = \dim_{\mathbb{K}_1} \mathbb{K}_2 \dim_{\mathbb{k}} \mathbb{K}_1$, alors $\dim_{\mathbb{k}} \mathbb{K}_2 < \infty$ et l'extension $\mathbb{K}_2$ est de degré fini. Elle est donc algébrique sur $\mathbb{k}$. Nous avons donc construit la tour d'extension algébrique

$$\mathbb{k} = \mathbb{K}_0 \subset \mathbb{K}_1 \subset k(\alpha_1) = \mathbb{k}[\alpha_1] \subset \mathbb{K}_2 = k(\alpha_1, \alpha_2) = \mathbb{k}[\alpha_1][\alpha_2] \subset \mathbb{K}.$$

Construisons par récurrence $\mathbb{K}_i = \mathbb{K}_{i-1}[\alpha_i]$. Montrons que $\mathbb{K}_i = \mathbb{K}[\alpha_1, \cdots, \alpha_i]$. Tout polynôme $P \in \mathbb{k}[X_1, \cdots, X_i]$ peut s'écrire

$$P(X_1, \cdots, X_i) = \sum_{j=1}^{k_i} P_j(X_1, \cdots, X_i^j$$

avec $P_j \in \mathbb{k}[X_1, \cdots, X_{j-1}]$. Ainsi $\mathbb{K}[$
$alpha_1, \cdots, \alpha_{i_1}][\alpha_i] = \mathbb{K}[\alpha_i, \cdots, \alpha_i] = \mathbb{K}_{i_1}[\alpha_i] = \mathbb{K}_i$. Comme $\mathbb{K}_i$ est un corps on a $\mathbb{K}_i = \mathbb{K}(\alpha_i, \cdots, \alpha_i)$ et $[\mathbb{K}_i; \mathbb{K}] = [\mathbb{K}_i; \mathbb{K}_{i-1}][\mathbb{K}_{i-1}; \mathbb{K}]$ est fini. Ainsi $\mathbb{K}_i$ est une extension algébrique sur $\mathbb{k}$.

Remarques.

1. Le degré de l'extension algébrique $\mathbb{K}[\alpha_1, \cdots, \alpha_n]$ est inférieure ou égale au produit des degrés des éléments algébriques α_i sur $\mathbb{k}$.
2. La proposition ci-dessus est en fait basée sur la construction d'extension algébrique que nous pouvons présenter ainsi : soit

   $$\mathbb{k} = \mathbb{K}_0 \subset \mathbb{K}_1 \subset \cdots \subset \mathbb{K}_n \subset \mathbb{K}$$

   une tour d'extension de $\mathbb{k}$ contenue dans $\mathbb{K}$ telle que
   a) il existe des éléments $\alpha_1, \cdots \alpha_n \in \mathbb{K}$ algébrique sur $\mathbb{k}$ avec α_i algébrique sur $\mathbb{K}_{i-1}$.
   b) $\mathbb{K}_i = \mathbb{K}i - 1[\alpha - i]$
   Alors $\mathbb{K}_n$ est une extension algébrique de degré fini

   $$d = d_1 \cdots d_n$$

   où $d_i = [\mathbb{K}_i, \mathbb{K}_{i-1}]$.

Proposition 35 *(transitivité de l'algébricité) Soit $\Bbbk \subset \mathbb{K}_1 \subset \mathbb{K}$ une tour d'extension.*
1. Si $\mathbb{K}_1$ est une extension algébrique de $\Bbbk$ et $\mathbb{K}$ est une extension algébrique de $\mathbb{K}_1$, alors $\mathbb{K}$ est une extension algébrique de $\Bbbk$.
2. Si $\mathbb{K}$ est une extension algébrique de $\Bbbk$ alors $\mathbb{K}$ est une extension algébrique de $\mathbb{K}_1$ et $\mathbb{K}_1$ est une extension algébrique de $\Bbbk$.

Démonstration.

1. Soit $\alpha \in \mathbb{K}$ Montrons qu'il est algébrique sur $\Bbbk$. Comme $\mathbb{K}$ est une extension algébrique de $\mathbb{K}_1$, tout élément de $\mathbb{K}$ et donc $\alpha \in \mathbb{K}$ est algébrique sur $\mathbb{K}_1$. Soit P_α le polynôme minimal de α. Par hypothèse $P_\alpha \in \mathbb{K}_1[X]$. Posons $P_\alpha = a_0 + a_1X + \cdots + a_nX^n$ avec $a_i \in \mathbb{K}_1$. Chaque élément a_i est algébrique sur $\Bbbk$. L'extension $\Bbbk(a_0, \cdots, a_n)$ de $\Bbbk$ est donc algébrique de degré fini. Posons $\mathbb{L} = \Bbbk(a_0, \cdots, a_n)$ et considérons l'extension monogène $\mathbb{L}(\alpha)$ de $\mathbb{L}$. Elle est de degré fini. par conséquent, l'extension $\mathbb{L}(\alpha)$ de $\Bbbk$ vérifie
$$[\mathbb{L}(\alpha); \Bbbk] = [\mathbb{L}(\alpha); \mathbb{L}] \cdot [\mathbb{L}; \Bbbk]$$
Comme $[\mathbb{L}; \Bbbk]$ est fini ainsi que $[\mathbb{L}(\alpha); \mathbb{L}]$, on en déduit que $\mathbb{L}(\alpha)$ est une extension de degré fini de $\Bbbk$. Considérons à présent l'extension $\Bbbk(\alpha)$ de $\Bbbk$. Elle vérifie
$$\Bbbk(\alpha) \subset \mathbb{L}(\alpha)$$
et donc $[\Bbbk(\alpha); \Bbbk] \leq [\mathbb{L}(\alpha); \Bbbk]$. Ainsi $[\Bbbk(\alpha); \Bbbk]$ est fini et l'extension monogène $\Bbbk(\alpha)$ est algébrique sur $\Bbbk$. L'élément α est donc algébrique sur $\Bbbk$.
2. Supposons que $\mathbb{K}$ soit une extension algébrique de $\Bbbk$. Alors tout élément de $\mathbb{K}$ donc de $\mathbb{K}_1$ est algébrique sur $\Bbbk$. Ainsi $\mathbb{K}_1$ est une extension algébrique de $\Bbbk$. De même si $\alpha \in \mathbb{K}$, comme α est algébrique sur $\Bbbk$, il existe $P \in \Bbbk[X]$ tel que $P(\alpha) = 0$. Comme $\Bbbk \subset \mathbb{K}$ on peut considérer $P \in \mathbb{K}_1[X]$ et α est algébrique sur $\mathbb{K}_1$.

3.4.4 Application : les corps quadratiques

Définition 28 *On appelle corps quadratique toute extension de degré 2 de $\mathbb{Q}$ dans $\mathbb{C}$*

Ainsi $\mathbb{K}$ est un corps quadratique si on a la tour d'extension
$$\mathbb{Q} \subset \mathbb{Q} \subset \mathbb{C}$$
avec $[\mathbb{K}; \mathbb{Q}] = 2$.

Exemples

1. Soit $d \in \mathbb{N}$ un entier vérifiant $d > 2$. Supposons que $\sqrt{d} \notin \mathbb{Q}$. Alors $\mathbb{Q}(\sqrt{d})$ est un corps quadratique. En effet le polynôme minimal de $\sqrt{d}$ est $P = X^2 - d$. Il est eneffet irréductible dans $\mathbb{Q}$ et $P(\sqrt{d}) = 0$. On en déduit
$$\mathbb{Q}[\sqrt{d}] = \mathbb{Q}(\sqrt{d})$$
et $[\mathbb{Q}(\sqrt{d}; \mathbb{Q}] = d$ $P_\alpha = 2$.
Ainsi $\mathbb{Q}(\sqrt{d})$ est un corps quadratique. Notons qu'une base du $\mathbb{Q}$-espace vectoriel $\mathbb{Q}(\sqrt{d})$ est donnée par $\{1, \sqrt{d}\}$.

2. Si $d \in \mathbb{Z}$, alors $\sqrt{d} \in \mathbb{C}$ et $\sqrt{d} \notin \mathbb{Q}$. L'extension $\mathbb{Q}(\sqrt{d})$ est un corps quadratique.

Théorème 12 *Soit $\mathbb{K}$ un corps quadratique. Il existe $d \in \mathbb{Z} - \{0, 1\}$ sans facteur carré tel que $\mathbb{K} = \mathbb{Q}(\sqrt{d})$.*

Démonstration. Soit $\alpha \in \mathbb{K}, \alpha \notin \mathbb{Q}$. Comme

$$[\mathbb{K}, \mathbb{Q}] = 2 = [\mathbb{K}; \mathbb{Q}(\alpha)] \cdot [\mathbb{Q}(\alpha); \mathbb{Q}]$$

on en déduit $[\mathbb{Q}(\alpha); \mathbb{Q}] = 1$ ou 2. Si $[\mathbb{Q}(\alpha); \mathbb{Q}] = 1$, alors $\mathbb{Q}(\alpha) = \mathbb{Q}$ et $\alpha \in \mathbb{Q}$ ce qui est contraire à l'hypothèse. Ainsi $[\mathbb{Q}(\alpha); \mathbb{Q}] = 2$ et donc $\mathbb{K} = \mathbb{Q}(\alpha)$.

Le polynôme minimal P_α de α s'écrit donc

$$P_\alpha = X^2 + aX + b$$

avec $a, b \in \mathbb{Q}$. Considérons sa forme canonique dans $\mathbb{Q}[X]$

$$P_\alpha = \left(X + \frac{a}{2}\right)^2 - \left(\frac{a^2}{4} - b\right).$$

Comme $P_\alpha(\alpha) = 0$, on a $\left(\alpha + \frac{a}{2}\right)^2 - \left(\frac{a^2}{4} - b\right) = 0$. Posons $\beta = \alpha + \frac{a}{2}$. Alors $\beta \notin \mathbb{Q}$ et vérifie $\beta^2 - \frac{a^2-4b}{4} = 0$. Son polynôme minimal est $X^2 - \frac{a^2-4b}{4}$ et donc $\mathbb{K} = \mathbb{Q}(\alpha) = \mathbb{Q}(\beta)$. Comme, $\frac{a^2-4b}{4} \in \mathbb{Q}$, posons $\frac{a^2-4b}{4} = \frac{p}{q}$. Alors $\beta^2 = \frac{p}{q}$ et $\gamma = q\beta$ vérifie $\gamma^2 = (q\beta)^2 = pq$. Comme $pq \in \mathbb{Z}$, nous pouvons le factoriser sous la forme $pq = r^2 d$ avec $r, d \in \mathbb{Z}$ et $d \neq 0, d \neq 1$ et sans facteur carré. On en déduit

$$\gamma^2 = r^2 d$$

soit $\gamma = r\sqrt{d}$ ou $\gamma = r\sqrt{-d}$. Mais P_γ et donc $P_{\frac{\gamma}{r}}$ les polynômes minimaux de γ et $\frac{\gamma}{2}$ sont de degré 2. Donc $\mathbb{K} = \mathbb{Q}\left(\frac{\gamma}{r}\right) = \mathbb{Q}(\sqrt{d})$ ou $= \mathbb{Q}(\sqrt{-d})$.

newpage

3.5 EXERCICES

Exercice 1. Déterminer le degré des extensions $\mathbb{Q}(\sqrt{7})$ et $\mathbb{Q}(\sqrt[3]{7})$ de $\mathbb{Q}$. A-t-on $\mathbb{Q}(\sqrt{7}) \subset \mathbb{Q}(\sqrt[3]{7})$? Pour quels nombres premiers p et q a-t-on $\mathbb{Q}(\sqrt{p})$ et $\mathbb{Q}(\sqrt[3]{q})$?

Exercice 2. Trouver le polynôme minimal de $\sqrt[6]{2}$ dans $\mathbb{Q}$ et dans $\mathbb{Q}(\sqrt{2})$.

Exercice 3. Déterminer le degré des extensions de $\mathbb{Q}$ suivantes et en trouver une base.

1. $\mathbb{Q}(j)$
2. $\mathbb{Q}(cos\frac{2\pi}{3})$
3. $\mathbb{Q}(sin\frac{2\pi}{3})$
4. $\mathbb{Q}(cos\frac{2\pi}{5})$, $\mathbb{Q}(e^{\frac{2i\pi}{5}})$ et $\mathbb{Q}(\sqrt{5})$. Quels sont les liens entre ces trois corps ? (Montrer que $1 + X + \cdots + X^4$ est irréductible dans $\mathbb{Q}$ et plus généralement $1 + X + \cdots + X^{p-1}$ est irréductible dans $\mathbb{Q}$ si p est premier).

Exercice 4. Soit $\Bbbk \subset \mathbb{K}$ une extension de corps. Soit $\alpha \in \mathbb{K}$ un élément algébrique sur $\Bbbk$. Si $P_\alpha \in \Bbbk[X]$ est le polynôme minimal de α, montrer que toutes les racines de P_α dans $\mathbb{K}$ admettent P_α comme polynôme minimal.

Exercice 5. Soit $\Bbbk \subset \mathbb{C}$ une extension de corps par $\mathbb{C}$. Soit $\alpha \in \mathbb{C}$ un élément algébrique sur $\Bbbk$. Montrer que α est racine simple de son polynôme minimal P_α.

Exercice 6. Soit $\Bbbk \subset \mathbb{K}$ une extension de corps et $\alpha \in \mathbb{K}$ un élément algébrique sur $\Bbbk$. Soit $P_\alpha \in \Bbbk[X]$ le polynôme minimal α. Montrer que l'extension $\Bbbk(\alpha)$ de $\Bbbk$ est isomorphe au corps de rupture de P_α.

Exercice 7. Construire les familles $\mathcal{F}_1 \subset \mathcal{F}_2 \subset \mathcal{F}_3$ des points constructibles à partir de $\mathcal{F}_1 = (O, I)$. Quels sont les réels constructibles ainsi déterminés.

Exercice 8. Problème de la trisection de l'angle. Montrer que $x_1 = cos\frac{\pi}{3}$ est constructible mais $x_2 = cos\frac{\pi}{9}$ ne l'est pas.

Exercice 9.

1. Déterminer $\mathbb{Q}(\sqrt{2})$ et $\mathbb{Q}(\sqrt{3})$. Montrer que $\mathbb{Q}(\sqrt{2}) \cap \mathbb{Q}(\sqrt{3}) = \mathbb{Q}$. En déduire le degré de $\mathbb{Q}(\sqrt{2}, \sqrt{3})$.
2. Soit $\alpha = \sqrt{2} + \sqrt{3}$. Est-ce un nombre algébrique sur $\mathbb{Q}$. Montrer que $\mathbb{Q}(\alpha) = \mathbb{Q}(\sqrt{2}, \sqrt{3})$
3. En déduire les sous-corps de $\mathbb{Q}(\alpha)$.

Exercice 10. Soit $\Bbbk$ un corps et $P \in \Bbbk[X]$ un polynôme irréductible de degré n. Montrons que si $\Bbbk \subset \mathbb{K}$ est une extension de degré fini m premier avec n alors P est irréductible sur $\mathbb{K}$.

Exercice 11.

1. Déterminer le degré de l'extension $\mathbb{Q}(\sqrt[5]{10}, \sqrt[3]{7})$ sur $\mathbb{Q}$.
2. Déterminer le degré de l'extension $\mathbb{Q}(\sqrt[5]{10} + \sqrt[3]{7})$ sur $\mathbb{Q}$.

Exercice 12. Résultant. Discriminant de deux polynômes.

Soir $\Bbbk$ un sous-corps de $\mathbb{C}$. Considérons deux polynômes $P_1, P_2 \in \Bbbk[X]$ de degré respectif p et q.

$$P_1 = a\prod_{i=1}^{p}(X - \alpha_i), P_2 = b\prod_{i=1}^{q}(X - \beta_i),$$

leur décomposition dans $\mathbb{C}[X]$ ($\alpha - i, \beta_i \in \mathbb{C}$.) On appelle résultant de P_1 et P_2 le nombre complexe

$$R(P_1, P_2) = a^q b^p \prod_{\substack{1 \leq i \leq p \\ 1 \leq j \leq q}} (\alpha_i - \beta_i)$$

Si P_1 ou P_2 sont nuls, on pose $R(P_1, P_2) = 0$.

1. Montrer que $R(P_1, P_2) = 0$ si et seulement si P_1 et P_2 ont une racine commune.
2. Montrer que $R(P_1, P_2) = 0$ si et seulement si $\begin{cases} PGCD(P_1, P_2) = 0 \text{ ou} \\ d\,PGCD \geq 1 \end{cases}$
3. On suppose $P_2 = b$ de degré 0 avec $b \neq 0$. Calculer $R(P_1, P_2)$.
4. On suppose que P_1 et P_2 non nuls. Montrer que

$$R(P_1, P_2) = a^p \prod_{i=1}^{p} P_2(\alpha_i)$$

$$R(P_2, P_1) = (-1)^{pq} R(P_1, P_2)$$

5. Soient α et β deux nombres algébriques complexes sur $\mathbb{Q}$. Soient P_1 et $P_2 \in \mathbb{Q}[X]$ deux polynômes de degré respectif p et q tel que $P_1(\alpha) = P_2(\beta) = 0$. Soit $R(Z) = R(P_1(X), P_2(Z - X))$ le résultant des polynômes $P_1(X)$ et $P_2(Z - X)$ de $\Bbbk[X]$. Montrer que $\alpha + \beta$ est racine de $R(Z)$.
6. En déduire le polynôme minimal de $\sqrt{2} + \sqrt{3}, \sqrt{2} + \sqrt[4]{2}, \sqrt{2} + \sqrt[3]{3}, \sqrt[5]{10} + \sqrt[3]{7}$.

Exercice 13. Soit $\Bbbk \subset \mathbb{K}$ une extension de degré fini de $\mathbb{K}$. Supposons que $[\mathbb{K}; \Bbbk]$ soit un nombre premier. Montrer que $\mathbb{K}$ est une extension monogène.

Exercice 14. Déterminer tous les éléments primitifs du corps quadratique $\mathbb{Q}(\sqrt{d})$ (on suppose $\sqrt{d} \notin \mathbb{Q}$.)

Exercice 15. Soit $\Bbbk$ un corps de caractéristique différente de 2 et $\mathbb{K}$ une extension de $\Bbbk$ de degré 2. Montrer qu'il existe $\alpha \in \Bbbk - \mathbb{R}^2$ et $\beta \in \mathbb{K}$ tel que $\beta^2 = \alpha$ et $\mathbb{K} = \Bbbk(\beta)$.

Exercice 16.

Exercice 17.

Chapitre 4

Automorphismes de corps. Groupes de Galois

4.1 Endomorphismes de corps

Soit $\mathbb{K}$ un corps commutatif et soit $\varphi : \mathbb{K} \to \mathbb{K}$ un endomorphisme de corps. Ceci signifie que φ vérifie

$$\begin{cases} \varphi(x+y) = \varphi(x) + \varphi(y) \\ \varphi(xy) = \varphi(x)\varphi(y) \end{cases}$$

pour tous $x, y \in \mathbb{K}$. On a en particulier

$$\varphi(0) = \varphi(0) + \varphi(0) \text{ etdonc } \varphi(0) = 0$$

$$\varphi(1) = \varphi(1)\varphi(1)$$

et si $\varphi \neq 0$ alors $\varphi(1) = 1$. Notons que $\varphi(1) = 0$ implique $\varphi(x) = \varphi(x \cdot 1) = \varphi(x)\varphi(1) = 0$ pour tout x et donc $\varphi \equiv 0$ dans ce cas.

Proposition 36 *Soit f un endomorphisme du corps $\mathbb{K}$. Alors l'ensemble*

$$Fix(f) = \{x \in \mathbb{K} \ / \ f(x) = x\}$$

est un sous-corps de $\mathbb{K}$.

Démonstration. Comme $f(1) = 1$, alors $1 \in Fix(f)$. Soient $a, b \in Fix(f)$. Alors $f(a+b) = f(a)+f(b) = a+b$, donc $a + b \in Fix(f)$. D' même $f(ab) = f(a)f(b) = ab$ et $a \in Fix(f)$. Ainsi $Fix(f)$ est un sous-anneau de $\mathbb{K}$. On a de plus

$$f(a^{-1}) = f(a)^{-1} = a^{-1}$$

et donc pour tout $a \in Fix(f)$, $a^{-1} \in Fix(f)$ donc $Fix(f)$ est un sous-corps de $\mathbb{K}$.

Proposition 37 *Soit H une partie non vide de l'ensemble des endomorphismes du corps $\mathbb{K}$. Alors l'ensemble*

$$Fix(H) = \{x \in \mathbb{K} \ / \ \forall f \in H, f(x) = x\}$$

est un sous-corps de $\mathbb{K}$.

Démonstration. En effet $Fix(H) = \cap_{f\in H} Fix(f)$ et donc $Fix(H)$ est une intersection de sous-corps, c'est donc un sous-corps de $\mathbb{K}$.

Notons que $Fix(H)$ est parfois appelé le corps des invariants de H.

4.2 Automorphismes de corps

4.2.1 Définition

Définition 29 *Soit $\mathbb{K}$ un corps commutatif. On appelle automorphisme de corps tout isomorphisme de corps*

$$\varphi : \mathbb{K} \longrightarrow \mathbb{K}.$$

Ceci signifie que φ vérifie

$$\begin{cases} \varphi(x+y) = \varphi(x) + \varphi(y), \\ \varphi(xy) = \varphi(x)\varphi(y) \end{cases}$$

pour tous $x, y \in \mathbb{K}$, et φ est surjective. Rappelons que tout homomorphisme de corps est injectif et donc la subjectivité de φ est équivalente à la bijectivité. Rappelons également que si φ est un homomorphisme de corps alors

$$\begin{cases} \varphi(0) = 0, \\ \varphi(1) = 1 \end{cases}$$

4.2.2 Le groupe $Aut(\mathbb{K})$

On note par $Aut(\mathbb{K})$ l'ensemble des automorphismes du corps $\mathbb{K}$.

Proposition 38 *L'ensemble $Aut(\mathbb{K})$ des automorphismes du corps $\mathbb{K}$ est un groupe pour la composition.*

La démonstration est évidente. Cette proposition montre que $Aut(\mathbb{K})$ est un sous-corps du groupe $S(\mathbb{K})$ des permutations de $\mathbb{K}$.

4.2.3 Exemples

Automorphismes de $\mathbb{Q}$

Si $\varphi : \mathbb{Q} \to \mathbb{Q}$ est un automorphisme de corps, on a $\varphi(1) = 1$, d'où $\varphi(n) = \varphi(1 + 1 + \cdots + 1) = \varphi(1) + \varphi(1) + \cdots + \varphi(1) = n$. Si $q \neq 0$, $q \in \mathbb{Z}$ alors $\varphi(\frac{q}{q}) = \varphi(q)\varphi(\frac{1}{q}) = 1$. Donc $\varphi(\frac{1}{q}) = \frac{1}{q}$ et par conséquence, si $\frac{p}{q} \in \mathbb{Q}$ alors $\varphi(\frac{p}{q}) = \varphi(p)\varphi(\frac{1}{q}) = \frac{p}{q}$. Ainsi

$$Aut\mathbb{Q} = \{Id\}.$$

Automorphismes de $\mathbb{R}$

Le raisonnement précédent montre que si $\varphi \in Aut(\mathbb{R})$ alors $\varphi(x) = x$ pour tout $x \in \mathbb{Q}$.

Soit $x \geq 0, x \in \mathbb{R}$. Il existe $y \in \mathbb{R}$ tel que $x = y^2$. On en déduit $\varphi(x) = \varphi(y^2) = \varphi(y)\varphi(y) = \varphi(y)^2$. Ainsi $\varphi(x) \geq 0$. (Rappelons que muni de la relation $\geq$, $\mathbb{R}$ est un corps ordonné). La propriété $x \geq 0 \Rightarrow \varphi(x) \geq 0$ implique que φ est une application croissante. On en déduit que φ est une application continue. En effet soit $\epsilon > 0, \epsilon \in \mathbb{R}$ et soit $\eta = \varphi^{-1}(\epsilon)$. Si $x - x_0 < \eta$ alors comme φ est croissante, $\varphi(x - x_0) = \varphi(x) - \varphi(x_0) < \varphi(\eta) = \epsilon$. De même $x - x_0 > -\eta$ implique $\varphi(x) - \varphi(x_0) > -\epsilon$. Ainsi pour $\epsilon > 0$ donné, $|x - x_0| < \eta \Rightarrow |\varphi(x) - \varphi(x_0)| < \epsilon$. Conclusion : tout automorphisme du corps $\mathbb{R}$ est continue. Comme sa restriction à $\mathbb{Q}$ est l'identité et comme $\mathbb{Q}$ est dense dans $\mathbb{R}$, la continuité implique que φ est l'identité sur $\mathbb{R}$. Ainsi

$$Aut(\mathbb{R}) = \{Id\}.$$

Automorphismes de $\mathbb{C}$

Contrairement au cas précédent, un automorphisme du corps $\mathbb{C}$ n'est pas nécessairement continu, la continuité des automorphismes de $\mathbb{R}$ reposant sur la croissance et donc sur le fait que $\mathbb{R}$ est un corps ordonné, ce qui n'est pas le cas de $\mathbb{C}$.

Proposition 39 *Tout automorphisme continu du corps $\mathbb{C}$ est soit l'identité, soit la conjugaison*

$$\sigma : z \to \overline{z}$$

Démonstration. La topologie considérée sur $\mathbb{C}$ est la topologie métrique usuelle, pour cette topologie les opérations de corps sont continues. Soit $\varphi : \mathbb{C} \to \mathbb{C}$ un automorphisme de corps. Il vérifie $\varphi(0) = 0, \varphi(1) = 1$, t comme précédemment, on en déduit que $\varphi(r) = r$ pour tout $r \in \mathbb{Q}$. Soit $a \neq 0, a \in \mathbb{Q}$ et $b \in \mathbb{C}$ tel que $b^2 = a$. Comme $\varphi(b)^2 = \varphi(b^2) = \varphi(a) = a$ alors $\varphi(b)$ est racine de $X^2 = a$ et donc $\varphi(b) = \pm$ on en déduit pour $a = -1$ et $b = i$ que $\varphi(i) = \pm i$. Comsidérons alors l'extension $\mathbb{Q}[i]$ de $\mathbb{Q}$. Comme $\varphi(i) = \pm i$, φ restreint à $\mathbb{Q}[i]$ est égal à l'identité où à la conjugaison. Or $\mathbb{Q}$ est dense dans $\mathbb{R}$ et donc $\mathbb{Q}[i]$ est dense dans $\mathbb{C}$. Comme φ est continue sur $\mathbb{C}$ et égal à l'identité ou à la conjugaison sur la partie dense $\mathbb{Q}[i]$, elle est aussi égal à l'identité ou à la conjugaison sur $\mathbb{C}$.

Conséquence. Soit $Aut_0(\mathbb{C})$ le sous-groupe de $Aut(\mathbb{C})$ formé des automorphismes continus. Alors

$$Aut_0(\mathbb{C}) = \{Id, \sigma\}$$

où $\sigma(z) = \overline{z}$.

Dans le cas réel, nous avons vu que $Aut_0(\mathbb{R}) = Aut(\mathbb{R})$. Ce n'est plus le cas dans $\mathbb{C}$.

Théorème 13 *Il existe des automorphismes de $\mathbb{C}$ non continus.*

Examinons dans un premier temps comment étendre un isomorphisme de sous-corps de $\mathbb{C}$ en un isomorphisme de sous-corps intermédiaire.

Soit $\Bbbk_1$ et $\Bbbk_2$ deux sous-corps de $\mathbb{C}$ et $f : \Bbbk_1 \to \Bbbk_2$ un isomorphisme de corps.

a) Soit $\alpha \in \mathbb{C} - \Bbbk_1$ un élément algébrique sur $\Bbbk_1$. On peut alors étendre f en un isomorphisme de corps

$$\tilde{f} : \Bbbk_1(\alpha) \to \Bbbk_2(\beta)$$

tel que $\tilde{f}_{|_{k_1}} = f$ et $\tilde{f}(\alpha) = \beta$ et

β est algébrique sur k_2. Si $P_\alpha = \sum_{i=0}^{n} a_i X^i$ est le polynôme minimal de α, alors le polynôme minimal de β est $P_\beta = \sum_{i=0}^{n} f(a_i) X^i$.

b) Supposons α transcendant sur k_1. On peut étendre f en un isomorphisme de corps $\tilde{f}$ sur k_1 et $\tilde{f}(\alpha) = \beta$ est transcendant sur k_2. ‘

En particulier sir k_2 n'a pas d'élément transcendant, on ne peut étendre $\tilde{f}$ à $k_1(\alpha)$.

Lemme 5 *Soit φ un automorphisme non continu de $\mathbb{C}$. Alors $\varphi(\mathbb{R})$ est dense dans $\mathbb{C}$.*

En effet si $\varphi(\mathbb{R})$ n'et pas continu dans $\mathbb{R}$, il existe $b \in \mathbb{R}$ tel que $\varphi(b) \in \mathbb{C} - \mathbb{R}$. Soient $q_1, q_2 \in \mathbb{Q}$. On a

$$\varphi(q_1 b + q_2) = \varphi(q_1)\varphi(b) + \varphi(q_2).$$

Rappelons que tout automorphisme de $\mathbb{C}$ est l'identité sur $\mathbb{Q}$. Ainsi

$$\varphi(q_1 b + q_2) = q_1 \varphi(b) + q_2.$$

Fixons q_1. L'ensemble $\{\varphi(q_1 b + q_2), q_2 \in \mathbb{Q}\}$ est dense dans l'ensemble $\{q_1\varphi(b) + x, x \in \mathbb{R}\}$ isomorphe à $\mathbb{R}$. Faisons varier q_1. On obtient un ensemble dense dans le plan. Or cet ensemble est contenu dans $\varphi(\mathbb{R})$ et $\varphi(\mathbb{R})$ est dense dans $\mathbb{C}$.

Les exemples suivants montrent qu'il existent "beaucoup" d'isomorphismes de corps dans des extensions de $\mathbb{Q}$ dans $\mathbb{C}$ engendrés par un nombre fini d'éléments. Considérons par exemple $\mathbb{Q}(\sqrt{7})$. Comme $\sqrt{7}$ est algébrique sur $\mathbb{Q}$ de degré deux

$$\mathbb{Q}(\sqrt{7}) = \{a + b\sqrt{7}, a, b \in \mathbb{Q}\}.$$

Soit

$$\sigma : \mathbb{Q}(\sqrt{7}) \to \mathbb{Q}(\sqrt{7})$$

définie par $\sigma(a + b\sqrt{7}) = a - b\sqrt{7}$, soit $\sigma(\sqrt{7}) = -\sqrt{7}$. D'après les remarques ci-dessus, les seules extensions de l'identité sur $\mathbb{Q}$ à $\mathbb{Q}(\sqrt{7})$ sont Id et σ. Considérons à présent $\mathbb{Q}(\sqrt[4]{7})$. Considérée comme une extension de $\mathbb{Q}(\sqrt{7})$ le polynôme minimal appartient à $\mathbb{Q}(\sqrt{7})[X]$ et est égal à $X^2 - \sqrt{7}$. L'automorphisme σ de $\mathbb{Q}(\sqrt{7})$ envoie $X^2 - \sqrt{7}$ dans $X^2 + \sqrt{7}$. Mais les racines de $X^2 + \sqrt{7}$ sont $\pm i\sqrt{7}$. Ainsi toute extension $\tilde{\sigma}$ de $\sigma \in Aut(\mathbb{Q}(\sqrt{7}))$ à $\mathbb{Q}(\sqrt[4]{7})$ vérifie

$$\tilde{\sigma}(\sqrt{7}) = i\sqrt{7} \text{ ou } \tilde{\sigma}(\sqrt{7}) = -i\sqrt{7}.$$

Par exemple, soit $x \in \mathbb{Q}(\sqrt[4]{7})$ extension de degré deux de $\mathbb{Q}(\sqrt{7})$. Il s'écrit $x = x_1 + x_2\sqrt[4]{7}$ avec $x - 1, x_2 \in \mathbb{Q}(\sqrt{7})$ et donc

$$x = a + b\sqrt{7} + c\sqrt[4]{7} + d\sqrt[4]{7^3}, a, b, c, d \in \mathbb{Q}.$$

Alors $\tilde{\sigma}(x) = a + ib\sqrt{7} - c\sqrt[4]{7} - id\sqrt[4]{7^3}$ est un isomorphimse de coprs qui étend σ.

Considérons à présent l'extension $\mathbb{Q}(\sqrt[4]{7}, \pi)$ de $\mathbb{Q}$. Il existe beaucoup de possibilités pour étendre $\tilde{\sigma}$ à $\mathbb{Q}(\sqrt[4]{7}, \pi)$. Ces automorphimes ne coïncident pas avec l'identité ni la conjugaison sur $\mathbb{C}$. SI nous prouvons ue de tels automorphimes s'étendent en des automorphimes de $\mathbb{C}$, nous en déduirons l'existence d'automorphimes de $\mathbb{C}$ non continus. On montre dans un premier temps le résultat suivant :

Proposition 40 *Soient $\Bbbk_1$ et $\Bbbk_2$ deux sous-corps de $\mathbb{C}$ et $f : \Bbbk_1 \to \Bbbk_2$ un isomorphisme de corps. Alors f s'étend en un isomorphisme*

$$\widetilde{f} : A(\Bbbk_1, \mathbb{C}) \to A(\Bbbk_2, \mathbb{C}).$$

Rappelons que $A(\Bbbk_1, \mathbb{C})$ est le sous-corps de $\mathbb{C}$ formé des éléments de $\mathbb{C}$ algébrique sur $\Bbbk_1$. On considère la famille $\mathcal{F}$ constitué des isomorphismes étendant f à un sous-corps de $A(\Bbbk_1, \mathbb{C})$. Alors $\mathcal{F}$ est une famille inductive

(voir chapitre 1 cours Algèbre multilinéaire www.ramm-algebra-center.monsite-orange.fr)

non vide car elle contient f. Elle admet un élément maximal qui est l'isomorphisme $\widetilde{f}$ cherché. Notons que $Im\widetilde{f}$ est un sous-corps algébriquement clos de $\mathbb{A}(\Bbbk, \mathbb{C})$ contenant $\Bbbk$. C'est donc $\mathbb{A}(\Bbbk, \mathbb{C})$.

Théorème 14 *Tout automorphisme d'un sous-corps de $\mathbb{C}$ s'étend en un automorphisme de $\mathbb{C}$.*

Soit φ un automorphisme d'un sous-corps de $\mathbb{C}$ et soit $\mathcal{F}$ la famille d'automorphismes qui étendent φ à un sous-corps de $\mathbb{C}$. Cette famille est inductive et d'après le lemme de Zorm admet un élément maximal θ. Montrons que θ est un automorphisme de $\mathbb{C}$. Si ce n'est pas le cas, soit $\mathbb{K}$ un sous-corps de $\mathbb{C}$ qui soit le domaine de θ. Soit $\alpha \in \mathbb{C} - \mathbb{K}$. Si α est algébrique sur $\mathbb{K}$, alors $\mathbb{A}(\mathbb{K}, \mathbb{C}) \not\supseteq \mathbb{K}$ et d'après la proposition précédente, θ s'étend à $\mathbb{A}(\mathbb{K}, \mathbb{Q})$ ce qui contredit la maximalisé de θ. Donc s'il existe $\alpha \in \mathbb{C} - \mathbb{K}$, α est transcendant sur $\mathbb{K}$. On peut étendre θ à $\mathbb{K}(\alpha)$ et $\theta(\alpha)$ est transcendant dans $\Im\theta$. Ceci contredit la maximalisé de θ, donc $\mathbb{K} = \mathbb{C}$.

4.2.4 Automorphismes d'un corps fini

Commençons par étudier les automorphismes des corps premier $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$. Soient p un nombre premier et φ un automorphisme du corps $\mathbb{F}_p$. Pour tout $r \in \{0, 1, \cdots, p-1\}$, notons par $\overline{r}$ la classe de r dans $\mathbb{F}_p$. L'automorphisme φ vérifie

$$\varphi(\overline{0}) = \overline{0},\ \varphi(\overline{1}) = \overline{1}.$$

Il vérifie donc

$$\varphi(\overline{r}) = \overline{r}$$

pour tout $r \in \{0, 1, \cdots, p-1\}$. Ainsi

Proposition 41 *Soit p un nombre premier, alors*

$$Aut(\mathbb{F}_p) = \{Id\}.$$

Soit $\mathbb{K}$ un corps fini. Sa caractéristique p est non nulle et il existe un entier n tel que $\mathbb{K}$ contienne p^n éléments. Nous avons noté par $\mathbb{F}_{p^n}$ un tel corps, ce qui est justifié car il est unique à isomorphisme de corps près.

Proposition 42 *Le groupe $Aut(\mathbb{F}_{p^n})$ des automorphismes du corps fini $\mathbb{F}_{p^n}$ est un groupe cyclique d'ordre n engendré par l'automorphisme de Frobenius*

$$\mathcal{F} : x \in \mathbb{F}_{p^n} \longrightarrow x^p$$

de $\mathbb{F}_{p^n}$.

Démonstration. Rappelons que le corps $\mathbb{F}_{p^n}$ contient p^n éléments. Son groupe multiplicatif $\mathbb{F}_{p^n}^*$ contient $p^n - 1$ éléments. Il est cyclique et isomorphe au groupe $\mathbb{Z}/(p^n - 1)\mathbb{Z}$. Ainsi tout élément non nul de $\mathbb{F}_{p^n}$ est d'ordre un diviseur de $p^n - 1$. On en déduit que tout élément $x \in \mathbb{F}_{p^n}$ vérifie

$$x^{p^n} = x.$$

Soit $\mathcal{F}$ l'homomorphisme de Frobenius de $\mathbb{F}_{p^n}$. Comme $\mathbb{F}_{p^n}$ est de caractéristique p, il s'écrit

$$\mathcal{F}(x) = x^p.$$

Cet homomorphisme est injectif et comme $\mathbb{F}_{p^n}$ est fini, il est surjectif et donc

$$\mathcal{F} \in Aut(\mathbb{F}_{p^n}).$$

Considérons à présent le sous-groupe H de $Aut(\mathbb{F}_{p^n})$ engendré par $\mathcal{F}$. Comme

$$\mathcal{F}^k = x^{p^k}$$

on a $\mathcal{F}^n = x^{p^n} = x$ pour tout $x \in \mathbb{F}_{p^n}$ et donc $\mathcal{F}$ est d'ordre fini, son ordre étant un diviseur de n. Comme $\mathbb{F}_{p^n}^*$ est isomorphe au groupe $\mathbb{Z}/(p^n - 1)\mathbb{Z}$, l'ordre de $\mathcal{F}$ est exactement n. Ainsi le sous-groupe H engendré par $\mathcal{F}$ est cyclique d'ordre n. On en déduit donc que $Aut(\mathbb{F}_{p^n})$ contient un sous-groupe cyclique d'ordre n. Revenons à l'étude générale de $Aut(\mathbb{F}_{p^n})$. Rappelons que le corps premier de $\mathbb{F}_{p^n}$ est $\mathbb{F}_p$. Soit σ un automorphisme de $\mathbb{F}_{p^n}$. D'après la proposition ci-dessus, il vérifie

$$\sigma(x) = x, \quad \forall x \in \mathbb{F}_p.$$

On en déduit que σ est un $\mathbb{F}_p$-isomorphisme linéaire du $\mathbb{F}_p$-espace vectoriel $\mathbb{F}_{p^n}$ et

$$\dim_{\mathbb{F}_p} \mathbb{F}_{p^n} = [\mathbb{F}_{p^n}, \mathbb{F}_p] = n.$$

Mais tout $\mathbb{F}_p$-isomorphisme linéaire de $\mathbb{F}_{p^n}$ n'est pas un automorphisme du corps $\mathbb{F}_{p^n}$. Nous devons déterminer, parmi ces isomorphismes linéaires, ceux qui sont des homomorphismes du groupe multiplicatif $\mathbb{F}_{p^n}^*$. Supposons qu'il existe $n+1$ automorphismes $\sigma_1, \cdots, \sigma_{n+1}$ de $\mathbb{F}_{p^n}$ qui soient l'identité sur le sous-corps premier $\mathbb{F}_p$. Soit $\{e_1, \cdots, e_n\}$ une base du $\mathbb{F}_p$-espace vectoriel $\mathbb{F}_{p^n}$. Considérons les vecteurs $V_i = (\sigma_i(e_1), \cdots, \sigma_i(e_n))$, $i = 1, \cdots, n+1$. Ils appartiennent à l'espace vectoriel $\mathbb{F}_{p^n}^n$, considéré comme un $\mathbb{F}_{p^n}$-espace vectoriel. Il est donc de dimension n et la famille $\{V_1, \cdots, V_{n+1}\}$ est liée. Il existe des scalaires $\beta_1, \cdots, \beta_{n+1}$ appartenant au corps de base $\mathbb{F}_{p^n}$ tels que

$$\beta_1 V_1 + \cdots + \beta_{n+1} V_{n+1} = 0$$

soit

$$\beta_1 \sigma_1(e_i) + \cdots + \beta_{n+1} \sigma_{n+1}(e_i) = 0$$

pour $i = 1, \cdots, n$. Mais ceci implique

$$\beta_1 \sigma_1(x) + \cdots + \beta_{n+1} \sigma_{n+1}(x) = 0$$

pour tout vecteur $x \in \mathbb{F}_{p^n}$. On en déduit

$$\beta_1\sigma_1 + \cdots + \beta_{n+1}\sigma_{n+1} = 0$$

avec $\beta_1, \cdots, \beta_{n+1} \in \mathbb{F}_{p^n}$ non tous nuls. Pour montrer que ceci entraine une contradiction, nous considérons les automorphismes σ_i comme des homomorphismes du groupe multiplicatif $\mathbb{F}_{p^n}^*$. Ce sont donc des caractères du groupe $\mathbb{F}_{p^n}^*$ dans le corps $\mathbb{F}_{p^n}$. Rappelons qu'étant donné un groupe G et un corps $\mathbb{K}$, un caractère de G dans $\mathbb{K}$ est un homomorphisme de groupe de G dans $\mathbb{K}^*$. D'après le théorème d'Artin, des caractères distincts $\chi_1, \cdots, \chi_k$ du groupe G, sont linéalrement indépendants au sens suivant : si

$$\lambda_1\chi_1 + \cdots + \lambda_k\chi_k = 0$$

avec $\lambda_1, \cdots, \lambda_k \in \mathbb{K}$, alors $\lambda_1 = \cdots = \lambda_k = 0$. Appliquons ce résultat aux automorphismes σ_i considérés comme caractères du groupe $\mathbb{F}_{p^n}^*$ dans le corps $\mathbb{F}_{p^n}$. Comme ils sont distincts, ils sont indépendants et donc $\beta_1 = \cdots = \beta_{n+1} = 0$ ce qui contredit le fait qu'ils aient été choisis non tous nuls. Ainsi l'ordre du groupe $Aut(\mathbb{F}_{p^n})$ est au plus n. Comme il contient un sous-groupe d'ordre n, on a le résultat cherché.

4.3 Groupe de Galois d'une extension

4.3.1 $\Bbbk$-homomorphismes, $\Bbbk$-automorphismes

Définition 30 *Soient $\Bbbk \subset \mathbb{K}_1$ et $\Bbbk \subset \mathbb{K}_2$ deux extensions du corps $\Bbbk$. On appelle $\Bbbk$-homomorphisme de $\mathbb{K}_1$ dans $\mathbb{K}_2$ tout homomorphisme de corps*

$$\varphi : \mathbb{K}_1 \to \mathbb{K}_2$$

laissant invariant les éléments de $\Bbbk$ c'est-à-dire

$$\forall \alpha \in \Bbbk, \varphi(\alpha) = \alpha$$

Comme $\mathbb{K}_1$ et $\mathbb{K}_2$ sont des extensions de $\Bbbk$, ce sont des $\Bbbk$-espaces vectoriels. Si φ est un $\Bbbk$-homomorphisme alors pour tout $x \in \mathbb{K}_1$ et $\alpha \in \Bbbk$,

$$\varphi(\alpha x) = \varphi(\alpha)\varphi(x) = \alpha\varphi(x).$$

Ainsi φ est une application $\Bbbk$-linéaire.

Définition 31 *Soit $\Bbbk \subset \mathbb{K}$ une extension du corps $\Bbbk$. Tout $\Bbbk$-homomorphisme de $\mathbb{K}$ dans $\mathbb{K}$ bijectif est appelé un $\Bbbk$-automorphisme de $\mathbb{K}$.*

Si $\varphi : \mathbb{K} \to \mathbb{K}$ est un $\Bbbk$-automorphisme, c'est un endomorphisme $\Bbbk$-linéaire. Comme c'est un automorphisme de corps, il est injectif. Ainsi φ est un automorphisme si et seulement s'il est surjectif.

Proposition 43 *Soit $\Bbbk \subset \mathbb{K}$ une extension de degré fini. Alors tout $\Bbbk$-homomorphisme de $\mathbb{K}$ dans $\mathbb{K}$ est un $\Bbbk$-automorphisme.*

Démonstration. En effet comme $\mathbb{K}$ est un $\mathbb{k}$-espace vectoriel de dimension finie, tout endomorphisme linéaire injectif

$$\varphi : \mathbb{K} \to \mathbb{K}$$

est bijectif. Alors φ est un $\mathbb{k}$-automorphisme.

4.3.2 Groupe de Galois d'une extension $\mathbb{k} \subset \mathbb{K}$

Il est clair que la composée de deux $\mathbb{k}$-automorphismes de $\mathbb{K}$ est encore un $\mathbb{k}$-automorphisme de $\mathbb{K}$

Définition 32 *On appelle groupe de Galois d'une extension $\mathbb{k} \subset \mathbb{K}$, le groupe des $\mathbb{k}$-automorphismes de $\mathbb{K}$ pour la composition.*

On notera par $Gal(\mathbb{K}/\mathbb{k})$ le groupe de Galois de l'extension $\mathbb{k} \subset \mathbb{K}$. Il est clair que $Gal(\mathbb{K}/\mathbb{k})$ est un sous-groupe de $Aut(\mathbb{K})$.

Proposition 44 *Soit $\mathbb{K}$ un corps et P son sous-corps premier. Alors le groupe de Galois $Gal(\mathbb{K}/P)$ de l'extension de P par $\mathbb{K}$ est égal à $Aut(\mathbb{K})$.*

Démonstration. On sait que $Gal(\mathbb{K}/P)$ est un sous-groupe de $Aut(\mathbb{K})$. Soit $\varphi \in Aut(\mathbb{K})$. Nous avons vu que

$$Fix(\varphi) = \{x \in \mathbb{K},\ \varphi(x) = x\}$$

est un sous-corps de $\mathbb{K}$. Il contient donc le sous-corps premier P. Ainsi pour tout $x \in P$ on a $\varphi(x) = x$ et donc $\varphi \in Gal(\mathbb{K}/P)$. On en déduit que $Aut(\mathbb{K}) = Gal(\mathbb{K}/P)$.

Exemple. Comme $\mathbb{Q}$ est le corps premier de $\mathbb{R}$ on a :

$$Gal(\mathbb{R}/\mathbb{Q}) = Aut(\mathbb{R}) = \{Id\}.$$

4.3.3 Groupe de Galois d'une extension de degré fini

Théorème 15 *Soit $\mathbb{k} \subset K$ une extension de degré fini n. Le groupe de Galois $Gal(\mathbb{K}/\mathbb{k})$ est alors un groupe fini et on a :*

$$|Gal(\mathbb{K}/\mathbb{k})| \leq n$$

où $|Gal(\mathbb{K}/\mathbb{k})|$ désigne l'ordre du groupe de Galois.

Démonstration. En fait nous avons déjà établi cette démonstration dans le chapitre précédent lors de la détermination des groupes des automorphismes d'un corps fini.

Considérons une base $\{e_1, \cdots, e_n\}$ une base du $\mathbb{k}$-espace vectoriel $\mathbb{K}$. Rappelons que tout élément de $Gal(\mathbb{K}/\mathbb{k})$ est un $\mathbb{k}$-automorphisme de $\mathbb{K}$. C'est donc un $\mathbb{k}$-isomorphisme linéaire de $\mathbb{K}$. L'inverse n'est pas vrai. Un élément de $Gal(\mathbb{K}/\mathbb{k})$ est un $\mathbb{k}$-endomorphisme linéaire de $\mathbb{K}$ qui est aussi un automorphisme

du groupe multiplicatif $\mathbb{K}^*$. Supposons que le groupe de Galois contiennent $(n+1)$ éléments distincts $\varphi_1, \cdots, \varphi_n$. Considérons la famille des vecteurs du $\mathbb{K}$-espace vectoriel $\mathbb{K}^n$:

$$\begin{cases} V_1 = (\varphi_1(e_1), \cdots, \varphi_1(e_n)), \\ \cdots \\ V_{n+1} = (\varphi_{n+1}(e_1), \cdots, \varphi_{n+1}(e_n)). \end{cases}$$

Comme $\mathbb{K}^n$ est un espace vectoriel de dimension n sur $\mathbb{K}$ ces $(n+1)$-vecteurs sont liés. Il existe donc des coefficients $a_1, \cdots, a_{n+1} \in \mathbb{K}$ tels que $a_1 V_1 + \cdots a_{n+1} V_{n+1} = 0$. On en déduit

$$a_1\varphi_1(e_i) + \cdots a_{n+1}\varphi_{n+1}(e_i) = 0$$

pour tout $i = 1, \cdots, n$. Ceci implique que l'application :

$$a_1\varphi_1 + \cdots a_{n+1}\varphi_{n+1} : V \to a_1\varphi_1(V) + \cdots a_{n+1}\varphi_{n+1}(V)$$

est une application $\Bbbk$-linéaire sur le $\Bbbk$-espace vectoriel $\mathbb{K}$ nulle sur tous les vecteurs de base $e_1, \cdots, e_n$ de cet espace. Elle est donc nulle. Ainsi nous avons montrer qu'il existait des scalaires $a_1, \cdots, a_{n+1} \in \mathbb{K}$ non tous nuls tels que

$$a_1\varphi_1 + \cdots a_{n+1}\varphi_{n+1} = 0.$$

Or chacune des applications φ_i est un homomorphisme du groupe $\mathbb{K}^*$. Dans ce cas l'identité précédente est impossible. Ceci découle directement du théorème d'Artin (voir chapitre précédent) ou plus généralement du lemme de Dedekind (voir cours sur la théorie des groupes) :

Lemme de Dedekind *Soient G un groupe et $\mathbb{K}$ un corps. On considère une famille $(\varphi_i)_{i\in I}$ d'homomorphismes de groupes*

$$\varphi_i : G \to \mathbb{K}^*$$

où $\mathbb{K}^*$ est le groupe multiplicatif de $\mathbb{K}$. On suppose $\varphi_i \neq \varphi_j$ pour tous $i, j \in I, i \neq j$. Pour toute famille $(\lambda_i)_{i\in I}$ d'éléments de $\mathbb{K}$ vérifiant

$$\forall g \in G, \sum_{i\in I} \lambda_i \varphi_i(g) = 0$$

alors $\forall i \in I, \lambda_i = 0$.

Revenons à notre démonstration. La relation $a_1\varphi_1 + \cdots a_{n+1}\varphi_{n+1} = 0$ implique d'après le lemme de Dedekind que tous les a_i sont nuls ce qui est contraire à l'hypothèse faite sur les a_i. Donc le groupe de Galois contient au plus n éléments.

Proposition 45 *Soit $\Bbbk \subset K$ une extension de degré fini. L'ensemble*

$$Fix(Gal(\mathbb{K}/\Bbbk)) = \{x \in \mathbb{K}\ , \forall \varphi \in Gal(\mathbb{K}/\Bbbk), \varphi(x) = x\}$$

est un sous-corps de $\mathbb{K}$ contenant $\Bbbk$ et l'extension $Fix(Gal(\mathbb{K}/\Bbbk)) \subset \mathbb{K}$ est de degré fini. De plus

$$Gal(\mathbb{K}/\Bbbk) = Gal(\mathbb{K}/Fix(Gal(\mathbb{K}/\Bbbk)))$$

et

$$|Gal(\mathbb{K}/\Bbbk)| = [\mathbb{K}, Fix(Gal(\mathbb{K}/\Bbbk))].$$

Démonstration. Soit $\varphi \in Gal(\mathbb{K}/\Bbbk)$. Alors, d'après la définition du corps $Fix(Gal(\mathbb{K}/\Bbbk))$, il laisse fixe les éléments de ce corps. Comme $Fix(Gal(\mathbb{K}/\Bbbk)) \subset \mathbb{K}$ est une extension de corps, on en déduit

$$\varphi \in Gal(\mathbb{K}/Fix(Gal(\mathbb{K}/\Bbbk))$$

et donc

$$Gal(\mathbb{K}/\Bbbk) \subset Gal(\mathbb{K}/Fix(Gal(\mathbb{K}/\Bbbk)).$$

L'inclusion inverse est évidente, ainsi

$$Gal(\mathbb{K}/\Bbbk) = Gal(\mathbb{K}/Fix(Gal(\mathbb{K}/\Bbbk)).$$

Déterminons à présent l'ordre de ce groupe de Galois. Comme $\mathbb{K}$ est une extension de degré fini, le groupe $Gal(\mathbb{K}/\Bbbk)$ est d'ordre fini et

$$|Gal(\mathbb{K}/\Bbbk)| \leq [\mathbb{K}, \Bbbk].$$

D'après le résultat précédent, on en déduitt

$$|Gal(\mathbb{K}/\Bbbk)| = |Gal(\mathbb{K}/Fix(Gal(\mathbb{K}/\Bbbk))| \leq [\mathbb{K}, Fix(Gal(\mathbb{K}/\Bbbk))].$$

Posons $n = [\mathbb{K}, Fix(Gal(\mathbb{K}/\Bbbk))]$ et soit $\{e_1, \cdots, e_n\}$ une base du F-espace vectoriel $\mathbb{K}$ où F désigne, pour simplifier l'écriture, le corps $Fix(Gal(\mathbb{K}/\Bbbk))$. Posons $m = |Gal(\mathbb{K}/\Bbbk)|$. L'inégalité ci-dessus s'écrit

$$m \leq n.$$

Supposons $m \neq n$. Soit $\varphi_1, \cdots, \varphi_m$ les éléments de $Gal(\mathbb{K}/\Bbbk)$. Considérons les vecteurs

$$\begin{cases} V_1 = (\varphi_1(e_1), \cdots, \varphi_m(e_1)), \\ \cdots \\ V_n = (\varphi_1(e_n), \cdots, \varphi_m(e_n)). \end{cases}$$

Comme chaque $\varphi_i(e_j) \in \mathbb{K}$, ces m vecteurs appartient au $\mathbb{K}$-espace vectoriel $\mathbb{K}^n$. Ils engendrent un sous-espace vectoriel H de $\mathbb{K}^n$. Posons $r = \dim H$. Extrayons de la famille $\{V_1, \cdots, V_n\}$ une base de H et supposons, ce qui ne nuit pas à la généralité, que cette base soit $\{V_1, \cdots, V_r\}$. On a en particulier

$$V_{r+1} = a_1 V_1 + \cdots + a_r V_r$$

avec $a_i \in \mathbb{K}$ pour $i = 1, \cdots r$. Ceci est équivalent à écrire

$$\varphi_j(e_{r+1}) = a_1 \varphi_j(e_1) + \cdots + a_r \varphi_j(e_r)$$

pour tout $j = 1, \cdots, m$. Ceci signifie que tout élément du groupe $Gal(\mathbb{K}/\Bbbk)$ vérifie cette identité. Nous allons montrer que ces coefficients a_i appartiennent à $F = Fix(Gal(\mathbb{K}/\Bbbk))$. Soit $g \in Gal(\mathbb{K}/\Bbbk)$. Alors

$$g \circ \varphi_j(e_{r+1}) = g(a_1 \varphi_j(e_1) + \cdots + \varphi_j(e_r)) = g(a_1) g(\varphi_j(e_1)) + \cdots + g(a_r) g(\varphi_j(e_r)).$$

Mais tout élément $\varphi \in Gal(\mathbb{K}/\Bbbk)$ vérifie

$$\varphi(e_{r+1}) = a_1 \varphi(e_1) + \cdots + a_r \varphi(e_r)$$

et en particulier les applications $g \circ \varphi_j$, c'est-à-dire que l'on a

$$g \circ \varphi_j(e_{r+1}) = a_1 g \circ \varphi_j(e_1) + \cdots + a_r g \circ \varphi_j(e_r).$$

Comme on a aussi

$$g \circ \varphi_j(e_{r+1}) = g(a_1)g \circ \varphi_j(e_1) + \cdots + g(a_r)g \circ \varphi_j(e_r),$$

alors

$$(a_1 - g(a_1))g \circ \varphi_j(e_1) + \cdots + (a_r - g(a_r))g \circ \varphi_j(e_r) = 0.$$

Considérons l'inverse g^{-1} de g dans $Gal(\mathbb{K}/\Bbbk)$. Alors

$$g^{-1}((a_1-g(a_1))g\circ\varphi_j(e_1)+\cdots+(a_r-g(a_r))g\circ\varphi_j(e_r)) = (g^{-1}(a_1)-a_1)\varphi_j(e_1)+\cdots+(g^{-1}(a_r)-a_r)\varphi_j(e_r) = 0$$

Ceci est équivalent à

$$(g^{-1}(a_1) - a_1)V_1 + \cdots + (g^{-1}(a_r) - a_r)V_r = 0.$$

Comme les vecteurs $V_1, \cdots, V_r$ sont $\mathbb{K}$ linéairement indépendants, alors

$$g^{-1}(a_1) = a_1, \cdots, g^{-1}(a_r) = a_r$$

pour tout $g \in Gal(\mathbb{K}/\Bbbk)$.. Ainsi chacun des coefficients a_i est dans le corps F des éléments fixes de $Gal(\mathbb{K}/\Bbbk)$. On en déduit que pour chaque $\varphi \in Gal(\mathbb{K}, \Bbbk)$, on a

$$\varphi(e_{r+1}) = a_1\varphi(e_1) + \cdots a_r\varphi(e_r) = \varphi(a_1e_1 + \cdots + a_re_r).$$

Ceci est en particulier vrai pour $\varphi = Id$. Ceci donne

$$e_{r+1} = a_1e_1 + \cdots + a_re_r$$

avec $a_i \in F$. Mais les vecteurs $e_1, \cdots, e_n$ sont linéairement indépendants dans le F-espace vectoriel $\mathbb{K}$. Ceci est impossible et contredit l'hypothèse $m \neq n$. D'où

$$m = n$$

et

$$|Gal(\mathbb{K}/\Bbbk)| = [\mathbb{K}, Fix(Gal(\mathbb{K}/\Bbbk))].$$

Exemple.

Soit l'extension $\mathbb{Q} \subset \mathbb{Q}(\sqrt{2})$. Elle est de degré 2. Le groupe de Galois $Gal(\mathbb{Q}(\sqrt{2})/\mathbb{Q})$ est fini et son ordre vérifie

$$|Gal(\mathbb{Q}(\sqrt{2})/\mathbb{Q})| \leq 2.$$

Mais $Fix(Gal(\mathbb{Q}\sqrt{2})/\mathbb{Q}))$ est un corps vérifiant

$$\mathbb{Q} \subset Fix(Gal(\mathbb{Q}(\sqrt{2})/\mathbb{Q})) \subset \mathbb{Q}(\sqrt{2}).$$

Ainsi $[Fix(Gal(\mathbb{Q}(\sqrt{2})/\mathbb{Q})); \mathbb{Q}] = 1$ ou 2. Dans le premier cas $Fix(Gal(\mathbb{Q}(\sqrt{2})/\mathbb{Q})) = \mathbb{Q}$ et

$$|Gal(\mathbb{Q}(\sqrt{2})/\mathbb{Q})| = 2.$$

Dans le deuxième cas $Fix(Gal(\mathbb{Q}(\sqrt{2})/\mathbb{Q})) = \mathbb{Q}(\sqrt{2})$ et $Gal(\mathbb{Q}(\sqrt{2})/\mathbb{Q}) = Id$. Montrons que la première hypothèse est vérifiée. Soit σ l'automorphisme de $\mathbb{Q}(\sqrt{2})$ défini par

$$\sigma(a + b\sqrt{2}) = a - b\sqrt{2}.$$

Il vérifie $\sigma(a) = a$ pour tout $a \in \mathbb{Q}$ et σ appartient à $Gal(\mathbb{Q}(\sqrt{2})/\mathbb{Q})$. On a donc

$$Gal(\mathbb{Q}(\sqrt{2})/\mathbb{Q}) = \{Id, \sigma\}$$

et ce groupe est isomorphe à $\mathbb{Z}/2\mathbb{Z}$.

4.4 Extensions galoisiennes finies

4.4.1 Définition et exemples

Définition 33 *Soit $\Bbbk$ un corps (commutatif). On appelle extension galoisienne finie de $\Bbbk$ toute extension de corps $\mathbb{K}$ de $\Bbbk$ de degré fini tel que*

$$|Gal(\mathbb{K}/\Bbbk)| = [\mathbb{K};\Bbbk].$$

Exemples.

1. D'après l'exemple du paragraphe précédent, $\mathbb{Q}(\sqrt{2}) = \mathbb{Q}[\sqrt{2}]$ est une extension galoisienne finiee $\mathbb{Q}$ de degré 2.
2. Soit $\Bbbk \subset \mathbb{K}$ une extension de degré fini et soit $F = Fix(Gal(\mathbb{K}/\Bbbk))$ le corps des éléments fixes de $Gal(\mathbb{K}/\Bbbk)$. Alors
$$Gal(\mathbb{K}/\Bbbk) = Gal(\mathbb{K}/F)$$
et
$$|Gal(\mathbb{K}/\Bbbk)| = [\mathbb{K};F].$$
Ainsi l'extension de F par $\mathbb{K}$ est galoisienne finie.

4.4.2 Extensions algébriques monogènes galoisiennes

Soit $\Bbbk \subset \Bbbk[\alpha]$ une extension algébrique monogène de $\Bbbk$. Soit $P_\alpha \in \Bbbk[X]$ le polynôme minimal de α. Donc $\Bbbk[\alpha]$ est une extension algébrique de $\Bbbk$ de degré fini égal au degré du polynôme minimal de α. Comme l'extension est de degré fini son groupe de Galois vérifie

$$|Gal(\Bbbk[\alpha];\Bbbk| \leq [\Bbbk[\alpha];\Bbbk] = d(P_\alpha).$$

En général une telle extension n'est pas galoisienne. Plus précisément on a

Théorème 16 *Soit $\Bbbk[\alpha]$ une extension algébrique monogène de $\Bbbk$ et soit P_α le polynôme minimal de α. Alors l'extension $\Bbbk \subset \Bbbk[\alpha]$ est galoisienne finie si et seulement si P_α admet n racines distinctes dans $\Bbbk[\alpha]$ où n est le degré de P_α.*

Démonstration. Nous allons démontrer ce résultat en plusieurs étapes :

1. Soit $\varphi \in Gal(\Bbbk[\alpha];\Bbbk)$ alors $\varphi(\alpha)$ est une racine de P_α. Posons $P_\alpha = \sum_{i=1}^n a_i X^i$. Donc $P_\alpha(\varphi(\alpha)) = \sum_{i=1}^n a_i(\varphi(\alpha))^i = \sum_{i=1}^n a_i\varphi^i(\alpha) = \sum_{i=1}^n \varphi(a_i)\varphi(\alpha^i) = \sum_{i=1}^n \varphi(a_i\alpha^i) = \varphi(\sum_{i=1}^n a_i\alpha^i) = \varphi(P_\alpha(\alpha))\varphi(0) = 0$. Ainsi $\varphi(\alpha)$ est une racine de P_α.
2. Soit $\beta \in \Bbbk[\alpha]$ une racine de P_α. Alors il existe $\varphi \in Gal(\Bbbk[\alpha];\Bbbk)$ tel que $P_\alpha = P_\beta$. En effet si β est une racine de P_α il est algébrique sur $\Bbbk$. Comme $P_\alpha(\beta) = 0$ et que P_α est irréductible alors P_α est le polynôme minimal de β. Ainsi l'extension $\Bbbk[\beta]$ de $\Bbbk$ est aussi de degré n. Comme $\beta \in \Bbbk[\alpha]$ alors $\Bbbk[\beta] \subset \Bbbk[\alpha]$. Comme les $\Bbbk$-espaces vectoriels $\Bbbk[\beta]$ et $\Bbbk[\alpha]$ sont de même dimensions on a $\Bbbk[\beta] = \Bbbk[\alpha]$. Il existe donc $\varphi \in Gal(\Bbbk[\alpha];\Bbbk)$ tel que $\varphi(\alpha) = \beta$. Plus précisément cet automorphisme est défini par :
$$\varphi(b_0 + b_1\alpha + \cdots + b_n\alpha^n) = b_0 + b_1\beta + \cdots + b_n\beta^n$$
avec $b_i \in \Bbbk$.

3. L'ordre du groupe de Galois est égal au nombre de racines de P_α qui sont dans $\mathbb{k}[\alpha]$. En effet si $\beta_1, \cdots, \beta_r$ sont des racines distinctes de P_α dans $\mathbb{k}[\alpha]$, chacune de ces racines β_i définit un $\mathbb{k}$-automorphisme φ_i tel que $\beta_i = \varphi_i(\alpha)$. Ces automorphismes sont bien entendu distincts. Inversement si φ_1 et φ_2 sont deux automorphismes distincts de $Gal(\mathbb{k}[\alpha]; \mathbb{k})$ alors $\beta_1 = \varphi_1(\alpha)$ et $\beta_2 = \varphi_2(\alpha)$ sont des racines distinctes car tout $\mathbb{k}$-automorphisme de $\mathbb{k}[\alpha]$ est entièrement déterminé par l'image de α. Ainsi les $\mathbb{k}$-automorphimes de $\mathbb{k}[\alpha]$ correspondent bijectivement aux racines distinctes de P_α dans $\mathbb{k}[\alpha]$.
4. Les résultats ci-dessus montrent que si P_α admet n racines distinctes dans $\mathbb{k}[\alpha]$ alors le groupe de Galois $Gal(\mathbb{k}[\alpha]; \mathbb{k})$ est d'ordre n et l'extension $\mathbb{k}[\alpha]$ est donc galoisienne.

4.4.3 Exemple d'extension galoisienne finie : les corps finis

Soit $\mathbb{k}$ un corps fini de caractéristique p contenant $q = p^n$ éléments. Soit

$$\mathcal{F} : \mathbb{k} \to \mathbb{k}$$

l'automorphisme de Frobenius $\mathcal{F}^n(x) = x^p$. Il vérifie

$$\mathcal{F}^2(x) = x^{p^2}, \cdots, \mathcal{F}^n = Id_{\mathbb{k}}.$$

$\mathbb{k}$ étant de caractéristique p, c'est une extension de $\mathbb{F}_p$. Soit α un générateur du groupe cyclique $\mathbb{k}^*$. Comme $|\mathbb{k}| = q = p^n$, on a $|\mathbb{k}^*| = q - 1$ et $\alpha^{q-1} = 1$. Soit l un entier vérifiant $1 \leq l < n$. Alors

$$1 < p^l - 1 < p^n - 1 = q - 1$$

et donc $\alpha^{p^l - 1} \neq 1$. Ainsi

$$\mathcal{F}^l(\alpha) \neq \alpha$$

pour tout l tel que $1 \leq l < n$. On en déduit que $\mathcal{F}$ est un automorphisme d'ordre n de $\mathbb{k}$. Mais d'après la proposition ? (chap ? ?) , $\mathbb{k} = \mathbb{F}_p(\alpha)$ est une extension algébrique de $\mathbb{F}_p$ de degréé $p^n - 1$. Mais

$$|Gal(\mathbb{k}/\mathbb{F}_p)| \leq [\mathbb{k}, \mathbb{F}_p] = p^n - 1.$$

Or $Id, \mathcal{F}, \cdots, \mathcal{F}^{p^n - 2}$ sont des automorphismes de $\mathbb{F}_p$ qui se réduisent à l'identité sur $\mathbb{F}_p$. Ils appartiennent au groupe de Galois de l'extension $\mathbb{F}_p \subset \mathbb{k}$. On en déduit

Proposition 46 *Soit $\mathbb{k}$ un corps fini de caractéristique p. Alors l'extension $\mathbb{F}_p \subset \mathbb{k}$ est galoisienne finie.*

Soit $\mathbb{K}$ un corps fini qui soit une extension de $\mathbb{k}$ alors $\mathcal{F}^n : \mathbb{K} \to \mathbb{K}$ est un automorphisme de $\mathbb{K}$ qui est l'identité sur $\mathbb{k}$. Ainsi

$$\mathcal{F}^n \in Gal(\mathbb{K}/\mathbb{k})$$

pour toute extension finie de $\mathbb{k}$. Cet automorphisme est appelé l'automorphisme de $\mathbb{K}$ sur $\mathbb{k}$.Le corps $\mathbb{k}$ La proposition précédente implique alors

Proposition 47 *Soit $\mathbb{k}$ un corps fini de caractéristique p contenant $q = p^n$ éléments. Si $\mathbb{K}$ est un corps fini et une extension de $\mathbb{k}$, alors l'extension $\mathbb{k} \subset \mathbb{K}$ est galoisienne finie. Son groupe de Galois est le groupe cyclique engendré par l'automorphisme de Frobenius $\mathcal{F}$ de $\mathbb{K}$ sur $\mathbb{k}$.*

Chapitre 5

Extensions associées à un polynôme

Jusqu'à présent, les extensions qui nous ont plus particulièrement intéressé étaient les extensions algébriques de degré fini. A une extension algébrique monogène, nous avons associé un polynôme, le polynôme minimal de l'élément algébrique associé à cette extension et décrit des propriétés de ce polynôme qui permettaient de décrire l'extension en question. Par exemple, deux extensions monogènes algébriques dont les éléments algébriques correspondants avaient le même polynôme minimal sont isomorphes. Nous allons aborder la notion d'extension directement à partir d'un polynôme et décrire, à partir d'un polynôme donné, des extensions associées à ce polynôme.

Rappelons que tous les corps considérés sont commutatifs, et lorsque nous parlons de corps, celui-ci est commutatif.

5.1 Corps de rupture d'un polynôme

Cette notion a déjà été présentée au chapitre 1 comme exemple de construction de corps. Nous la rappelons ici car elle va jouer un rôle important pour la suite.

5.1.1 Définition

Soient $\Bbbk$ un corps commutatif et $\Bbbk[X]$ l'anneau des polynômes à une indéterminée à coefficients dans $\Bbbk$. Soit $P \in \Bbbk[X]$ un polynôme irréductible de degré au moins égal à 1. Il ne s'écrit donc pas comme un produit de deux polynômes de $\Bbbk[X]$ de degré au moins 1. L'idéal (P) de l'anneau $\Bbbk[X]$, défini par

$$(P) = \{PQ,\ Q \in \Bbbk[X]\},$$

est un idéal maximal et donc l'anneau quotient $\mathbb{K}_P = \Bbbk[X]/(P)$ est un corps, appelé le corps de rupture de P.

Soit $\pi : \Bbbk[X] \to \mathbb{K}_P$ la surjection canonique. C'est un homomorphisme surjectif d'anneaux. Identifions $\Bbbk$ à l'ensemble des polynômes de degré 0 de $\Bbbk[X]$. Alors la restriction $\pi|_{\Bbbk}$ de π au sous-anneau $\Bbbk$ de $\Bbbk[X]$ est un homomorphisme de corps

$$\pi|_{\Bbbk} : \Bbbk \to \mathbb{K}_P,$$

Il est donc injectif. Ainsi $\Bbbk$ s'identifie au sous-corps $\pi(\Bbbk)$ de $\mathbb{K}_P$. On a donc

Proposition 48 *Soit $P \in \mathbb{k}[X]$ un polynôme irréductible. Alors le corps de rupture $\mathbb{K}_P = \mathbb{k}[X]/(P)$ de P est une extension de corps de $\mathbb{k}$. Il est appelé le corps de rupture de P.*

Posons $\alpha = \pi(X)$. Si t est un élément de $\mathbb{K}_p$, il existe un polynôme $Q \in \mathbb{k}[X]$ tel que $t = \pi(Q)$. Si $Q = \sum a_i X^i$ avec $a_i \in \mathbb{k}$, alors $\pi(Q) = \sum a_i \overline{X}^i = \sum a_i \alpha^i$ car π est un homomorphisme d'anneaux. On en déduit

$$t = \sum a_i \alpha^i$$

et donc $t \in \mathbb{k}[\alpha]$. Comme $\mathbb{K}_p$ est un corps

$$\mathbb{K}_P = \mathbb{k}[\alpha] = \mathbb{k}(\alpha).$$

Proposition 49 *Le corps de rupture $\mathbb{K}_p$ du polynôme irréductible $P \in \mathbb{k}[X]$ est une extension monogène algébrique de $\mathbb{k}$ de degré*

$$[\mathbb{K}_p; \mathbb{k}] = d(P)$$

où $d(P)$ est le degré du polynôme P.

En effet, par construction $\pi(P) = 0$ ce qui est équivalent à

$$P(\alpha) = 0.$$

Comme P est irréductible, P est le polynôme minimal de α.

Conséquence. Etant donné un polynôme irréductible $P \in \mathbb{k}[X]$ de degré supérieur à 1, il existe une extension monogène algébrique dans laquelle P a une racine. Cette remarque permet de donner un sens plus large à cette définition concernant tout polynôme irréductible ou non.

Définition 34 *Soit P un polynôme de $\mathbb{k}[X]$. Une extension $\mathbb{K}$ de $\mathbb{k}$ est appelé corps de rupture de P sur $\mathbb{k}$ s'il existe dans $\mathbb{K}$ une racine de P et si $\mathbb{K} = \mathbb{k}[\alpha]$.*

Il est clair que si P est irréductible, le corps $\mathbb{K}_P$ est un corps de rupture au sens large. Notons toutefois que si P n'est pas irréductible, il existe un corps de rupture tel que

$$[\mathbb{K}; \mathbb{k}] \leq d(P).$$

En effet comme P n'est pas irréductible il s'écrit $P = P_1 P_2$ et nous pouvons supposer qu'un de ces deux polynômes P_i est irréductible. Prenons par exemple P_1. Alors $\mathbb{K}_{P_1}$ est un corps de rupture de P_1 donc de P et on a

$$[\mathbb{K}_{P_1}; \mathbb{k}] = d(P_1) \leq d(P).$$

Par contre si P est irréductible, deux corps de rupture $\mathbb{k}[\alpha]$ et $\mathbb{k}[\beta]$ de P sont isomorphes à $\mathbb{K}_P$. Ces corps sont dits conjugués.

5.1.2 Sur le groupe de Galois d'un corps de rupture

Soit P un polynôme irréductible et soit $\mathbb{K}_P$ son corps de rupture. Si n est le degré de P, alors $\mathbb{K}_P$ est une extension monogène algébrique, $\mathbb{K}_P = \Bbbk[\alpha]$ de $\Bbbk$ de degré n. Toutefois cette extension n'est pas en général galoisienne. Pour s'en convaincre, il suffit de se reporter au chapitre précédent sur le calcul du groupe de Galois d'une extension monogène algébriquee. Celle-ci est algébrique si l'extension contient toutes les racines de P et si ces racines sont simples. Ce qui n'est pas en général le cas.

Exemple. Considérons par exemple le polynôme $P = X^4 - 2$ de $\mathbb{Q}[X]$. Il est irréductible d'après le critère d'Eisenstein. Son corps de rupture $\mathbb{K}_P$ est une extension de degré 4. Soit $\alpha = \sqrt[4]{2}$. Tout $\mathbb{Q}$-automorphismes de $\mathbb{Q}[\sqrt[4]{2}]$ est entièrement défini par la donnée de l'image de $\sqrt[4]{2}$. Ainsi les seuls $\mathbb{Q}$-automorphismes de $\mathbb{Q}[\sqrt[4]{2}]$ sont σ_1 et σ_2 définis par

$$\begin{cases} \sigma_1(\sqrt[4]{2}) = \sqrt[4]{2} \\ \sigma_2(\sqrt[4]{2}) = -\sqrt[4]{2}. \end{cases}$$

Ainsi $|Gal(\mathbb{K}_P/\mathbb{Q})| = 2 < [\mathbb{K}_P; \mathbb{Q}] = 4$. Cette extension n'est pas galoisienne finie.

Nous allons donc associer à P un nouveau corps en considérant "toutes" les racines de P et s'approcher d'une extension galoisienne finie.

5.2 Corps de décomposition d'un polynôme irréductible

Définition 35 *Soit $\Bbbk$ un corps et soit $P \in \Bbbk[X]$ un polynôme de degré n. On dit qu'une extension de corps $\Bbbk \subset \mathbb{K}$ est un corps de décomposition de P sur $\Bbbk$ si*

1. *il existe $a, \alpha_1, \cdots, \alpha_n \in \mathbb{K}$ tel que $P = a(X - \alpha_1)\cdots(X - \alpha_n)$ dans $\mathbb{K}[X]$,*
2. *$\mathbb{K} = \Bbbk(\alpha_1, \cdots, \alpha_n)$.*

Ainsi $\mathbb{K}$ est une extension algébrique de degré fini de $\Bbbk$ dans laquelle P se factorise en polynôme de degré 1. En "gros", $\mathbb{K}$ est obtenu par adjonction des racines de P. Ceci se comprend facilement si $\Bbbk$ est un sous-corps de $\mathbb{C}$. On cherche les racines de P dans $\mathbb{C}$ et on construit ensuite $\mathbb{K}$.

Théorème 17 *Soit $\Bbbk$ un corps et soit $P \in \Bbbk[X]$ un polynôme de degré supérieur n ou égal à 1. Alors*

1. *Il existe un corps de décomposition de P de degré inférieur ou égal à $n!$.*
2. *Deux corps de décomposition de P sont $\Bbbk$-isomorphes.*

Le théorème montre l'existence et surtout l'unicité à isomorphisme près du corps de décomposition de P. Pour cela nous parlerons du corps de décomposition de P sur $\Bbbk$ et nous le noterons $\mathbb{D}_{\Bbbk}(P)$.

Démonstration. Nous allons prouver l'existence du corps de décomposition en raisonnant par récurrence sur le degré de P.

- Supposons P de degré 1. alors $\mathbb{K} = \Bbbk$ est un corps de décomposition de P.
- Supposons que tout polynôme de degré m sur $\Bbbk$ admet un corps de décomposition. Soit P un polynôme de degré $m+1$. Si $\mathbb{K}_P$ est son corps de rupture, il existe $\alpha \in \mathbb{K}_P$ tel que $P(\alpha) = 0$ et $\Bbbk[\alpha] = \mathbb{K}_p$. Dans le corps $\Bbbk[\alpha]$, P se factorise

$$P = (X - \alpha)P_1$$

avec $P_1 \in \Bbbk[\alpha][X]$ et $d(P_1) = m$. D'après l'hypothèse de récurrence, P_1 admet un corps de décomposition $\mathbb{K}_1$ sur $\Bbbk[\alpha]$ et dans ce corps P_1 se factorise

$$P_1 = a(X - \alpha_1) \cdots (X - \alpha_n)$$

avec $a, \alpha_1, \cdots, \alpha_n \in \mathbb{K}_1$. Ainsi dans $\mathbb{K}_1$ on a

$$P = a(X - \alpha)(X - \alpha_1) \cdots (X - \alpha_n)$$

et donc ce polynôme P se factorise en polynôme de degré 1. Chaque $\alpha_i, i = 1, \cdots, n$, est algébrique sur $\Bbbk$ car se sont des racines de P. De plus, d'après l'hypothèse de récurrence, $\mathbb{K}_1 = \Bbbk[\alpha](\alpha_1, \cdots, \alpha_n)$ est une extensoion finie algébrique, par définition d'un corps de décomposition. Ainsi

$$\mathbb{K}_1 = \Bbbk[\alpha](\alpha_1, \cdots, \alpha_n) = \Bbbk(\alpha, \alpha_1, \cdots, \alpha_n)$$

et $\mathbb{K}_1$ est un corps de décomposition de P.

- On en déduit que tout polynôme de degré supérieur ou égal à 1 sur $\Bbbk$ admet un corps de décomposition.

Montrons à présent qu'un tel corps est unique à isomorphisme près. Soient $\mathbb{K}_1$ et $\mathbb{K}_2$ deux corps de décomposition du polynôme P. Nous allons montrer l'existence d'un $\Bbbk$-isomorphisme entre $\mathbb{K}_1$ et $\mathbb{K}_2$ par récurrence sur le degré de $[\mathbb{K}_1; \Bbbk]$. Posons $n = [\mathbb{K}_1; \Bbbk]$ (ce degré est fini car $\mathbb{K}_1$ est engendré par les racines de P).

— Si $n = 1$ alors $\Bbbk = \mathbb{K}_1$, le polynôme P admet toutes ces racines dans $\Bbbk$ et le résultat est évident.

— Supposons le résultat vrai pour tous les corps de décomposition de P de degré inférieur à n sur $\Bbbk$. Comme $n > 1$, les racines de P ne sont pas toutes dans $\Bbbk$ donc P admet un facteur irréductible Q de degré $d > 1$ dans $\Bbbk$. Soit α une racine de Q, donc de P, appartenant à $\mathbb{K}_1$. Comme Q est irréductible, $[\Bbbk[\alpha]; \Bbbk] = d(Q)$ et donc $[\Bbbk[\alpha]; \Bbbk] > 1$. Il est clair que $\mathbb{K}_1$ et $\mathbb{K}_2$ sont des corps de décomposition de P sur $\Bbbk[\alpha]$ et on a

$$[\mathbb{K}_1; \Bbbk] = [\mathbb{K}_1; \Bbbk[\alpha]].[\Bbbk[\alpha]; \Bbbk] = n$$

et donc $[\mathbb{K}_1; \Bbbk[\alpha]] < n$. Selon l'hypothèse de récurrence, il existe un isomorphisme de corps $f : \mathbb{K}_1 \to \mathbb{K}_2$ tel que f soit l'identité sur $\Bbbk[\alpha]$. C'est donc aussi l'identité sur $\Bbbk$.

On en déduit le théorème.

Consequence. Si P est un polynôme de degré n, son corps de décomposition existe et est unique (à isomorphisme près). On le note $\mathbb{D}_{\Bbbk}(P)$. Dans ce corps $P = a(X-\alpha)(X-\alpha_1) \cdots (X-\alpha_n)$ avec $a, \alpha_1, \cdots, \alpha_n \in \mathbb{D}_{\Bbbk}(P)$ et $\mathbb{D}_{\Bbbk}(P) = \Bbbk(\alpha_1, \cdots, \alpha_n)$.

Définition 36 *Soit p un polynôme de $\Bbbk[X]$ et $\mathbb{D}_{\Bbbk}(P)$ son corps de décomposition. Alors le groupe de Galois $|Gal(\mathbb{D}_{\Bbbk}(P)/\Bbbk|$ de l'extension $\Bbbk \subset \mathbb{D}_{\Bbbk}(P)$ est appelé le Groupe de Galois du polynôme P ou de l'équation polynomiale $P(x) = 0$.*

Ainsi le corps de décomposition de $P \in \Bbbk[X]$ est une extension algébrique de degré fini dans laquelle P se faxtorise en produit de polynôme de premier degré. Si P est de degré n, alors P admet dans son corps de décomposition n racines distinctes ou confondues. De plus, de par sa construction, on a

$$[\mathbb{D}_{\Bbbk}(P), \Bbbk] \leq n!.$$

5.3 Le groupe de Galois d'un polynôme séparable

5.3.1 Polynômes séparables

Soit $P \in \Bbbk[X]$ et soit $\mathbb{D}_{\Bbbk}(P)$ son corps de décomposition. Comme $\mathbb{D}_{\Bbbk}(P)$ est une extension de $\Bbbk$, on peut considérér P comme un polynôme à coefficients dans cette extension. Par définition du corps de décomposition, le polynôme P s'écrit alors

$$P = a(X - \alpha_1) \cdots (X - \alpha_r)$$

avec $a, \alpha_1, \cdots \alpha_r \in \mathbb{D}_{\Bbbk}(P)$. Mais les racines $\alpha_1, \cdots \alpha_r$ peuvent être confondues.

Définition 37 *On dit que le polynôme $P \in \Bbbk[X]$ est séparable si P n'a pas de racine multiple dans son corps de décomposition $\mathbb{D}_{\Bbbk}(P)$.*

Ainsi, si P est de degré n et séparable, alors il admet n racine distinctes dans $\mathbb{D}_{\Bbbk}(P)$. Soit P' le polynôme dérivé de P. Si $P = a_0 + a_1X + \cdots + a_nX^n$ avec $a_i \in \Bbbk$ pour $i = 1, \cdots, n$, alors son polynôme dérivé s'écrit

$$P' = a_1 + 2a_2X + 3a_3X^2 + \cdots + na_nX^{n-1}.$$

Considérons P comme un polynôme à coefficients dans $\mathbb{D}_{\Bbbk}(P)$. Soit $\alpha \in \mathbb{D}_{\Bbbk}(P)$ une racine de P. On a alors

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

et α est une racine simple si et seulement si $Q(\alpha) \neq 0$. Or

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

et donc

$$P'(\alpha) = Q(\alpha).$$

Ainsi α est une racine simple de P si et seulement si elle n'est pas racine dans $\mathbb{D}_{\Bbbk}(P)$ du polynôme dérivé P'. Cette notion d'être séparable dépend évidemment du corps de base. Par exemple soit $P = X^2 + 1 \in \mathbb{Q}[X]$. Son corps de décomposition est $\mathbb{Q}[i]$ et il est séparable dans $\mathbb{Q}$. Par contre, soit $P = X2 + 1 \in \mathbb{F}_2[X]$. Son corps de décomposition est $\mathbb{F}_2$. Il s'écrit $P = (X + 1)^2$. Il n'est pas séparable dans $\mathbb{F}_2$.

Proposition 50 *Soit $\Bbbk$ un corps de caractéristique 0. Alors tout polynôme irréductible de $\Bbbk[X]$ est séparable.*

Démonstration. En effet, supposons que P admette une racine multiple α dans le corps de décomposition $\mathbb{D}_{\Bbbk}(P)$. Comme α est algébrique sur $\Bbbk$, il admet un polynôme minimal P_α. Comme $P'(\alpha) = 0$, le polynôme dérivé vérifie $P' = P_\alpha Q$. Or $P(\alpha) = 0$ et le polynôme P est irréductible. Donc $P = aP_\alpha$ avec $a \in \Bbbk$ non nul. Donc P divise le polynôme dérivé P', ce qui est impossible sauf si $P' = 0$. Comme $\Bbbk$ est de caractéristique 0, ceci implique P de degré 0. Or par hypothèse, P est irréductible et donc de degré non nul. D'où la proposition.

Proposition 51 *Soit $\Bbbk$ un corps de caractéristique p, $p \neq 0$. Soit $P = a_0 + a_1X + \cdots + a_nX^n$ un polynôme irréductible de $\Bbbk[X]$. Il est séparable si et seulement si il existe k, $k = 1, \cdots, n$, tel que $ka_k \neq 0$.*

Démonstration. En effet, posons $P = a_0 + a_1X + \cdots + a_nX^n$. Alors $P' = a_1 + 2a_2X + 3a_3X^2 + \cdots + na_nX^{n-1}$. Supposons P irréductible. La démonstration ci-dessus montre que P est séparable si et seulement si P' est non nul. Ceci est équivalent à dire que chacun des coefficients ka_k n'est pas un multiple de p.

Corollaire 3 *Soit $\Bbbk$ un corps fini de caractéristique p, $p \neq 0$. Alors tout polynôme irréductible de $\Bbbk[X]$ est séparable.*

Démonstration. Soit $P \in \Bbbk[X]$ un polynôme irréductible. Si P n'est pas séparable il est de la forme

$$P = a_0 + a_1X^p + a_2X^{2p} + \cdots + a_kX^{kp}.$$

Mais comme $\Bbbk$ est fini de caractéristique p, l'homomorphisme de Frobenius

$$\mathcal{F}(x) = x^p$$

est un automorphisme de $\Bbbk$. Ainsi, pour chacun des coefficients a_i, il existe $b_i \in \Bbbk$ tel que $a_i = b_i^p$. Ainsi

$$P = b_0^p + b_1^pX^p + b_2X^{2p} + \cdots + b_k^pX^{kp} = b_0^p + (b_1X)^p + (b_2X^2)^p + \cdots + (b_kX^k)^p.$$

Mais comme $\mathcal{F}(x+y) = \mathcal{F}(x) + \mathcal{F}(y)$, on en déduit

$$P = (b_0 + b_1X + b_2X^2 + \cdots + b_kX^k)^p.$$

Or P est irréductible, on a donc une contradiction.

5.3.2 Corps parfaits

Définition 38 *On dit qu'un corps $\Bbbk$ est parfait si tout polynôme irréductible de $\Bbbk[X]$ est séparable.*

Ainsi tout corps de caractéristique 0 est parfait. De même, tout corps fini est parfait. Il nous reste donc à caractériser les corps infinis de caractéristique non nulle parfait.

Proposition 52 *Soit $\Bbbk$ un corps infini de caractéristique p, $p \neq 0$. Alors $\Bbbk$ est parfait si et seulement si l'homomorphisme de Frobenius*

$$\mathcal{F} : x \in \Bbbk \to x^p$$

est surjectif.

Démonstration. Si l'homomorphisme de Frobénius est surjectif, il est bijectif. On retrouve la situation décrite dans le cas des corps finis. En recopiant la démonstration du corollaire précédent, on en déduit que tout polynôme irréductible est séparable et le corps est parfait. Réciproquement, soit $\Bbbk$ un corps parfait infini de caractéristique p non nulle. Soit $a \in \Bbbk$. Nous voulons montrer qu'il existe $b \in \Bbbk$ tel que $a = b^p$. Considérons le polynôme $P = X^p - a$. Son corps de rupture $\mathbb{D}_{\Bbbk}(P)$ est une extension algébrique monogène de $\Bbbk$. Soit $b \in \mathbb{D}_{\Bbbk}(P)$ une racine de P. Son polynôme minimal P_b dans $\Bbbk[X]$ est irréductible. Il est donc séparable. Comme $b^p - a = 0$, le polynôme P admet b comme racine et divise donc P_b dans $\Bbbk[X]$. Il divise donc P_b dans $\mathbb{D}_{\Bbbk}(P)[X]$. Mais dans $\mathbb{D}_{\Bbbk}(P)[X]$, on a

$$P = X^p - a = X^p - b^p = (X - b)^p.$$

On en déduit que $P_b = X - b$. Comme $P_b \in \Bbbk[X]$, alors $b \in \Bbbk$. La surjectivité est prouvée.

5.3.3 Calcul de $|Gal(\mathbb{D}_{\Bbbk}(P)/\Bbbk|$, P séparable

Soit P un polynôme de $\Bbbk[X]$ de degré n et soit $\mathbb{D}_{\Bbbk}(P)$ son corps de décomposition. Supposons que P soit séparable c'est-à-dire que dans $\mathbb{D}_{\Bbbk}(P)$ on ait $P = a(X-\alpha_1)\cdots(X-\alpha_n)$ avec $\alpha_i \neq \alpha_j$ pour tout $i, j = 1, \cdots, n$. Dans ce cas on a le résultat :

Proposition 53 *Soit P un polynôme séparable de $\Bbbk[X]$. Alors*

$$|Gal(\mathbb{D}_{\Bbbk}(P)/\Bbbk)| = [\mathbb{D}_{\Bbbk}(P); \Bbbk]$$

et l'extension $\Bbbk \subset \mathbb{D}_{\Bbbk}(P)$ est galoisienne de degré fini.

Démonstration. Montrons par récurrence sur $d = [\mathbb{D}_{\Bbbk}(P); \Bbbk]$ que le nombre de $\Bbbk$-automorphismes de $\mathbb{D}_{\Bbbk}(P)$ est égal à d.

- Si $d = 1$, alors $\mathbb{D}_{\Bbbk}(P) = \Bbbk$ et $[\mathbb{D}_{\Bbbk}(P); \Bbbk] = 1 = |Gal(\Bbbk/\Bbbk)|$.
- Supposons $d \geq 2$ et le résultat vrai pour tous les corps de décomposition de degré inférieur ou égal à $d-1$ de polynômes ayant des racines distinctes. Soit P un polynôme de $\Bbbk[X]$ tel que $[\mathbb{D}\Bbbk](P); \Bbbk] = d$. Comme $d \geq 2$, les racines de P ne sont pas toutes dans $\Bbbk$ et P a un diviseur irréductible Q dans $\Bbbk[X]$. On a $d(Q) = m \geq 2$. On a alors

$$\begin{cases} Q = a_1(X-\alpha_1)\cdots(X-\alpha_m) \\ P = a(X-\alpha_1)\cdots(X-\alpha_m)\cdots(X-\alpha_n). \end{cases}$$

  Considérons le corps $\Bbbk[\alpha_1]$. Le polynôme Q est irréductible dans $\Bbbk$ et vérifie $Q(\alpha_1) = 0$. Le polynôme minimal P_{α_1} de α_1 est donc du type $P_{\alpha_1} = bQ$ et donc

$$[\Bbbk[\alpha_1]; \Bbbk] = m$$

  et il existe exactement m homomorphismes de $\Bbbk[\alpha_1] \to \mathbb{D}_{\Bbbk}(P)$ qui prolongent l'identité sur $\Bbbk[\alpha_1]$et donc sur $\Bbbk$.

5.4 Extensions séparables

Dans le paragraphe précédent, nous avons vu la notion de polynômes séparables et son intérêt sur la groupe de Galois. Ceci conduit à étudier particulièrement les éléments algébriques dont le polynôme minimal associé est séparable.

5.4.1 Eléments séparables

Soit $\Bbbk \subset \mathbb{K}$ une extension de corps.

Définition 39 *Un élément $\alpha \in \mathbb{K}$ algébrique sur $\Bbbk$ est dit séparable sur $\Bbbk$, si son polynôme minimal P_α est séparable.*

Notons que cette définition est équivalente à dire qu'il existe un polynôme $P \in \Bbbk[X]$ séparable tel que $P(\alpha) = 0$. En effet s'il existe un polynôme séparable P ayant α comme racine, il admet toutes ses racines

dans son corps de décomposition et ces racines son simples. Comme P_α est un diviseur irréductible de P, P_α admet toutes ses racines dans $\mathbb{D}_{\Bbbk}(P)$ et les racines son simples. La réciproque est évidente.

Proposition 54 *Soit $\Bbbk$ un corps de caractéristique 0 ou bien un corps infini de caractéristique $p \neq 0$. Soit $\mathbb{K} = \Bbbk(\alpha_1, \cdots, \alpha_n)$ une extension engendré par des éléments séparables. Alors $\mathbb{K}$ est une extension monogène algébrique de $\Bbbk$.*

Démonstration. Par hypothèse, le corps $\Bbbk$ est infini. Montrons le résultat pour $n = 2$. Un raisonnement par récurrence permettra alors de conclure. Soit $\mathbb{K} = \Bbbk(\alpha, \beta)$ une extension engendrée par deux éléments algébriques supposés séparables. Soient P_α et P_β les polynômes irréductibles de ces éléments. Par hypothèse, ces polynômes sont séparables. Ils ont donc des racines distinctes dans leur corps de décomposition. Soient $(\alpha = \alpha_1, \cdots, \alpha_l)$ les racines de P_α et $(\beta = \beta_1, \cdots, \beta_m)$ celles de P_β. Pour les considérer comme éléments d'un même corps, on considère le polynôme $P = P_\alpha P_\beta$ et le
K_1 le corps de décomposition de P. Les racines de P_α et P_β dans $\mathbb{K}_1$ sont toujours respectivement $(\alpha = \alpha_1, \cdots, \alpha_l)$ et $(\beta = \beta_1, \cdots, \beta_m)$ et ces racines sont distinctes dans $\mathbb{K}_1$. Considérons les polynômes de $\mathbb{K}_1[X]$

$$(\alpha - \alpha_i) + (\beta - \beta_j)X$$

pour $i = 1, \cdots, l$ et $j = 2, \cdots, m$. Chacun de ces polynômes admet dans $\mathbb{K}_1$ une unique racine γ_{ij}. Ils admettent donc au plus une racine dans $\Bbbk$. Soit $a \in \Bbbk$ tel que

$$(\alpha - \alpha_i) + (\beta - \beta_j)a \neq 0$$

pour $i = 1, \cdots, l$ et $j = 2, \cdots, m$. Un tel élément existe toujours car $\Bbbk$ est supposé infini. Posons

$$\theta = \alpha + a\beta.$$

Alors $\theta \in \mathbb{K}$ car $\alpha, \beta \in \mathbb{K}$ et $a \in \Bbbk$. On en déduit que l'extension $\Bbbk(\theta)$ en un sous-corps de $\mathbb{K}$. Considérons le polynôme $Q \in \mathbb{K}[X]$ défini par

$$Q(X) = P_\alpha(\theta - aX).$$

Considérons Q comme un polynôme de $\mathbb{K}_1[X]$. On a

$$Q(\beta) = P_\alpha(\theta - a\beta) = P_\alpha(\alpha) = 0.$$

Ainsi β est aussi une racine de Q. De plus pour $j = 2, \cdots, m$, on a

$$Q(\beta_j) = P_\alpha(\theta - a\beta_j) = P_\alpha(\alpha + a(\beta - \beta_j).$$

Or $\alpha + a(\beta - \beta_j) \neq \alpha_i$ pour $i = 1, \cdots, l$. Donc $P_\alpha(\alpha + a(\beta - \beta_j) \neq 0$ et donc β_j n'est pas racine de Q pour $j = 2, \cdots, m$. Ainsi Q et P_β n'ont qu'une seule racine commune β. Considérons le PGCD R des polynômes P_β et Q dans $\mathbb{K}_1[X]$. Il admet une seule racine β dans $\mathbb{K}_1$. Or, comme P_α est séparable dans $\mathbb{K}_1[X]$, il en est de même de R et s'il n'est pas de degré un, admet une autre racine, qui sera aussi racine de P_α. Donc R est du premier degré et admet une seule racine β.

Considérons à présent l'extension monogène algébrique $\Bbbk[\theta]$ de $\Bbbk$. Comme $P_\alpha \in \Bbbk[X]$, alors $P_\alpha \in \Bbbk[\theta][X]$. De même $Q \in \Bbbk[\theta][X]$. On en déduit que $R \in \Bbbk[\theta][X]$. Ainsi

$$\beta \in \Bbbk[\theta].$$

De même comme $\alpha = \theta - a\beta$, on a

$$\alpha \in \Bbbk[\theta].$$

On en déduit

$$\mathbb{K} = \Bbbk(\alpha, \beta) \subset \Bbbk[\theta]$$

et donc

$$\mathbb{K} = \Bbbk(\alpha, \beta) = \Bbbk[\theta]$$

D'où la proposition.

Théorème 18 *Soit $\Bbbk$ un corps de caractéristique 0. Soit $\mathbb{K}$ une extension de $\Bbbk$ de degré fini. Il existe alors $\theta \in \mathbb{K}$ tel que*

$$\mathbb{K} = \Bbbk[\theta].$$

Un tel élément $\theta \in \mathbb{K}$ est appelé un élément primitif de $\mathbb{K}$.

Démonstration. Si $\mathbb{K}$ une extension de $\Bbbk$ de degré fini, elle est donc obtenu comme adjonction d'un nombre fini d'éléments algébriques sur $\Bbbk$. Les polynômes minimaux de chacun de ces éléments sont irréductibles sur $\Bbbk$. Comme ce corps est de caractéristique 0, il est parfait et donc les polynômes minimaux sont séparables. Ainsi les générateurs de $\mathbb{K}$ sont algébriques séparables. La proposition précédent permet de conclure.

Exemple. Soit le corps $\mathbb{Q}(\sqrt{2}, \sqrt{3})$. C'est une extension de degré fini de $\mathbb{Q}$. Alors $\theta = \sqrt{2} + \sqrt{3}$ est un élément primitif de $\mathbb{Q}(\sqrt{2}, \sqrt{3})$. On fera la démonstration à titre d'exercice.

5.4.2 Extensions séparables

Définition 40 *Soit $\Bbbk \subset \mathbb{K}$ une extension algébrique de corps. Elle est dite séparable si tout élément $\alpha \in \mathbb{K}$ est séparable sur $\Bbbk$.*

Nous pouvons résumer les résultats ci-dessus par

Théorème 19 *Soit $\Bbbk$ un corps de caractéristique 0 ou bien un corps de caractéristique $p \neq 0$ fini. Alors toute extension de degré fini de $\Bbbk$ est séparable sur $\Bbbk$.*

Démonstration. En effet dans ces cas, le corps est parfait.

Proposition 55 *Soit $\Bbbk \subset \mathbb{K} \subset \mathbb{K}_1$ une tour d'extension. Si $\mathbb{K}_1$ est séparable sur $\Bbbk$ alors $\mathbb{K}_1$ est séparable sur $\mathbb{K}$ et $\mathbb{K}$ est séparable sur $\Bbbk$.*

Démonstration. Soit α un élément de $\mathbb{K}_1$. Soit $P_\alpha \in \Bbbk[X]$ le polynôme minimal de α sur $\Bbbk$. Or α est aussi algébrique sur $\mathbb{K}$. Soit Q_α le polynôme minimal de α sur $\mathbb{K}$. Alors Q_α est un diviseur de P_α. Comme P_α est séparable, Q_α aussi et donc $\mathbb{K}_1$ est séparable sur $\mathbb{K}$.

Montrons maintenant que $\mathbb{K}$ est séparable sur $\Bbbk$. Dans le cas contraire, il existe $\beta \in \mathbb{K}$ qui n'est pas séparable sur $\Bbbk$. Donc le polynôme minimal $P_\beta \in \Bbbk[X]$ de β n'est pas séparable et admet au moins une racine multiple dans $\mathbb{D}_\beta(P)$. Or si $\beta \in \mathbb{K}$ il est aussi dans $\mathbb{K}_1$ qui est une extension séparable de $\Bbbk$ donc P_β est aussi le polynôme minimal de β considéré comme élément de $\mathbb{K}_1$. Ainsi β ne serait pas séparable dans $\mathbb{K}_1$ sur $\Bbbk$ ce qui est contraire à l'hypothèse.

5.5 EXERCICES

Exercice 1. Soit P un polynôme irréductible ou non de $\Bbbk[X]$. On appelle corps de rupture de P sur $\Bbbk$ toute extension $\mathbb{K}$ de $\Bbbk$ tel que $\mathbb{K}$ contienne une racine α de P et $\mathbb{K} = \Bbbk[\alpha]$.

1. Montrer que tout polynôme P non constant appartenant à $\Bbbk[X]$ admet un corps de rupture $\mathbb{K}$ tel que $[\mathbb{K}; \Bbbk] \leq d(P)$.
2. On suppose P irréductible de degré supérieur ou égal à 1. Montrer que pour toute extension $\mathbb{K}_1$ de $\Bbbk$ et toute racine β de P dans $\mathbb{K}_1$ il existe un unique $\Bbbk$-homomorphisme $\varphi : \mathbb{K}_P = \frac{\Bbbk[X]}{(P)} \to \mathbb{K}_1$ tel que $\varphi(\alpha) = \beta$ où α est la racine P définie par $\alpha = \pi(X)$ (voir cours).
3. Décrire cet homomorphisme de corps lorsque $P = X^2 - 2, \Bbbk = \mathbb{Q}$ et $\mathbb{K}_1 = \mathbb{R}$.

Exercice 2. On considère le polynôme $P = X^3 + 2X + 2 \in \mathbb{Q}[X$.

1. Montrer que P est irréductible.
2. Soit $\mathbb{K}_p$ le corps de rupture de P et α la racine de P associéé. Exprimer $\dfrac{1}{\alpha}, \dfrac{1}{\alpha^2 + \alpha + 1}$ et $\alpha^6 + 3\alpha^4 + 2\alpha^3 + 6\alpha$ en fonction de $1, \alpha$ et α^2.
3. Montrer que $a = \alpha^6 + 3\alpha^4 + 2\alpha^3 + 6\alpha$ est un élément algébrique sur $\mathbb{Q}$. Déterminer son polynôme minimal.

Exercice 3. Déterminer les corps de décomposition des polynômes suivants de $\mathbb{Q}[X]$:

1. $P_1 = X^3 - 1$
2. $P_2 = X^4 - 7$
3. $P_3 = X^5 + X^4 + X^3 + X^2 + X + 1$
4. $P_4 = X^4 + 1$

Exercice 4. On considère dans $\mathbb{Q}[X]$ le polynôme $X^3 - 2$.

1. Déterminer le corps de rupture de ce polynôme. Peut-on décomposer P en facteurs de degré 1 dans son corps de rupture ?
2. Déterminer $\mathbb{D}_{\mathbb{Q}}(P)$ le corps de décomposition de P et son degré.
3. Est-ce que ce corps de décomposition de P est une extension séparable ?
4. Déterminer le groupe de Galois $Gal(\mathbb{D}_{\mathbb{Q}}(P); \mathbb{Q})$. Montrer que ce groupe est isomorphe au groupe symétrique σ_3.

Exercice 5. Soient $\Bbbk$ un corps et P un polynôme de $\Bbbk[X]$. Montrer que P admet une racine multiple si et seulement si le degré du PGCD de P et de P', le polynôme dérivé de P, est de degré au moins égal à 1.

Exercice 6. Soit $\Bbbk$ un corps de caractéristique $p \neq 0$. Soit P un polynôme irréductible de $\Bbbk[X]$.

1. Supposons que P admette des racines multiples. Montrer qu'il existe un polynôme $Q \in \Bbbk[X]$ irréductible et sans racine multiple et un entier $r \geq 1$ tel que
$$P(X) = Q(X^{p^r}).$$
2. Soit $a \in \Bbbk$. Montrer que le polynôme $X^{p^r} - a$ possède une seule racine. Montrer que cette racine est multiple d'ordre p^r. A quelle condition ce polynôme est irréductible ?
3. On suppose de plus que $\mathcal{P}k$ est un corps fini. Montrer que si P admet une racine multiple, toutes ses racines sont multiples et de même ordre.

Exercice 7. On considère l'extension $\mathbb{Q}(\sqrt{2}, \sqrt{3})$ de $\mathbb{Q}$.

1. Déterminer le degré de cette extension.
2. Montrer que $\sqrt{2} + \sqrt{3}$ est un élément primitif de cette extension.

Chapitre 6

Extensions galoisiennes

Nous avons défini dans le chapitre précédent des extensions associées à un polynôme donné, à savoir son corps de décomposition, et ces extensions ont des propriétés remarquables. Pour compléter cette étude, il nous reste à savoir caractériser les extensions qui sont définies par des corps de décomposition.

6.1 Extensions normales

Définition 41 *Soit $\Bbbk \subset \mathbb{K}$ une extension finie de corps. Elle est dite normale si tout polynôme irréductible appartenant à $\Bbbk[X]$ admettant une racine dans $\mathbb{K}$ à toute ses racines dans $\mathbb{K}$.*

Le résultat fondamental suivant montre que l'on récupère ainsi les extensions espérées.

Théorème 20 *Soit $\Bbbk \subset \mathbb{K}$ une extension finie du corps $\Bbbk$. Alors $\mathbb{K}$ est une extension normale de $\Bbbk$ si et seulement si $\mathbb{K}$ est le corps de décomposaition d'un polynôme de $\Bbbk[X]$.*

Démonstration. Supposons que $\mathbb{K}$ soit une extension normale de $\Bbbk$. Soit $\alpha \in \mathbb{K}$, $\alpha \notin \Bbbk$. Comme $\mathbb{K}$ est une extension finie, cet élément est algébrique. Soit $P_\alpha \in \Bbbk[X]$ son polynôme minimal. Comme $\mathbb{K}$ est une extension normale, P_α qui a une racine, α, dans $\mathbb{K}$ a toutes ses racines dans $\mathbb{K}$. Ainsi $\mathbb{K}$ contient $\mathbb{D}_{\Bbbk} P_\alpha$, le corps de décomposition de P_α. Si $\mathbb{K} = \mathbb{D}_{\Bbbk} P_\alpha$, on a le résultat voulu. Sinon, $\mathbb{K}$ est une extension de $\mathbb{D}_{\Bbbk} P_\alpha$. Il existe $\beta \in \mathbb{K} - \mathbb{D}_{\Bbbk} P_\alpha$, et pour cet élément, on considère aussi son polynôme irréductible $P_\beta \in \mathbb{D}_{\Bbbk} P_\alpha[X]$. On considère à présent le polynôme $P_\alpha P_\beta$. Il a une racine dans $\mathbb{K}$ et donc il a toutes ses racines dans ce corps. On en déduit que $\mathbb{K}$ contient le corps de décomposition $\mathbb{D}_{\Bbbk}(P_\alpha P_\beta)$. Or ce corps contient $\mathbb{D}_{\Bbbk} P_\alpha$ et on la tour d'extension

$$\Bbbk \subset \mathbb{D}_{\Bbbk} P_\alpha \subset \mathbb{D}_{\Bbbk}(P_\alpha P_\beta) \subset \mathbb{K}.$$

On réitère cette construction, et comme $\mathbb{K}$ est de degré fini, cette suite stationne et $\mathbb{K}$ est un corps de décomposition.

Inversement, supposons qu'il existe $P \in \Bbbk[X]$ tel que $\mathbb{K} = \mathbb{D}_{\Bbbk} P$. Soit $Q \in \Bbbk[X]$ un polynôme irréductible ayant une racine dans $\mathbb{K}$. Soit α cette racine. Comme Q est irréductible, alors $Q = P_\alpha$. Soit $\mathbb{K}_1 = \mathbb{D}_{\Bbbk} P_\alpha$ le corps de décomposition de $Q = P_\alpha$. Si β est une autre racine de Q dans $\mathbb{K}_1$, alors α et β ont le même

polynôme minimal. Elle sont conjuguées. Soit φ un $\Bbbk$ isomorphisme de $\Bbbk[\alpha]$ sur $\Bbbk[\beta]$ tel que $\varphi(\alpha) = \beta$. On a

$$P(\beta) = P(\varphi(\alpha)) = \varphi(P(\alpha)) = 0.$$

Ainsi β est une racine de P et donc $\beta \in \mathbb{K}$. L'extension $\mathbb{K}$ est donc normale.

Théorème 21 *Soit $\Bbbk \subset \mathbb{K}$ une extension finie du corps $\Bbbk$. Alors $\mathbb{K}$ est une extension normale de $\Bbbk$ si et seulement si pour toute tour d'extension $\Bbbk \subset \mathbb{K} \subset \mathbb{K}_1$ et tout homomorphisme de corps $\varphi : \mathbb{K} \to \mathbb{K}_1$ égal à l'identité sur $\Bbbk$, alors $\varphi(\mathbb{K}) = \mathbb{K}$.*

Démonstration. Supposons que $\Bbbk \subset \mathbb{K}$ soit une extension finie normale du corps $\Bbbk$. Soit $\Bbbk \subset \mathbb{K} \subset \mathbb{K}_1$ et $\varphi : \mathbb{K} \to \mathbb{K}_1$ un homomorphisme de corps égal à l'identité sur $\Bbbk$. Il existe un polynôme unitaire P tel que $\mathbb{K}$ soit le corps de décomposition de P : $\mathbb{K} = \mathbb{D}_{\Bbbk}(P)$. Ainsi dans $\mathbb{K}$ on a

$$P = (X - \alpha_1)(X - \alpha_2) \cdots (X - \alpha_n)$$

les α_i appartenant à $\mathbb{K}$. Comme φ est l'identité sur $\mathbb{K}$, le polynôme $Q = \varphi(P) = P$. Rappelons que $\varphi(P)$ désigne le polynôme $\varphi(a_0) + \varphi(a_1)X + \cdots + \varphi(a_n)X^n$ si $P = a_0 + a_1X + \cdots + a_nX^n$. Mais

$$Q = (X - \varphi(\alpha_1))(X - \varphi(\alpha_2)) \cdots (X - \varphi(\alpha_n)).$$

C'est donc un polynôme de $\mathbb{K}_1[X]$. Ses racines sont $\varphi(\alpha_i)$ et pour chaque i il existe j tel que $\varphi(\alpha_i) = \alpha_j$. Ainsi pour tout i, $\varphi(\alpha_i) \in \mathbb{K}$. Comme les α_i sont les générateurs de $\mathbb{K}$, alors $\varphi(\mathbb{K}) \subset \mathbb{K}$. Mais comme φ est injectif et $\mathbb{K}$ un $\Bbbk$-espace vectoriel de dimension finie, alors $\varphi(\mathbb{K}) = \mathbb{K}$.

Réciproquement, soit $P \in \Bbbk[X]$ un polynôme irréductible ayant une racine $\alpha \in \mathbb{K}$. Comme $\mathbb{K}$ est une extension de degré fini, il existe $\alpha_1, \cdots \alpha_n$ dans $\mathbb{K}$ tels que $\mathbb{K} = \Bbbk[\alpha_1, \cdots, \alpha_n]$. Soient P_{α_i} le polynôme minimal de α_i dans $\Bbbk$ et soit Q le polynôme

$$Q = PP_{\alpha_1} \cdots P_{\alpha_n}.$$

C'est un polynôme de $\Bbbk[X]$. Considérons le comme un polynôme de $\mathbb{K}[X]$. Soit $\mathbb{K}_1 = \mathbb{D}_{\mathbb{K}}(Q)$ son corps de décomposition dans $\mathbb{K}$. On a donc une tours d'extension

$$\Bbbk \subset \mathbb{K} \subset \mathbb{K}_1.$$

Or $\mathbb{K}_1$ est aussi le corps de décomposition de Q dans $\Bbbk$. En effet, Q admet comme racines $\alpha_1, \cdots, \alpha_n$ et aussi d'autres racines $\beta_1, \cdots, \beta_l$ dans $\mathbb{K}_1$ et on a

$$\mathbb{K}_1 = \mathbb{K}[\alpha_1, \cdots, \alpha_n, \beta_1, \cdots, \beta_l].$$

Mais comme

$$\mathbb{K} = \Bbbk[\alpha_1, \cdots, \alpha_n],$$

alors

$$\mathbb{K}_1 = \Bbbk[\alpha_1, \cdots, \alpha_n, \beta_1, \cdots, \beta_l].$$

Ainsi $\mathbb{K}_1$ est le corps de décomposition dans $\Bbbk$ de Q. Soit α' une racine de P dans $\mathbb{K}_1$. Comme P est irréductible, c'est le polynôme minimal de α et α'. Il existe un isomorphisme

$$\varphi : \Bbbk[\alpha] \to \Bbbk[\alpha']$$

qui est égal à l'identité sur $\Bbbk$ et tel que $\varphi(\alpha) = \alpha'$. . Mais α et α' sont aussi des racines de Q. Ainsi φ se prolonge en un isomorphisme

$$\phi : \mathbb{K}_1 \to \mathbb{K}_1$$

sur le corps de décomposition, égal à φ sur $\Bbbk[\alpha]$. Par hypothèse, on a alors

$$\phi(\mathbb{K}) = \mathbb{K}.$$

Ainsi

$$\phi(\alpha) = \varphi(\alpha) = \alpha'$$

et

$$\alpha' \in \mathbb{K}.$$

Le corps $\mathbb{K}$ contient donc les racines de P et on a bien une extension normale.

Un cas particulier intéressant est celui où $\mathbb{K}_1$ est la clôture algébrique $\overline{\Bbbk}$ de $\Bbbk$ et donc $\mathbb{K}$ est une extension normale de $\Bbbk$ contenu dans $\overline{\Bbbk}$. Dans ce cas, tout $\Bbbk$-homomorphisme

$$\varphi : \mathbb{K} \to \overline{\Bbbk}$$

est un $\Bbbk$-automorphisme de $\mathbb{K}$ et donc appartient à $Gal(\mathbb{K}/\Bbbk)$.

6.2 Tours d'extensions normales

Nous allons voir que la normalité n'est pas une notion transitive. Nous avons néanmoins le résultat suivant :

Proposition 56 *Soit $\mathbb{K}$ une extension normale de $\Bbbk$. Alors $\mathbb{K}$ est une extension normale de tout corps $\Bbbk_1$ vérifiant*

$$\Bbbk \subset \Bbbk_1 \subset \mathbb{K}.$$

Démonstration. Considérons un homomorphisme

$$\varphi : \mathbb{K} \to \overline{\Bbbk}$$

prolongeant l'identité sur $\Bbbk_1$. On peut le considérer comme un homomorphisme prolongeant l'identité sur $\Bbbk$. C'est donc un $\Bbbk$-automorphisme. Donc, d'après le théorème précédent, $\mathbb{K}$ est une extension normale de $\Bbbk_1$.

Remarque. Considérons une tour d'extension

$$\Bbbk \subset \Bbbk_1 \subset /K.$$

Supposons que $\mathbb{K}$ soit une extension normale de $\Bbbk$ Alors c'est aussi une extension normale de $\Bbbk_1$, mais il n'y a aucune raison que $\Bbbk_1$ soit une extension normale de $\Bbbk$. Ceci est même faux en général. Prenons par exemple le polynôme $P = X^3 - 2 \in \mathbb{Q}[X]$. Soit $\mathbb{K}$ son corps des racines. Il est égal à $\mathbb{Q}[\sqrt[3]{2}, j\sqrt[3]{2}, j^2\sqrt[3]{2}]$. C'est une extension normale de $\mathbb{Q}$. Soit $\Bbbk_1 = \mathbb{Q}[\sqrt[3]{2}]$. Le polynôme P admet une racine dans $\Bbbk_1$ mais les autres racines n'appartiennent pas à ce corps. Ainsi $\Bbbk_1$ n'est pas une extension normale de $\mathbb{Q}$.

6.3 Extensions normales séparables

Rappelons qu'une extension algébrique $\Bbbk \subset \mathbb{K}$ de $\Bbbk$ est séparable si tout élément de $\mathbb{K}$ est séparable, c'est-à-dire s'il est racine d'un polynôme séparable, ou bien, ce qui est équivalent, si son polynôme minimal n'a que des racines simples dans son corps de décomposition. On en déduit

6.3.1 Définition et caractérisation

Théorème 22 *Soit $\Bbbk \subset \mathbb{K}$ une extension finie du corps $\Bbbk$. Alors $\mathbb{K}$ est une extension normale séparable de $\Bbbk$ si et seulement si $\mathbb{K}$ est le corps de décomposition d'un polynôme séparable. .*

De telles extensions se caractérisent de la manière suivante :

Théorème 23 *Soit $\Bbbk \subset \mathbb{K}$ une extension finie du corps $\Bbbk$. Alors $\mathbb{K}$ est une extension normale séparable de $\Bbbk$ si et seulement si $\Bbbk$ est le corps $Fix(Gal(\mathbb{K}/\Bbbk))$.*

Démonstration. Supposons que $\Bbbk \subset \mathbb{K}$ soit une extension normale séparable de $\Bbbk$. Pour tout $\alpha \in \mathbb{K}$, le polynôme minimal $P_\alpha \in \Bbbk[X]$ a toutes ses racines simples. Rappelons que le corps $Fix(Gal(\mathbb{K}/\Bbbk))$ est constitué des éléments de $\mathbb{K}$ laissés fixes par les $\Bbbk$-automorphismes du groupe de Galois. Soit $\alpha \in Fix(Gal(\mathbb{K}/\Bbbk))$. Comme il appartient à $\mathbb{K}$, il est algébrique sur $\Bbbk$. Comme $\mathbb{K}$ est une extension normale, P_α est séparable dans $\mathbb{K}$. Ainsi

$$P_\alpha = (X-\alpha)(X-\alpha_2)\cdots(X-\alpha_n)$$

avec $\alpha, \alpha_2, \cdots, \alpha_n \in \mathbb{K}$ et ces racines sont deux à deux distinctes. Mais ces racines α_i ont toutes pour polynôme minimal P_α. Elles sont donc conjuguées. sur $\Bbbk$. Considérons la clôture algébrique $\overline{\Bbbk}$ de $\Bbbk$. Les racines de P_α sont aussi dans $\overline{\Bbbk}$. En tant qu'éléments de $\overline{\Bbbk}$, ces racines sont conjuguées dans $\Bbbk$. Il existe pour $i = 2, \cdots, n$, donc un élément $\varphi_i \in Gal(\overline{\Bbbk}/\Bbbk)$ tel que $\varphi_i(\alpha) = \alpha_i$. Comme $\mathbb{K}$ est une extension normale, pour chaque $\varphi_i : \overline{\Bbbk} \to \mathbb{K}$, il existe un unique $\Bbbk$-automorphisme ϕ_i de $\mathbb{K}$ tel que $\phi_i(\alpha) = \alpha_i$. Mais par hypothèse, $\alpha \in Fix(Gal(\mathbb{K}/\Bbbk))$. Ainsi

$$\alpha_i = \phi_i(\alpha) = \alpha.$$

Comme par hypothèse toutes les racines sont distinctes, on en déduit que $P\alpha$ n'admet que α comme racine et donc $P_\alpha = X - \alpha$. Ainsi $\alpha \in \Bbbk$ et $\Bbbk = Fix(Gal(\mathbb{K}/\Bbbk))$.

Réciproquement, montrons que tout polynôme unitaire irréductible $P \in \Bbbk[X]$ ayant une racine dans $\mathbb{K}$ possède toutes ses racines dans $\mathbb{K}$ et que ces racines sont simples. Soit donc $P \in \Bbbk[X]$ et soit $\alpha \in \mathbb{K}$ une racine de P. Soit A l'ensemble des racines de P dans $\mathbb{K}$. Soit $\varphi \in Gal(\mathbb{K}/\Bbbk)$. Alors, comme φ laisse les éléments de $\Bbbk$ invariants, on a $\varphi(P) = P$. On en déduit que pour tout $\beta \in A$, on a $\varphi(\beta) \in A$. En effet

$$0 = P(\beta) = \varphi(P)(\beta) = P(\varphi(\beta)).$$

On en déduit que $\varphi(A) = A$ et donc φ peut être considéré comme une permutation de A. Considérons le polynôme

$$Q = \prod_{\beta \in A} (X - \beta).$$

Ce polynôme appartient à $\mathbb{K}[X]$ et pour tout $\varphi \in Gal(\mathbb{K}/\Bbbk)$ on a

$$\varphi(Q) = \prod_{\beta \in A} (X - \varphi(\beta)) = Q.$$

Ainsi tous les coefficients de Q sont invariants par les éléments du groupe de Galois. Par hypothèse $Fix(Gal(\mathbb{K}/\Bbbk)) = \Bbbk$ et donc $Q \in \Bbbk[X]$. Mais les racines de Q qui sont des racines de P sont simples et Q divise P. Or P est irréductible, donc $Q = P$ et A est l'ensemble des racines de P. Ainsi P a toutes ses racines dans $\mathbb{K}$.

6.3.2 Un exemple d'extension normale séparable

Théorème 24 *Soient $\mathbb{K}$ un corps et G un sous-groupe fini de $Aut(\mathbb{K})$ le groupe des automorphismes de $\mathbb{K}$. Soit*

$$\Bbbk = Fix(G) = \{x \in \mathbb{K},\ \varphi(x) = x\ \forall \varphi \in G\}$$

le corps fixe de G. Alors $\mathbb{K}$ est une extension normale séparable finie de $\Bbbk$ et

$$[\mathbb{K}; \Bbbk] = |G|.$$

Démonstration. La démonstration est un peu semblable à la précédente. Notons $n = |G|$. Soit $\alpha \in \mathbb{K}$. Soit $A = \{\varphi_1, \cdots, \varphi_r\}$ le sous ensemble maximal de G tel que $\varphi_i(\alpha) \neq \varphi_j(\alpha)$ pour tout $i, j = 1, \cdots, r$ et $i \neq j$. Comme A est maximal, il contient l'identité. Considérons le polynôme

$$P = (X - \varphi_1(\alpha)) \cdots (X - \varphi_r(\alpha)).$$

Ce polynôme admet α comme racine. Par définition de A one en déduit que $P \in \Bbbk[X]$ où $\Bbbk = \mathbb{K}^G$. Donc α est un élément algébrique sur $\Bbbk$. Ainsi l'extension $\Bbbk \subset \mathbb{K}$ est algébrique. Soit P_α son polynôme minimal. Comme α est racine de P, P_α divise P et donc toutes ses racines sont simples, ce qui était le cas pour P. On en déduit que l'extension $\Bbbk \subset \mathbb{K}$ est normale et séparable. Montrons qu'elle est de degré fini. Comme P_α divise P son degré est inférieur ou égal à $r = d(P)$. Choisissons $\alpha \in \mathbb{K}$ tel que $s = [\Bbbk[\alpha]; \Bbbk]$ soit maximal. On a $s \leq n$. Supposons que $\Bbbk[\alpha] \neq \mathbb{K}$. Il existe $\beta \in \mathbb{K}$, $\beta \notin \Bbbk[\alpha]$. Considérons l'extension finie $\Bbbk[\alpha, \beta]$. Elle vérifie

$$[\Bbbk[\alpha, \beta], \Bbbk] > [\Bbbk[\alpha]; \Bbbk] = s.$$

Mais il existe un élément primitif $\gamma \in \mathbb{K}$, c'est-à-dire

$$\Bbbk[\alpha, \beta] = \Bbbk[\gamma].$$

On en déduit

$$[\Bbbk[\gamma]; \Bbbk] > s$$

ce qui contredit la maximalisé de s. Ainsi

$$\Bbbk[\alpha] = \mathbb{K}$$

et donc $\mathbb{K}; \Bbbk] \leq n$. Ainsi $\mathbb{K}$ est une extension finie normale séparable. C'est le corps de décomposition d'un polynôme séparable Q et $Gal(\mathbb{K}/\Bbbk)$ est le groupe de Galois de Q. On en déduit

$$[\mathbb{K}; \Bbbk] = |Gal(\mathbb{K}/\Bbbk)|.$$

Mais G est un sous-groupe de ce groupe de Galois, donc $n \leq [\mathbb{K}; \Bbbk]$. On en déduit

$$n = |G| = [\mathbb{K}; \Bbbk].$$

6.4 Extensions galoisiennes

6.4.1 Définition

Dans le chapitre 4, nous avons défini la notion d'extension galoisienne finie comme une extension de degré fini dont le groupe de Galois est d'ordre égal à ce degré. Soit $\mathbb{k} \subset \mathbb{K}$ une telle extension. Considérons $\mathbb{K}_1$ le corps fixe du groupe de Galois $Gal(\mathbb{K}/\mathbb{k})$. On a $\mathbb{k} \subset \mathbb{K}_1$ et $|Gal(\mathbb{K}/\mathbb{k})| = [\mathbb{K}; \mathbb{K}_1]$ (voir le paragraphe 4.4). Or, par hypothèse, $|Gal(\mathbb{K}/\mathbb{k})| = [\mathbb{K}; \mathbb{k}]$. Ainsi

$$[\mathbb{K}; \mathbb{K}_1] = [\mathbb{K}; \mathbb{k}]$$

et donc

$$\mathbb{k} = \mathbb{K}_1 = Fix(Gal(\mathbb{K}/\mathbb{k}).$$

On en déduit que cette extension est normale séparable.

Inversement, soit G le groupe de Galois d'un polynôme $P \in \mathbb{k}[X]$, c'est-à-dire correspondant à l'extension de $\mathbb{k}$ par le corps de décomposition de P. Tout élément $\varphi \in G$ envoie les racines distinctes de P sur les racines distinctes de P. Ainsi φ peut être assimilé à une permutation de l'ensemble des racines distinctes de P. Si P admet r racines distinctes, G s'identifie à un sous-groupe du groupe symétrique $\sum_r$ et donc $|G|$ divise $r!$. Si P est séparable sur $\mathbb{k}$, il existe donc $[\mathbb{K}; \mathbb{k}]$ $\mathbb{k}$-automorphismes et donc dans ce cas

$$|G| = [\mathbb{K}; \mathbb{k}].$$

On a donc une extension finie galoisienne. Nous pouvons donc redéfinir cette notion ainsi :

Définition 42 *On appelle extension galoisienne toute extension finie normale et séparable.*

Nous pourrions remplacer dans cette définition extension finie par algébrique. Mais nous ne ferons pas usage d'une telle généralisation.

6.4.2 Les sous-groupes du groupe de Galois

Considérons une extension galoisienne $\mathbb{k} \subset \mathbb{K}$ de $\mathbb{k}$. Alors $\mathbb{k}$ coïncide avec le corps fixe $Fix(Gal(\mathbb{K}/\mathbb{k})$ du groupe de Galois, c'est-à-dire

$$\mathbb{k} = \{x \in \mathbb{K},\ \varphi(x) = x\ \forall \varphi \in Gal(\mathbb{K}/\mathbb{k})\}.$$

Nous avons vu aussi que si $\mathbb{K}_1$ est un corps intermédiaire, c'est-à-dire si on a la tour d'extension

$$\mathbb{k} \subset \mathbb{K}_1 \subset \mathbb{K}$$

alors $\mathbb{K}$ est une extension galoisienne de $\mathbb{K}_1$. Par contre $\mathbb{K}_1$ n'est pas nécessairement une extension galoisienne de $\mathbb{k}$. Nous verrons en exercice, que $\mathbb{k} \subset \mathbb{K}_1$ est galoisienne si et seulement si $\mathbb{K}_1$ est invariant globalement par tout les éléments de $Gal(\mathbb{K}/\mathbb{k})$. Nous allons voir le lien entre les sous-corps intermédiaire d'une extension galoisienne et les sous-groupes du groupe de Galois de cette extension.

Proposition 57 *Soit $\mathbb{k} \subset \mathbb{K}$ une extension galoisienne de $\mathbb{k}$ et soit $\mathbb{K}_1$ un corps intermédiaire $\mathbb{k} \subset \mathbb{K}_1 \subset \mathbb{K}$. Alors le groupe de Galois $Gal(\mathbb{K}/\mathbb{K}_1)$ de l'extension galoisienne de $\mathbb{K}_1$ est un sous-groupe de $Gal(\mathbb{K}/\mathbb{k})$. De plus si l'extension $\mathbb{k} \subset \mathbb{K}_1$ est une extension galoisienne, alors le groupe de Galois $Gal(\mathbb{K}_2/\mathbb{k})$ est un sous-groupe distingué de $Gal(\mathbb{K}/\mathbb{k})$.*

Démonstration. En effet, si $\phi \in Gal(\mathbb{K}/\mathbb{K}_1)$, alors ϕ est un automorphisme de $\mathbb{K}$ tel que $\phi(x) = x$ pour tout $x \in \mathbb{K}_1$. En particulier $\phi(x) = x$ pour tout $x \in \mathbb{k}$ et donc $\phi \in Gal(\mathbb{K}/\mathbb{k})$. Supposons maintenant que l'extension $\mathbb{k} \subset \mathbb{K}_1$ soit galoisienne. Alors pour tout $\phi_1 \in Gal(\mathbb{K}/\mathbb{k})$ sa restriction ϕ_1 à $\mathbb{K}_1$ vérifie $\phi(\mathbb{K}_1) = \mathbb{K}_1$ et défini un élément de $Gal(\mathbb{K}_1/\mathbb{k})$. L'application

$$\Psi : Gal(\mathbb{K}/\mathbb{k}) \to Gal(\mathbb{K}_1/\mathbb{k})$$

qui a ϕ fait correspondre ϕ_1 est un homomorphisme surjectif de groupes. Son noyau correspond aux $\mathbb{k}$-homomorphismes de $\mathbb{K}$ vérifiant $\phi_1 = Id$. C'est donc un $\mathbb{K}_1$-automorphisme de $\mathbb{K}$ et donc le noyau de Ψ est $Gal(\mathbb{K}/\mathbb{K}_1)$. C'est donc un sous-groupe distingué de $Gal(\mathbb{K}/\mathbb{k})$. Notons que sous ces hypothèses $Gal(\mathbb{K}_1/\mathbb{k})$ est isomorphe au groupe quotient

$$\frac{Gal(\mathbb{K}/\mathbb{k})}{Gal(\mathbb{K}/\mathbb{K}_1)}$$

Théorème 25 *Soit $\mathbb{k} \subset \mathbb{K}$ une extension galoisienne de $\mathbb{k}$. L'application*

$$\Delta : \mathbb{K}_1 \to Gal(\mathbb{K}/\mathbb{K}_1)$$

de l'ensemble des corps intermédiaires de l'extension $\mathbb{k} \subset \mathbb{K}$ dans l'ensemble des sous-groupes du groupe de Galois $Gal(\mathbb{K}/\mathbb{k})$ est bijective et décroissante relativement à la relation d'ordre donnée par l'inclusion.

Démonstration. Soit $\mathbb{K}_1$ un corps intermédiaire de l'extension galoisienne $\mathbb{k} \subset \mathbb{K}$. On a la tour

$$\mathbb{k} \subset \mathbb{K}_1 \subset \mathbb{K}$$

et l'extension $\mathbb{K}_1 \subset \mathbb{K}$ est galoisienne. D'après la proposition précédente, l'application Δ est bien définie. Montrons qu'elle est bijective. Comme $\mathbb{K}_1 \subset \mathbb{K}$ est galoisienne, ceci implique en particulier que $\mathbb{K}_1 = Fix(Gal(\mathbb{K}/\mathbb{K}_1))$. Soient $\mathbb{K}_1$ et $\mathbb{K}_2$ deux corps intermédiaires de l'extension $\mathbb{k} \subset \mathbb{K}$. Alors

$$\mathbb{K}_1 = Fix(Gal(\mathbb{K}/\mathbb{K}_1)), \quad \mathbb{K}_2 = Fix(Gal(\mathbb{K}/\mathbb{K}_2)).$$

Si $\mathbb{K}_1$ et $\mathbb{K}_2$ sont des sous-corps de $\mathbb{K}$ distincts, alors les corps fixes $Fix(Gal(\mathbb{K}/\mathbb{K}_1))$ et $\mathbb{K}_2 = Fix(Gal(\mathbb{K}/\mathbb{K}_2))$ sont distincts ce qui impliquent que les groupes de Galois $Gal(\mathbb{K}/\mathbb{K}_1)$ et $Gal(\mathbb{K}/\mathbb{K}_2)$ soient distincts. Ainsi l'application Δ est injective. Montrons qu'elle est surjective. Soit H un sous-groupe de $Gal(\mathbb{K}/\mathbb{k})$. Alors H est un sous-groupe fini de $Aut(\mathbb{K})$ et donc $\mathbb{K}$ est une extension galoisienne de $Fix(H) = \{x \in \mathbb{K},\ \phi(x) = x \forall \phi \in H\}$. Ainsi $\mathbb{K}_1 = Fix(H)$ est une extension intermédiaire et $\Delta(\mathbb{K}_1) = H$. L'application Δ est donc surjective et donc bijective.

Montrons qu'elle est croissante pour l'inclusion. Soient $\mathbb{K}_1$ et $\mathbb{K}_2$ deux corps intermédiaires tels que $\mathbb{K}_1 \subset \mathbb{K}_2$. Soil $\phi \in Gal(\mathbb{K}/\mathbb{K}_2) = \Delta(\mathbb{K}_2)$. Alors $\phi(x) = x$ pour tout $x \in \mathbb{K}_2$ et donc $\phi(x) = x$ pour tout $x \in \mathbb{K}_1$. Ainsi $\phi \in Gal(\mathbb{K}/\mathbb{K}_1)$ et donc $\Delta(K_2) \subset \Delta(\mathbb{K}_1)$. Inversement, si $\mathbb{K}_1$ et $/K_2$ sont des corps intermédiaires tels que $Gal(\mathbb{K}/\mathbb{K}_2) \subset Gal(\mathbb{K}/\mathbb{K}_1)$. Comme $\mathbb{K}_1 = Fix(Gal(\mathbb{K}/\mathbb{K}_1)$, pour tout $x \in \mathbb{K}_1$ on a $\phi(x) = x$ pour tout $\phi \in Gal(\mathbb{K}/\mathbb{K}_1)$ et donc $\phi(x) = x$ pour tout $\phi \in Gal(\mathbb{K}/\mathbb{K}_2)$. Ainsi $\mathbb{K}_1 \subset Fix(Gal(\mathbb{K}/\mathbb{K}_2) = \mathbb{K}_2$.

Exemple. Considérons le polynôme irréductible $P = X^3 - 2$ de $\mathbb{Q}[X]$. Soit $\mathbb{K} = \mathbb{D}_{\mathbb{Q}}(P)$ son corps de décomposition. Comme P est séparable sur $\mathbb{Q}$ l'extension $\mathbb{Q} \subset \mathbb{K}$ est galoisienne. Les racines de P sont $\sqrt[3]{2}, j\sqrt[3]{2}, j^2\sqrt[3]{2}$ et donc $\mathbb{K} = \mathbb{Q}(\sqrt[3]{2}, j)$. On en déduit

$$|Gal(\mathbb{K}/\mathbb{Q})| = [\mathbb{Q}[j]; \mathbb{Q}].[\mathbb{K}, \mathbb{Q}[j]] = 2 \times 3 = 6.$$

Tout élément de $\mathbb{K}$ s'écrit

$$\alpha = a_0 + a_1\sqrt[3]{2} + a_2(\sqrt[3]{2})^2$$

avec $a_0, a_1, a_2 \in \mathbb{Q}[j]$. Il existe deux $\mathbb{Q}$-automorphismes de $\mathbb{Q}[j]$:

$$\phi_1 = Id, \quad \phi_2(x+jy) = x + j^2 y \quad x, y \in \mathbb{Q}.$$

Les automorphismes de $\mathbb{K}$ qui prolongent ϕ_1 sont

$$\begin{cases} \varphi_1(a_0 + a_1\sqrt[3]{2} + a_2\sqrt[3]{4}) = a_0 + a_1\sqrt[3]{2} + a_2\sqrt[3]{4} \\ \varphi_2(a_0 + a_1\sqrt[3]{2} + a_2\sqrt[3]{4}) = a_0 + ja_1\sqrt[3]{2} + j^2a_2\sqrt[3]{4}, \\ \varphi_3(a_0 + a_1\sqrt[3]{2} + a_2\sqrt[3]{4}) = a_0 + j^2a_1\sqrt[3]{2} + ja_2\sqrt[3]{4}. \end{cases}$$

On en déduit que $Gal(\mathbb{K}/\mathbb{Q}[j]) = \{Id, \varphi_1, \varphi_2, , \varphi_3\}$ et $\mathbb{Q}[j]$ et le sous-corps fixe de ce groupe. Notons les relations dans $Gal(\mathbb{K}/\mathbb{Q}[j])$:

$$\begin{cases} \varphi_2 \circ \varphi_2 = \varphi_3, \\ \varphi_2 \circ \varphi_3 = \varphi_3 \circ \varphi_2 = \varphi_1, \\ \varphi_3 \circ \varphi_3 = \varphi_2. \end{cases}$$

Les automorphismes de $\mathbb{K}$ qui prolongent ϕ_2 sont, en écrivant $\overline{a} = \phi_2(a), a \in \mathbb{Q}[j]$:

$$\begin{cases} \varphi_4(a_0 + a_1\sqrt[3]{2} + a_2\sqrt[3]{4}) = \overline{a_0} + \overline{a_1}\sqrt[3]{2} + \overline{a_2}\sqrt[3]{4}, \\ \varphi_5(a_0 + a_1\sqrt[3]{2} + a_2\sqrt[3]{4}) = \overline{a_0} + j\overline{a_1}\sqrt[3]{2} + j^2\overline{a_2}\sqrt[3]{4}, \\ \varphi_6(a_0 + a_1\sqrt[3]{2} + a_2\sqrt[3]{4}) = \overline{a_0} + j^2\overline{a_1}\sqrt[3]{2} + j\overline{a_2}\sqrt[3]{4}. \end{cases}$$

On a donc les relations

$$\begin{cases} \varphi_4 \circ \varphi_4 = \varphi_5 \circ \varphi_5 = \varphi_6 \circ \varphi_6 = Id, \\ \varphi_4 \circ \varphi_5 = \varphi_5 \circ \varphi_6 = \varphi_3, \\ \varphi_5 \circ \varphi_4 = \varphi_4 \circ \varphi_6 = \varphi_2. \end{cases}$$

Ainsi le groupe de Galois de P est

$$Gal(\mathbb{K}/\mathbb{Q}) = \{Id, \varphi_2, \varphi_3, \varphi_4, \varphi_5, \varphi_6\}.$$

Il est isomorphe au groupe symétrique $\sum_3$ d'indice 3, un isomorphisme étant donné par

$$\begin{cases} \varphi_1 = Id \to Id, \\ \varphi_2 \to c, \\ \varphi_3 \to c^2, \\ \varphi_4 \to \tau_{13}, \\ \varphi_5 \to \tau_{23}, \\ \varphi_6 \to \tau_{12}. \end{cases}$$

Le groupe symétrique $\sum_3$ possède 5 sous-groupes propres :

$$\{Id\},\ \{Id, \tau_{12}\},\ \{Id, \tau_{13}\}, ,\ \{Id, \tau_{23}\},\ \{Id, c, c^2\},$$

ce qui montre que $Gal(\mathbb{K}/\mathbb{Q})$ contient 6 et seulement 6 sous-groupes :

$$G_1 = \{\varphi_1\},\ G_2 = \{\varphi_1, \varphi_6\},\ G_3 = \{\varphi_1, \varphi_4\}, ,\ G_4 = \{\varphi_1, \varphi_5\}, \quad G_5 = \{\varphi_1, \varphi_2, \varphi_3\},\ Gal(\mathbb{K}/\mathbb{Q}).$$

Pour chacun de ces sous-groupes G_i correspond un sous-corps de $\mathbb{K}$ défini comme le sous-corps fixe du sous-groupe de $Gal(\mathbb{K}/\mathbb{Q})$ isomorphe à G_i. Ainsi

1. A G_1 correspond $\mathbb{K}_1 = \mathbb{K}$,
2. A G_2 correspond $K_2 = Fix(\{Id, \varphi_6\} = \mathbb{Q}[j\sqrt[3]{2}]$
3. A G_3 correspond $K_3 = Fix(\{Id, \varphi_4\} = \mathbb{Q}[\sqrt[3]{2}]$
4. A G_4 correspond $K_4 = Fix(\{Id, \varphi_5\} = \mathbb{Q}[j^2\sqrt[3]{2}]$
5. A G_5 correspond $K_5 = Fix(\{Id, \varphi_2, \varphi_3\} = \mathbb{Q}[j]$.

En effet, calculons K_2. Soit $u \in \mathbb{K}$. Il s'écrit

$$u = x_0 + jy_0 + (x_1 + jy_1)\sqrt[3]{2} + (x_2 + jy_2)\sqrt[3]{4}$$

avec $x_i, y_i \in \mathbb{Q}$, $i = 0, 1, 2$. Alors

$$\varphi_6(u) = x_0 + j^2y_0 + (x_1 + j^2y_1)j^2\sqrt[3]{2} + (x_2 + j^2y_2)j\sqrt[3]{4}.$$

Ainsi $\varphi_6(u) = u$ si et seulement si

$$u = x_0 + jy_1\sqrt[3]{2} - x_2j^2\sqrt[3]{4} = x_0 + y_1(j\sqrt[3]{2}) - x_2(j\sqrt[3]{2})^2$$

avec $x_0, y_1, x_2 \in \mathbb{Q}$. On a donc $u \in \mathbb{Q}[j\sqrt[3]{2}]$ ce qui montre que $K_2 = \mathbb{Q}[j\sqrt[3]{2}]$. Le calcul est similaire pour les autres cas.

Théorème 26 *Soit $\Bbbk \in \mathbb{K}$ une extension galoisienne du corps $\Bbbk$. Soient $\mathbb{K}_1$ et $\mathbb{K}_2$ deux corps intermédiaires et$G_1 = Gal(\mathbb{K}/\mathbb{K}_1)$ et $G_2 = Gal(\mathbb{K}/\mathbb{K}_2)$ leurs groupes de Galois. Si les corps $\mathbb{K}_1$ et $\mathbb{K}_2$ sont isomorphes, G_1 et G_2 sont des sous-groupes isomorphes de $Gal(\mathbb{K}/\Bbbk)$*

Démonstration. Rappelons que deux sous-groupes G_1 et G_2 d'un groupe G sont conjugués, s'il existe $h \in G$ tel que $G_2 = h^{-1}G_1h$. Supposons les osu-corps K_1 et K_2 de $\mathbb{K}$ isomorphes. Soit

$$\rho : K_1 \to K_2$$

cet isomorphisme.

6.5 Des extensions galoisiennes de $\mathbb{Q}$: les corps cyclotomiques

6.5.1 Racines primitives de l'unité

Soit n un entier supérieur ou égal à 1. Le polynôme complexe $P = X^n - 1$ admet n racines distinctes complexes

$$\xi_0 = 1, \xi_1 = e^{\frac{2i\pi}{n}}, \cdots, \xi_k = e^{\frac{2ik\pi}{n}}, \cdots, \xi_{n-1} = e^{\frac{2i(n-1)\pi}{n}}.$$

Considérons l'application

$$\rho : \mathbb{Z} \to \mathbb{C}^*$$

donnée par

$$\rho(k) = e^{\frac{2ik\pi}{n}}.$$

C'est un homomorphisme de groupes. Son noyau est l'ensemble des entiers k tels que $e^{\frac{2ik\pi}{n}} = 1$ c'est-à-dire des entiers $k = np, p \in \mathbb{Z}$. Ainsi ker $\rho = n\mathbb{Z}$ et Im ρ est isomorphe à $\mathbb{Z}\mathfrak{n}\mathbb{Z}$. Or l'image de $/rho$ est l'ensemble des racines n-ièmes de 1. Notons par Δ_n l'ensemble de ces racines :

$$U_n = \{\xi_0 = 1, \xi_1 = e^{\frac{2i\pi}{n}}, \cdots, \xi_k = e^{\frac{2ik\pi}{n}}, \cdots, \xi_{n-1} = e^{\frac{2i(n-1)\pi}{n}}\}.$$

On a donc montré

Proposition 58 *L'ensemble des racines n-ièmes de* 1 *:*

$$U_n = \{\xi_0 = 1, \xi_1 = e^{\frac{2i\pi}{n}}, \cdots, \xi_k = e^{\frac{2ik\pi}{n}}, \cdots, \xi_{n-1} = e^{\frac{2i(n-1)\pi}{n}}\}$$

est un sous-groupe cyclique de $\mathbb{C}^*$ *isomorphe à* $\mathbb{Z}/\mathfrak{n}\mathbb{Z}$.

Comme les générateurs du groupe cyclique $\mathbb{Z}/n\mathbb{Z}$ sont les nombres p premiers avec n, on en déduit que les générateurs de U_n sont les racines $\xi_p = e^{\frac{2ip\pi}{n}}$ où p est premier avec n.

Définition 43 *On appelle racine primitive n-ième de l'unité les générateurs du groupe cyclique* U_n*, c'est-à-dire les racines* $\xi_p = e^{\frac{2ip\pi}{n}}$ *où* p *est premier avec* n.

Notons par $\varphi_E(n)$ la fonction d'Euler définie par $\varphi_E(n) =$ le nombre d'entier $p > 1$ premiers avec n. Alors le nombre de racines primitives n-ièmes de 1 est égal à $\varphi_E(n)$. On notera U_n^{Pr} l'ensemble de ces racines primitives n-ièmes de 1.

6.5.2 Polynômes cyclotomiques

Considérons le polynôme $P = X^n - 1$ considéré comme un polynôme de $\mathbb{Q}[X]$. Son corps de décomposition est $\mathbb{Q}[\xi_1, \cdots, \xi_{n-1}]$. Dans cette extension $\mathbb{Q}[\xi_1, \cdots, \xi_{n-1}]$, P s'écrit

$$P = (X-1)(X-\xi_1)\cdots(X-\xi_{n-1}).$$

Comme $\mathbb{Q}[\xi_1, \cdots, \xi_{n-1}]$ est un corps de décomposition d'un polynôme irréductible séparable de $\mathbb{Q}[X]$, c'est une extension galoisienne de $\mathbb{Q}$ et

$$|Gal(\mathbb{Q}[\xi_1, \cdots, \xi_{n-1}]/\mathbb{Q})| = n.$$

En effet, comme pour tout k, $2 \leq k \leq n-1$, on a $\xi_k = \xi_1^k$, alors

$$\mathbb{Q}[\xi_1, \cdots, \xi_{n-1}] = \mathbb{Q}[\xi_1]$$

et le polynôme minimal dans $\mathbb{Q}$ de ξ_1 est P.

Nous allons à présent nous intéresser à une autre extension associée aux racines primitives.

Définition 44 *On appelle polynôme cyclotomique d'indice* n *sur* $\mathbb{Q}$*, le polynôme de* $\mathbb{C}[X]$ *(ou de* $\mathbb{Q}[\xi_1, \cdots, \xi_{n-1}][X]$*)*

$$\Phi_n = \prod_{\xi \in U_n^{Pr}} (X - \xi).$$

Par exemple si n est premier, alors $U_n^{pr} = U_n - 1$ et donc

$$\Phi_n = (X-\xi_1)\cdots(X-\xi_{n-1}) = \frac{X^n - 1}{X - 1} = X^{n-1} + X^{n-2} + \cdots + X + 1.$$

Nous voyons sur cet exemple que, si n est premier, alors

$$X^n - 1 = (X-1)\Phi_n(X).$$

Cette identité admet une généralisation pour n quelconque.

Proposition 59 *Pour tout entier $n \geq 1$, on a*

$$X^n - 1 = \prod_{d|n} \Phi_d(X)$$

où $d \mid n$ veut dire que d est un diviseur de n.

Démonstration. En effet, on a

$$X^n - 1 = (X-1)(X-\xi_1)\cdots(X-\xi_{n-1}) = (X-\xi_1)\cdots(X-\xi_{n-1})(X-\xi_n)$$

avec $\xi_n = 1$. Soit ξ une racine primitive n-ième de 1. Alors les racines de l'unté sont $\xi, \xi^2, \cdots, \xi^n$ et on a

$$X^n - 1 = \prod_{k=1,\cdots,n} (X - \xi^k).$$

Pour tout entier $k = 1, \cdots, n$, il existe un diviseur d de n et un entier r premier avec d tels que

$$PPCM(k,n) = kd = nr.$$

Ainsi $X - \xi^k = X - \xi^{\frac{n}{d}r}$ où d est un diviseur de n.On peut donc écrire

$$X^n - 1 = \prod_{d|n} \prod_{r=1,\cdots n, PGCD(r,d)=1} (X - \xi^{\frac{n}{d}r}).$$

Mais si d divise n, on a $\xi^{\frac{n}{d}d} = 1$ et donc $\xi^{\frac{n}{d}}$ est une racine d-ième de l'unité. Comme ξ est une racine primitive n-ième, $\xi^{\frac{n}{d}}$ est une racine primitive d-ième et donc

$$\Phi_d(X) = (X - \xi^{\frac{n}{d}})(X - (\xi^{\frac{n}{d}})^2)\cdots(X - (\xi^{\frac{n}{d}})^d).$$

On en déduit

$$X^n - 1 = \prod_{d|n} \Phi_d(X).$$

Remarque. Nous avons défini Φ_n comme le polynôme dont les racines sont simples et données par les racines primitives n-ième de 1. Au cours de la démonstration ci-dessus nous avons vu que $\mathbb{Q}_n$ pouvait être défini à partir d'une racine primitive quelconque ξ par

$$\Phi_n = \prod_{r=1,\cdots,n, PGCD(r,n)=1} (X - \xi^k).$$

Proposition 60 *Tout polynôme cyclotomique sur $\mathbb{Q}$ est à coefficients dans $\mathbb{Z}$ et irréductible sur $\mathbb{Q}$.*

Démonstration. Montrons par récurrence sur n que $\Phi_n \in \mathbb{Z}[X]$. Si $n = 1$, alors

$$\Phi_1 = X - 1 \in \mathbb{Z}[X].$$

Supposons que pour tout entier k, $2 \leq k \leq n-1$, le polynôme Φ_k soit dans $\mathbb{Z}[X]$. Nous avons vu que

$$X^n - 1 = \prod_{d|n} \Phi_d(X).$$

Nous pouvons écrire cette identité sous la forme

$$X^n - 1 = (\prod_{d|n, d\neq n} \Phi_d(X))\Phi_n.$$

Ceci montre que Φ_n est obtenu par division euclidienne des polynômes $X^n - 1$ et $(\prod_{d|n,d\neq n} \Phi_d(X))$. Comme par hypothèse ces deux polynômes sont dans $\mathbb{Z}[X]$, le quotient Φ_n est un polynôme de $\mathbb{Q}[X]$. Mais ces deux polynômes sont aussi unitaires. Ainsi Φ_n, obtenu par division, est à coefficients entiers.

Montrons que Φ_n est irréductible sur $\mathbb{Q}$. Soit ξ une racine nième de l'unité et soit $P_\xi \in \mathbb{Q}[X]$ le polynôme minimal de ξ. Comme Φ_n admet ξ comme racine, P_ξ divise Φ_n. Il existe donc un ensemble I d'entiers plus petit ou égal à n tels que

$$P_\xi = \prod_{k\in I}(X - \xi^k).$$

En effet, nous avons vu que si ξ est une racine primitive n-ième de 1, alors toute racine primitive n-ième de 1 est une puissance ξ^k de cette racine avec k premier avec n et que

$$\Phi_n = \prod_{k \ premier \ avec \ n} (X - \xi^k).$$

Plus précisément, ces racines primitives peuvent être obtenues en considérant toutes les puissances ξ^k lorsque k est premier et ne divise pas n. Soit k un tel entier. Montrons que pour cet entier, $P_\xi(\xi^k) = 0$. On sait que P_ξ divise $X^n - 1$. Posons

$$X^n - 1 = P_\xi R$$

avec $R \in \mathbb{Q}[X]$. Comme les polynômes $X^n - 1$ et P_ξ appartiennent à $\mathbb{Z}[X]$ est sont unitaires, alors $R \in \mathbb{Z}[X]$. Il est clair que ξ^k est aussi racine de $X^n - 1$. Ainsi

$$(\xi^k)^n - 1 = 0 = P_\xi(\xi^k)R(\xi^k).$$

Supposons $P_\xi(\xi^k) \neq 0$. Alors $R(\xi^k) = 0$. Soit ρ_k le polynôme de $\mathbb{Q}[X]$ défini par

$$\rho_k = X^k.$$

Alors $R_1 = R(\rho)$ vérifie $R_1(\xi) = R(\xi^k) = 0$. Donc P_ξ divise R_1 dans $\mathbb{Q}[X]$. On a donc

$$R_1 = P_\xi R_2.$$

Mais P_ξ et R_1 sont dans $\mathbb{Z}[X]$ et unitaires. On en déduit que $R_2 \in \mathbb{Z}[X]$. Réduisons modulo k l'égalité précédente et notons, pour un polynôme $P \in \mathbb{Z}[X]$, par $\overline{P}$ le polynôme correspondant dans $\mathbb{Z}/k\mathbb{Z}[X]$. On obtient :

$$\overline{R_1} = \overline{P_\xi R_2}.$$

Mais $R_1 = R(\rho_k)$. On en déduit

$$\overline{R_1} = (\overline{R})^k.$$

On en déduit que tout facteur irréductible $\overline{P_1}$ de $\overline{P_\xi}$ divise $(\overline{R})^k$ et donc divise $\overline{R}$ dans $\mathbb{Z}/k\mathbb{Z}[X]$. Or

$$X^n - 1 = P_\xi R$$

dans $\mathbb{Q}[X]$. On en déduit

$$X^n - \bar{1} = \overline{P_\xi R}$$

dans $\mathbb{Z}/k\mathbb{Z}[X]$. Ainsi $(\overline{P_1})^2$ est un facteur de $X^n - 1$ dans $\mathbb{Z}/k\mathbb{Z}[X]$. Mais le théorème de Bezout montre que $X^n - 1$ et sa dérivée formelle $\overline{n}X^{n-1}$ sont premier entre eux. En effet on a

$$\overline{n}X^{n-1}(\overline{n}^{-1}X) - (X^n - \bar{1}) = \bar{1}.$$

Donc P_1 ne peut être facteur d'ordre 2 de $X^n - \bar{1}$ et donc l'hypothèse $P_\xi(\xi^k) \neq 0$ mène à une contradiction. Ainsi pour tout k premier ne divisant pas n,

$$P_\xi(\xi^k) = 0.$$

Ainsi toutes les racines primitives sont racines de P_ξ et donc P_ξ est de degré supérieur ou égal à $\varphi(n)$ le nombre de racines primitives. Or P_ξ divise Φ_n qui est de degré $\varphi(n)$. Donc

$$\Phi_n = P_\xi.$$

Comme P_ξ est irréductible sur $\mathbb{Q}$, il en est de même de Φ_n.

Définition 45 *Soit n un entier positif. On appelle corps cyclotomique C_n, le corps de décomposition du polynôme cyclotomique Φ_n.*

Si ξ est une racine primitive n-ième de l'unité, alors son polynôme minimal coïncide avec le polynôme cyclotomique Φ_n. Or toutes les racines de Phi_n sont des puissance de ξ. On en déduit que le corps de décomposition de $/Phi_n$ est égale à l'extension $\mathbb{Q}[\xi]$ de $\mathbb{Q}$. Ainsi

$$C_n = \mathbb{Q}[\xi].$$

Comme Φ_n est séparable et ses racines sont distinctes, alors l'extension

$$\mathbb{Q} \subset C_n$$

est galoisienne et on a

$$|Gal(C_n, /Q)| = \phi(n).$$

Proposition 61 *Soit n un entier positif. Alors l'extension de $\mathbb{Q}$*

$$\mathbb{Q} \subset C_n$$

par le corps cyclotomique d'indice n est galoisienne. De plus son groupe de Galois est abélien.

Démonstration. Il nous reste à prouver que le groupe de Galois de cette extension est abélien. Si $\lambda \in Gal(C_n/\mathbb{Q})$, alors comme $C_n = \mathbb{Q}[\xi]$, l'image de ξ par λ est une racine de Φ et il existe k tel que $\lambda(\xi)\xi^k$ avec k premier avec n. Notons cet élément du groupe de Galois par λ_k. On définit ainsi une application

$$\lambda_k \to k$$

du groupe de Galois dans l'ensemble des entiers inférieurs à n et premier avec n. Or cet ensemble correspond à l'ensemble des éléments inversibles de $\mathbb{Z}/n\mathbb{Z}$. On définit ainsi un isomorphisme du groupe de Galois sur le groupe des inversibles de $\mathbb{Z}/n\mathbb{Z}$. Il est abélien.

6.6 EXERCICES

Exercice 1. Montrer que toute extension de degré 2 d'un corps $\mathbb{k}$ est normale.

Exercice 2. Soit le polynôme $P = X^3 - 2$. Montrer que le corps de décomposition $\mathbb{D}_{\mathbb{Q}}(P)$ de P est une extension normale de $\mathbb{Q}$. Soit $\mathbb{K} = \mathbb{Q}(\sqrt[3]{2})$. Montrer que $\mathbb{D}_{\mathbb{Q}}(P)$ est une extension normale sur $\mathbb{K}$. Est-ce que $\mathbb{K}$ est une extension normale sur $\mathbb{Q}$?

Exercice 3. On considère sur $\mathbb{Q}$ le polynôme $P_1 = X^2 - 2$. Montrer que son corps de décomposition $\mathbb{K}_1$ est une extension normale de $\mathbb{Q}$. Soit $P_2 \in \mathbb{K}_1[X]$ le polynôme $X^2 - \sqrt{2}$. Montrer que son corps de décomposition $\mathbb{K}_2$ sur $\mathbb{K}_1$ est une extension normale sur $\mathbb{K}_1$. Est-ce que $\mathbb{K}_2$ est une extension normale de $\mathbb{Q}$.

Exercice 4. Soit $\mathbb{k} \subset \mathbb{k}_1 \subset \mathbb{K}$ une tour d'extension telle que $\mathbb{K}$ soit une extension normale de $\mathbb{k}$. Montrer que $\mathbb{k}_1$ est une extension normale de $\mathbb{k}$ si et seulement si tout élément $\varphi \in Gal(\mathbb{K}/\mathbb{k})$ vérifie $\varphi(\mathbb{k}_1) = \mathbb{k}_1$.

Exercice 5. Soit le polynôme $X^4 - 5$ de $\mathbb{Q}[X]$. Déterminer son groupe de Galois. Déterminer tous les sous-groupes de ce groupe.

Exercice 6. Soit Φ_n le polynôme cyclotomique d'indice n sur $\mathbb{Q}$. Déterminer son corps de décomposition et son groupe de Galois.

Chapitre 7

Le théorème de Galois

Ce chapitre est la partie fondamentale de ce cours. On y donne le célèbre théorème de Galois montrant qu'une équation polynômiale générale de degré 5 ou plus ne peut être résolue par la méthode classique des radicaux utilisées pour les degrés 2,3 ou 4.

Rappelons que tous les corps considérés sont commutatifs, et lorsque nous parlons de corps, celui-ci est commutatif. Nous supposerons de plus, dans tout ce chapitre, que les corps considérés sont de caractéristique 0.

7.1 Extension d'un corps par radicaux

7.1.1 Définition

Définition 46 *Soit $\Bbbk \subset \mathbb{K}$ une extension de $\Bbbk$. On dit que c'est une extension par radicaux s'il existe une tour d'extensions simples*

$$\Bbbk = \mathbb{K}_0 \subset \mathbb{K}_1 \subset \mathbb{K}_2 \subset \cdots \subset \mathbb{K}_l = \mathbb{K}$$

telle que pour $i = 1, \cdots, l$ on ait

$$\mathbb{K}_{i+1} = \mathbb{K}_i[\alpha_i]$$

avec $\alpha_i \in \mathbb{K}_{i+1}$ et il existe un entier n_i tel que $\alpha_i^{n_i} \in \mathbb{K}_i$.

On en déduit que $\mathbb{K}_i = \Bbbk[\alpha_1, \cdots, \alpha_i]$ et en particulier $\mathbb{K}$ est une extension de degré fini $\mathbb{K} = \Bbbk[\alpha_1, \cdots, \alpha_l]$. Considérons par exemple le polynôme $P = X^3 - 2 \in \mathbb{Q}[X]$. Nous avons vu au chapitre précédent que son corps de décomposition $\mathbb{K} = \mathbb{D}_{\mathbb{Q}}(P)$ était une extension galoisienne de $\mathbb{Q}$ pour laquelle nous avions déterminé tous les sous-corps intermédiaires. Nous avons en particulier la tour d'extension

$$\mathbb{Q} \subset \mathbb{Q}[j] \subset \mathbb{Q}[j, \sqrt[3]{2}] = \mathbb{K}.$$

Comme $j^3 = 1 \in \mathbb{Q}$ et $(\sqrt[3]{2})^3 = 2 \in \mathbb{Q}[j]$, on en déduit que cette extension est une extension de $\mathbb{Q}$ par radicaux. Nous avons vu dans cet exemple que le groupe de Galois était isomorphe au groupe symétrique

$\sum_3$. Ce groupe a une propriété particulière qui va jouer un rôle essentiel dans la suite, il est résoluble. Avant de poursuivre, faisons un bref rappel sur cette notion.

7.1.2 Groupes finis résolubles

Soit G un groupe fini, noté multiplicativement. On appelle commutateur de deux éléments $x, y \in G$, l'élément noté $[x, y]$ et défini par

$$[x, y] = xyx^{-1}y^{-1}.$$

En particulier, si x et y commutent, $[x, y] = 1$ l'élément neutre de G. On appelle premier groupe dérivé de G, noté $D^1(G)$ le sous-groupe de G engendré par les commutateurs. C'est un sous-groupe normal de G.

Par exemple, si $G = \sum_3 = \{Id, \tau_{12}, \tau_{13}, \tau_{23}, c, c^2\}$ alors

$$D^1(\sum_3) = \{Id, c, c^2\}.$$

Appelons deuxième groupe dérivé de G, le sous-groupe

$$D^2 = D^1(D^1(G))$$

et plus généralement, le sous-groupe dérivé d'ordre k de G est défini par

$$D^k(G) = D^1(D^{k-1}(G).$$

On construit ainsi une suite décroissante de sous-groupes normaux

$$G \supseteq D^1(G) \supseteq /D^2(G) \supseteq \cdots \supseteq D^k(G) \supseteq \cdots .$$

Cette suite est soit stationnaire et dans ce cas il existe k tel que $D^k(G) = D^{k+1}(G) = \cdots$ soit, comme G est d'ordre fini, il existe k tel que $D^k(G) = \{1\}$.

Définition 47 *On dit que le groupe fini G est résoluble, s'il existe un entier k tel que $D^k(G) = \{1\}$.*

Par exemple $D^1(\sum_3) = \{Id, c, c^2\}$, $D^2(\sum_3) = \{Id\}$. Le groupe $\sum_3$ est résoluble. On peut montrer également que $\sum_4$ est résoluble. Par contre les groupes $\sum_n$ pour $n \geq 5$ ne sont pas résolubles. Pour voir cela, on étudie le sous-groupe A_n de $\sum_n$ constitué de toutes les permutations de signature paires. Il est d'indice 2 et il est non commutatif et simple, c'est-à-dire ne contient aucun sous-groupes normaux autre que lui même et celui réduit à l'élément neutre. On en déduit que A_n n'est pas résoluble. La conclusion est une conséquence de

Proposition 62 *Tout sous-groupe d'un groupe résoluble est résoluble.*

Une caractérisation pratique des groupes résolubles est la suivantes :

Proposition 63 *Un groupe fini G est résoluble si et seulement si il existe une suite décroissante de sous-groupes*

$$G = G_0 \supset G_1 \supset \cdots \supset G_k = \{1\}$$

telle que

1. *G_i soit un sous-groupe normal de G_{i-1}, $i = 1, \cdots k$,*
2. *Les groupes quotient G_{i-1}/G_i sont commutatifs, $i = 1, \cdots, k$.*

7.1.3 Exemple. Le corps de décomposition de $X^n - a$

Considérons le polynôme $X^n - a \in \mathbb{k}[X]$ où $\mathbb{k}$ est un corps de caractéristique 0. On se propose, à titre d'exemple, de déterminer son groupe de Galois.

1. Le corps $\mathbb{k}$ contient une racine n-ième primitive de l'unité.

Nous avons étudié les racines n-ièmes de l'unité sur le corps $\mathbb{C}$. Cette notion s'étends aisément aux corps quelconques, mais nous nous limitons ici aux corps de caractéristique 0. Soit n un entier positif non nul. Une racine n-ième de l'unité sur $\mathbb{k}$ est une racine dans la clôture algébrique $\widetilde{\mathbb{k}}$ de $\mathbb{k}$ du polynôme $X^n - 1$. Tout comme pour $\mathbb{k} = \mathbb{Q}$, on montre que

L'ensemble des racines n-ièmes de l'unité sur $\mathbb{k}$ est un groupe cyclique d'ordre n.

Tour générateur de ce groupe est appelé une racine primitive. Soit ϵ une telle racine primitive. Alors

$$\epsilon^n = 1$$

et

$$\{1, \epsilon, \epsilon^2, \cdots, \epsilon^{n-1}\}$$

est l'ensemble des racines n-ièmes. En particulier, toute racine primitive s'écrit ϵ^r avec $1 \leq r \leq n-1$ et r premier avec n.

Par hypothèse, $\mathbb{k}$ contient une racine primitive n-ième de l'unité. Soit $\epsilon \in \mathbb{k}$ cette racine. Considérons une racine α du polynôme $P = X^n - a$. Nous pouvons supposer que cette arcine n'est pas dans $\mathbb{k}$, sinon $\mathbb{k}$ serait le corps de décomposition de ce polynôme et son groupe de Galois sur $\mathbb{k}$ serait trivial. Ainsi $\alpha \notin \mathbb{k}$ et

$$\alpha^n = a.$$

L'extension monogène $\mathbb{k}[\alpha]$ de $\mathbb{k}$ contient donc les éléments suivants :

$$\alpha, \epsilon, \epsilon\alpha, \epsilon^2\alpha, \cdots, \epsilon^{n-1}\alpha.$$

Or

$$P(\epsilon^i\alpha) = (\epsilon^i\alpha)^n - a = \alpha^n - a = 0.$$

Donc les n éléments $\alpha, \epsilon\alpha, \epsilon^2\alpha, \cdots, \epsilon^{n-1}\alpha$ sont tous des racines de P. Ce sont donc toutes les racines de P et donc $\mathbb{k}[\alpha]$ est le corps de décomposition de P. On en déduit que le groupe de Galois de P est

$$Gal(\mathbb{D}_{\mathbb{k}}(P)/\mathbb{k}) = Gal(\mathbb{k}[\alpha]/\mathbb{k}).$$

Ainsi tout élément $\varphi \in Gal(\mathbb{D}_{\mathbb{k}}(P)/\mathbb{k})$ est entièrement défini par l'image de la racine α, qui est aussi une racine de P. Posons

$$\varphi(\alpha) = \epsilon^k\alpha$$

avec $1 \leq k \leq n-1$. Soit φ_1 un autre élément de $Gal(\mathbb{D}_{\Bbbk}(P)/\Bbbk)$ distinct de φ. Il existe k_1 distinct de k avec $1 \leq k_1 \leq n-1$ et

$$\varphi(\alpha) = \epsilon^{k_1}\alpha.$$

Alors

$$\varphi_1(\varphi(\alpha)) = \varphi_1(\epsilon^k\alpha) = \epsilon^k\varphi(\alpha) = \epsilon^{k+k_1}\alpha = (\varphi_1(\alpha)).$$

Ainsi

$$\varphi\varphi_1 = \varphi_1\varphi$$

pour tout $\varphi, \varphi_1 \in Gal(\mathbb{D}_{\Bbbk}(P)/\Bbbk)$. Ce groupe est donc abélien.

Proposition 64 *Soit $\Bbbk$ un corps de caractéristique 0 contenant une racine primitive n-ième de l'unité. Soit $a \in \Bbbk$ un élément non nul. Alors le groupe de Galois du polynôme*

$$X^n - a$$

est un groupe abélien d'ordre n.

2. Le corps $\Bbbk$ ne contient aucune racine n-ième primitive de l'unité.

Soit α une racine de $P = X^n - a$ que l'on suppose ne pas appartenir à $\Bbbk$. Considérons ϵ une racine primitive n-ième de l'unité dans $\Bbbk$. Par hypothèse $\epsilon \notin \Bbbk$ et donc $\Bbbk[\epsilon]$ est une extension propre de $\Bbbk$. Considérons la tour d'extension

$$\Bbbk \subset \Bbbk[\epsilon], \subset \Bbbk[\epsilon, \alpha].$$

Alors

1. $\Bbbk[\epsilon]$ est une extension galoisienne de $\Bbbk$ et

   $$Gal(\Bbbk[\epsilon]/\Bbbk)$$

   est abélien. En effet $\Bbbk[\epsilon]$ est le corps de décomposition de $X^n - 1$ sur $\Bbbk$. C'est donc une extension normale et séparable de $\Bbbk$. Elle est donc galoisienne. Le groupe de Galois est abélien : soient $\varphi_1, \varsigma\varphi_2$ deux éléments de ce groupe. Ils sont caractérisés par

   $$\varphi_1(\epsilon) = \epsilon^{k_1}, \quad \varphi(\epsilon) = \epsilon^{k_2}$$

   et

   $$\varphi_1(\varphi_2(\epsilon)) = \varphi_1(\epsilon^{k_2}) = \epsilon^{k_1+k_2} = \varphi_2(\varphi_1(\epsilon)).$$

   Ainsi $\varphi_1\varphi_2$ et $\varphi_2\varphi_1$ coïncident sur le générateur. Ils sont égaux et $Gal(\Bbbk[\epsilon]/\Bbbk)$ est un groupe abélien.
2. $\Bbbk[\epsilon, \alpha]$ est une extension galoisienne de $\Bbbk[\epsilon]$. En effet, considérons le polynôme $P = X^n - a \in \Bbbk[\epsilon][X]$. On a $P(\alpha) = 0$ et

   $$P(\epsilon^k\alpha) = (\epsilon^k\alpha)^n - a = \alpha^n - a = 0$$

   et donc $\Bbbk[\epsilon, \alpha]$ est le corps de décomposition du polynôme $X^n - a \in \Bbbk[\epsilon][X]$. Comme précédemment, on montre que le groupe de Galois $Gal(\Bbbk[\epsilon, \alpha]/\Bbbk[\epsilon])$ est un groupe abélien. Mais

   $$\Bbbk[\epsilon, \alpha] = \Bbbk[\alpha, \epsilon\alpha, \cdots, \epsilon^{n-1}\alpha].$$

   On en déduit que l'extension

   $$\Bbbk \subset \Bbbk[\epsilon, \alpha]$$

est normale et séparable car $\Bbbk[\epsilon, \alpha]$ est le corps de décomposition de $P = X^n - a$ sur $\Bbbk$. C'est donc une extension galoisienne finie. On a ainsi une tour d'extension

$$\Bbbk \subset \Bbbk[\epsilon] \subset \Bbbk[\epsilon, \alpha]$$

où $\Bbbk[\epsilon, \alpha]$ est normale sur $\Bbbk$ donc sur $\Bbbk[\epsilon]$. Dans ce cas $Gal(\Bbbk[\epsilon, \alpha]/\Bbbk[\epsilon])$ est un sous-groupe normal de $Gal(\Bbbk[\epsilon, \alpha]/\Bbbk)$ et

$$Gal(\Bbbk[\epsilon]/\Bbbk) = \frac{Gal(\Bbbk[\epsilon, \alpha]/\Bbbk)}{Gal(\Bbbk[\epsilon, \alpha]/\Bbbk[\epsilon])}.$$

Nous sommes ainsi dans la situation suivante : si $G = Gal(\Bbbk[\epsilon, \alpha]/\Bbbk)$ et $H = Gal(\Bbbk[\epsilon, \alpha]/\Bbbk[\epsilon])$, alors $G/H = Gal(\Bbbk[\epsilon]/\Bbbk)$. Comme H est un sous-groupe normal résoluble (il est abélien) de G et le groupe quotient G/H est résoluble (il est aussi abélien), alors le groupe G est résoluble.

Proposition 65 *Soit $\Bbbk$ un corps de caractéristique 0 ne contenant pas de racine primitive n-ième de l'unité. Soit $a \in \Bbbk$ un élément non nul. Alors le groupe de Galois du polynôme*

$$X^n - a$$

est un groupe résoluble.

7.1.4 Le groupe de Galois d'une extension normale par radicaux

Commençons par généraliser quelques résultats mis en évidence dans l'exemple ci-dessus et qui se généralisent sans difficulté. Soit $\Bbbk$ un corps de caractéristique 0. Soit $\mathbb{K}$ une extension galoisienne finie. C'est en particulier le corps de décomposition d'un polynôme séparable de $\Bbbk[X]$. Soit ξ une racine primitive de l'unité (dans $\tilde{\mathbb{K}}$). Si $\xi \in \Bbbk$, alors $\Bbbk = \Bbbk[\xi]$. Sinon $\Bbbk[\xi]$ est une extension galoisienne de $\Bbbk$. Considérons $\mathbb{K}[\xi]$. Il est clair que $\mathbb{K}[\xi]$ est une extension galoisienne de $\mathbb{K}$ qui ont la même clôture algébrique $\tilde{\mathbb{K}}$. Montrons que dans l'extension

$$\Bbbk \subset \Bbbk[\xi] \subset \mathbb{K}[\xi]$$

les extensions $\Bbbk \subset \mathbb{K}[\xi]$ et $\Bbbk[\xi] \subset \mathbb{K}$ sont normales donc galoisiennes finies. Soit $\varphi : \mathbb{K}[\xi] \to \tilde{\mathbb{K}} = \widetilde{\mathbb{K}[\xi]}$ un $\Bbbk$-homomorphisme. Il est clair $\varphi(\xi) \in \Bbbk[\xi]$ car $(\varphi(\xi)^n = 1)$. De plus , par hypothèse, l'extension $\mathbb{K}$ de $\Bbbk$ est normale. Donc l'image par φ de $\mathbb{K}$ dans sa clôture algébrique est égale à $\mathbb{K}$. Donc $\varphi(\mathbb{K}[\xi]) \subset \mathbb{K}[\xi]$ ce qui montre que l'extension

$$\Bbbk \subset \mathbb{K}[\xi]$$

sest normale. On en déduit en particulier que l'extension

$$\Bbbk[\xi] \subset \mathbb{K}[\xi]$$

est aussi normale. Comme nous avons supposé que le corps $\Bbbk$ était de caractéristique 0, alors il est parfait et toute extension algébrique est séparable. Ainsi les extensions ci-dessus sont aussi séparables et donc galoisiennes finies. Comparons alors les groupes de Galois $Gal(\mathbb{K}[\xi]/\Bbbk)$, $Gal(\mathbb{K}[\xi]/\Bbbk[\xi])$ et $Gal(\Bbbk[\xi]/\Bbbk)$. Les propriétés de ces groupes sont liées à la tour d'extension

$$\Bbbk \subset \Bbbk[\xi] \subset \mathbb{K}[\xi].$$

Comme $\Bbbk[\xi]$ est une extension de $\Bbbk$ par une racine primitive de l'unité, chaque élément de $Gal(\Bbbk[\xi]/\Bbbk)$ est défini par l'image de ξ. Soit $\varphi \in Gal(\Bbbk[\xi]/\Bbbk)$. Alors $\varphi(\xi)^n = 1$ et donc il existe r tel que $\varphi(\xi) = \xi^r$.

C'est aussi une racine primitive et donc r est premier avec n. On en déduit que $Gal(\Bbbk[\xi]/\Bbbk)$ est abélien. Considérons maintenant $Gal(\mathbb{K}[\xi]/\Bbbk)$. Comme l'extension $\Bbbk \subset \mathbb{K}[\xi]$ est galoisienne et finie, le groupe de Galois $Gal(\mathbb{K}[\xi]/\Bbbk[\xi])$ est un sous groupe normal de $Gal(\mathbb{K}[\xi]/\Bbbk)$ et

$$Gal((\Bbbk[\xi]/\Bbbk) = Gal(\mathbb{K}[\xi]/\Bbbk)/Gal(\mathbb{K}[\xi]/\Bbbk[\xi]).$$

Pour les mêmes raisons, on aura

$$Gal((\mathbb{K}/\Bbbk) = Gal(\mathbb{K}[\xi]/\Bbbk)/Gal(\mathbb{K}[\xi]/\mathbb{K}).$$

Mais contrairement à l'exemple ci-dessus, nous ne pouvons, sans hypothèse supplémentaire, trouver d'autres propriétés de ces groupes.

Théorème 27 *Soit $\Bbbk \subset \mathbb{K}$ une extension galoisienne finie du corps $\Bbbk$ de caractéristique 0. Si cette extension est aussi une extension par radicaux, alors le groupe de Galois $Gal(\mathbb{K}/\Bbbk)$ est résoluble.*

Démonstration. Par hypothèse, il existe une tour d'extension

$$\Bbbk \subset \Bbbk[\alpha_1] \subset \cdots \subset \Bbbk[\alpha_1, \cdots, \alpha_l] = \mathbb{K}$$

telle que $\alpha_i^{n_i} = a_i \in \Bbbk[\alpha_1, \cdots, \alpha_{i-1}]$. Posons

$$n = n_1 \cdots n_l.$$

Soit ξ une racine primitive n-ième de l'unité et considérons, comme ci-dessus, l'extension $\Bbbk[\xi]$. Considérons la tour d'extensions

$$\Bbbk[\xi] \subset \Bbbk[\xi, \alpha_1] \subset \cdots \subset \Bbbk[\xi, \alpha_1, \cdots, \alpha_l] = \mathbb{K}[\xi].$$

Chacun des corps $\Bbbk[\xi, \alpha_1, \cdots, \alpha_i]$ contient une racine de l'unité et l'extension

$$\Bbbk[\xi, \alpha_1, \cdots, \alpha_{i-1}] \subset \Bbbk[\xi, \alpha_1, \cdots, \alpha_i]$$

correspond à l'extension par une racine du polynôme $X^{n_i} - a_i$ de $\Bbbk[\xi, \alpha_1, \cdots, \alpha_{i-1}][X]$. Nous avons vu que dans ce cas cette extension est galoisienne et finie et le groupe de Galois est abélien. Mais par hypothèse $\Bbbk \subset \mathbb{K}$ est une extension galoisienne finie. Il en est de même de $\Bbbk[\xi] \subset \mathbb{K}[\xi]$. Donc $\mathbb{K}[\xi]$ est une extension galoisienne finie sur chacun des corps intermédiaires $\Bbbk[\xi, \alpha_1, \cdots, \alpha_i]$. Considérons les groupes de Galois $Gal(\mathbb{K}[\xi]/\Bbbk[\xi, \alpha_1, \cdots, \alpha_i])$. On en déduit que $Gal(\mathbb{K}[\xi]/\Bbbk[\xi, \alpha_1, \cdots, \alpha_i])$ est un sous groupe normal de $Gal(\mathbb{K}[\xi]/\Bbbk[\xi]$. On a donc la suite décroissante de sous-groupes normaux

$$Gal(\mathbb{K}[\xi]/\Bbbk[\xi]) \supset Gal(\mathbb{K}[\xi]/\Bbbk[\xi, \alpha_1]) \supset \cdots \supset Gal(\mathbb{K}[\xi]/\Bbbk[\xi, \alpha_1, \cdots, \alpha_{l-1}]) \supset \{Id\}$$

et chaque quotient successif $Gal(\mathbb{K}[\xi]/\Bbbk[\xi, \alpha_1, \cdots, \alpha_i])/Gal(\mathbb{K}[\xi]/\Bbbk[\xi, \alpha_1, \cdots, \alpha_{i-1}])$ est isomorphe à $Gal(\Bbbk[\xi, \alpha_1,$ est abélien. On en déduit que $Gal(\mathbb{K}[\xi]/\Bbbk[\xi])$ est un groupe résoluble. Les considérations précédentes :

$$Gal((\Bbbk[\xi]/\Bbbk) = Gal(\mathbb{K}[\xi]/\Bbbk)/Gal(\mathbb{K}[\xi]/\Bbbk[\xi])$$

avec $Gal((\Bbbk[\xi]/\Bbbk)$ abélien et maintenant $Gal(\mathbb{K}[\xi]/\Bbbk[\xi])$ impliquent que

$$Gal(\mathbb{K}[\xi]/\Bbbk)$$

est résoluble. Mais

$$Gal((\mathbb{K}/\Bbbk) = Gal(\mathbb{K}[\xi]/\Bbbk)/Gal(\mathbb{K}[\xi]/\mathbb{K})$$

et donc $Gal((\mathbb{K}/\Bbbk)$ est résoluble.

7.2 Polynômes résolubles par radicaux

7.2.1 Polynômes résolubles par radicaux

Définition 48 *Soit $P \in \Bbbk[X]$ un polynôme à coefficients dans $\Bbbk$. Il est dit résoluble par radicaux sur $\Bbbk$ si toutes les racines de P appartiennent à une extension $\mathbb{K}$ par radicaux de $\Bbbk$.*

Ceci signifie qu'il existe une extension par radicaux de $\Bbbk$:

$$\Bbbk = \mathbb{K}_0 \subset \mathbb{K}_1 \subset \mathbb{K}_2 \subset \cdots \subset \mathbb{K}_l = \mathbb{K}$$

telle que le corps de décomposition $\mathbb{D}_{\Bbbk}(P)$ de P dans $\Bbbk$ soit contenu dans $\mathbb{K}$ (et pas nécessairement égal à $\mathbb{K}$). Notons également que cette définition n'implique pas que $\mathbb{K}$ soit une extension normale de $\Bbbk$.

Théorème 28 *Soit $P \in \Bbbk[X]$ un polynôme à coefficients dans $\Bbbk$ de caractéristique 0. Si P est résoluble par radicaux, alors le groupe de Galois de P :*

$$Gal(\mathbb{D}_{\Bbbk}(P)/\Bbbk)$$

est résoluble, où $(\mathbb{D}_{\Bbbk}(P)$ est un corps de décomposition de P.

Démonstration. Comme P est résoluble par radicaux, ses racines appartiennent à une extension $\mathbb{K}$ de $\Bbbk$ qui est une extension par radicaux. Pour pouvoir appliquer le théorème précédent, il faudrait que cette extension soit galoisienne finie, ce qui n'est pas en général le cas.

Lemme 6 *Soit $P \in \Bbbk[X]$ un polynôme à coefficients dans $\Bbbk$. Supposons qu'il existe une extension par radicaux $\mathbb{K}$ de $\Bbbk$ contenant le corps de décomposition $\mathbb{D}_{\Bbbk}(P)$ de P sur $\Bbbk$. Alors il existe une extension par radicaux contenant $\mathbb{D}_{\Bbbk}(P)$ telle que $\mathbb{K}$ soit une extension galoisienne finie de $\Bbbk$.*

Démonstration. Soit $\mathbb{K}$ une extension par radicaux de $\Bbbk$ contenant le corps des racines de P. Notons par $\widetilde{\mathbb{K}}$ la clôture algébrique de $\mathbb{K}$. Soit A l'ensemble des $\Bbbk$-homomorphismes

$$\varphi : \mathbb{K} \to \widetilde{\mathbb{K}}.$$

Soit $\mathbb{L}$ le sous-corps de $\widetilde{\mathbb{K}}$ engendré par $\{\varphi(\mathbb{K}),\ \varphi \in A\}$. Pour $\varphi \in A$ fixé, $\varphi(\mathbb{K})$ est un sous-corps de $\widetilde{\mathbb{K}}$ qui est $\Bbbk$-isomorphe à $\mathbb{K}$. Ceci implique immédiatement que c'est aussi une extension par radicaux de $\Bbbk$. Montrons que $\mathbb{L}$ qui est un sous-corps engendré par des sous-corps qui sont extensions par radicaux de $\Bbbk$ est aussi une extension par radicaux de $\Bbbk$. Soient φ_1 et $\varphi_2 \in A$. Alors $\varphi_1(\mathbb{K})$ et $\varphi_2(\mathbb{K})$ sont des extensions par radicaux, contenant les racines de P. Ceci signifie que l'on ait

$$\Bbbk \subset \Bbbk[\beta_1] \subset \cdots \subset \varphi_1(\mathbb{K}) = \Bbbk[\beta_1, \cdots, \beta_s]$$

avec $\beta_i^{m_i} \in \Bbbk[\beta_1, \cdots, \beta_{i-1}$ et

$$\Bbbk \subset \Bbbk[\gamma_1] \subset \cdots \subset \varphi_2(\mathbb{K}) = \Bbbk[\gamma_1, \cdots, \gamma_r]$$

avec $\beta_i^{r_i} \in \Bbbk[\gamma_1, \cdots, \gamma_{i-1}$. Dans ce cas l'extension finie $\Bbbk[[\beta_1, \cdots, \beta_s, \gamma_1, \cdots, \gamma_r]$ est une extension finie par radicaux de $\Bbbk$ engendrée par $\varphi_1(\mathbb{K})$ et $\varphi_2(\mathbb{K})$ et contient les racines de P. On en déduit que $\mathbb{L}$ est une extension finie par radicaux de $\mathcal{P}$. Montrons qu'elle est normale. Comme $\mathbb{L}$ est une extension finie de $\mathbb{K}$ qui est elle même une extension de degré fini : $\mathbb{K} = \Bbbk[\alpha_1, \cdots, \alpha_l]$. Soit P_{α_i} le polynôme minimal de α_i dans $\Bbbk[X]$. Alors, par construction, $\mathbb{L}$ est le corps des racines du polynôme $P_{\alpha_1} P_{\alpha_2} \cdots P_{\alpha_l}$. C'est donc une extension normale.

Revenons à la démonstration du théorème. D'après le lemme, il existe une extension galoisienne finie $\mathbb{L}$ qui soit une extension par radicaux de $\Bbbk$. On en déduit que le groupe de Galois

$$Gal(\mathbb{L}/\Bbbk)$$

est un groupe résoluble. Mais comme $\mathbb{D}_{\Bbbk}(P)$ est une extension intermédiaire, on a

$$Gal(\mathbb{D}_{\Bbbk}(P)/\Bbbk) = \frac{Gal((\mathbb{L}/\Bbbk)}{Gal((\mathbb{L}/\mathbb{D}_{\Bbbk}(P)}.$$

Ainsi $Gal(\mathbb{L}/\Bbbk)$ est le quotient d'un groupe résoluble. Il est donc résoluble. G

7.2.2 La réciproque du théorème de Galois

Théorème 29 *Soit $P \in \Bbbk[X]$ un polynôme de degré supérieur ou égal à 1 où $\Bbbk$ est un corps de caractéristique 0. Alors si le groupe de Galois de P est résoluble, P est résoluble par radicaux.*

Démonstration. Rappelons que le groupe de Galois de P est, par définition, $Gal(\mathbb{D}_{\Bbbk}(P)/\Bbbk)$. Posons

$$n = [\mathbb{D}_{\Bbbk}(P); \Bbbk)] = |Gal(\mathbb{D}_{\Bbbk}(P)/\Bbbk)|.$$

Soit ξ une racine primitive n-ième de l'unité dans la clôture algébrique $\widetilde{\mathbb{D}_{\Bbbk}(P)}$ de $\mathbb{D}_{\Bbbk}(P)$. Supposons dans un premier temps que $\xi \in \Bbbk$, c'est-à-dire $\Bbbk[\xi] = \Bbbk$. Notons, pour simplifier $\mathbb{K}$ le corps des racines de P. Comme le groupe $G = Gal(\mathbb{D}_{\Bbbk}(P)/\Bbbk)$ est résoluble, il existe une suite finie décroissante $\{G_i\}$ de sou-groupes de G telle que

1. $G = G_0 \supset G_1 \supset \cdots \supset G_r = \{0\}$,
2. pour $i = 1, \cdots, r$, G_i est un sous-groupe normal de G_{i-1},
3. pour $i = 0, \cdots, r-1$, le groupe quotient G_i/G_{i+1} est cyclique d'ordre premier.

A chacun de ces sous-groupes G_i correspond le sous-corps intermédiaires $\mathbb{K}_i = Fix(G_i)$ et G_i est le groupe de Galois de l'extension $\Bbbk \subset \mathbb{K}_i$. De plus $\mathbb{K}_i$ est une extension normale de $\Bbbk$. On en déduit que le groupe de Galois $Gal(\mathbb{K}/\mathbb{K}_i)$ est un sous-groupe distingué de $Gal(\mathbb{K}/\Bbbk)$ et

$$Gal(\mathbb{K}_i/\Bbbk) = \frac{Gal(\mathbb{K}/\Bbbk)}{Gal(\mathbb{K}/\mathbb{K}_i)}.$$

On en déduit que

$$Gal(\mathbb{K}_{i+1}/\mathbb{K}_i) = \frac{Gal(\mathbb{K}/\mathbb{K}_i)}{Gal(\mathbb{K}/\mathbb{K}_{i+1})} = \frac{G_i}{G_{i+1}}.$$

Ainsi K_{i+1} est une extension de $\mathbb{K}_i$ dont le groupe de Galois est cyclique d'ordre premier. Soit φ un générateur de ce groupe. Alors φ est une application linéaire du $\mathbb{K}_i$-espace vectoriel $\mathbb{K}_{i+1}$. Si n_i est l'ordre

du groupe de Galois de cette extension, c'est par hypothèse un nombre premier. Si λ est une valeur propre de φ, alors $\varphi(\lambda^{n_i} = \varphi^{n_i}(\lambda) = 1$ et donc $\lambda^{n_i} = 1$. Le polynôme $Q = X^n - 1$ est donc un polynôme annotateur de φ. Par hypothèse, ce polynôme est séparable et a toutes ses racines dans $\mathbb{k}$ (on a supposé que $\mathbb{k}$ contenait une racine primitive de l'unité). Ainsi φ est une application linéaire diagonalisable. Si on suppose que $\varphi \neq Id$, alors il existe une valeur propre $\lambda \neq 1$. Si λ_1 et λ_2 sont deux valeurs propres de φ, alors comme φ est aussi un homomorphisme de corps, $\lambda_1 \cdot \lambda_2$ et λ_1^{-1} sont aussi des valeurs propres de φ. Ainsi, l'ensemble des valeurs propres de φ est un sous-groupes du groupes des racine n_i-ième de l'unité. C'est donc un sous-groupe cyclique. Son ordre d divise n_i et donc toutes les valeurs propres sont des racines d-ième de l'unité ce qui implique que φ est d'ordre d. D'où $d = n_i$ et les racines n_i-ième de l'unité sont des valeurs propres Ainsi ξ est une valeur propre de φ. Soit α un vecteur propre associé. On a

$$\varphi(\alpha) = \xi\alpha$$

On en déduit

$$\varphi(\alpha^{n_i}) = \alpha^{n_i}$$

et donc $\beta = \alpha^{n_i}$ est invariant par φ. Comme $\varphi \in Gal(\mathbb{K}_{i+1}/\mathbb{K}_i)$ qui est cyclique, il est invariant par tous les éléments de ce groupe de Galois. Il appartient donc à K_i. Les éléments conjugués à α sont $\varphi^k(\alpha) = \xi^k\alpha$ pour $k = 0, \cdots n_i - 1$. Ces éléments sont tous distincts, donc $\mathbb{K}_{i+1} = \mathbb{K}_i[\alpha]$. On a donc construit une extension par radicaux contenant le corps de décomposition de P.

Nous avons supposé au cours de cette démonstration que $\mathbb{k}$ contenait une racine primitive ξ de l'unité. Si cela n'est pas le cas, nous opérons comme précédemment, en considérant les extensions $\mathbb{k}[\xi]$ et $\mathbb{D}_{\mathbb{k}}(P)[\xi]$. Le reste de la démonstration est alors analogue à ce que nous venons de faire.

Chapitre 8

Résolution des équations polynomiales

Le théorème de Galois précise qu'une équation polynomiale est résoluble par radicaux si et seulement si son groupe de Galois est résoluble. Nous allons appliquer ce résultat aux équations polynomiales de petit degré et montrer que dès le degré 5, il existe des équations non résolubles par radicaux. Dans tout ce chapitre, on suppose que le corps $\Bbbk$ est un sous-corps de $\mathbb{C}$ (ou bien que $\Bbbk$ est de caractéristique 0 contenu dans un corps algébriquement clos). Soit $P \in \Bbbk[X]$. On notera par

$$Gal(P/\Bbbk)$$

le groupe de Galois de P, c'est-à-dire, $Gal(\mathbb{D}_\Bbbk(P)/\Bbbk)$ où $\mathbb{D}_\Bbbk(P)$ est le corps des racines, ou un corps de décomposition du polynôme P.

8.1 Equations de degré 2

On considère le polynôme

$$P = X^2 + aX + b$$

de degré 2 appartenant à $\Bbbk[X]$.

1. Supposons, dans un premier temps, que P soit réductible sur $\Bbbk$. Il s'écrit donc sous la forme

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

   avec $\alpha, \beta \in \Bbbk$. Dans ce cas on a

   $$\alpha = \frac{-a + \sqrt{a^2 - 4b}}{2a}, \quad \beta = \frac{-a + \sqrt{a^2 - 4b}2a}{2a}$$

   et donc, si $\Delta = a^2 - 4b$, alors

   $$\sqrt{\Delta} \in \Bbbk.$$

   Le corps de décomposition est $\Bbbk$ et donc

   $$Gal(P/\Bbbk) = \{Id\}.$$

   On remarque, que dans ce cas, le groupe de Galois est trivial, donc résoluble et l'équation est bien résoluble par radicaux.

2. Supposons P irréductible sur $\Bbbk$. Soit α et β ses racines dans $\mathbb{C}$, ou dans la cloture algébrique de $\Bbbk$. Comme $P(\alpha) = 0$ et que P est unitaire et irréductible, c'est le polynôme minimal de α. Comme $P(\beta) = 0$, les racines α et β sont conjuguées dans $\Bbbk$ et donc $\beta \in \Bbbk[\alpha]$. Ainsi

$$\mathbb{D}_{\Bbbk}(P) = \Bbbk[\alpha].$$

Tout élément $\varphi \in Gal(P/\Bbbk)$ est déterminé par l'image $\varphi(\alpha)$. Comme $\varphi(\alpha)$ est aussi une racine de P, alors
— Soit $\varphi(\alpha) = \alpha$ et $\varphi = Id$,
— Soit $\varphi(\alpha) = \beta$. Dans ce second cas, nous pouvons identifier φ à la transposition $\sigma = (12)$ du groupe symétrique $\mathcal{S}_2$.
On en déduit

$$Gal(P/\Bbbk) = \mathcal{S}_2.$$

Rappelons que le groupe $\mathcal{S}_2 = \{Id, (12)\}$ est un groupe fini d'ordre 2 et donc abélien (et donc résoluble). Ainsi, toute équation polynomiale de degré 2 est résoluble par radicaux.

8.2 Equations de degré 3

On considère le polynôme

$$P = X^3 + aX^2 + bX + c$$

de degré 3 appartenant à $\Bbbk[X]$. Considéronsla transformation $Y = X + \frac{a}{3}$. Alors

$$X^3 + aX^2 + bX + c = Y^3 - aY^2 + 3(\frac{a}{3})^2 Y - (\frac{a}{3})^3 + aY^2 - 2a\frac{a}{3}Y + a\frac{a}{3}^2 + bY - b\frac{a}{3} + c = Y^3 + pY + q$$

avec $p = -2a\frac{a}{3} + 3(\frac{a}{3})^2 + b$ et $q = -(\frac{a}{3})^3 + a\frac{a}{3}^2 - b\frac{a}{3} + c$. Le polynôme P devient $Y^3 + pY + q$ et la résolution de P est équivalente à celle de $Y^3 + pY + q$. Nous pouvons donc supposer que le polynôme P s'écrive sous la forme

$$P = X^3 + pX + q.$$

Soient α, β, γ les racines de P dans $\mathbb{C}$. Posons

$$\delta = (\alpha - \beta)(\beta - \gamma)(\gamma - \alpha).$$

8.2.1 Le corps de décomposition de $X^3 + pX + q$

Proposition 66 *Le corps de décomposition de $P = X^3 + pX + q$ sur $\Bbbk$ est $\Bbbk[\alpha, \delta]$.*

Démonstration. Par définition, le corps de décomposition de P est $\Bbbk[\alpha, \beta, \gamma]$. Si

$$\delta = (\alpha - \beta)(\beta - \gamma)(\gamma - \alpha),$$

alors

$$\Bbbk[\alpha, \delta] \subset \Bbbk[\alpha, \beta, \gamma].$$

Montrons l'inclusion inverse. Pour cela, rappelons (ou introduisons) la notion de discriminant d'un polynôme.

Définition 49 *Soit P un polynôme unitaire de $\mathbb{k}[X]$ de degré n. On appelle discriminant de P le scalaire*

$$D(P) = (-1)^{\frac{n(n-1)}{2}} Res(P, P')$$

où $Res(P, P')$ est le résultant de deux polynômes P et de sa dérivée formelle P', c'est-à-dire

$$Res(P, P') = \prod_{i=1}^{n} P'(\alpha_i)$$

où $\alpha_1, \cdots, \alpha_n$ sont les racines de P dans $\mathbb{C}$.

En particulier, nous avons pour $P = X^3 + pX + q$, $P' = 3X^2 + p$ et

$Res(P, P') = (3\alpha^2 + p)(3\beta^2 + p)(3\gamma^2 + p) = 27(\alpha^2\beta^2\gamma^2) + 9p(\alpha^2\beta^2 + \alpha^2\gamma^2 + \beta^2\gamma^2) + 3p^2(\alpha^2 + \beta^2 + \gamma^2) + p^3.$

Or les relations entre les racines et les coefficients s'écrivent :

$$\begin{cases} \alpha + \beta + \gamma = 0, \\ \alpha\beta + \alpha\gamma + \beta\gamma = p, \\ \alpha\beta\gamma = -q. \end{cases}$$

Ainsi

$$\alpha^2\beta^2\gamma^2 = q^2,$$

et

$$(\alpha + \beta + \gamma)^2 = 0 = \alpha^2 + \beta^2 + \gamma^2 + 2(\alpha\beta + \alpha\gamma + \beta\gamma)$$

soit

$$\alpha^2 + \beta^2 + \gamma^2 = -2p.$$

De même

$$(\alpha\beta + \alpha\gamma + \beta\gamma)^2 = p^2 = \alpha^2\beta^2 + \alpha^2\gamma^2 + \beta^2\gamma^2 + 2(\alpha + \beta + \gamma)(-q)$$

soit

$$\alpha^2\beta^2 + \alpha^2\gamma^2 + \beta^2\gamma^2 = p^2.$$

On en déduit

$$Res(P, P') = 27q^2 + 9p^3 - 6p^3 + p^3 = 27q^2 + 4p^3.$$

Ainsi, le discriminant du polynôme $P = X^3 + pX + q$ est

$$D(P) = -27q^2 - 4p^3.$$

Lemme 7 *Soient α, β, γ les racines de $P = X^3 + pX + q$ dans $\mathbb{C}$. Alors*

$$D(P) = -27q^2 - 4p^3 = (\alpha - \beta)^2(\alpha - \gamma)^2(\beta - \gamma)^2.$$

Démonstration. En effet on a dans $/C$:

$$P = (X - \alpha)(X - \beta)(X - \gamma).$$

Ainsi

$$P'(\alpha) = (\alpha - \beta)(\alpha - \gamma),\ P'(\beta) = (\beta - \alpha)(\beta - \gamma),\ P'(\gamma) = (\gamma - \alpha)(\gamma - \beta).$$

Or

$$Res(P, P') = P'(\alpha)P'(\beta)P'(\gamma) = -(\alpha - \beta)^2(\alpha - \gamma)^2(\beta - \gamma)^2.$$

On en déduit

$$D(P) = -Res(P, P') = (\alpha - \beta)^2(\alpha - \gamma)^2(\beta - \gamma)^2.$$

Conséquences. Le discriminant $D(P)$ est nul si et seulement si $\delta = 0$ c'est-à-dire P admet une racine double. Supposons par exemple $\alpha = \beta$. On en déduit $\gamma = -2\alpha$ et donc les racines sont dans ce cas $(\alpha, \alpha, -2\alpha)$. On a donc également

$$\alpha\beta + \alpha\gamma + \beta\gamma = \alpha^2 - 2\alpha^2 - 2\alpha^2 = -3\alpha^2 = p$$

et

$$\alpha\beta\gamma = -2\alpha^3 = -q.$$

Si $\alpha \neq 0$, alors $\alpha = \dfrac{3q}{2p}$ et donc $\alpha \in \mathbb{k}$. Dans ce cas le corps de décomposition est $\mathbb{k}$ et le groupe de Galois du polynôme P est réduit à l'Identité.

Supposons dorénavant que $D(P) \neq 0$, ce qui est équivalent à $\delta \neq 0$ et les racines sont toutes distinctes. Alors

$$\delta = (\alpha - \beta)(\beta - \gamma)(\gamma - \alpha)$$

implique

$$\beta - \gamma = \frac{\delta}{(\alpha - \beta)(\gamma - \alpha)} = \frac{\delta}{\alpha(\beta + \gamma) - \alpha^2 - \beta\gamma} = \frac{\delta}{-2\alpha^2 + \frac{q}{\alpha}}.$$

Ainsi $\beta - \gamma \in \mathbb{k}[\alpha, \delta]$. Mais $\beta + \gamma = -\alpha$. On en déduit que β et γ appartiennent à $\mathbb{k}[\alpha, \delta]$. Ainsi $\mathbb{k}[\alpha, \beta, \gamma] \subset \mathbb{k}[\alpha, \delta]$. On en déduit la proposition.

Corollaire 4 *Soit $P = X^3 + pX + q \in \mathbb{k}[X]$ dont le discriminant est non nul. Alors*

1. *Si $\delta \in \mathbb{k}$, le corps de décomposition de P est $\mathbb{k}[\alpha]$ et*

$$[\mathbb{k}[\alpha]; \mathbb{k}] = 3.$$

2. *Si $\delta \notin \mathbb{k}$, le corps de décomposition de P est $\mathbb{k}[\alpha, \delta]$ et*

$$[\mathbb{k}[\alpha, \delta]; \mathbb{k}] = 6.$$

Démonstration. En effet, si $\delta \in \mathbb{k}$, le corps de décomposition de P est $\mathbb{k}[\alpha]$. Comme $P(\alpha) = 0$ et P unitaire, il est irréductible car aucune des racines n'est dans $\mathbb{k}$. C'est donc le polynôme minimal de α et donc

$$[\mathbb{k}[\alpha]; \mathbb{k}] = 3.$$

Si $\delta \notin \mathbb{k}$, le corps de décomposition de P est $\mathbb{k}[\alpha, \delta]$. Dans ce cas on a

$$[\mathbb{k}[\delta]; \mathbb{k}] = 2$$

car
delta est de degré 2. En effet $\delta^2 = D(P)$ et donc δ est racine du polynôme $X^2 - D(P) \in \mathbb{k}[X]$. Ce polynôme étant irréductible dans $\mathbb{k}$, on a bien que δ est de degré 2. De même

$$[\mathbb{k}[\alpha]; \mathbb{k}] = 3.$$

On en déduit

$$[\mathbb{k}[\alpha, \delta]; \mathbb{k}] = 6.$$

8.2.2 Le groupe de Galois de $X^3 + pX + q$

Proposition 67 *Soient $P = X^3 + pX + q \in \mathbb{k}[X]$ et $D(P) = -27q^2 - 4p^3$ son discriminant.*

1. *Si $D(P) = 0$, alors $Gal(P/\mathbb{k}) = \{Id\}$.*
2. *Si $D(P) \neq 0$ et $\sqrt{D(P)} \in \mathbb{k}$, alors $Gal(P/\mathbb{k}) = \mathbb{Z}/3\mathbb{Z}$.*
3. *Si $D(P) \neq 0$ et $\sqrt{D(P)} \notin \mathbb{k}$, alors $Gal(P/\mathbb{k}) = \mathcal{S}_3$.*

Démonstration. Nous avons déjà examiné le premier cas. Supposons donc $D(P) \neq 0$ et $\sqrt{D(P)} \in \mathbb{k}$. Ceci signifie que $\delta \neq 0$ et $\delta \in \mathbb{k}$. Le corps de décomposetion de P est dans ce cas $\mathbb{k}[\alpha]$ qui est une extension de degré 3, le polynôme minimal de α étant égal à P. Comme l'extension

$$\mathbb{k} \subset \mathbb{k}[\alpha]$$

est une extension par un corps de décomposition, elle est normale. C'est donc une extension galoisienne ce qui implique que le groupe de Galois $Gal(P/\mathbb{k})$ est d'ordre 3. Comme tout groupe d'ordre 3 est isomorphe à $\mathbb{Z}/3\mathbb{Z}$, on en déduit

$$Gal(P/\mathbb{k}) = \mathbb{Z}/3\mathbb{Z}.$$

Supposons à présent $D(P) \neq 0$ et $\sqrt{D(P)} \notin \mathbb{k}$. Le corps de décomposition est $\mathbb{k}[\alpha, \delta]$ et l'extension

$$\mathbb{k} \subset \mathbb{k}[\alpha, \delta]$$

est de degré 6. Ainsi le groupe de Galois est dans ce cas d'ordre 6. Mais ce groupe de Galois est isomorphe à un sous-groupe de $\mathcal{S}_3$. Ainsi

$$Gal(P/\mathbb{k}) = \mathcal{S}_3.$$

Les éléments de ce groupe sont donnés par

$$\begin{cases} \varphi_1(\alpha) = \alpha & \varphi_1(\beta) = \beta & \varphi_1(\gamma) = \gamma \\ \varphi_2(\alpha) = \beta & \varphi_2(\beta) = \alpha & \varphi_2(\gamma) = \gamma \\ \varphi_3(\alpha) = \gamma & \varphi_3(\beta) = \beta & \varphi_2(\gamma) = \alpha \\ \varphi_4(\alpha) = \alpha & \varphi_4(\beta) = \gamma & \varphi_4(\gamma) = \beta \\ \varphi_5(\alpha) = \beta & \varphi_5(\beta) = \gamma & \varphi_5(\gamma) = \alpha \\ \varphi_2(\alpha) = \gamma & \varphi_2(\beta) = \alpha & \varphi_2(\gamma) = \beta. \end{cases}$$

Théorème 30 *Tout polynôme de degré 3 de $\mathbb{k}[X]$ est résoluble par radicaux.*

Démonstration. En effet, le groupe de Galois, qui est soit trivial, soit $\mathbb{Z}/3\mathbb{Z}$ soit $\mathcal{S}_3$ est résoluble.

Remarque Le théorème ci-dessus nous assure de l'existence de formules donnant les racines d'un polynôme de degré 3 mais ne permet pas d'écrire ces formules. Rappelons que pour le degré 2, ces formules s'apprennent en classe de lycée et s'écrivent sous la forme suivante :

Soit $P = X^2 + aX + b$ un polynôme de $\Bbbk[X]$ où $\Bbbk$ est un sous-corps de $\mathbb{C}$. Alors les racines s'écrivent dans $\mathbb{C}$ ou dans le corps de décomposition de P :

$$\alpha = \frac{-a + \sqrt{a^2 - 4b}}{2},\ \beta = \frac{-a - \sqrt{a^2 - 4b}}{2}.$$

En degré 3, les formules, dites de Cardan ou de Tartaglia-Cardan, sont un peu plus compliquées. Soit $P = X^3 + pX + q$ un polynôme de $\Bbbk[X]$. Ses racines s'écrivent

$$\begin{cases} \alpha_1 = \sqrt[3]{\frac{1}{2}(-q + \sqrt{\frac{4p^3 + 27q^2}{27}})} + \sqrt[3]{\frac{1}{2}(-q - \sqrt{\frac{4p^3 + 27q^2}{27}})}, \\ \alpha_2 = j\sqrt[3]{\frac{1}{2}(-q + \sqrt{\frac{4p^3 + 27q^2}{27}})} + j^2\sqrt[3]{\frac{1}{2}(-q - \sqrt{\frac{4p^3 + 27q^2}{27}})}, \\ \alpha_3 = j^2\sqrt[3]{\frac{1}{2}(-q + \sqrt{\frac{4p^3 + 27q^2}{27}})} + j\sqrt[3]{\frac{1}{2}(-q - \sqrt{\frac{4p^3 + 27q^2}{27}})} \end{cases}$$

où $j = e^{2i\pi/3}$.

8.3 Equations de degré 4

On considère le polynôme $P = X^4 + aX^3 + bX^2 + cX + d$. Comme pour le degré 3, la transformation $Y = X + \frac{a}{4}$ transforme P en un polynôme de degré 4 de la forme $X^4 + pX^2 + qX + r$ et la résolution par radicaux de P est équivalente à celle du polynôme réduit. On peut donc supposer que $P = X^4 + pX^2 + qX + r$.

Proposition 68 *Tout polynôme de degré 3 $P = X^4 + pX^2 + qX + r$ de $\Bbbk[X]$ se décompose sous la forme*

$$P = (X^2 + aX + b)(X^2 - aX + d)$$

avec $a, b, c, d \in \Bbbk$.

Démonstration. En effet

$$(X^2 + aX + b)(X^2 + cX + d) = X^4 + (a + c)X^3 + (b + d + ac)X^2 + (ad + bc)X + bd.$$

Par identification, on obtient

$$\begin{cases} a + c = 0, \\ b + d + ac = p, \\ ad + bc = q, \\ bd = r. \end{cases}$$

D'où $c = -a$, $b + d = p + a^2$, $d - b = \frac{q}{a}$ et donc

$$b = \frac{1}{2}(p + a^2 - \frac{q}{a}),\ d = \frac{1}{2}(p + a^2 + \frac{q}{a}).$$

Mais $bd = r$ ce qui donne

$$4ra^2 = a^2(p + a^2)^2 - q^2.$$

Ceci est une équation bicarré en a. Posons $A = a^2$. Alors A est racine de

$$A(p + A)^2 - 4rA - q^2 = 0.$$

Le polynôme $X(p + X)^2 - 4rX - q^2$ est de degré 3 et appartient à $\Bbbk[X]$. D'après le paragraphe précédent, on sait trouver les racines d'une telle équation. On en déduit la proposition.

Corollaire 5 *Tout polynôme de degré 4 de $\Bbbk[X]$ est réductible. Il est donc résoluble par radicaux.*

8.4 Equations de degré 5

Nous avons vu que toute équation polynômiale de degré 2,3 ou 4 est résoluble par radicaux. Ceci s'explique aisément car le groupe de Galois du polynôme est un sous groupe respectivement de $\mathcal{S}_2$, de $\mathcal{S}_3$ ou de $\mathcal{S}_4$. Mais comme chacun de ces groupes est résoluble, il en est de même de leurs sous-groupes, en particulier du groupe de Galois du polynôme. Donc, en vertu du théorème de Galois, l'équation est résoluble par radicaux. Tout change dès le degré 5 car de $\mathcal{S}_5$ n'est plus résoluble. Donc tout polynôme dont le groupe de Galois est de $\mathcal{S}_5$ ne peut être résoluble par radicaux. Rappelons, toutefois, que certaines équations polynômiales de degré 5 peuvent être résolubles par radicaux. Il suffit que le groupe de Galois soit un sous-groupe résoluble de de $\mathcal{S}_5$. La plus simple est associée au polynôme $P = X^5$ dont le groupe de gallois est réduit à l'identité. De même si toutes les racines de P sont dans $\Bbbk$, le corps de racines est aussi $\Bbbk$ et donc le groupe de Galois est l'identité. Nous avons également vu que le groupe de Galois de $X^5 - a$ était résoluble. Ce polynôme est aussi résoluble par radicaux.

8.4.1 Un polynôme de degré 5 non résoluble par radicaux

.

Considérons le polynôme suivant de $\mathbb{Q}[X]$

$$P = X^5 - 10X + 5.$$

D'après le critère d'Eisenstein, si nous prenons pour entier premier $p = 5$, il divise tous les coefficients sauf $a_5 = 1$et dee plus $p^2 = 25$ ne divise pas $a_0 = 5$, on en déduit que P est irréductible sur $\mathbb{Q}$. Ses racines n'appartiennent pas à $\mathbb{Q}$. Son corps de décomposition est donc une extension propre de $\mathbb{Q}$. Pour déterminer le nombre de racines réelles regardons les variations de la fonction polynomiale $y = x^5 - 5x + 10$. Sa dérivée est

$$y' = 5x^4 - 5 = 5(x^4 - 1) = 5(x - 1)(x + 1)(x^2 + 1).$$

Comme $y(1) = -4$ et $y(-1) = 14$, on en déduit que P admet 3 racines réelles et deux racines complexes conjuguées. Notons $\alpha_1, \alpha_2, \alpha_3$ les racines réelles et $\beta, \overline{\beta}$ les deux racines complexes conjuguées. Soit G le groupe de Galois de P :

$$G = Gal(\mathbb{D}_{\mathbb{Q}}(P)/\mathbb{Q}).$$

Considérons l'élément $\varphi \in G$ défini par

$$\varphi(a) = a, a \in \mathbb{R};\ \varphi(i) = -i.$$

En particulier $\varphi(\beta) = \overline{\beta}$. Comme β est une racine de P, l'extension $\mathbb{Q}[\beta]$ de $\mathbb{Q}$ a pour degré, le degré du polynôme minimal de β. Comme P est unitaire et irréductible, c'est le polynôme minimal de β et donc

$$[\mathbb{Q}[\beta]; \mathbb{Q}] = 5.$$

On en déduit

$$[\mathbb{D}_{\mathbb{Q}}(P); \mathbb{Q}] = [\mathbb{D}_{\mathbb{Q}}(P); \mathbb{Q}[\beta]].[\mathbb{Q}[\beta]; \mathbb{Q}] = 5k$$

avec $k = [\mathbb{D}_{\mathbb{Q}}(P); \mathbb{Q}[\beta]]$. Ainsi

$$|G| = 5k.$$

Or le théorème de Cauchy relatif aux groupes finis précisent que pour tout premier p divisant l'ordre de G, il existe un élément de G d'ordre p. En particulier, il existe un élément ϕ du groupe de Galois G tel que $\phi^5 = Id$. Rappelons que G contient également l'automorphisme φ défini par $\varphi(\beta) = \overline{\beta}$ qui est d'ordre 2. Or on peut identifier G à un sous-groupe du groupe symétrique $\mathcal{S}_5$. Ce sous-groupe contient un cycle d'ordre 5 et une transposition. Or ces deux éléments forment un système de générateurs de $\mathcal{S}_5$. Ainsi

$$G = \mathcal{S}_5.$$

Mais $\mathcal{S}_5$ n'est pas résoluble. Ainsi le groupe de Galois de P n'est pas résoluble et P n'est pas résoluble par radicaux.

8.4.2 Généralisations

Les arguments ci-dessus, plus le fait que tout système composé d'un p-cycle, avec p premier et d'une transposition est un système de générateurs de $\mathcal{S}_p$, montrent le résultat suivant :

Proposition 69 *Soit $P \in \mathbb{Q}[X]$ un polynôme unitaire irréductible de degré p avec p premier et $p \geq 5$. Supposons que P possède exactement deux racines complexes conjuguées et non réelles. Alors P n'est pas résoluble par radicaux.*

Chapitre 9

Annexe1 : Le groupe symétrique $\mathcal{S}_n$

9.1 Définition de $\mathcal{S}_n$. Générateurs

9.1.1 Permutations

Soit $E_n = \{1, 2, \cdots, n-1, n\}$. On appelle permutation de n-éléments toute bijection de E_n. Un telle permutation se notera

$$\sigma = \begin{pmatrix} 1 & 2 & \cdots & n \\ \sigma(1) & \sigma(2) & \cdots & \sigma(n) \end{pmatrix}$$

Comme la composée de deux permutations est encore une permutation, l'ensemble des permutations de E_n est stable pour cette opération.

Définition 50 *On appelle groupe symétrique d'indice n, et on le note $\mathcal{S}_n$, le groupe des permutation de E_n pour la composition.*

On en déduit que

$$|\mathcal{S}_n| = n!.$$

Ainsi, si nous notons par $\tau_{i,j}, 1 \leq i < j \leq n$ la transposition permutant i et j, c'est-à-dire la permutation définie par

$$\tau_{i,j}(i) = j,\ \tau_{i,j}(j) = i,\ \tau_{i,j}(k) = k, k \neq i, j$$

alors on a

— $\mathcal{S}_1 = \{Id\}$,
— $\mathcal{S}_2 = \{Id, \tau_{1,2}\}$,
— $\mathcal{S}_3 = \{Id, \tau_{1,2}, \tau_{1,3}, \tau_{2,3}, c, c^2\}$

où c est la permutation cyclique

$$c = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$$

9.1.2 Transpositions, cycles

Soit $\sigma \in \mathcal{S}_n$. On appelle support de σ le sous ensemble de E_n, noté supp(σ), défini par

$$\text{supp}(\sigma) = \{k \in E_n,\ \sigma(k) \neq k\}.$$

Nous avons défini ci-dessus la notion de transposition. Supposons $i < j \in E_n$. Si $\tau_{i,j}$ est une telle transposition, alors

$$\text{supp}(\tau_{i,j}) = \{i, j\}.$$

Cette permutation vérifie également

$$\tau_{i,j}^2 = Id,\ \tau_{i,j}^{-1} = \tau_{i,j}.$$

Théorème 31 *L'ensemble des transpositions $\{\tau_{i,j}, i \neq j \in E_n\}$ est un système de générateurs de $\mathcal{S}_n$.*

Démonstration. Ceci signifie que toute permutation appartenant à $\mathcal{S}_n$ s'écrit (de manière non unique) comme un produit de transpositions. Démonrtrons par récurrence ce théorème. Il est évident pour $n = 2$. Supposons le résultat vrai pour tous les groupes $\mathcal{S}_p$ avec $p < n$. Soit $\sigma \in E_n$.

- Si σ vérifie $\sigma(n) = n$, alors sa restriction $\tilde{\sigma}$ à $E_{n-1} = \{1, \cdots, n-1\}$ est une permutation et donc appartient à $\mathcal{S}_{n-1}$. Par hypothèse, c'est le produit de transpositions de $\mathcal{S}_{n-1}$. Chacune de ces transpositions $\tilde{\tau}$ définit de manière évidente une transposition τ de $\mathcal{S}_n$ en posant $\tau(k) = \tilde{\tau}(k)$ pour tout $k \in E_{n-1}$ et $\tau(n) = n$. Dans ce cas σ est le produit des transpositions τ.
- Supposons que $\sigma(n) = k \neq n$. Considérons la transposition $\tau = \tau_{k,n}$. Alors $\tau\sigma(n) = n$ et donc, en posant $\sigma_1 = \tau\sigma$, σ_1 est une permutation de E_n vérifiant $\sigma_1(n) = n$. D'après le premier cas, σ_1 est un produit de transpositions. Comme $\sigma = \tau\sigma_1$, on en déduit que σ s'écrit aussi comme un produit de transpositions.

La démonstration ci-dessus donne également un procédé pour construire la décomposition d'une permutation en produit de transposition. Mais il est à noter que ce système générateur est assez gros car in contient $\frac{n(n-1)}{2}$ éléments. Nous pouvons réduire ce système.

Théorème 32 *L'ensemble des transpositions $\{\tau_{i,i+1},\ i = 1, \cdots, n-1\}$ est un système de générateurs de $\mathcal{S}_n$.*

Démonstration. Comme les transpositions engendrent $\mathcal{S}_n$, Il suffit de montrer que toute transposition est un produit de transpositions du type $\tau_{i,i+1}$. Raisonons par récurrence sur l'entier k en supposant le résultat vrai pour toutes les permutations $\tau_{i,j}$ avec $j - i \leq k$. Soit $\tau_{i,j}$ une transposition. Supposons $j - i = k$.

$$\tau_{i,j} = \tau_{j-1,j}\tau_{i,j-1}\tau_{j-1,j}.$$

Mais la transposition $\tau_{i,j-1}$ est telle que $(j-1) - i = k - 1 < k$. C'est par hypothèse un produit de transposition $\tau_{i,i+1}$. il en est donc de même de $\tau_{i,j}$.

9.1.3 Signature d'une permutation

La décomposition d'une permutation en produit de transpositions n'est pas unique. Il en est de même pour la décomposition en produit de transpositions simples c'est-à-dire du type $\tau_{i,j}$. Toutefois ces décompositions permettent de mettre en évidence un invariant de la permutation donnée, c'est-à-dire un objet (ici un élément du groupe $\mathbb{Z}/2\mathbb{Z}$) défini par une décomposition, mais qui ne dépend pas du choix de cette décomposition.

Définition 51 *Soit $\sigma \in \mathcal{S}_n$. On dit que que σ présente une inversion en (i,j), $i<j \in E_n$, si $\sigma(i) > \sigma(j)$. Si $N(\sigma)$ désigne le nombre d'inversions présentées par σ, alors l'entier*

$$\varepsilon(\sigma) = (-1)^{N(\sigma)}$$

est appelé la signature de σ.

Proposition 70 *Soient σ_1 et σ_2 deux permutations de E_n. Alors*

$$\varepsilon(\sigma_1\sigma_2) = \varepsilon(\sigma_1)\varepsilon(\sigma_2).$$

Démonstration. Toute paire $(i,j) \in E_n \times E_n$ telle que $i<j$ est dans l'un des ensembles :

$$\begin{cases} A_1 = \{(i,j), \sigma_2(i) < \sigma_2(j) \text{ et } \sigma_1(\sigma_2(i)) < \sigma_1(\sigma_2(j))\}, \\ A_2 = \{(i,j), \sigma_2(i) < \sigma_2(j) \text{ et } \sigma_1(\sigma_2(j)) < \sigma_1(\sigma_2(i))\}, \\ A_3 = \{(i,j), \sigma_2(j) < \sigma_2(i) \text{ et } \sigma_1(\sigma_2(i)) < \sigma_1(\sigma_2(j))\}, \\ A_4 = \{(i,j), \sigma_2(j) < \sigma_2(i) \text{ et } \sigma_1(\sigma_2(j)) < \sigma_1(\sigma_2(i))\}. \end{cases}$$

Soit N_i le carinal de A_i. On a

$$\begin{cases} N(\sigma_1\sigma_2) = N_2 + N_4, \\ N(\sigma_1) = N_2 + N_3, \\ N(\sigma_2) = N_3 + N_4. \end{cases}$$

Ceci implique

$$\varepsilon(\sigma_1)\varepsilon(\sigma_2) = (-1)^{N_2+N_3}(-1)^{N_3+N_4} = (-1)^{N_2+N_4} = \varepsilon(\sigma_1\sigma_2).$$

Cette dernière propriété peut s'interpréter en disant que l'application

$$\varepsilon : \mathcal{S}_n \to \{1,-1\}$$

est un homomorphisme de groupes (multiplicatifs). Comme la transposition $\tau_{1,2}$ a pour signature -1, cet homomorphisme est surjectif.

Remarque. Soit $\sigma \in \mathcal{S}_n$ et soit

$$\sigma = \tau_1\tau_2\cdots\tau_k$$

une décomposition de σ en produits de transpositions. Alors

$$\varepsilon(\sigma) = (-1)^k.$$

En effet, pour toute transposition τ, on a $\varepsilon(\tau) = -1$. On en déduit que si $sigma = \tau'_1\tau'_2\cdots\tau'_l$ est une autre décomposition de σ en produit de transpositions, alors l et k ont la même parité.

Définition 52 *On dit qu'une permutation $\sigma \in \mathcal{S}_n$ est paire si sa signature $\varepsilon(\sigma) = +1$.*

Comme ε est un morphisme de groupe, on en déduit que le produit de permutations paires est une permutation paire. De même, comme $\varepsilon(\sigma^{-1}) = \varepsilon(\sigma)$, l'inverse d'une permutation paire est paire.

Proposition 71 *L'ensemble des permutations paires de $\mathcal{S}_n$ est un sous-groupe distingué de $\mathcal{S}_n$. On le note $\mathcal{A}_n$ et on l'appelle le groupe alterné. On a*

$$|\mathcal{A}_n| = \frac{\mathcal{S}_n}{2} = \frac{n!}{2}.$$

Démonstration. Considérons en effet l'homéomorphisme surjectif

$$\varepsilon : \mathcal{S}_n \to \{-1, +1\}.$$

Son noyau est $\mathcal{A}_n$. Il définit, par factorisation, un isomorphisme de groupes

$$\overline{\varepsilon} : \frac{\mathcal{S}_n}{\mathcal{A}_n} \to \{-1, +1\}.$$

On en déduit que $|\mathcal{A}_n| = \frac{\mathcal{S}_n}{2} = \frac{n!}{2}$.

9.1.4 Cycles

Définition 53 *Soit $\sigma \in \mathcal{S}_n$ dont le support est $\{i_1, \cdots, i_k\}$. On dit que σ est un cycle si elle vérifie*

$$\sigma(i_1) = i_2, \sigma(i_2) = i_3, \cdots, \sigma(i_{k-1}) = i_k, \sigma(i_k) = i_1.$$

Si c est un tel cycle, on dira que k est sa longueur et on a

$$c^k = Id$$

et c est d'ordre k. Toute transposition est un cycle de longueur 2. Ainsi l'ensemble des cycles est aussi un système de générateurs de $\mathcal{S}_n$. Mais dans ce cas, nous allons pouvoir définir une décomposition unique, modulo une condition supplémentaire.

On dira que deux cycles c et c' sont disjoints, si leurs supports sont disjoints.

Théorème 33 *Toute permutation $\sigma \in \mathcal{S}_n$ s'écrit de manière unique sous la forme d'un produit*

$$\sigma = c_1 c_2 \cdots c_l$$

de cycles disjoints.

Démonstration. La démonstration proposée n'est rien d'autre qu'une manière d'écrire cette décomposition. Soit

$$\sigma = \begin{pmatrix} 1 & 2 & \cdots & n \\ \sigma(1) & \sigma(2) & \cdots & \sigma(n) \end{pmatrix}$$

une permutation. Soit $S = \{i_1, \cdots, i_l\}$ son support. Considérons i_1 et soit k_1 le plus petit entier tel que $\sigma^{k_1}(i_1) = i_1$. Alors la permutation

$$c_1 = \begin{pmatrix} i_1 & \sigma(i_1) & \cdots & \sigma^{k_1-1}(i_1) \\ \sigma(i_1) & \sigma^2(i_1) & \cdots & i_1 \end{pmatrix}$$

est un cycle de longueur k_1. Considérons maintenant le plus petit entier $j_1 \in S$ tel que $j_1 \notin S(c_1)$ le support de c_1. On réitère le procédé précédent et on définit un cycle de longueur k_2 définit par

$$c_2 = \begin{pmatrix} j_1 & \sigma(j_1) & \cdots & \sigma^{k_2-1}(j_1) \\ \sigma(j_1) & \sigma^2(j_1) & \cdots & j_1 \end{pmatrix}$$

Il est clair que les cycles c_1 et c_2 ont des supports disjoints. Ce procédé épuise par itération les éléments du support de σ. On en déduit la décomposition cherchée. L'unicité de cette décomposition est donc, d'après ce que nous venons de voir, unique mais à l'ordre des cycles près. L'unicité se démontre alors par récurrence sur l'ordre du support de σ.

Théorème 34 *Le système $\{\tau_{1,2}, c_n\}$ où c_n est le cycle de longueur n :*

$$c_n = \begin{pmatrix} 1 & 2 & \cdots & n \\ 2 & 3 & \cdots & 1 \end{pmatrix}$$

est un système de générateurs de $\mathcal{S}_n$.

Démonstration. Considérons le sous-groupe G de $\mathcal{S}_n$ engendré par $\{\tau_{1,2}, c_n\}$. Il contient la permutation

$$c_n \tau_{1,2} c_n^{-1}.$$

Mais $c_n \tau_{1,2} c_n^{-1} = \tau_{2,3}$. Ainsi $\tau_{2,3} \in G$. De même G contient $c_n \tau_{2,3} c_n^{-1} = \tau_{3,4}$. on en déduit que G contient toutes les transpositions $\tau_{i,i+1}$. Or ces transpositions engendrent $\mathcal{S}_n$ et donc $G = \mathcal{S}_n$.

Corollaire 6 *Tout sous-groupe de $\mathcal{S}_n$ contenant une transposition $\tau_{i,i+1}$ et le cycle c_n est égal à $\mathcal{S}_n$.*

Proposition 72 *Si $n \geq 3$, tout élément du groupe alterné $\mathcal{A}_n$ est un produit de cycles de longueur 3.*

Démonstration. Soit $\sigma \in \mathcal{A}_n$. Considérons une décomposition en produit de transpositions

$$\sigma = \tau_1 \tau_2 \cdots \tau_{2l}.$$

On peut supposer que dans cette décomposition, deux transpositions consécutives ne sont pas identiques. Considérons alors deux transpositions consécutives $\tau\tau'$. Si leur support (i, j) et (k, s) sont disjoints, alors

$$\tau\tau' = (i, j, k)(j, k, s)$$

où (i, j, k) désigne la permutation cyclique de support (i, j, k). C'est donc un produit de cycles de longueur k. Si τ et τ' ont des supports non disjoints, posons $\tau = (i, j)$ et $\tau' = (i, k)$. Alors $\tau\tau' = (i, j, k)$ qui est un cycle de longueur 3.

On dit que deux cycles c et c' de $\mathcal{S}_n$ sont conjugués s'il existe $\sigma \in \mathcal{S}_n$ tel que

$$c' = \sigma c \sigma^{-1}.$$

Si c et c' sont conjugués, ils ont même longueur. Inversement, deux cycles de même longueur sont conjugués. En effet, si S et S' sont les supports de S et S', les complémentaires $\bar{S}$ et $\bar{A}'$ sont des ensembles de même cardinalité $n - k$ où k est la longueur commune de c et c'. Il existe donc une bijection σ entre ces deux ensembles. Si $S = \{i_1, \cdots, i_k\}$ et $S' = \{j_1, \cdots, j_k\}$, on prolonge σ sur E_n en posant $\sigma(i_l) = j_l$ pour $l = 1, \cdots, k$. Ainsi $\sigma \in \mathcal{S}_n$ et on a $c' = \sigma c \sigma^{-1}$.

9.2 Propriétés algébriques du groupe $\mathcal{S}_n$

9.2.1 Groupes simples

Définition 54 *Soit G un groupe dont l'élément neutre est noté e. On dit que G est simple, s'il n'est pas réduit à $\{e\}$ et s'il n' a pas d'autre sous-groupe normal autre que G et $\{e\}$.*

Par exemple, si G est abélien et simple, alors il est cyclique d'ordre premier.

Théorème 35 *Le groupe alterné $\mathcal{A}_5$ est simple.*

Démonstration. Rappelons que $\mathcal{A}_5$ est le sous-groupe de $\mathcal{S}_5$ dont les éléments sont les permutations paires. Il est d'ordre 60. Considérons le cycle

$$c = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 3 & 1 & 4 & 5 \end{pmatrix}$$

de $\mathcal{S}_5$ que l'on notera pour simplifier $c = (1\ 2\ 3)$. On vérifie facilement que l'ensemble

$$c^{\mathcal{S}_5} = \{\sigma c \sigma^{-1},\ \sigma \in \mathcal{S}_5\}$$

contient 20 éléments. Comme c est un cycle de longueur 3, alors ses conjugués $\sigma c \sigma^{-1}$ sont aussi des cycles de longueur 3. En effet $\sigma c \sigma^{-1}$ est le cycle $(\sigma(1)\ \sigma(2)\ \sigma(3))$. De plus, tout cycle de longueur 3 est conjugué à c. On en déduit que $\mathcal{S}_5$ contient 20 cycles de longueur 3. Ceci implique que le sous-groupe de $\mathcal{S}_5$ formé des éléments σ tels que

$$\sigma c \sigma^{-1} = c$$

est d'ordre $120/20 = 6$. Il est constitué des permutations

$$Id,\ c_1 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 3 & 1 & 4 & 5 \end{pmatrix},\ c_2 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 1 & 2 & 4 & 5 \end{pmatrix},\ c_3 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 2 & 3 & 5 & 4 \end{pmatrix},\ c_1c_3,\ c_2c_3$$

Mais $c_3,\ c_1c_3,\ c_2c_3$ sont des permutations impaires. On en déduit que

$$\{\sigma \in \mathcal{A}_5,\ \sigma c\sigma^{-1} = c\}$$

contient 3 éléments. Ainsi

$$c^{\mathcal{A}_5} = \{\sigma c\sigma^{-1},\ \sigma \in \mathcal{A}_5\}$$

contient $60/3 = 20$ éléments et tous les cycles de longueur 3 sont conjugués dans $\mathcal{A}_5$. Considérons à présent un sous-groupe normal H de $\mathcal{A}_5$ distinct de $\{Id\}$. Si H contient un cycle de longueur 3, comme H est un sous- groupe normal, il contient tous les éléments conjugués à ce cycle. Il contient donc tous les cycles de longueur 3. Comme ils engendrent $\mathcal{A}_5$, on en déduit $H = \mathcal{A}_5$. Sinon, tout élément $\sigma \in H$ est soit un cycle de longueur 5 soit un produit de deux cycles disjoints de longuet 2. Dans le premier cas, posons $\sigma = (1, 2, 3, 4, 5)$. Soit $c = (1, 3, 2)$. Alors $c\sigma c^{-1}\sigma^{-1} \in H$ car H est un sous-groupe normal. Or ceci est égal au cycle $(1, 3, 4)$ de longueur 3. Ce qui est contraire à l'hypothèse. Si $\sigma = (1, 2)(3, 4)$, posons $c = (1, 2)(3, 5)$. dans ce cas $c\sigma c^{-1}\sigma^{-1} \in H$ et est égal à $(3, 5, 4)$ qui est aussi un cycle de longueur 3, ce qui est aussi impossible. Ainsi $H = \mathcal{A}_5$ et $\mathcal{A}_5$ est un groupe simple.