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 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

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

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 isomorphe à un sous-corps premier d'un 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 $f(x^{-1}) = (f(x))^{-1}$.

1.2 Caractéristique d'un corps

1.2.1 Définition

Considérons le sous-groupe $(e) = \{ne, n \in \mathbb{Z}\}$ 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 et on a

$$n_e e = 0.$$

et l'équation $ne = 0$ si et seulement si n 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 3 *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 4 *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 $Im(\varphi) = (e)$ et son noyau est soit nul, soit égale à $p\mathbb{Z}$ par définition de la caractéristique p. Supposons $p \neq 0$, le sous-groupe additif $(e) = \{0, e, \cdots, (p-1)e\}$ 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 5 *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 dénduit $adf = bcf$ 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 $\dfrac{a}{b}$ 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 idédal I de A, tel que $I \neq A$ est contenu dans un idéal maximal.

Proposition 6 *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 $I \subseteq J \subset A$. 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 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 7 *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*

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

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 8 *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 9 *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 non constant* $P \in \mathbb{K}[X]$ *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 $z \in \mathbb{C}$, $P(z) \neq 0$. Alors la fonction $g(z) = 1/f(z)$ 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 $\alpha = \frac{p}{q}$ 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 dău 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 10 *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 $\left(\frac{x}{x2 + y^2}, -\frac{y}{x^2 + y^2}\right)$. 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 11 *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

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

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 12 *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 $\left(\frac{x_1}{x_1^2 + x_2^2}, \frac{-x_2}{x_1^2 + x_2^2}, 0, 0\right)$. 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

   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 13 *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 14 *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 dans lequel chacune des équations

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

possède au moins une solution pour tout $a \in A^*$ et tout $b \in A$.

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 15 *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 Froebenius sur un corps fini

Proposition 16 *Soit $\mathbb{K}$ un corps fini de caractéristique p. Alors l'homéomorphisme 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 17 *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 18 *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 19 *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.

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 20 *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'applicaion $\varphi(u, v) = uv$ 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 $x_1 = 0$, $u = x_2 e_2$ 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.

Proposition 21 *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 $\Bbbk[\alpha]$ 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 $\frac{a_0+a_1\sqrt{2}}{b_0+b_1\sqrt{2}} = \frac{(a_0+a_1\sqrt{2})(b_0-b_1\sqrt{2})}{b_0^2-2b_1^2} = \left(\frac{a_0b_0-2a_1b_1}{b_0^2-2b_1^2}\right) + \left(\frac{-a_0b_1+a_1b_0}{b_0^2-2b_1^2}\right)\sqrt{2}$ 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 22 *Soit $\Bbbk \subset \mathbb{K}$ une extension de corps de degré finie. Il existe une tour d'extension*

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

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 $\mathbb{K} = \Bbbk = \Bbbk(1)$. 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

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

C'est un homomorphisme d'anneaux. 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 23 *Soit $\Bbbk \in \mathbb{K}$ 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. Il existe donc un unique polynôme non nul unitaire irréductible engendrant cet idéal.

Définition 19 *Soit α un élément algébrique sur pk. 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 $\Bbbk[X] = \Bbbk(\alpha)$ 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 on a*

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

où P_α est le polynôme minimal de α.

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

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

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 $\mathbb{Q}^n$ est dénombrable). Si $r(P)$ désigne l'ensemble fini des racines complexes du polynôme P, on a

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

Mais $\cup_{P\in\mathbb{Q}[X]} r(P)$ 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.

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 $\Bbbk[\alpha\beta]$ 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 β donc aussi sur $\Bbbk[\alpha]$. On en déduit que $[\Bbbk[\alpha][\beta], \Bbbk[\alpha]] < +\infty$. Ainsi $[\Bbbk[\alpha][\beta], \Bbbk] = [\Bbbk[\alpha][\beta], \Bbbk[\alpha]]\cdot[\Bbbk[\alpha], \Bbbk]$ est aussi finie 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 $[\mathbb{k}(\alpha), \mathbb{Q}] = n$. 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 $n\mathbb{N}$ tel que*

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

Pour la démonstration, voir mémoire ? en 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 24 *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 25 Racines rationnelles d'un polynômes de $\mathbb{Z}[X]$. *Soit $P(X) = a_0 + a_1X + \cdots + a_nX^n$ un polynôme à coefficients entiers tel que $a_0a_n \neq 0$. 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

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

soit

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

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

Proposition 26 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

$$a^2 P = \gamma_1\gamma_2 R_1 R_2 = a^2\gamma(P) R_1 R_2$$

d'où

$$a^2 P = a^2\gamma(P) R_1 R_2$$

et comme $a \neq 0$,

$$P = \gamma(P) R_1 R_2.$$

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

Proposition 27 Irréductibilité dans $\mathbb{Z}[X]$. Critère d'Eisenstein *Soit $P = a_0 + \cdots + a_n X^n$ un polynôme de $\mathbb{Z}[X]$ avec $a_0 a_n \neq 0$. 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.

Proposition 28 Irréductibilité dans $\mathbb{Z}/p\mathbb{Z}[X]$ et dans $\mathbb{Q}[X]$. *Soit $P = a_0 + \cdots + a_n X^n \in \mathbb{Z}[X]$ 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 $\mathbb{Z}/p\mathbb{Z}$ des coefficients a_i de P. Supposons $\overline{a_n} \neq 0$. Alors si $\overline{P}$ est irréductible dans $\mathbb{Z}/p\mathbb{Z}[X]$, le polynôme P est irréductible dans $\mathbb{Q}[X]$.*

Démonstration.

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 29 *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 30 *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 31 *Le corps $\mathbb{K}$ est une extension algébrique de $\Bbbk$ si $\mathbb{K} = \mathbb{A}_{\Bbbk,\mathbb{K}}$.*

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 donnée en **??** des corps algébriquement clos.

Proposition 32 *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 $\mathbb{k}$ s'identifie à un sous-corps de $\mathbb{k}(\alpha_1, \cdots, \alpha_n)$ et on déduit la tour d'extension

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

Proposition 33 *Soient $\alpha_1, \cdots, \alpha_n \in \mathbb{K}$ des éléments algébriques sur $\mathbb{k}$. Alors l'extension $\mathbb{k}(\alpha_1, \cdots, \alpha_n)$ est algébrique sur $\mathbb{k}$ et de degré fini. De plus $\mathbb{k}(\alpha_1, \cdots, \alpha_n) = \mathbb{k}[\alpha_1, \cdots, \alpha_n]$.*

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 34 *(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 $\mathbb{k}[X]$. 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 $\mathbb{k} \subset \mathbb{K}$ une extension de degré fini de $\mathbb{K}$. Supposons que $[\mathbb{K}; \mathbb{k}]$ 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 $\mathbb{k}$ un corps de caractéristique différente de 2 et $\mathbb{K}$ une extension de $\mathbb{k}$ de degré 2. Montrer qu'il existe $\alpha \in \mathbb{k} - \mathbb{R}^2$ et $\beta \in \mathbb{K}$ tel que $\beta^2 = \alpha$ et $\mathbb{K} = \mathbb{k}(\beta)$.

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 35 *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 36 *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 37 *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 $\mathbb{K}$.

4.3 Exemples

4.3.1 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

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

4.3.2 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

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

4.3.3 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 38 *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 $\mathbb{C}$ noncontinus.*

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 39 *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*

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

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)