MAT641: Théorie des corps

Introduction

Le but principal de ce cours est pour répondre les questions suivantes.

1. *Résolution des équations par radicaux.* Étant donné une équation quadratique sur $\mathbb{C}$:

$$ax^2 + bx + c = 0,$$

on sait que l'equation admet exactement deux racines

$$x_1 = \frac{-b + \sqrt{b^2 - 4ac}}{2a},\ x_2 = \frac{-b - \sqrt{b^2 - 4ac}}{2a}.$$

Maintenant, étant une équation de degré n sur $\mathbb{C}$:

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

est-ce que toutes les racinces s'obtiennent à partir des coefficients $a_0, \ldots, a_n$ par un nombre fini d'opérations d'addition, sous-traction, multiplication, division et extraction de la racine?

2. *La quadrature du cercle.* Étant donné un cercle, est-ce qu'on peut construire à la règle et au compas un carré ayant le même aire que le cercle donné?

3. *La duplication du cube.* Étant donné un cube, est-ce qu'on peut construire à la règle et au compas un cube qui double le volume du cube donné?

4. *La trisection de l'angle.* Étant donné un angle, est-ce qu'on peut construire à la règle et au compas deux demi-droites qui partagent l'angle donné en trois angles égaux?

5. *La construction des polygones réguliers.* Pour quel entier $n > 2$, on peut construire à la règle et au compas un polygone de n côtés égaux?

Chapitre I: Éléments

1.1. Anneaux commutatifs

1.1.1. Définition. Un anneau commutatif est un ensemble non vide A muni d'une addition

$$+ : A \times A \to A : (a, b) \mapsto a + b$$

et d'une multiplication

$$\bullet : A \times A \to A : (a, b) \mapsto ab$$

satisfaisant les axiomes suivants:

(1) A est un groupe abélien pour l'addition.

(2) $(ab)c = a(bc)$ et $ab = ba,$ pour tous $a, b, c \in A$.

(3) il existe un *identité*, noté 1_A, tel que $1_A a = a,$ pour tout $a \in A$.

(4) $a(b + c) = ab + ac,$ pour tous $a, b, c \in A$.

En outre, $a \in A$ est dit *inversible* s'il existe $b \in A$ tel que $ab = 1_A$.

Exemple. (1) L'ensemble $\mathbb{Z}$ des entiers est un anneau commutatif pour l'addition et la multiplication usuelles. Ici, 1 et -1 sont les seuls éléments inversibles.

(2) L'ensemble $\mathbb{Z}[\sqrt{-5}] = \{a + b\sqrt{-5} \mid a, b \in \mathbb{Z}\}$ des entiers de Gauss est un anneau commutatif pour l'addition et la multiplication usuelles. Ici, 1 et -1 sont les seuls éléments inversibles.

(3) Les ensembles $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ des nombres rationnels, réels, complexes, respectivement, sont des anneaux commutatifs pour l'addition et la multiplication usuelles. Dans chacun de ces exemples, tous les nombres non nuls sont inversibles.

Remarque. On voit que $A = \{0_A\}$ si, et seulement si, $1_A = 0_A$.

1.1.2. Définition. Soit A un anneau commutatif. Une partie non vide I de A s'appelle *idéal* si pour tous $r, s \in I$ et $a \in A$, on a $r - s \in I$ et $ra \in I$.

Exemple. (1) Soit $n \in \mathbb{Z}$. On voit que $n\mathbb{Z} = \{na \mid a \in \mathbb{Z}\}$ est un idéal de $\mathbb{Z}$.

(2) $\mathbb{Z}$ n'est pas un idéal de $\mathbb{Q}$.

Soit I un idéal de A. Pour tout $a \in A$, l'ensemble $a + I = \{a + r \,|\, r \in I\}$ s'appelle la *classe* de a *modulo* I. Remarquons que $a + I = b + I$ si et seulement si $a - b \in I$, pour tous $a, b \in A$. On pose $A/I = \{a + I \mid a \in A\}$, l'ensemble des classes modulo I.

1.1.3. Proposition. Soient A un anneau commutatif et I un idéal de A. Alors, pour tous $a + I, b + I \in A/I$, les opérations

$$(a + I) + (b + I) = (a + b) + I \quad \text{et} \quad (a + I)(b + I) = (ab) + I$$

sont correctement définies pour lesquelles A/I est un anneau commutatif, appelé *quotient* de A *modulo* I.

Remarque. Dans un contexte claire, on écrit simplement $\bar{a} = a + I$ et $\bar{A} = A/I$.

Exemple. Soit $n > 1$. On écrit $\mathbb{Z}_n = \mathbb{Z}/n\mathbb{Z}$. Alors $\mathbb{Z}_n = \{\bar{0}, \bar{1}, \cdots, \overline{n-1}\}$. On voit que $\bar{a}$ est inversible si, et seulement si, a est co-premier à n. En effet, s'il existe $\bar{b} \in \mathbb{Z}_n$ tel que $\bar{a}\bar{b} = \overline{ab} = \bar{1}$. Alors $ab - 1 \in n\mathbb{Z}$, c'est-à-dire, il existe $m \in \mathbb{Z}$ tel que $ab - mn = 1$. D'où, a et n sont co-premiers. Réciproquement, si a et n sont co-premiers. D'après le théorème de Bézout, il existe $b, c \in \mathbb{Z}$ tels que $ab + cn = 1$. Ceci nous donne $\bar{1} = \bar{a}\bar{b} + \bar{c}\bar{n} = \bar{a}\bar{b}$. Ainsi $\bar{a}$ est inversible.

1.1.4. Définition. Soient A et B des anneaux commutatifs. Une application $\phi : A \to B$ est un *homomorphisme* si pour tous $a, b \in A$,

(1) $\phi(a + b) = \phi(a) + \phi(b)$,

(2) $\phi(ab) = \phi(a)\phi(b)$,

(3) $\phi(1_A) = 1_B$.

En outre, ϕ est un isomorphisme si ϕ est, de surcroît, bijectif. Dans ce cas, on écrit $A \cong B$.

Exemple. Si I est un idéal de A, alors $p : A \to A/I : a \mapsto a + I$ est un homomorphisme surjectif, appelé la *projection canonique*.

1.1.5. Théorème. Soit $\phi : A \to B$ un homomorphisme d'anneaux commutatifs. Alors

(1) $\mathrm{Ker}(\phi) = \{a \in A \,|\, \phi(a) = 0_B\}$ est un idéal de A.

(2) Si ϕ est surjectif, alors l'application

$$\bar{\phi} : A/\mathrm{Ker}(\phi) \mapsto B : a + I \mapsto \phi(a)$$

est un isomorphisme. Donc $B \cong A/\mathrm{Ker}(\phi)$.

1.1.6. Définition. Soit A un anneau commutatif. Une partie B de A s'appelle *sous-anneau* de A si $1_A \in B$ et $a - b, ab \in B$ pour tous $a, b \in B$.

Remarque. (1) Si B est un sous-anneau de A, alors B lui-même est un anneau commutatif pour les opérations induites de celles de A ayant le même identité que A.

(2) L'intersection de sous-anneaux est un sous-anneau.

Exemple. (1) $\mathbb{Z}$ est un sous-anneau de $\mathbb{Q}$.

(2) L'ensemble $\mathbb{N}$ des entiers non négatifs n'est pas un sous-anneau de $\mathbb{Z}$.

1.1.7. Définition. Soit A un anneau commutatif. Soient B un sous-anneau de A et S une partie quelconque de A. Le plus petit sous-anneau de A contenant B et S est appelé le *sous-anneau engendré par S sur B* et noté $B[S]$.

Remarque. (1) $B[S]$ est l'intersection des sous-anneaux de A contenants B et S.
(2) Si $S \subseteq B$, alors $B[S] = B$.

1.1.8. Proposition. Soit A un anneau commutatif avec B un sous-anneau. Pour tout $a \in A$, on a

$$B[a] = \{b_0 + b_1 a + \cdots + b_n a^n \,|\, n \geq 0,\ b_i \in B\}.$$

Démonstration. Posons $C = \{b_0 + b_1 a + \cdots + b_n a^n \,|\, n \geq 0,\ b_i \in B\}$. On vérifie aisément que C est un sous-anneau de A contenant B et a. Donc $B[a] \subseteq C$. D'autre part, comme $a \in B[a]$ et $B \subseteq B[a]$, on a $b_0 + b_1 a + \cdots + b_n a^n \in B[a]$, pour tous $n \geq 0$ et $b_i \in B$. Donc $C \subseteq B[a]$. Par conséquent, $B[a] = C$. Ceci achève la démonstration.

Exemple. (1) $\mathbb{Z}\left[\frac{1}{3}\right] = \{a_0 + \frac{a_1}{3} + \cdots + \frac{a_n}{3^n} \mid n \geq 0,\ a_i \in \mathbb{Z}\}$.
(2) $\mathbb{Q}[\sqrt{2}] = \{a + b\sqrt{2} \,|\, a, b \in \mathbb{Q}\}$.

1.1.9. Corollaire. Soit A un anneau commutatif avec B un sous-anneau. Pour tous $a_1, \ldots, a_r \in A$, on a $B[a_1, \ldots, a_r] = \{\sum b_{i_1 \cdots i_r} a_1^{i_1} \cdots a_r^{i_r} \mid i_1, \ldots, i_r \in \mathbb{N},\ b_{i_1 \cdots i_r} \in B\}$.

Exemple. $\mathbb{Z}[\sqrt{3}, \sqrt{-5}] = \{a + b\sqrt{3} + c\sqrt{-5} + d\sqrt{-15} \,|\, a, b, c, d \in \mathbb{Z}\}$.

Pour $n \in \mathbb{Z}$ et $a \in A$, on définit

$$na = \begin{cases} \overbrace{a + \cdots + a}^{n \text{ fois}}, & \text{si} \quad n > 0; \\ 0_A, & \text{si} \quad n = 0; \\ \overbrace{(-a) + \cdots + (-a)}^{-n \text{ fois}}, & \text{si} \quad n < 0. \end{cases}$$

Remarque. (1) Pour tous $m, n \in \mathbb{Z}$ et $a \in A$, on a $(n+m)a = na + ma, (nm)a = n(ma)$.
(2) $K = \{n \cdot 1_A \mid n \in \mathbb{Z}\}$ est le plus petit sous-anneau de A.

1.1.10. Définition. Soit A un anneau commutatif. On définit la *caractéristique de A*, noté $\mathrm{car}(A)$, comme étant le plus petit entier $n > 0$ tel que $n1_A = 0_A$ si un tel entier existe; et sinon, $\mathrm{car}(A) = 0$.

Remarque. On a toujours $\mathrm{car}(A)1_A = 0_A$. Si $\mathrm{car}(A) > 0$, alors elle est l'ordre de 1_A en tant qu'élément du groupe abélien $(A, +, 0_A)$.

Exemple. (1) $\mathrm{car}(\mathbb{Z}) = 0$ puisque $n1 \neq 0$, pour tout $n > 0$.
(2) $\mathrm{car}(\mathbb{Z}_n) = n$, car $n \cdot \bar{1} = \bar{n} = \bar{0}$ et $s \cdot \bar{1} = \bar{s} \neq \bar{0}$ pour tout s avec $0 < s < n$.

1.1.11. Proposition. Soit A un anneau commutatif avec B un sous-anneau. Alors $\mathrm{car}(B) = \mathrm{car}(A)$.

Démonstration. Comme $1_B = 1_A$, on a $n1_B = n1_A$, pour tout $n > 0$. D'où, le résultat.

Exemple. Si A est un sous-anneau de $\mathbb{C}$, alors $\mathrm{car}(A) = 0$. En effet, $\mathrm{car}(\mathbb{C}) = \mathrm{car}(\mathbb{Z}) = 0$. Donc $\mathrm{car}(A) = \mathrm{car}(\mathbb{C}) = 0$.

1.2. Corps

1.2.1. Définition. Un *corps* F est un anneau commutatif tel que $1_F \neq 0_F$ et tout élément non nul est inversible.

Exemple. On voit que $\mathbb{Q}$, $\mathbb{R}$ et $\mathbb{C}$ sont des corps mais ni $\mathbb{Z}$ ni $\mathbb{Z}[\sqrt{-5}]$ n'est un corps.

1.2.2. Proposition. Soit F un corps. Pour $a, b \in F$, on a $ab = 0_F$ si, et seulement si, $a = 0_F$ ou $b = 0_F$. Par conséquent, $F^* = F\backslash\{0_F\}$ est un groupe abélien pour la multiplication, appelé *groupe multiplicatif* de F.

Démonstration. Soit $ab = 0_F$. Si $b \neq 0_F$, alors b^{-1} existe. Donc

$$a = a1_F = a(bb^{-1}) = (ab)b^{-1} = 0_F b^{-1} = 0_F.$$

Ceci achève la démonstration.

Exemple. Soit $n > 1$ un entier. Alors $\mathbb{Z}_n$ est un corps si, et seulement si, n est premier. En effet, si n n'est pas premier, alors $n = ab$ avec $0 < a, b < n$. Or $\bar{a}, \bar{b}$ sont tous non nuls tels que $\bar{a}\bar{b} = \overline{ab} = \bar{n} = \bar{0}$. D'après la proposition 1.2.2, $\mathbb{Z}_n$ n'est pas un corps. Supposons réciproquement que n est premier. Comme $0 < 1 < n$, on a $\bar{1} \neq \bar{0}$. En outre, si $\bar{a} \neq \bar{0}$, alors $n \not| a$. Ainsi a est co-premier à n, et donc $\bar{a}$ est inversible. Ceci montre que $\mathbb{Z}_n$ est un corps.

1.2.3. Proposition. Si F est un corps, alors $\mathrm{car}(F) = 0$, ou bien, $\mathrm{car}(F) = p$ un nombre premier.

Démonstration. Supposons $\mathrm{car}(F) = p > 0$. Comme $1 \cdot 1_F \neq 0_F$, on a $p > 1$. Si p n'est pas premier, alors $p = rs$ avec $0 < r, s < p$. D'après la minimalité de la caratéristique, $r1_F$ et $s1_F$ sont tous non nuls. Mais, $(r1_F)(s1_F) = (rs)1_F = p1_F = 0_F$, une contradiction à la proposition 1.2.2. Ceci achève la démonstration.

1.2.4. Corollaire. Soit F un corps avec $\mathrm{car}(F) = p > 0$. Pour tout $n \in \mathbb{Z}$, on a $n1_F = 0_F$ si, et seulement si, $p \,|\, n$.

Démonstration. Si $n = pr$ avec $r \in \mathbb{Z}$, alors $n1_F = (p1_F)(r1_F) = 0_F(r1_F) = 0_F$. Si $p \not| n$, alors p, n sont co-premiers car p est premier. Donc il existe $r, s \in \mathbb{Z}$ tels que $1 = pr+ns$. Donc

$$1_F = (rp + sn)1_F = (r1_F)(p1_F) + (s1_F)(n1_F) = (s1_F)(n1_F).$$

D'où $n1_F \neq 0_F$. Ceci achève la démonstration.

1.2.5. Définition. Soit F un corps.

(1) Un sous-anneau K de F s'appelle *sous-corps* si $a^{-1} \in K$ pour tout $a \in K$ non nul.

(2) Le corps F est dit *premier* si F est le seul sous-corps de F.

Exemple. (1) $\mathbb{Q}[\pi] = \{a_0 + a_1\pi + \cdots + a_n\pi^n \,|\, n \geq 0,\ a_i \in \mathbb{Q}\}$ est un sous-anneau de $\mathbb{R}$, mais pas un sous-corps.

(2) $\mathbb{Q}[\sqrt{-1}] = \{a + b\sqrt{-1} \,|\, a, b \in \mathbb{Q}\}$ est un sous-corps de $\mathbb{C}$. En effet, si $a + b\sqrt{-1} \neq 0$, alors $a^2 + b^2 \neq 0$, et donc

$$(a + b\sqrt{-1})^{-1} = \frac{a}{a^2 + b^2} - \frac{b}{a^2 + b^2}\sqrt{-1} \in \mathbb{Q}[\sqrt{-1}].$$

(3) Si p est un nombre premier, alors $\mathbb{Z}_p = \{\bar{0}, \bar{1}, \ldots, \overline{p-1}\}$ est un corps premier. En effet, si K est un sous-corps de $\mathbb{Z}_p$, alors $\bar{0}, \bar{1} \in K$. En outre, pour tout $0 < d < n$, on a $\bar{d} = d\bar{1} \in K$. Donc $K = \mathbb{Z}_p$.

(4) $\mathbb{Q}$ est un corps premier. En effet, si K est un sous-corps de $\mathbb{Q}$, alors $0, 1 \in \mathbb{Q}$. Donc pour tout $n \in \mathbb{Z},\ n \in K$. Ceci implique $n^{-1} \in K$ pour tout $n \in \mathbb{Z}$ non nul. Or tout $\alpha \in \mathbb{Q}$ s'écrit $\alpha = \frac{m}{n} = mn^{-1} \in K$. Par consśquent, $K = \mathbb{Q}$.

1.2.6. Proposition. Soit F un corps.

(1) F admet un sous-corps P qui est le plus petit parmi les sous-corps de F.

(2) Si K est un sous-anneau de F, alors $L = \{ab^{-1} \mid a, b \in K, b \neq 0\}$ est le plus petit sous-corps de F contenant K.

Démonstration. (1) Soient $\{F_\lambda \mid \lambda \in \Lambda\}$ les sous-corps de F. Posons $P = \cap_{\lambda\in\Lambda} F_\lambda$. On montrera que P est un sous corps de F. D'abord, $1_F \in F_\lambda,$ pour tout $\lambda \in \Lambda$. D'où, $1_F \in P$. Soient $a, b \in P$. Alors $a, b \in F_\lambda,$ pour tout $\lambda \in \Lambda$. Donc $a - b, ab \in F_\lambda$, et $a^{-1} \in F_\lambda$ lorsque $a \neq 0$, pour tout $\lambda \in \Lambda$. Par conséquent, $a - b, ab \in P$ et $a^{-1} \in P$ lorsque $a \neq 0$. Ceci montre que P est un sous-corps de F. Évidemment P est le plus petit sous-corps.

(2) Si $ab^{-1}+cd^{-1} \in L$, alors $ab^{-1}+cd^{-1} = (ad+bc)(bd)^{-1}$, $(ab^{-1})(cd^{-1})^{-1} = (ad)(bc)^{-1} \in L$. Ainsi L est un corps de F contenant K. Comme tout sous-corps est fermé pour les inverses, L est le plus petit sous-corps contenant K. La preuve s'achève.

Remarque. Il est évident que P est un corps premier, appelé le *corps premier* de F.

Exemple. Le corps premier de $\mathbb{C}$ est $\mathbb{Q}$. En effet, si K un sous-corps de $\mathbb{C}$, alors $1 \in K$. D'où $\mathbb{Q} \subseteq K$. Donc, $\mathbb{Q}$ est le plus petit sous-corps de $\mathbb{C}$.

1.2.7. Théorème. Soient F un corps et P son corps premier. Alors $P \cong \mathbb{Z}_p$ si $\text{car}(F) = p > 0$, et $P \cong \mathbb{Q}$ si $\text{car}(F) = 0$.

Démonstration. Posons $K = \{n \cdot 1_F \mid n \in \mathbb{Z}\}$. On voit aisément que K est un sous-anneau de F contenu dans P. En outre, $\phi : \mathbb{Z} \to K : n \mapsto n \cdot 1_F$ est un homomorphisme surjectif d'anneaux. On considère les deux cas suivants.

(1) $\text{car}(F) = p > 0$. Alors p est premier. D'après le corollaire 1.2.4, $n1_F = 0_F$ si, et seulement si, $n \in p\mathbb{Z}$. Cela veut dire $\text{Ker}(\phi) = p\mathbb{Z}$. D'après le théorème 1.1.5, $K \cong \mathbb{Z}_p$. Par conséquent, K est un corps, et donc un sous-corps de F. Comme P est le plus petit sous corps de F, on a $P \subseteq K$. Donc $P = K \cong \mathbb{Z}_p$.

(2) $\text{car}(F) = 0$. Alors $n1_F \neq 0_F$, pour tout $n \in \mathbb{Z}$ non nul. On vérifie aisément que $L = \{(m \cdot 1_F)(n \cdot 1_F)^{-1} \mid m, n \in \mathbb{Z},\ n \neq 0\}$ est un sous-corps de F contenu dans P. Donc $P = L$. Enfin,

$$\psi : \mathbb{Q} \to P : mn^{-1} \mapsto (m \cdot 1_F)(n \cdot 1_F)^{-1}$$

est un isomorphisme de corps. Ceci achève la démonstration.

1.2.8. Corollaire. Un corps P est premier si, et seulement si, $P \cong \mathbb{Q}$ ou $P \cong \mathbb{Z}_p$ avec p un nombre premier.

Remarquons que tout homomorphisme de corps est injectif.

1.2.9. Proposition (Dedekind). Soient E et F des corps et $\phi_i : E \to F$, $i = 1, \ldots, n$, des homomorphismes non nuls deux à deux distincts. Si $a_1, \ldots, a_n \in F$ sont non tous nuls, alors il existe $b \in E$ tel que

$$a_1\phi_1(b) + a_2\phi_2(b) + \cdots + a_n\phi_n(b) \neq 0.$$

Démonstration. Comme F est un corps, le résultat est vrai pour $n = 1$. Supposons que $n > 1$ et que le résultat est vrai pour $n - 1$. Supposons au contraire que

$$(1) \qquad a_1\phi_1(x) + \cdots + a_{n-1}\phi_{n-1}(x) + a_n\phi_n(x) = 0, \text{ pour tout } x \in E.$$

Il suit de l'hypothèse de récurrence que $a_1 \neq 0$. Comme $\phi_1 \neq \phi_n$, il existe $c \in E$ tel que $\phi_1(c) \neq \phi_n(c)$. D'après (1),

$$a_1\phi_1(cx) + \cdots + a_{n-1}\phi_{n-1}(cx) + a_n\phi_n(cx) = 0, \text{ pour tout } x \in E,$$

c'est-à-dire,

$$(2) \qquad a_1\phi_1(c)\phi_1(x) + \cdots + a_{n-1}\phi_{n-1}(c)\phi_{n-1}(x) + a_n\phi_n(c)\phi_n(x) = 0, \text{ pour tout } x \in F.$$

En soustrayant le produit de (1) par $\phi_n(c)$ de (2), on trouve

$$a_1(\phi_1(c) - \phi_n(c))\phi_1(x) + \cdots + a_{n-1}(\phi_{n-1}(c) - \phi_n(c))\phi_{n-1}(x) = 0, \text{ pour tout } x \in E,$$

qui est une contradiction à l'hypothèse de récurrence car $a_1(\phi_1(c) - \phi_n(c)) \neq 0$. Ceci achève la démonstration.

1.3. Polynômes irréductibles

Partout dans cette section, on se fixe A un anneau commutatif.

1.3.1. Définition. Soit

$$f(x) = a_0 + a_1x + \cdots + a_nx^n$$

un polynôme sur A, où $a_n \neq 0_A$ si f est non nul.

(1) Le constant a_0 s'appelle *terme constant* de f, et a_n le *coefficient directeur* lorsque f est non nul.

(2) Le degré $\partial(f)$ de f est défini par $\partial(f) = n$ si f est non nul, et $\partial(f) = -\infty$ sinon.

(3) $f(x)$ est dit *monique* si $a_n = 1_A$.

Remarque. On voit que $f(x) \in A$ si, et seulement si, $\partial(f) \leq 0$. Dans ce cas, on dit que f est un polynôme constant.

1.3.2. Proposition. L'ensemble $A[x]$ des polynômes sur A est un anneau commutatif pour l'addition et la multiplication de polynômes. En outre, A est un sous-anneau de $A[x]$.

1.3.3. Lemme. Soient $f, g \in A[x]$ non nuls. Alors

(1) $\partial(f + g) \leq \max\{\partial(f),\ \partial(g)\}$.

(2) $\partial(fg) \leq \partial(f) + \partial(g)$. L'égalité a lieu si, et seulement si, le produit des coefficients directeurs est non nul. C'est le cas lorsque f ou g a coefficient directeur inversible.

Exemple. Sur $\mathbb{Z}_4$, on a $(2x + 1)(2x + 2) = 2x + 2$. Donc $\partial((2x + 1)(2x + 2)) < \partial(2x + 1) + \partial(2x + 2)$.

Soit $f(x) = \sum_{i=0}^{n} a_ix^i \in A[x]$. Pour $a \in A$, on pose $f(a) = \sum_{i=0}^{n} a_ia^i \in A$.

1.3.4. Proposition. Soit $a \in A$. Alors l'application

$$\rho_a : A[x] \to A : f(x) \mapsto f(a)$$

est un homomorphisme d'anneaux, appelée *l'évaluation* en a.

Démonstration. Évidemment $\rho_a(1_A) = 1_A$. Pour tous $f, g \in A[x]$, on peut écrire $f = \sum_{i=0}^{n} a_i x^i$ et $g = \sum_{i=0}^{n} b_i x^i$. Alors $f+g = \sum_{i=0}^{n}(a_i+b_i)x^i$ et $fg = \sum_{k=0}^{2n}(\sum_{i+j=k} a_i b_j)x^k$. Donc

$$\rho_a(f+g) = \sum_{i=0}^{n}(a_i+b_i)a^i = \sum_{i=0}^{n} a_i a^i + \sum_{i=0}^{n} b_i a^i = \rho_a(f) + \rho_a(g)$$

et

$$\rho_a(fg) = \sum_{k=0}^{2n}(\sum_{i+j=k} a_i b_j)a^k = (\sum_{i=0}^{n} a_i a^i)(\sum_{j=0}^{n} b_j a^j) = \rho_a(f)\rho_a(g).$$

Ceci montre que ρ_a est un homomorphisme. La preuve se termine.

Le résultat suivant est évident.

1.3.5. Proposition. Un homomorphisme $\phi : A \to B$ d'anneaux commutatifs induit un homomorphisme

$$\psi : A[x] \to B[x] : \sum_{i=0}^{n} a_i x^i \mapsto \sum_{i=0}^{n} \phi(a_i) x^i$$

d'anneaux commutatifs.

1.3.6. Théorème. Soit $g(x)$ un polynôme sur A dont le coefficient directeur est inversible. Pour tout $f(x) \in A[x]$, il existe des polynômes uniques $q(x), r(x)$ sur A tels que

$$f(x) = g(x)q(x) + r(x),\ \partial(r) < \partial(g).$$

Démonstration. Posons $g = b_0 + \cdots + b_{m-1}x^{m-1} + b_m x^m$ avec $m \geq 0$ et b_m inversible. Si $m = 0$, alors $f(x) = g(x)(b_m^{-1}f(x)) + 0$ pour tout $f(x) \in A[x]$. Supposons que $m > 0$. Soit $f = a_0 + a_1 x + \cdots + a_n x^n$ avec $a_n \neq 0$. Si $n = 0$, on a $f(x) = 0g(x) + f(x)$ avec $\partial(f) < \partial(g)$. Supposons maintenant que $n > 0$ et l'énoncé est vrai pour tout polynôme de degré $< n$. Si $n < m$, alors $f(x) = 0g(x) + f(x)$ avec $\partial(f) < \partial(g)$. Si $n \geq m$, alors f et $a_n b_m^{-1} x^{n-m} g$ ont même coefficient directeur. Ainsi $h = f - a_n b_m^{-1} x^{n-m} g$ est de degré $< n$. D'après l'hypothèse de récurrence, $h = gq_1 + r$ avec $\partial(r) < \partial(g)$. Or $f(x) = (a_n b_m^{-1} x^{n-1} + q_1(x))g(x) + r(x)$. Ceci montre l'existence de q et r.

Soient $q_0(x), r_0(x) \in A[x]$ tels que $f = q_0 g + r_0$ avec $\partial(r_0) < \partial(g)$. Alors $(q - q_0)g = r - r_0$. Supposons au contraire que $q - q_0 \neq 0_A$, c'est-à-dire, $\partial(q - q_0) \geq 0$. Comme le coefficient directeur de g est inversible, $\partial(q - q_0) + \partial(g) = \partial((q - q_0)g) = \partial(r - r_0) < \partial(g)$. D'où, $\partial(g) < \partial(g)$, une contradiction. Ainsi $q = q_0$, et donc $r = r_0$. Ceci achève la démonstration.

Remarque. Si A est un corps, alors le théorème 1.3.6 est vrai pour tout polynôme non nul $g(x)$ sur A.

Exemple. (1) Considérons les polynômes rationnels $f(x) = 1 + x^7$ et $g(x) = 2 + 3x - x^4$. Alors $f = qg + r$, où $q = -x^3 - 3, r = 2x^3 + 9x + 7$.

(2) Considérons les polynômes $x^3 + 1$ et $2x + 2$ sur $\mathbb{Z}_4$. Alors ll n'existe pas de polynômes $q(x), r(x)$ tels que $x^3 + 1 = (2x + 2)q(x) + r(x)$ avec $\partial(r) < \partial(2x + 2)$. En effet, si oui, on a alors que $2x^3 + 2 = 2r(x)$ est degré < 1, une contradiction.

1.3.7. Définition. Soit $f \in A[x]$ non constant. On dit que $a \in A$ est une *racine* de f si $f(a) = 0_A$.

Remarque. (1) Si A est fini, alors on peut trouver les racines de f en calculant $f(a)$ pour tout $a \in A$.

(2) Si F est un corps, alors tout polynôme de degré 1 admet une racine dans F. Mais c'est pas nécessairement le cas sur un anneau. Par exemple, le polynôme $2x + 1$ sur $\mathbb{Z}_4$ n'a pas de racine dans $\mathbb{Z}_4$.

1.3.8. Proposition. Soit $f(x) \in A[x]$ non constant. Alors $a \in A$ est racine de $f(x)$ si, et seulement si, $f(x) = (x - a)q(x)$ avec $q(x) \in A[x]$.

Démonstration. D'après le théorème 1.3.6, $f(x) = (x - a)q(x) + r$ avec $q(x) \in A[x]$ et $r \in A$. Il suit de la proposition 1.3.4 que $f(a) = (a - a)q(a) + r = r$. Donc $f(a) = 0_A$ si, et seulement si, $r = 0_A$ si, et seulement si, $f(x) = (x - a)q(x)$. Ceci achève la démonstration.

1.3.9. Définition. Soit $f(x) \in A[x]$ non constant. On dit que f est *réductible sur* A s'il existe $g, h \in A[x]$ avec $\partial(g), \partial(h) > 0$ tels que $f = gh$; et *irréductible sur* A sinon.

Exemple. (1) Le polynôme $x^2 - 2$ est irréductible sur $\mathbb{Q}$, mais réductible sur $\mathbb{R}$.

(2) Le polynôme x sur $\mathbb{Z}_4$ est réductible. En effet, $x = (2x^2 + x)(2x + 1)$.

Remarque. Soient F un corps et $f \in F[x]$. Alors f est réductible sur F si, et seulement si, $f = gh$ avec $0 < \partial(g), \partial(h) < \partial(f)$. Par conséquent, si F est un corps fini, on peut déterminer si f est irréductible sur F ou non en calculant les produits des polynômes sur F de degré $< \partial(f)$.

1.3.10. Proposition. Soit $f \in A[x]$ avec $\partial(f) \geq 2$. Si f admet une racine dans A, alors f est réductible sur A.

Démonstration. Soit $a \in A$ tel que $f(a) = 0$. D'après la proposition 1.3.8, il existe $q(x) \in A[x]$ tel que $f(x) = (x - a)q(x)$. Donc $\partial(f) = \partial(q) + 1$ car $x - a$ est monique. D'où $\partial(q) > 0$. Ceci achève la démonstration.

Remarque. (1) La réciproque de la proposition 1.3.10 n'est pas vraie. Par exemple, sur $\mathbb{Z}_6$, on a $4x^2 - 1 = (2x + 1)(2x - 1)$, mais $4x^2 - 1$ n'a pas de racine dans $\mathbb{Z}_6$.

(2) Si un polynôme irréductible f sur A admet une racine dans A, alors $\partial(f) = 1$.

1.3.11. Proposition. Soit F un corps et soit $f(x) \in F[x]$ avec $2 \leq \partial(f) \leq 3$. Alors f est irréductible sur F si, et seulement si, f n'a pas de racine dans F.

Démonstration. Si f a racine dans F, alors f est réductible puisque $\partial(f) \geq 2$. Réciproquement, si f est réductible, alors $f = gh$ avec $g, h \in F[x]$ non constants. Comme $\partial(g) + \partial(h) = \partial(f) \leq 3$, on a $\partial(g) = 1$ ou $\partial(h) = 1$. Comme F est un corps, g ou h admet une racine dans F, et donc f en a une. Ceci achève la démonstration.

1.3.12. Théorème. Soient F un corps et I un idéal de $F[x]$.

(1) Il existe $p(x) \in F[x]$ tel que $I = (p(x)) = \{p(x)f(x) \mid f(x) \in F[x]\}$.

(2) Le quotient $F[x]/I$ est un corps si, et seulement si, $p(x)$ est irréductible sur F.

Démonstration. (1) Si $I = 0$, prenons $p(x) = 0$. Sinon, prenons $p(x) \in I$ non nul de degré minimal. Alors pour tout $f(x) \in I$, il existe $q(x), r(x) \in F[x]$ avec $\partial(r) < \partial(p)$ tels que $f(x) = p(x)q(x) + r(x)$. Comme $r(x) \in I$, on a $r(x) = 0$ par la minimalité de degré de $p(x)$.

(2) Si $p(x)$ est réductible sur F, alors $p = gh$, où $g, h \in F[x]$ avec $0 < \partial(g), \partial(h) < \partial(p)$. Donc $\bar{g}, \bar{h} \in F[x]/I$ sont tous non nuls tels que $\bar{g}\bar{h} = g\bar{h} = \bar{p} = \bar{0}$. D'après la proposition 1.2.2, $F[x]/I$ n'est pas un corps. Supposons réciproquement que $p(x)$ est premier. Si $\bar{f} \neq \bar{0}$, alors $p(x)$ ne divise pas $f(x)$. Ainsi f est co-premier à p. D'après le théorème de Bézout, il existe $g, h \in F[x]$ tels que $fg + ph = 1$. D'où, $\bar{f}\bar{g} = \bar{1}$, c'est-à-dire, $\bar{f}$ est inversible. Ainsi $F[x]/I$ est un corps. Ceci achève la démonstration.

1.4. Polynômes irréductibles rationnels

Dans cette section on considère le problème de déterminer si un polynôme sur $\mathbb{Q}$ est irréductible ou non.

1.4.1. Définition. Un polynôme non nul sur $\mathbb{Z}$ est dit *primitif* si le plus grand commun facteur de ses coefficients est 1.

Exemple. Le polynôme $x^3 + 2x + 3$ est primitif et $2x^2 + 4x + 10$ ne l'est pas.

Remarque. Si $f(x) \in \mathbb{Q}[x]$, alors il existe $\alpha \in \mathbb{Q}$ et un polynôme primitif $g(x) \in \mathbb{Z}[x]$ tels que $f(x) = \alpha g(x)$. Par exemple,

$$\frac{2}{3}x^3 + \frac{6}{5}x + 4 = \frac{2}{15}(5x^3 + 9x + 30).$$

1.4.2. Lemme. Si $f, g \in \mathbb{Z}[x]$ sont primitifs, alors fg l'est.

Démonstration. Posons $f(x) = \sum_{i=0}^{n} a_i x^i$ et $g(x) = \sum_{j=0}^{m} b_j x^j$. Alors $fg = \sum_{k=0}^{n+m} c_k x^k$ avec $c_k = \sum_{i+j=k} a_i b_j$. Si fg n'est pas primitif, alors il existe un entier premier p tel que $p \,|\, c_k$, pour tout $0 \leq k \leq n+m$. Comme f, g sont primitifs, il existe un indice minimal $r \geq 0$ tel que $p \nmid a_r$ et un indice minimal $s \geq 0$ tel que $p \nmid b_s$. En particulier, $p \nmid a_r b_s$. Si $r+s = 0$, alors $r = s = 0$. Donc $p \nmid a_0 b_0 = c_0$, une contradiction. Si $r + s > 0$, alors

$$c_{r+s} = \sum_{i+j=r+s} a_i b_j = a_r b_s + \sum_{i+j=r+s,\ (i,j)\neq(r,s)} a_i b_j.$$

Remarquons que si $(i,j) \neq (r,s)$, alors $i < r$ ou $j < s$, et donc $p \,|\, a_i b_j$. On en déduit que $p \nmid c_{r+s}$, une contradiction. Donc fg est primitif. Ceci achève la démonstration.

1.4.3. Théorème de Gauss. Soit $f(x) \in \mathbb{Z}[x]$ non constant. Alors f est irréductible sur $\mathbb{Q}$ si, et seulement si, f est irréductible sur $\mathbb{Z}$.

Démonstration. Il suffit de montrer la suffisance. Supposons que f est réductible sur $\mathbb{Q}$. Alors il existe $g, h \in \mathbb{Q}[x]$ avec $\partial(g), \partial(h) > 0$ tels que $f = gh$. Or on peut écrire $g = \alpha g_1, h = \beta h_1$ avec $\alpha, \beta \in \mathbb{Q}$ et $g_1, h_1 \in \mathbb{Z}[x]$ primitifs. Donc $f = \gamma g_1 h_1$, où $\gamma = \alpha\beta \in \mathbb{Q}$ et $g_1 h_1 \in \mathbb{Z}[x]$ est primitif d'après le lemme 1.4.2. Posons $g_1 h_1 = a_1 + a_1 x + \cdots + a_n x^n$ avec $a_i \in \mathbb{Z}$. Alors $\gamma a_i \in \mathbb{Z}$, pour tout $0 \leq i \leq n$, car $f \in \mathbb{Z}[x]$. En outre, comme le plus grand commun facteur de $a_0, a_1, \ldots, a_n$ est 1, il existe $s_i \in \mathbb{Z}$ tels $\sum_{i=0}^{n} a_i s_i = 1$. Ceci nous donne $\gamma = \gamma(\sum_{i=0}^{n} a_i s_i) = \sum_{i=0}^{n} (\gamma a_i) s_i \in \mathbb{Z}$. Par conséquent, $f = (\gamma g_1(x)) h_1(x)$ est réductible sur $\mathbb{Z}$. Ceci achève la démonstration.

Le résultat ci-dessus nous dit que le problème de déterminer un polynôme rationnel est irréductible ou non sur $\mathbb{Q}$ se ramène à déterminer un polynôme entier est irréductible ou non sur $\mathbb{Z}$. On donne deux méthodes pour ce faire.

D'abord, pour un entier $q > 1$, la projection canonique $\mathbb{Z} \mapsto \mathbb{Z}_q$ induit un homomorphisme

$$\mathbb{Z}[x] \to \mathbb{Z}_q[x] : f(x) = \sum_{i=0}^{n} a_i x^i \mapsto \bar{f}(x) = \sum_{i=0}^{n} \bar{a}_i x^i.$$

Remarquons $\partial(\bar{f}) \leq \partial(f)$ et l'égalité a lieu si, et seulement si $q \nmid a_n$.

1.4.4. Proposition. Soient $f(x) = \sum_{i=0}^{n} a_i x^i \in \mathbb{Z}[x]$ et $q > 0$ un entier avec $q \nmid a_n$. Si $\bar{f}$ est irréductible sur $\mathbb{Z}_q$, alors f est irréductible sur $\mathbb{Z}$.

Démonstration. Si f est réductible sur $\mathbb{Z}$, alors il existe $g, h \in \mathbb{Z}[x]$ avec $\partial(g), \partial(h) > 0$ tels que $f = gh$. Alors $\partial(g), \partial(h) < \partial(f)$. Or $\bar{f} = \overline{gh} = \bar{g}\bar{h}$. Si $\partial(\bar{g}) = 0$ ou $\partial(\bar{h}) = 0$, alors

$$\partial(\bar{f}) \leq \max\{\partial(\bar{g}), \partial(\bar{h})\} \leq \max\{\partial(g), \partial(h)\} < \partial(f).$$

D'où, $q | a_n$, une contradiction. Donc $\bar{f}$ est réductible sur $\mathbb{Z}_q$. Ceci achève la démonstration.

Remarque. (1) La réciproque n'est pas vraie. Par exemple, x^2-2 est irréductible sur $\mathbb{Z}$, mais sur $\mathbb{Z}_2$, on voit que $x^2-2=x^2$ est réductible.

(2) La condition $q \not| a_n$ est importante. Par exemple, sur $\mathbb{Z}_2$, le polynôme $2x^2+x-1=x-1$ est irréductible, mais $2x^2+x-1=(2x-1)(x+1)$ est réductible sur $\mathbb{Z}$.

Exemple. Considérons le polynôme rationnel

$$f(x)=\frac{5}{2}x^3+2x^2+\frac{3}{2}x+1.$$

Alors f est irréductible sur $\mathbb{Q}$ si, et seulement si, $g=2f=5x^3+4x^2+3x+2$ est irréductible sur $\mathbb{Q}$. Or sur le corps $\mathbb{Z}_2$, on a $\bar{g}(x)=x^3+x$ est réductible. On en déduit aucune conclusion. Sur $\mathbb{Z}_3$, on a $\bar{g}=-x^3+x-1$ qui n'a pas de racine dans $\mathbb{Z}_3$, et donc irréductible sur $\mathbb{Z}_3$ d'après la proposition 1.3.11. Par conséquent, g est irréductible sur $\mathbb{Z}$, et donc irréductible sur $\mathbb{Q}$ d'après le théorème de Gauss. Ceci montre que f est irréductible sur $\mathbb{Q}$.

1.4.5. Le critère d'Eisenstein. Soit $f(x)=a_0+a_1x+\cdots+a_nx^n\in\mathbb{Z}[x]$ avec $n>0$. Alors $f(x)$ est irréductible sur $\mathbb{Q}$ s'il existe un nombre premier p tel que

(1) $p|a_i$, $i=0,1,\ldots,n-1$, mais $p \not| a_n$; et

(2) $p^2 \not| a_0$.

Démonstration. Supposons au contraire que f soit réductible sur $\mathbb{Q}$. D'après le théorème de Gauss,

$$f=(b_0+b_1x+\cdots+b_rx^r)(c_0+c_1x+\cdots+c_sx^s),\ b_i,c_j\in\mathbb{Z}; b_r\neq 0, c_s\neq 0,\ r,s>0.$$

Comme $b_rc_s\neq 0$, on a $0<r,s<n$. Comme $p\,|\,a_0=b_0c_0$, on a $p\,|\,b_0$ ou $p\,|\,c_0$. On peut supposer $p\,|\,b_0$. Comme $p \not| a_n=b_rc_s$, on a $p \not| b_r$. Ainsi il existe un $0<t\leq r$ tel que $p\,|\,b_i$, pour tout $0\leq i<t$ et $p \not| b_t$. Remarquons

$$a_t=\sum_{i+j=t}b_ic_j=b_tc_0+\sum_{i+j=t,\ i<t}b_ic_j.$$

Comme $t\leq r<n$, on a $p|\,a_t$ par l'hypothèse et $p|\,b_ic_j$ pour tout $0\leq i<t$. Ceci implique $p\,|\,b_tc_0$. Comme $p \not| b_t$, on a $p\,|\,c_0$. Ainsi $p^2\,|\,b_0c_0=a_0$, une contradiction. Donc f est irréductible sur $\mathbb{Q}$. Ceci achève la démonstration.

Exemple. (1) Soit p premier. Pour tout $n>1$, d'après le critère d'Eisenstein, le polynôme x^n-p est irréductible sur $\mathbb{Q}$. Donc x^n-p n'a pas de racine dans $\mathbb{Q}$. Par conséquent, $\sqrt[n]{p}$ est irrationnel.

(2) Considérons le polynôme rationnel

$$f(x)=\frac{2}{9}x^5+\frac{5}{3}x^4+x^3+\frac{1}{3}.$$

Posons $g(x) = 9f(x) = 2x^5 + 15x^4 + 9x^3 + 3$. Appliquant le critère d'Eisenstein pour $p = 3$, on voit que g est irréductible sur $\mathbb{Q}$. Donc f l'est également.

1.4.6. Lemme. Soit $f(x) \in \mathbb{Q}[x]$ non constant et soient $a, b \in \mathbb{Q}$ avec a non nul. Alors $f(x)$ est irréductible sur $\mathbb{Q}$ si, et seulement si, $g(x) = f(ax + b)$ est irréductible sur $\mathbb{Q}$.

Démonstration. Si $f(x) = f_1(x)f_2(x),\ f_1, f_2 \in \mathbb{Q}[x]$ avec $\partial(f_1),\ \partial(f_2) > 0$, alors

$$g(x) = f(ax + b) = f_2(ax + b)f_2(ax + b) = g_1(x)g_2(x)$$

avec $g_i(x) = f_i(ax + b)$. Comme $a \neq 0$, on a $\partial(g_i) = \partial(f_i) > 0$. Ainsi $g(x)$ est réductible sur $\mathbb{Q}$. D'autre part, si $g(x)$ est réductible sur $\mathbb{Q}$, alors $f(x) = g(\frac{1}{a}\, x - \frac{b}{a})$ est réductible sur $\mathbb{Q}$. Ceci achève la démonstration.

1.4.7. Corollaire. Soit p un nombre premier. Alors

$$\Phi_p(x) = x^{p-1} + x^{p-2} + \cdots + x + 1,$$

appelé *polynôme cyclotomique*, est irréductible sur $\mathbb{Q}$.

Démonstration. Posons $g(x) = \Phi_p(x + 1)$. Comme $(x - 1)\Phi_p(x) = x^p - 1$, on a

$$xg(x) = (x + 1)^p - 1 = x^p + \binom{p}{1}x^{p-1} + \cdots + \binom{p}{p-2}x^2 + \binom{p}{p-1}x.$$

D'où,

$$g(x) = x^{p-1} + \binom{p}{1}x^{p-2} + \cdots + \binom{p}{p-2}x + \binom{p}{p-1}.$$

Comme p est premier, on a $p | \binom{p}{i}$, pour tout $1 \leq i \leq p-1$ et $p^2 \nmid \binom{p}{p-1} = p$. D'après le critère d'Eisenstein, $g(x)$ est irréductible sur $\mathbb{Q}$. Il suit du lemme 1.4.6 que $\Phi_p(x)$ est irréductible sur $\mathbb{Q}$. Ceci achève la démonstration.

1.5. Exercices

1. Décrire le sous-anneau de $\mathbb{C}$ engendré par $\sqrt[3]{2}$ et $\sqrt{-7}$ sur $\mathbb{Z}$.

2. Considérer le polynôme $f(x) = 2x^4 + x^3 + 5x^2 - 1$ sur $\mathbb{Z}_6$. Trouver les racines de $f(x)$ dans $\mathbb{Z}_6$.

3. Considérer les polynômes sur $\mathbb{Z}_6$ suivants:

$$f(x) = 3x^5 - x^3 + 2x^2 + 1, \quad g(x) = x^3 + x^2 + x - 2.$$

   Trouver le quotient et les reste de $f(x)$ par $g(x)$.

4. Considérer l'idéal I de $\mathbb{Z}_2[x]$ engendré par $p(x) = x^3 + x + 1$. Soit $f(x) = ax^2 + bx + c$ un polynôme sur $\mathbb{Z}_2$ n'appartenant pas à I. Trouver un polynôme $g(x)$ sur $\mathbb{Z}_2$ tel que $(f + I)(g + I) = 1 + I$.

4. Soient A un anneau commutatif et I un idéal de A. Montrer que A/I est un corps si et seulement si I est un idéal maximal de A, c'est-à-dire, $I \neq A$ et il n'y a aucun idéal J de A tel que $I \subset J \subset A$.

5. Montrer que tout homomorphisme de corps $\phi : E \to F$ est injectif.

6. Un domaine intègre est un anneau commutatif non nul dont l'ensemble des éléments non nuls est fermé pour la multiplication. Montrer que tout domaine intègre fini est un corps.

7. Soit $f(x)$ un polynôme sur un corps F. Si f est de degré $n \geq 0$, montrer que f a au plus n racines dans F. *Indication*: À l'aide de la proposition 3.8, procéder par récurence sur n.

8. Soit F un corps infini. Si $f(x), g(x) \in F[x]$ sont tels que $f(a) = g(a)$ pour tout $a \in F$, montrer que $f(x) = g(x)$. *Indication*: Appliquer le numéro précédent au polynôme $f - g$.

9. Montrer qu'une racine rationnelle d'un polynôme entier monique est un entier.

10. Déterminer les polynômes suivants sont réductibles ou irréductibles:

    (1) $x^4 + 1$ sur $\mathbb{Q}$.

    (2) $x^3 - 5$ sur $\mathbb{Z}_{11}$.

    (3) $x^3 - 7x^2 + 3x + 3$ sur $\mathbb{Q}$.

    (4) $x^4 - 10x + 1$ sur $\mathbb{Q}$.

11. Soit F un corps. Si $a_0 + a_1x + \cdots + a_{n-1}x^{n-1} + a_nx^n$ avec $n > 1$ est irréductible sur F, montrer que $a_n + a_{n-1}x + \cdots + a_1x^{n-1} + a_0x^n$ l'est également.

12. Soit $a > 1$ un entier. Montrer que $\sqrt{a}$ est un entier ou un nombre irrationnel.

Chapitre II: Extensions de corps

2.1. Degré d'une extension

2.1.1. Définition. Soient F et E des corps. Si F est un sous-corps de E, on dit alors que $E : F$ est une *extension de corps*, ou bien, que E est une *extension* de F.

Exemple. (1) Le corps $\mathbb{C}$ est une extension du corps $\mathbb{R}$.
(2) $\mathbb{R} : \mathbb{Q}$ est une extension de corps.
(3) Si F est un corps, alors

$$F(x) = \{\frac{f(x)}{g(x)} \mid f, g \in F[x], g \neq 0\}$$

est un corps, appelé le *corps des fractions rationnelles* sur F. Aisément $F(x)$ est une extension de F.

Si $E : F$ est une extension de corps, on voit aisément que E est un espace vectoriel sur F pour l'addition de E et la multiplication externe

$$\bullet : F \times E \to E : (a, \alpha) \mapsto a\alpha$$

induite de la multiplication de E.

2.1.2. Définition. Le *degré* d'une extension de corps $E : F$, notée $[E : F]$, est défini comme étant la dimension de l'espace vectoriel E sur F.

Exemple. (1) $[\mathbb{C} : \mathbb{R}] = 2$, car $\dim_{\mathbb{R}} \mathbb{C} = 2$.
(2) Pour tout corps F, on a $[F(x) : F] = \infty$. En effet, $\{1, x, \ldots, x^n, \ldots\}$ est une famille libre infinie de vecteurs de $F(x)$. Par conséquent, $F(x)$ est de dimension infinie sur F.

2.1.3. Lemme. Soit $E : F$ une extension de corps. Alors $[E : F] = 1$ si, et seulement si, $E = F$.

Démonstration. Si $E = F$, alors $\{1_E\}$ est une base de E sur F. Donc $[E : F] = 1$. Supposons réciproquement $[E : F] = 1$. Prenons $\{\alpha\}$ une base de E sur F. Alors il existe $a \in F$ tel que $1 = a\alpha$. Donc a est non nul et $\alpha = a^{-1} \in F$ car F est un sous-corps de E. Or pour tout $\beta \in E$, il existe $b \in F$ tel que $\beta = b\alpha$. Ainsi $\beta \in F$. Ceci donne $E \subseteq F$, et donc $E = F$. La preuve se termine.

2.1.4. Définition. Une extension de corps $E : F$ est dite *finie* ou *infinie* si $[E : F]$ est fini ou infini, respectivement. On dit aussi que E est *fini* ou *infini* sur F, respectivement.

Exemple. (1) Le corps $\mathbb{C}$ est fini sur $\mathbb{R}$, mais il est infini sur $\mathbb{Q}$.

(2) Pour tout corps F, le corps $F(x)$ des fractions rationnelles sur F est infini sur F.

2.1.5. Théorème. Soient $F \subseteq L \subseteq E$ des corps. Alors l'extension $E : F$ est finie si, et seulement si, les extensions $E : L$ et $L : F$ sont toutes finies. Dans ce cas, on a

$$[E : F] = [E : L][L : F].$$

Démonstration. Supposons premièrement que $[E : F] = n$, c'est-à-dire, $\dim_F E = n$. Comme L est un sous-espace de E, on a $[L : F] = \dim_F L \leq n$. En outre, prenons une F-base $\{\alpha_1, \ldots, \alpha_n\}$ de E. Alors tout $\alpha \in E$ s'écrit $\alpha = a_1\alpha_1 + \cdots + a_n\alpha_n$, $a_1, \cdots, a_n \in F \subseteq L$. Donc le L-espace vectoriel E est engendré par $\alpha_1, \ldots, \alpha_n$. Par conséquent, $[E : L] = \dim_L E \leq n$.

Supposons maintenant que $[E : L] = r$ et $[L : F] = s$, c'est-à-dire, $\dim_L E = r$ et $\dim_F L = s$. Prenons une L-base $\{\beta_1, \ldots, \beta_r\}$ de E et une F-base $\{\gamma_1, \ldots, \gamma_s\}$ de L. Si $\alpha \in E$, alors $\alpha = \sum_{i=1}^{r} b_i\beta_i$ avec $b_i \in L$. Et pour tout $1 \leq i \leq r$, on a $b_i = \sum_{j=1}^{s} c_{ij}\gamma_j$ avec $c_{ij} \in F$. Ainsi $\alpha = \sum_{i,j} c_{ij}\beta_i\gamma_j, c_{ij} \in F$. Ceci montre que le F-espace E est engendré par $\{\beta_i\gamma_j \,|\, 1 \leq i \leq r, 1 \leq j \leq s\}$. Enfin, si $a_{ij} \in F$ sont tels que $\sum_{i,j} a_{ij}\beta_i\gamma_j = 0$, alors $\sum_{i=1}^{r}(\sum_{j=1}^{s} a_{ij}\gamma_j)\beta_i = 0$ avec $\sum_{j=1}^{s} a_{ij}\gamma_j \in L$. Comme les β_i sont linéairement indépendants sur L, on a $\sum_{j=1}^{s} a_{ij}\gamma_j = 0$, pour tout $1 \leq i \leq r$. Mais les γ_j sont linéairement indépendants sur F, on a $a_{ij} = 0$, pour tous $1 \leq j \leq s, 1 \leq i \leq r$. Donc $\{\beta_i\gamma_j \,|\, 1 \leq i \leq r, 1 \leq j \leq s\}$ est une base de E sur F. Par conséquent, $[E : F] = rs = [E : L][L : F]$. Ceci achève la démonstration.

2.1.6. Définition. Soit $E : F$ une extension de corps.

(1) Un élément $\alpha \in E$ est dit *algébrique sur* F s'il est une racine d'un polynôme non nul sur F; et *transcendant sur* F sinon.

(2) L'extension $E : F$ est dite *algébrique* (ou bien, E est dit *algébrique sur* F) si tout élément de E est algébrique sur F.

Exemple. (1) F est toujours algébrique sur lui-même. En effet, tout $\alpha \in F$ est racine de $x - \alpha \in F[x]$.

(2) L'extension $\mathbb{C} : \mathbb{R}$ est algébrique. En effet, tout nombre complexe $\alpha = a + b\sqrt{-1}$ avec $a, b \in \mathbb{R}$ est une racine du polynôme réel $x^2 - 2ax + a^2 + b^2$.

(3) Le nombre réel $\alpha = \sqrt[3]{2 + 3\sqrt{5}}$ est algébrique sur $\mathbb{Q}$. En effet, $\alpha^3 = 2 + 3\sqrt{5}$, et donc $(\alpha^3 - 2)^2 = 45$. D'où, $\alpha^6 - 4\alpha^3 - 41 = 0$, c'est-à-dire, α est une racine de $x^6 - 4x^3 - 41$.

(4) Un résultat célèbre de Lindemann dit que le nombre réel π est transcendant sur $\mathbb{Q}$. Donc l'extension $\mathbb{R} : \mathbb{Q}$ n'est pas algébrique. Remarquons que π est algébrique sur $\mathbb{R}$.

2.1.7. Lemme. Soit $E : F$ une extension de corps. Alors $\alpha \in E$ est algébrique sur F si, et seulement si, il existe $n > 0$ tel que la famille $\{1, \alpha, \ldots, \alpha^n\}$ est liée sur F.

Démonstration. Supposons premièrement que α est algébrique sur F. Alors il existe $f(x) = a_0 + a_1x + \cdots + a_nx^n \in F[x]$ non nul tel que $f(\alpha) = a_0 + a_1\alpha + \cdots + a_n\alpha^n = 0$. Donc $\{1, \alpha, \ldots, \alpha^n\}$ est liée sur F.

Supposons réciproquement que $\{1, \alpha, \ldots, \alpha^n\}$ avec $n > 0$ est liée sur F. Alors il existe $a_0, a_1, \ldots, \alpha_n \in F$ non tous nuls tels que $a_0 \cdot 1 + a_1 \cdot \alpha + \cdots + a_n \cdot \alpha^n = 0$. Cela veut dire que $a_0 + a_1x + \cdots + a_nx^n$ est un polynôme non nul sur F dont α est une racine. Donc α est algébrique sur F. Ceci achève la démonstration.

Exemple. Soit $F(x)$ le corps des fractions rationnelles sur F. Alors $x \in F(x)$ est transcendant sur F. En effet, pour tout $n > 0$, la famille $\{1, x, \ldots, x^n\}$ est libre sur F. Donc x est transcendant sur F.

2.1.8. Proposition. Toute extension finie de corps $E : F$ est algébrique.

Démonstration. Soit $[E : F] = n \geq 1$. Pour tout $\alpha \in E$, la famille $\{1, \alpha, \ldots, \alpha^n\}$ est liée sur F. Donc α est algébrique sur F. Ceci achève la démonstration.

Remarque. La réciproque de la proposition 2.1.8 n'est pas vraie.

2.2 Extensions de corps simples

Partout dans cette section, on se fixe $E : F$ une extension de corps.

2.2.1. Définition. Soit S une partie de E. Le plus petit sous-corps de E contenant F et S, noté $F(S)$, s'appelle le *sous-corps de E engendré par S sur F*.

Remarque. (1) $F[S] \subseteq F(S)$.
(2) $F(S)$ est l'intersection des sous-corps de E contenant F et S.
(3) Si $S \subseteq F$, alors $F(S) = F$.

Exemple. (1) $\mathbb{R}(\sqrt{-1}) = \mathbb{R}[\sqrt{-1}] = \mathbb{C}$.
(2) Le corps $F(x)$ est engendré par le polynôme x sur F.

2.2.2. Lemme. Soient S_1, S_2 des parties de E.
(1) Si $S_1 \subseteq S_2$, alors $F(S_1) \subseteq F(S_2)$.
(2) $F(S_1 \cup S_2) = F(S_1)(S_2) = F(S_2)(S_1)$.
(3) Si $\alpha_1, \alpha_2, \ldots, \alpha_n \in E$, alors $F(\alpha_1, \alpha_2, \ldots, \alpha_n) = F(\alpha_1)(\alpha_2)\cdots(\alpha_n)$.

Démonstration. (1) Si $S_1 \subseteq S_2$, alors $F(S_2)$ est un sous-corps de E contenant F et S_1. Par définition, $F(S_1) \subseteq F(S_2)$.

(2) D'après la partie (1), on a $F(S_1) \subseteq F(S_1 \cup S_2)$. Comme $S_2 \subseteq F(S_1 \cup S_2)$, on a $F(S_1)(S_2) \subseteq F(S_1 \cup S_2)$. D'autre part, $F(S_1)(S_2)$ contient F et $S_1 \cup S_2$. Cela implique $F(S_1 \cup S_2) \subseteq F(S_1)(S_2)$. Par conséquent, $F(S_1 \cup S_2) = F(S_1)(S_2)$. Comme la partie (3) suit immédiatement de la partie (2), la preuve se termine.

2.2.3. Définition. On dit que $E : F$ est une *extension simple* (ou bien, que E est simple sur F) s'il existe $\alpha \in E$, appelé un *élément primitif*, tel que $E = F(\alpha)$.

Exemple. (1) $\mathbb{C} : \mathbb{R}$ est une extension simple dont $\sqrt{-1}$ est un élément primitif.

(2) L'extension $F(x) : F$ est simple dont le polyôme x est un élément primitif.

(3) L'extension $\mathbb{Q}(\sqrt{2}, \sqrt{3}) : \mathbb{Q}$ est simple. En effet, on a $\alpha = \sqrt{2} + \sqrt{3} \in \mathbb{Q}(\sqrt{2}, \sqrt{3})$, et donc $\mathbb{Q}(\alpha) \subseteq \mathbb{Q}(\sqrt{2}, \sqrt{3})$. D'autre part, comme $(\alpha - \sqrt{2})^2 = 3$ et $(\alpha - \sqrt{3})^2 = 2$, on a

$$\sqrt{2} = \frac{\alpha^2 - 1}{2\alpha},\ \sqrt{3} = \frac{\alpha^2 + 1}{2\alpha} \in \mathbb{Q}(\alpha).$$

Donc $\mathbb{Q}(\sqrt{2}, \sqrt{3}) \subseteq \mathbb{Q}(\alpha)$. Par conséquent, $\mathbb{Q}(\sqrt{2}, \sqrt{3}) = \mathbb{Q}(\alpha)$ est simple sur $\mathbb{Q}$.

2.2.4. Théorème. Soit $E = F(\alpha)$ une extension simple de F avec α transcendant sur F. Alors $E = \{f(\alpha)g(\alpha)^{-1} \mid f, g \in F[x], g \neq 0\} \cong F(x)$, le corps des fractions rationnelles.

Démonstration. Supposons que α est transcendant sur F. Comme $g(\alpha) \neq 0$ pour tout $g(x) \in F[x]$ non nul, $L = \{f(\alpha)g(\alpha)^{-1} \mid f, g \in F[x], g \neq 0\}$ est un sous-corps de E contenant F et α. Ceci implique $E = F(\alpha) \subseteq L$, et donc $E = \{f(\alpha)g(\alpha)^{-1} \mid f, g \in F[x], g \neq 0\}$. Or

$$\phi : F(x) \mapsto F(\alpha) : \frac{f(x)}{g(x)} \mapsto f(\alpha)g(\alpha)^{-1}$$

est un isomorphisme de corps. Ceci achève la démonstration.

2.2.5. Définition. Soit $\alpha \in E$ algébrique sur F. Un un polynôme monique $m(x)$ sur F dont α est racine s'appelle *polynôme minimal* de α sur F si le degré de $m(x)$ est minimal parmi les degrés des polynômes non nuls sur F dont α est racine.

Exemple. (1) Pour tout $a \in F,\ x - a$ est un polynôme minimal de a sur F.

(2) $\sqrt{2}$ est racine de $x^2 - 2 \in \mathbb{Q}[x]$ et il n'est pas racine d'un polynôme de degré 1 sur $\mathbb{Q}$ puisque $\sqrt{2} \notin \mathbb{Q}$. Donc $x^2 - 2$ est un polynôme minimal de $\sqrt{2}$ sur $\mathbb{Q}$.

2.2.6. Lemme. Soit $\alpha \in E$ algébrique sur F et $m(x)$ un polynôme minimal de α.

(1) $m(x)$ est irréductible sur F.

(2) S $f(x) \in F[x]$, alors $f(\alpha) = 0$ si, et seulement si, $m(x)|f(x)$.

Démonstratio. (1) Supposons au contraire que $m(x) = m_1(x)m_2(x)$ avec $m_i(x) \in F[x]$ et $0 < \partial(m_i(x)) < \partial(m(x))$. Comme $0 = m(\alpha) = m_1(\alpha)m_2(\alpha)$, on a $m_1(\alpha) = 0$ ou

$m_2(\alpha) = 0$. Ceci contredit la minimalité du degré de $m(x)$. Donc $m(x)$ est irréductible sur F.

(2) Pour tout $f(x) \in F[x]$, on a $f(x) = m(x)q(x) + r(x)$, où $q(x), r(x) \in F[x]$ avec $\partial(r(x)) < \partial(m(x))$. Si $m(x)|f(x)$, alors $r(x) = 0$ et $f(x) = m(x)q(x)$. Ainsi $f(\alpha) = m(\alpha)q(\alpha) = 0$. Supposons réciproquement que $f(\alpha) = 0$. Comme $m(\alpha) = 0$, on a $r(\alpha) = 0$. Il suit de la minimalité de $\partial(m(x))$ que $r(x) = 0$, et donc $m(x)|f(x)$. Ceci achève la démonstration.

2.2.7. Corollaire. Soit $\alpha \in E$ algébrique sur F.

(1) α admet un seul polynôme minimal sur F, noté $m_{_F}^{\alpha}(x)$.

(2) Si $p(x) \in F[x]$ est irréductible monique tel que $p(\alpha) = 0$, alors $m_{_F}^{\alpha}(x) = p(x)$.

Démonstration. (1) Soient $m_1(x), m_2(x)$ des polynômes minimaux de α sur F. D'après le lemme 2.2.6(2), $m_1(x)|m_2(x)$ et $m_2(x)|m_1(x)$. D'où, $m_1(x) = am_2(x)$ avec $a \in F$. Comme $m_1(x), m_2(x)$ sont tous moniques, on a $a = 1$, c'est-à-dire, $m_1(x) = m_2(x)$.

(2) D'après le lemme 2.2.6(2), $m_{_F}^{\alpha}(x)|p(x)$. Comme $p(x)$ est irréductible sur F, on a $p(x) = b\, m_{_F}^{\alpha}(x)$ avec $b \in F$. Comme $p(x), m_{_F}^{\alpha}(x)$ sont moniques, on a $b = 1$, et donc $m_{_F}^{\alpha}(x) = p(x)$. Ceci achève la démonstration.

On définit *degré* de α sur F comme étant le degré de son polynôme minimal sur F.

Exemple. Soit p un nombre premier. Considérons le nombre complexe

$$\zeta = \cos\frac{2\pi}{p} + i\sin\frac{2\pi}{p}.$$

Comme $\zeta^p = 1$, ζ est racine de $x^p - 1 = (x-1)(x^{p-1} + \cdots + x + 1)$. Comme $\zeta \neq 1$, on voit que ζ est racine de $\Phi_p(x)$ qui est monique. D'après du corollaire 1.4.7, $\Phi_p(x)$ est irréductible sur $\mathbb{Q}$. D'après le corollaire 2.2.7, $\Phi_p(x)$ est le polynôme minimal de ζ sur $\mathbb{Q}$. Ceci montre que ζ est de degré $p-1$ sur $\mathbb{Q}$.

2.2.8. Proposition. Soit L un corps intermédiaire entre F et E. Si $\alpha \in E$ est algébrique sur F, alors α est algébrique sur L avec $m_{_L}^{\alpha}(x)$ divisant $m_{_F}^{\alpha}(x)$ sur L.

Démonstration. Remarquons que $m_{_F}^{\alpha}(x)$ est un polynôme non nul sur L. Comme $m_{_F}^{\alpha}(\alpha) = 0$, on voit que α algébrique sur L. Et d'après le corollaire 2.2.6(2), $m_{_L}^{\alpha}(x)|m_{_F}^{\alpha}(x)$. Ceci achève la démonstration.

Exemple. Considérons les corps $\mathbb{Q} \subseteq \mathbb{R} \subseteq \mathbb{C}$ et $\alpha = \sqrt{1-\sqrt{2}} \in \mathbb{C}$. On voit aisément que α est racine de $x^2+\sqrt{2}-1 \in \mathbb{R}[x]$. N'ayant aucune racine réelle, $x^2+\sqrt{2}-1$ est irréductible sur $\mathbb{R}$. D'après le corollaire 2.2.7(2), $m_{_{\mathbb{R}}}^{\alpha}(x) = x^2+\sqrt{2}-1$. En outre, comme $(\alpha^2-1)^2 = 2$, on voit que α est racine de $x^4-2x^2-1 \in \mathbb{Q}[x]$. Comme $(x+1)^4-2(x+1)^2-1 = x^4+4x^3+4x^2-2$ est irréductible sur $\mathbb{Q}$, d'après le lemme 1.4.6, il en de même pour $x^4 - 2x^2 - 1$. Par

conséquent, $m_{\mathbb{Q}}^{\alpha}(x) = x^4 - 2x^2 - 1$. On vérifie $m_{\mathbb{R}}^{\alpha}(x) | m_{\mathbb{Q}}^{\alpha}(x)$ sur $\mathbb{R}$ par la factorisation $x^4 - 2x^2 - 1 = (x^2 + \sqrt{2} - 1)(x^2 - \sqrt{2} - 1)$.

2.2.9. Théorème. Soit $E = F(\alpha)$ une extension simple de F avec α algébrique sur F de degré n.

(1) $E \cong F[x]/(m_{F}^{\alpha}(x))$.

(2) $\{1, \alpha, \ldots, \alpha^{n-1}\}$ est une F-base de E. En particulier, $[E : F] = n$ et

$$E = \{a_0 + a_1\alpha + \cdots + a_{n-1}\alpha^{n-1} \mid a_i \in F\} = F[\alpha].$$

Démonstration. (1) D'abord, $F[\alpha] = \{f(\alpha) \mid f(x) \in F[x]\}$. Considérons l'application d'évaluation $\rho : F[x] \to F[\alpha] : f(x) \mapsto f(\alpha)$. Si $f(x) \in F[x]$, alors $f(x) \in \mathrm{Ker}(\rho)$ si, et seulement si, $f(\alpha) = 0$ si, et seulement si, $m_{F}^{\alpha}(x) | f(x)$. Par conséquent, $\mathrm{Ker}(\rho) = (m_{F}^{\alpha}(x))$. Comme ρ est surjectif, on a $F[\alpha] \cong F[x]/(m_{F}^{\alpha}(x))$. Comme $m_{F}^{\alpha}(x)$ est irréductible sur F d'après le corollaire 2.2.7(2), $F[x]/(m_{F}^{\alpha}(x))$ est un corps. Par conséquent, $F[\alpha]$ est un sous-corps de E contenant F et α. Donc $E = F(\alpha) \subseteq F[\alpha]$. Ainsi $E = F[\alpha]$.

(2) D'après l'hypothèse, $\partial(m_{F}^{\alpha}(x)) = n$. Si $a_0, a_1, \ldots, a_{n-1} \in F$ sont non tous nuls, alors α n'est pas racine de $a_0 + a_1x + \cdots + a_{n-1}x^{n-1}$ d'après la minimalité de $\partial(m_{F}^{\alpha}(x))$, c'est-à-dire, $a_0 \cdot 1 + a_1 \cdot \alpha + \cdots + a_{n-1} \cdot \alpha^{n-1} \neq 0$. Donc $\{1, \alpha, \ldots, \alpha^{n-1}\}$ est une famille libre sur F. Enfin, tout $\beta \in E$ s'écrit $\beta = f(\alpha)$ avec $f(x) \in F[x]$. Or $f(x) = m_{F}^{\alpha}(x)q(x) + r(x)$ où $q(x), r(x) \in F[x]$ avec $\partial(r(x)) < \partial(m_{F}^{\alpha}(x)) = n$. Écrivons $r(x) = b_0 + b_1x + \cdots + b_{n-1}x^{n-1}, b_i \in F$. Alors

$$\beta = f(\alpha) = m_{F}^{\alpha}(\alpha)q(\alpha) + r(\alpha) = b_0 \cdot 1 + b_1 \cdot \alpha + \cdots + b_{n-1} \cdot \alpha^{n-1}.$$

Donc $\{1, \alpha, \ldots, \alpha^{n-1}\}$ est une F-base de E. Ceci achève la démonstration.

Exemple. Considérons $\mathbb{Q}(\alpha)$, où

$$\alpha = -\frac{1}{2} + \frac{\sqrt{-3}}{2}.$$

On sait que $m_{\mathbb{Q}}^{\alpha}(x) = \Phi_3(x) = x^2 + x + 1$. Donc $\mathbb{Q}(\alpha) = \{a + b\alpha \mid a, b \in \mathbb{Q}\}$. Pour trouver $(\alpha + 4)^{-1}$, il faut trouver $u(x), v(x) \in \mathbb{Q}[x]$ tels que $(x+4)u(x) + \Phi_3(x)v(x) = 1$. En utilisant l'algorithme d'Euclid, on a

$$(x + 4)\frac{3 - x}{13} + \frac{1}{13}(x^2 + x + 1) = 1.$$

Donc

$$1 = (\alpha + 4)\frac{3 - \alpha}{13} + \frac{1}{13}(\alpha^2 + \alpha + 1) = (\alpha + 4)\frac{3 - \alpha}{13}.$$

D'où

$$(\alpha + 4)^{-1} = \frac{3}{13} - \frac{\alpha}{13}.$$

2.2.10. Corollaire. Les conditions suivantes sont équivalentes pour $\alpha \in E$:

(1) α est algébrique sur F.

(2) $[F(\alpha) : F]$ est fini.

(3) $F(\alpha)$ est algébrique sur F.

(4) $F(\alpha) = F[\alpha]$.

Démonstration. Il suit du théorème 2.2.9 que (1) implique (2). En outre, l'implication que (2) implique (3) suit de la proposition 2.1.8.

Si $F(\alpha)$ est algébrique sur F, en particulier, α l'est. Il suit du théorème 2.2.9 que $F(\alpha) = F[\alpha]$. Ceci montre que (3) implique (4).

Supposons enfin que $F(\alpha) = F[\alpha]$. Si $\alpha = 0$, alors α est évidemment algébrique sur F. Sinon, α est inversible et $\alpha^{-1} = f(\alpha)$ avec $f(x) \in F[x]$ non nul. Donc $\alpha f(\alpha) = 1$. Cela veut dire que α est racine de $g(x) = xf(x) - 1$, qui est clairement non nul. Donc α est algébrique sur F. Ceci montre que (4) implique (1). La preuve se termine.

Exemple. L'extension $\mathbb{R} : \mathbb{Q}$ n'est pas simple. En effet, supposons au contraire $\mathbb{R} = \mathbb{Q}(\alpha)$ avec $\alpha \in \mathbb{R}$. Si α est algébrique, alors $\mathbb{R} = \mathbb{Q}(\alpha)$ est algébrique sur $\mathbb{Q}$ d'après le corollaire 2.2.10, une contradiction au fait que π est transcendant sur $\mathbb{Q}$. Si α est transcendant sur $\mathbb{Q}$, alors $\mathbb{R} \cong \mathbb{Q}(x)$ d'après le théorème 2.2.4. Comme $\mathbb{Q}$ est dénombrable

$$\mathbb{Q}(x) = \left\{ \frac{a_0 + a_1 x + \cdots a_n x^n}{b_0 + b_1 x + \cdots + b_m x^m} \mid n, m \geq 0, a_i, b_j \in \mathbb{Q} \right\}$$

l'est aussi. Ceci implique que $\mathbb{R}$ est dénombrable, une contradiction. Donc $\mathbb{R}$ n'est pas simple sur $\mathbb{Q}$.

2.2.11. Théorème. L'extension $E : F$ est finie si, et seulement si, $E = F(\alpha_1, \ldots, \alpha_s)$ avec $\alpha_1, \ldots, \alpha_s$ algébriques sur F.

Démonstration. Supposons d'abord $[E : F] = n$. D'après la proposition 2.1.8, E est algébrique sur F. Soit $\{\alpha_1, \ldots, \alpha_n\}$ une base de E sur F. Alors tout $\beta \in E$ s'écrit comme $\beta = a_1\alpha_1 + \cdots + a_n\alpha_n$ avec $a_i \in F$, et donc $\beta \in F(\alpha_1, \ldots, \alpha_n)$. Ceci montre que $E = F(\alpha_1, \ldots, \alpha_n)$, où α_i sont algébriques sur F puisque E est algébrique sur F.

Supposons récipquement que $E = F(\alpha_1, \ldots, \alpha_s)$ avec les α_i algébriques sur F. Si $s = 1$, d'après le théorème 2.2.9, $[E : F]$ est égal au degré de α_1 sur F. Supposons que $s > 1$ et que $F(\alpha_1, \ldots, \alpha_{s-1})$ est fini sur F. D'après la proposition 2.2.8, α_s est algérique sur $F(\alpha_1, \ldots, \alpha_{s-1})$ et donc $E = F(\alpha_1, \ldots, \alpha_{s-1})(\alpha_s)$ est fini. Or il suit du théorème 2.1.5 que E est fini sur F. Ceci achève la démonstration.

2.2.12. Définition. On dit qu'un complexe α est un *nombre algébrique* si α est algébrique sur $\mathbb{Q}$.

Exemple. Les complexes $\sqrt{-1}$ et $\sqrt[3]{1-2\sqrt{5}}$ sont des nombres algébriques, mais 2π ne l'est pas.

2.2.13. Théorème. Les nombres algébriques forment un sous-corps de $\mathbb{C}$ qui est algébrique sur $\mathbb{Q}$.

Démonstration. Soit A l'ensemble des nombres algébriques de $\mathbb{C}$. Soient $\alpha, \beta \in A$ avec $\beta \neq 0$. D'après le théorème 2.2.11, $\mathbb{Q}(\alpha, \beta)$ est finie et donc algébrique sur $\mathbb{Q}$. Comme $\alpha - \beta, \alpha\beta, \alpha\beta^{-1} \in \mathbb{Q}(\alpha, \beta)$, on voit que $\alpha - \beta, \alpha\beta, \alpha\beta^{-1}$ sont algébriques sur $\mathbb{Q}$, c'est-à-dire, $\alpha - \beta, \alpha\beta, \alpha\beta^{-1} \in A$. Donc A est un sous-corps de $\mathbb{C}$. Ceci achève la démonstration.

2.3. Corps de rupture

Partout dans cette section, on se fixe F un corps. Un polynôme $f(x)$ sur F de degré $n > 0$ est dit *scindé sur* F si $f(x) = a(x - a_1) \cdots (x - a_n)$ avec $a, a_1, \ldots, a_n \in F$, c'est-à-dire, $f(x)$ admet exactement n racines dans F en comptant les multiplicités. On voit aisément si $f(x) = b(x - b_1) \cdots (x - b_n)$ avec $b, a_1, \ldots, a_n \in F$, alors $a = b$ and $\{a_1, \ldots, a_n\} = \{b_1, \ldots, b_n\}$.

Exemple. (1) Tout polynôme de degré 1 est scindé.

(2) Le polynôme $(x^2 + x + 1)(x + 1)$ sur $\mathbb{Z}_2$ n'est pas scindé sur $\mathbb{Z}_2$, car $x^2 + x + 1$ n'a pas de racine dans $\mathbb{Z}_2$.

2.3.1. Lemme. Soit $p(x) \in F[x]$ monique et irréductible. Alors il existe une extension simple $F(\alpha)$ de F telle que $p(x)$ soit polynôme minimal de α sur F.

Démonstration. Comme $p(x)$ irréductible, $L = F[x]/(p(x))$ est un corps. En identifiant $a \in F$ avec $\bar{a} \in L$, on a $F \subseteq L$. Soit $p(x) = a_0 + \cdots + a_{n-1}x^{n-1} + x^n$, et posons $\alpha = \bar{x} \in L$. Alors

$$\begin{aligned} p(\alpha) &= a_0 + \cdots + a_{n-1}\alpha^{n-1} + \alpha^n \\ &= \bar{a_0} + \cdots + \bar{a}_{n-1}\bar{x}^{n-1} + \bar{x}^n \\ &= \overline{a_0 + \cdots + a_{n-1}x^{n-1} + x^n} \\ &= \overline{p(x)} = 0. \end{aligned}$$

D'après le corollaire 2.2.7(2), $m_F^\alpha(x) = p(x)$. Enfin pour tout $\beta \in L$, $\beta = \overline{f(x)}$ avec $f(x) = b_0 + b_1x + \cdots + b_mx^m \in F[x]$. Donc

$$\begin{aligned} \beta &= \overline{b_0 + b_1x + \cdots + b_mx^m} \\ &= \bar{b}_0 + \bar{b}_1\bar{x} + \cdots + \bar{b}_m\bar{x}^m \\ &= b_0 + b_1\alpha + \cdots + b_m\alpha^m \in F(\alpha). \end{aligned}$$

Ainsi $L = F(\alpha)$ est une extension simple de F. Ceci achève la démonstration.

Remarque. Si $|F| = q$ et $\partial(p(x)) = n$, alors le degré de $F[x]/(p(x))$ sur F est n. Par conséquent, $|F[x]/(p(x))| = q^n$.

Exemple. On sait que $p(x) = x^2 + x + 1$ est irréductible sur $\mathbb{Z}_2$. Donc

$$L = \mathbb{Z}_2[x]/(p(x)) = \{0, 1, \alpha, \alpha + 1\} \quad \text{où} \quad \alpha = \bar{x},$$

est un corps. Remarquons que $\alpha^2 + \alpha + 1 = 0$. Les opérations de L sont données par les tableaux suivants:

$+$	0	1	α	$\alpha+1$
0	0	1	α	$\alpha+1$
1	1	0	$\alpha+1$	α
α	α	$\alpha+1$	0	1
$\alpha+1$	$\alpha+1$	α	1	0

$\times$	0	1	α	$\alpha+1$
0	0	0	0	0
1	0	1	α	$\alpha+1$
α	0	α	$\alpha+1$	1
$\alpha+1$	0	$\alpha+1$	1	α

Étant considéré comme un polynôme sur L, $p(x)$ admet α pour racine. En divisant $p(x)$ par $x - \alpha$, on trouve $x^2 + x + 1 = (x - \alpha)(x - (1 + \alpha))$. Donc $p(x)$ est scindé sur L.

2.3.2. Théorème de Kronecker. Si $f(x) \in F[x]$ est non constant, alors $f(x)$ est scindé sur une extension E de F.

Démonstration. Procédons par récurrence sur $n = \partial(f(x))$. Si $n = 1$, alors $f(x)$ est scindé sur F. Supposons que $n > 1$ et que l'énoncé est vraie pour $n - 1$. Prenons $p(x)$ un facteur irréductible de $f(x)$. D'après le lemme 2.3.1, il existe un corps $E_1 \supseteq F$ et $\alpha_1 \in E_1$ tels que $p(\alpha_1) = 0$, et donc $f(\alpha_1) = 0$. Par conséquent, $f(x) = (x - \alpha_1)g(x)$ avec $g(x) \in E_1[x]$. Comme $\partial(g(x)) = n - 1$, par l'hypothèse de récurrence, il existe un corps $E \supseteq E_1$ tel que $g(x) = a(x - \alpha_2) \cdots (x - \alpha_n)$ avec $\alpha_2, \ldots, \alpha_n \in E$. Ceci donne $f = a(x - \alpha_1)(x - \alpha_2) \cdots (x - \alpha_n)$, c'est-à-dire, $f(x)$ est scindé sur E. Ceci achève la démonstration.

2.3.3. Définition. Soit $f(x) \in F[x]$ non constant. Un corps E contenant F s'appelle un *corps de rupture sur* F lorsque les conditions suivantes sont vérifiées:

(1) $f(x)$ est scindé sur E, et

(2) si M est un corps avec $F \subseteq M \subseteq E$ sur lequel $f(x)$ est scindé, alors $M = E$.

Exemple. (1) Si $f(x) \in F[x]$ est scindé sur F, alors F est le seul corps de rupture de $f(x)$ sur F.

(2) Considérons $g(x) = x^3 - 1 \in \mathbb{Q}[x]$. Alors $g(x)$ est scindé sur $\mathbb{C}$, puisque

$$g(x) = (x - 1)\left(x + \frac{1}{2} - \frac{\sqrt{-3}}{2}\right)\left(x + \frac{1}{2} + \frac{\sqrt{-3}}{2}\right).$$

Mais $g(x)$ est également scindé sur $\mathbb{Q}(\sqrt{-3})$. Donc $\mathbb{C}$ n'est pas un corps de rupture de $g(x)$ sur $\mathbb{Q}$. D'autre part, si M est un corps avec $\mathbb{Q} \subseteq M \subseteq \mathbb{Q}(\sqrt{-3})$ sur lequel $g(x)$ est scindé, alors $-\frac{1}{2} + \frac{\sqrt{-3}}{2} \in M$, et donc $\sqrt{-3} \in M$. Ceci montre que $\mathbb{Q}(\sqrt{-3})$ est un corps de rupture de $g(x)$ sur $\mathbb{Q}$.

(3) Considérons encore $x^3 - 1 \in \mathbb{R}[x]$. Alors $x^3 - 1$ n'est pas scindé sur $\mathbb{R}$ et il est scindé sur $\mathbb{C}$. Donc $\mathbb{C}$ est un corps de rupture de $x^3 - 1$ sur $\mathbb{R}$ puisqu'il n'y a pas d'autre corps intermédiare entre $\mathbb{R}$ et $\mathbb{C}$.

(4) Dans l'exemple suivant le lemme 2.3.1, $L = \{0, 1, \alpha, \alpha + 1\}$ est un corps de rupture de $x^2 + x + 1$ sur $\mathbb{Z}_2$.

2.3.4. Lemme. Soit $f(x) \in F[x]$ non constant. Alors une extension E de F est un corps de rupture de $f(x)$ sur F si, et seulement si, les conditions suivantes sont vérifiées:

(1) $f(x) = a(x - \alpha_1) \cdots (x - \alpha_n),\ a \in F,\ \alpha_1, \ldots, \alpha_n \in E$, et

(2) $E = F(\alpha_1, \cdots, \alpha_n)$.

Démonstration. Supposons d'abord que les conditions sont vérifiées. Alors $f(x)$ est scindé sur E d'après (1). Si $f(x)$ est scindé sur un corps intemédiaire M entre F et E, alors $f(x) = a(x - \beta_1) \cdots (x - \beta_n), a \in F,\ \beta_j \in M$. Donc $\{\beta_1, \ldots, \beta_n\}$ est l'ensemble des racines de $f(x)$ dans E. Ceci implique $\{\beta_1, \ldots, \beta_n\} = \{\alpha_1, \ldots, \alpha_n\}$. Par conséquent, $E = F(\alpha_1, \ldots, \alpha_n) \subseteq M$, et donc $M = E$. Ceci montre que E est un corps de rupture de $f(x)$ sur F.

Supposons réciproquement que E est un corps de rupture de $f(x)$ sur F. Alors $f(x)$ est scindé sur E. Donc $f(x) = a(x - \alpha_1) \cdots (x - \alpha_n),\ a \in F,\ \alpha_1, \ldots, \alpha_n \in E$. Comme $F \subseteq F(\alpha_1, \cdots, \alpha_n) \subseteq E$, et $f(x)$ est scindé sur $F(\alpha_1, \cdots, \alpha_n)$, on a $E = F(\alpha_1, \cdots, \alpha_n)$ d'aprés la définition de corps de rupture. Ceci achève la démonstration.

Exemple. (1) Considérons $x^n - 1 = (x - \zeta_0)(x - \zeta_1) \cdots (x - \zeta_{n-1}) \in \mathbb{Q}[x]$, où

$$\zeta_k = \cos \frac{2k\pi}{n} + i \sin \frac{2k\pi}{n}, k = 0, 1, \ldots, n - 1.$$

Comme $\zeta_k = \zeta_1^k,$ pour tout $0 \leq k < n$, on voit que $\mathbb{Q}(\zeta_0, \zeta_1, \ldots, \zeta_{n-1}) = \mathbb{Q}(\zeta_1)$ est un corps de rupture de $x^n - 1$ sur $\mathbb{Q}$.

(2) $\mathbb{C}$ est un corps de rupture de $x^2 + 1$ sur $\mathbb{R}$. En effet, $x^2 + 1 = (x - i)(x + i)$ et $\mathbb{C} = \mathbb{R}(i, -i)$. Par contre, le corps de rupture de $x^2 + 1$ sur $\mathbb{Q}$ est $\mathbb{Q}(i)$. En effet, $x^2 + 1 = (x - i)(x + i)$ et $\mathbb{Q}(i) = \mathbb{Q}(i, -i)$.

2.3.5. Corollaire. Soit $f(x) \in F[x]$ non constant. Alors

(1) $f(x)$ admet un corps de rupture sur F.

(2) Tout corps de rupture de $f(x)$ sur F est fini sur F.

(3) Si E et E' sont des corps de rupture de $f(x)$ sur F tels que E et E' sont contenus dans un même corps L, alors $E = E'$.

Démonstration. (1) D'après le théorème de Kronecker, il existe un corps $L \supseteq F$ tel que $f(x) = a(x-\alpha_1)\cdots(x-\alpha_n), a \in F,\ \alpha_i \in L$. D'après le lemme 2.3.4, $E = F(\alpha_1, \cdots, \alpha_n)$ est un corps de rupture de $f(x)$ sur F.

(2) Soit E un corps de rupture de $f(x)$ sur F. Alors $f(x) = a(x-\alpha_1)\cdots(x-\alpha_n)$ et $E = F(\alpha_1, \ldots, \alpha_n)$. Comme chaque α_i est algébriques sur F, E est fini sur F d'après le théorème 2.2.11.

(3) Comme E est un corps de rupture de $f(x)$ sur F, $f(x) = a(x-\alpha_1)\cdots(x-\alpha_n),\ E = F(\alpha_1, \ldots, \alpha_n)$. De même $f(x) = a(x-\beta_1)\cdots(x-\beta_n),\ E' = F(\beta_1, \ldots, \beta_n)$. Comme $E \subseteq L$ et $E' \subseteq L$, on a $\{\alpha_1, \ldots, \alpha_n\} = \{\beta_1, \ldots, \beta_n\}$, et donc $E = F(\alpha_1, \ldots, \alpha_n) = F(\beta_1, \ldots, \beta_n) = E'$. Ceci achève la démonstration.

2.3.6. Définition. Soient E et L des extensions de F. On dit qu'un homomorphisme $\phi : E \to L$ est un F-homomorphisme si $\phi(a) = a,\ a \in F$ (c'est-à-dire, ϕ est une application linéaire de F-espaces vectoriels). De même, on définit F-isomorphisme et F-automorphisme.

Exemple. (1) $\mathbb{C} \to \mathbb{C} : a + bi \mapsto a - bi$ est un $\mathbb{R}$-automorphisme de $\mathbb{C}$.

(2) Soient E et E' des sous-corps de $\mathbb{C}$. Alors tout homomorphisme $\phi : E \to E'$ est un $\mathbb{Q}$-homomorphisme.

En effet, $\mathbb{Q} \subseteq E$ et $\mathbb{Q} \subseteq E'$. Comme $\phi(1) = 1$ par définition, on a $\phi(n) = n,$ pour tout $n \in \mathbb{Z}$. D'où, $\phi(\frac{n}{m}) = \frac{n}{m},$ pour tout $\frac{n}{m} \in \mathbb{Q}$.

(3) Le seul F-automorphisme de F est $\mathbb{1}_F$.

2.3.7. Lemme. Soient E et E' des extensions de F avec $E = F(\alpha_1, \ldots, \alpha_n)$. Soient $\phi, \psi : E \to E'$ des F-homomorphismes. Alors $\phi = \psi$ si, et seulement si, $\phi(\alpha_i) = \psi(\alpha_i),\ i = 1, \ldots, n$.

Démonstration. Il suffit de montrer la suffisance. Supposons $\phi(\alpha_i) = \psi(\alpha_i),\ i = 1, \ldots, n$. Comme F est un F-homomorphisme, on a $\phi(a) = a = \psi(a)$ pour tout $a \in F$. Donc pour tout $f = \sum a_{i_1,\ldots,i_n} x_1^{i_1} \cdots x_n^{i_n} \in F[x_1, \ldots, x_n]$ et $\beta = f(\alpha_1, \ldots, \alpha_n) \in E$, on a

$$\phi(\beta) = \sum \phi(a_{i_1,\ldots,i_n})\phi(\alpha_1)^{i_1} \cdots \phi(\alpha_n)^{i_n} = \sum \psi(a_{i_1,\ldots,i_n})\psi(\alpha_1)^{i_1} \cdots \psi(\alpha_n)^{i_n} = \psi(\beta).$$

En outre, si $\beta \neq 0$, alors $\phi(\beta^{-1}) = (\phi(\beta))^{-1} = (\psi(\beta))^{-1} = \psi(\beta^{-1})$. Comme

$$E = F(\alpha_1, \ldots, \alpha_n) = \left\{ \frac{f(\alpha_1, \ldots, \alpha_n)}{g(\alpha_1, \ldots, \alpha_n)} \mid f, g \in F[x_1, \ldots, x_n], g(\alpha_1, \ldots, \alpha_n) \neq 0 \right\},$$

on a $\phi(\alpha) = \psi(\alpha)$ pour tout $\alpha \in E$. Ceci achève la démonstration.

Rappelons que tout homomorphisme de corps $\phi : F \to F'$ induit un homomorphisme d'anneaux, noté encore ϕ, come suit:

$$\phi : F[x] \to F'[x] : \sum a_i x^i \mapsto \sum \phi(a_i) x^i.$$

2.3.8. Lemme. Soit $\phi : F \to F'$ un isomorphisme de corps. Soient $F(\alpha)$ et $F'(\alpha')$ des extensions algébriques simples de F et de F', respectivement. Alors, il existe un unique isomorphisme $\Phi : F(\alpha) \to F'(\alpha')$ tel que $\Phi|_F = \phi$ et $\Phi(\alpha) = \alpha'$ si, et seulement si, $\phi(m_F^\alpha(x)) = m_{F'}^{\alpha'}(x)$.

Démonstration. Supposons $\phi(m_F^\alpha(x)) = m_{F'}^{\alpha'}(x)$. Posons $I = (m_F^\alpha(x))$ et $I' = (m_{F'}^{\alpha'}(x))$. Alors $\phi^{-1}(I') = I$. Donc $\phi : F[x] \to F'[x]$ induit un isomorphisme de corps

$$\psi : F[x]/I \to F'[x]/I' : \overline{f} \mapsto \overline{\phi(f)}$$

tel que $\psi(x+I) = x+I'$ et $\psi(a+I) = \phi(a)+I'$ pour tout $a \in F$. D'après le théorème 2.2.9, on a des isomorphismes de corps:

$$F(\alpha) \to F[x]/I : f(\alpha) \mapsto \overline{f(x)} \quad \text{et} \quad F'[x]/I' \to F'(\alpha') : \overline{g(x)} \mapsto g(\alpha').$$

Donc $\Phi : F(\alpha) \to F'(\alpha') : f(\alpha) \mapsto (\phi(f))(\alpha')$ est un isomorphisme tel que $\Phi(\alpha) = \alpha'$ et $\Phi(a) = \phi(a)$ pour tout $a \in F$. L'unicité de Φ suit du lemme 2.3.7.

Supposons réciproquement que $\Phi : F(\alpha) \to F'(\alpha')$ est un isomorphisme tel que $\Phi(\alpha) = \alpha'$ et $\Phi(a) = \phi(a)$, pour tout $a \in F$. Posons $m_F^\alpha(x) = \sum_{i=0}^n a_i x^i$ et $g(x) = \phi(m_F^\alpha(x)) = \sum_{i=0}^n a_i' x^i$ avec $a_i' = \phi(a_i)$. Alors $g(x)$ est monique et irréductible sur F' puisque $m_F^\alpha(x)$ l'est sur F. En outre,

$$g(\alpha') = \sum a_i' \alpha'^i = \sum \Phi(a_i)\Phi(\alpha)^i = \Phi(\sum a_i \alpha^i) = \Phi(0) = 0.$$

D'où, $m_{F'}^{\alpha'}(x) = g(x)$. Ceci achève la démonstration.

2.3.9. Corollaire. Soient $F(\alpha)$ et $F(\beta)$ des extensions algébriques simples de F. Alors il existe un unique F-isomorphisme $\phi : F(\alpha) \to F(\beta)$ tel que $\phi(\alpha) = \beta$ si, et seulement si, α et β ont le même polynôme minimal sur F.

Exemple. (1) Le polynôme $x^4 - 2x^2 - 1 \in \mathbb{Q}[x]$ est irréductible dont $\alpha = \sqrt{1-\sqrt{2}}$ et $\beta = \sqrt{1+\sqrt{2}}$ sont racines. Donc α et β ont le même polynôme minimal sur $\mathbb{Q}$. Par conséquent, il existe un $\mathbb{Q}$-isomorphisme $\phi : \mathbb{Q}(\alpha) \to \mathbb{Q}(\beta)$ tel que $\phi(\alpha) = \beta$. Donc $\mathbb{Q}(\alpha) \cong \mathbb{Q}(\beta)$.

(2) $\mathbb{Q}(\sqrt{2}) \ncong \mathbb{Q}(\sqrt{3})$. En effet, si $\phi : \mathbb{Q}(\sqrt{2}) \to \mathbb{Q}(\sqrt{3})$ est un isomorphisme de corps, alors il est un $\mathbb{Q}$-isomorphisme. Posons $\gamma = \phi(\sqrt{2})$. Alors γ et $\sqrt{2}$ ont même polynôme minimal sur $\mathbb{Q}$, c'est-à-dire, $x^2 - 2$. Écrivons $\gamma = a + b\sqrt{3}$ avec $a, b \in \mathbb{Q}$. Alors $\gamma^2 =$

$\phi^2(\sqrt{2}) = \phi(\sqrt{2}^{\,2}) = \phi(2) = 2$. Si $a = 0$, alors $\sqrt{\frac{2}{3}}$ est rationnel, contradiction. Si $b = 0$, alors $\sqrt{2}$ est rationnel, contradiction. Si $ab \neq 0$, alors $\sqrt{3}$ est rationnel, contradiction.

2.3.10. Théorème. Soit $\phi : F \to F'$ un isomorphisme de corps. Soient $f(x) \in F[x]$ non constant et $g(x) = \phi(f) \in F'[x]$. Soient E et E' des corps de rupture de $f(x)$ sur F et de $g(x)$ sur F', respectivement. Alors il existe un isomorphisme $\Phi : E \to E'$ tel que $\Phi|_F = \phi$ et Φ envoie les racines de $f(x)$ sur celles de $g(x)$.

Démonstration. Posons $n = \partial f$. Si $n = 1$, alors $E = F$ et $E' = F'$. Donc on peut prendre $\Phi = \phi$. Supposons que $n > 1$ et que l'énoncé est vrai pour $n - 1$. Par l'hypothèse, $f(x) = a(x-\alpha_1)\cdots(x-\alpha_n)$ avec $a \in F$ et $E = F(\alpha_1, \ldots, \alpha_n)$; et $g(x) = a'(x-\beta_1)\cdots(x-\beta_n)$ avec $a' = \phi(a) \in F'$, $E' = F'(\beta_1, \ldots, \beta_n)$. Prenons $p(x)$ un facteur monique irréductible de $f(x)$, alors $q(x) = \phi(p(x))$ est un facteur monique irréductible de $g(x)$. On peut supposer $p(\alpha_1) = 0$ et $q(\beta_1) = 0$. Alors $m_F^{\alpha_1}(x) = p(x)$ et $m_{\beta_1}^{F'}(x) = q(x) = \phi(m_F^{\alpha_1}(x))$. D'après le lemme 2.3.8, il existe $\psi : F(\alpha_1) \to F'(\beta_1)$ tel que $\psi|_F = \phi$ et $\psi(\alpha_1) = \beta_1$. Posons $f_1(x) = a(x - \alpha_2)\cdots(x - \alpha_n)$. Comme $f(x) = (x - \alpha_1)f_1(x) \in F(\alpha_1)[x]$, on a $f_1(x) \in F(\alpha_1)[x]$. En outre, $E = F(\alpha_1)(\alpha_2, \ldots, \alpha_n)$. Donc E est un corps de rupture de $f_1(x)$ sur $F(\alpha_1)$. De même, E' est un corps de rupture de $g_1(x) = a'(x - \beta_2)\cdots(x - \beta_n)$ sur $F'(\beta_1)$. Comme

$$(x - \beta_1)g_1(x) = g = \phi(f) = \psi(f) = \psi((x - \alpha_1)f_1) = (x - \beta_1)\psi(f_1),$$

on voit que $g_1(x) = \psi(f_1(x))$. Par l'hypothèse de récurrence, il existe un isomorphisme de corps $\Phi : E \to E'$ tel que $\Phi|_{F(\alpha_1)} = \psi$ et $\{\Phi(\alpha_2), \ldots, \Phi(\alpha_n)\} = \{\beta_2, \ldots, \beta_n\}$. Par conséquent, $\Phi|_F = \psi|_F = \phi$ et $\{\Phi(\alpha_1), \Phi(\alpha_2), \ldots, \Phi(\alpha_n)\} = \{\beta_1, \beta_2, \ldots, \beta_n\}$. Ceci achève la démonstration.

2.3.11. Corollaire. Tout polynôme non constant sur F admet un corps de rupture sur F, qui est unique à F-isomorphisme près.

2.4. Corps algébriquement clos

2.4.1. Définition. On dit qu'un corps F est *algébriquement clos* si tout polynôme non constant sur F est scindé dans $F[x]$.

Exemple. Le corps $\mathbb{C}$ est algébriquement clos, mais $\mathbb{R}$ ne l'est pas. En effet, $x^2 + 1$ n'est pas scindé sur $\mathbb{R}$.

2.4.2. Théorème. Soit F un corps. Les conditions suivantes sont équivalentes:
(1) F est algébriquement clos.

(2) Tout polynôme non constant sur F admet une racine dans F.

(3) Tout polynôme irréductible sur F est de degré 1.

(4) F est la seule extension algébrique de lui-même.

(5) F est la seule extension finie de lui-même.

Démonstration. Les implications que (1) implique (2), que (2) implique (3) suivent immédiatement de la définition.

Supposons que (3) est valide. Soit E une extension algébrique de F. Pour tout $\alpha \in E$, $m_F^\alpha(x)$ est irréducitible sur F. Par (3), $\partial(m_F^\alpha(x)) = 1$. Donc $[F(\alpha) : F] = 1$, c'est-à-dire, $\alpha \in F$. Ceci montre $E = F$.

Supposons que (4) est valide. Si E est une extension finie de F, alors E est une extension algébrique de F d'après la proposition 2.1.8. Donc $E = F$ par (4).

Supposons enfin que (5) est valide. Soit $f(x) \in F[x]$ non constant. Prenons E un corps de rupture de $F(x)$ sur F. D'après le corollaire 2.3.5, l'extension $E : F$ est finie. Donc $E = F$ par (5). Cela veut dire que $f(x)$ est scindé sur F. Par conséquent, F est algébriquement clos. Ceci achève la démonstration.

Remarque. Bien qu'un corps F soit algébriquement clos, $F(x)$ est une extension propre de F.

Exemple. Le corps des nombres algébriques A est algébriquement clos. En effet, soit $f(x) = \sum_{i=0}^{n} a_i x^i \in A[x]$. Alors $f(x) \in \mathbb{Q}(a_0, \ldots, a_n)[x]$. Comme les a_i sont algébriques sur $\mathbb{Q}$, d'après le théorème 2.2.11, $\mathbb{Q}(a_0, \ldots, a_n)$ est fini sur $\mathbb{Q}$. Comme $\mathbb{C}$ est algébriquement clos, $f(x)$ admet une racine α dans $\mathbb{C}$. En particulier, α est algébrique sur $\mathbb{Q}(a_0, \ldots, a_n)$, et donc $\mathbb{Q}(a_0, \ldots, a_n)(\alpha)$ est fini sur $\mathbb{Q}(a_0, \ldots, a_n)$. D'après le théorème 2.1.5, $\mathbb{Q}(a_0, \ldots, a_n, \alpha)$ est fini sur $\mathbb{Q}$. Par conséquent, α est algébrique sur $\mathbb{Q}$, c'est-à-dire, $\alpha \in A$. D'après le théorème 2.4.2, A est algébriquement clos.

2.4.3. Définition. Soit F un corps. On dit qu'une extension E de F est une *clôture algébrique* de F si

(1) E est algébrique sur F.

(2) E est algébriquement clos.

Exemple. (1) $\mathbb{C}$ est une clôture algébrique de $\mathbb{R}$, mais non de $\mathbb{Q}$ puisque $\mathbb{C}$ n'est pas algébrique sur $\mathbb{Q}$.

(2) Le corps des nombres algébriques A est une clôture algébrique de $\mathbb{Q}$. En effet, A est algébriquement clos et A est algébrique sur $\mathbb{Q}$ par définition.

On accepte sans preuve le résultat important suivant.

2.4.4. Théorème. Tout corps F admet une clôture algébrique qui est unique à F-isomorphisme près.

2.5. Racines multiples

On se fixe F un corps. Soit $f(x) \in F[x]$ dont a est racine. On sait que $x-a$ divise $f(x)$ sur F. On dit que a est une *racine multiple* si $(x-a)^2$ divise $f(x)$ sur $F[x]$; et *racine simple* sinon.

2.5.1. Proposition. Soit $f(x) \in F[x]$ non constant. S'il existe un corps de rupture de $f(x)$ sur F dans lequel $f(x)$ n'a pas de racine multiple, alors $f(x)$ n'a pas de racine multiple dans toute extension de F. Dans ce cas, on dit $f(x)$ n'a pas de racine multiple.

Démonstartion. Supposons que L est un corps de rupture de $f(x)$ sur F et $f(x) = a(x-\alpha_1)\cdots(x-\alpha_n),\ \alpha_i \in L,\ \alpha_i \neq \alpha_j$ lorsque $i \neq j$. Soit E une extension de F. Prenons E' un corps de rupture de $f(x)$ sur E. Ainsi $f(x) = a(x-\beta_1)\cdots(x-\beta_n),\ \beta_j \in E'$. Remarquons que $F(\beta_1,\ldots,\beta_n)$ est aussi un corps de rupture de $f(x)$ sur F. D'après le théorème 2.3.10, il existe un F-isomorphisme $\phi : L = F(\alpha_1,\ldots,\alpha_n) \to F(\beta_1,\ldots,\beta_n)$ tel que $\{\phi(\alpha_1),\ldots,\phi(\alpha_n)\} = \{\beta_1,\ldots,\beta_n\}$. Comme ϕ est bijectif, les $\phi(\alpha_i)$ sont deux à deux distincts, c'est-à-dire, les β_i sont deux à deux distincts. Donc $f(x)$ n'a pas de racine multiple dans E'. En particulier, $f(x)$ n'a pas de racine multiple dans E. Ceci achève la démonstration.

2.5.2. Définition. Soit $f(x) = a_0 + a_1x + \cdots + a_nx^n \in F[x]$. On appelle *dérivée* de $f(x)$, notée $D(f)$, le polynôme $a_1 + 2a_2x + \cdots + na_nx^{n-1}$.

Le résultat suivant est évident.

2.5.3. Lemme. Soient $f(x), g(x) \in F[x]$. Alors
(1) $D(f+g) = D(f) + D(g)$.
(2) $D(fg) = fD(g) + gD(f)$.
(3) Pour tout $a \in F$, on a $D(a) = 0$ et $D(af) = aD(f)$.

Remarque. Même si $D(f) = 0$, f n'est pas nécessairement un constant. Par exemple, sur le corps $\mathbb{Z}_2$, on a $D(x^2) = 2x = 0$.

2.5.4. Lemme. Soient E une extension de F et soient $f(x), g(x) \in F[x]$. Alors f et g sont co-premiers sur F si, et seulement si, ils sont co-premiers sur E.

Démonstraion. La suffisance est évidente. Supposons que $f(x)$ et $g(x)$ sont co-premiers sur F. Alors il existe $u(x), v(x) \in F[x]$ tels que $f(x)u(x) + g(x)v(x) = 1$. D'où, $f(x), g(x)$ sont co-premiers sur E. Ceci achève la démonstration.

2.5.5. Proposition. Soit $f(x) \in F[x]$ non constant. Alors $f(x)$ n'a pas de racine multiple si, et seulement si, f et $D(f)$ sont co-premiers sur F.

Démonstration. Soit E un corps de rupture de f sur F. Si f a une racine multiple $\alpha \in E$, alors $f(x) = (x-\alpha)^2 g(x)$ avec $g \in E[x]$. Comme $D(f) = 2(x-\alpha)g + (x-\alpha)^2 D(g)$, on voit que f et $D(f)$ ne sont pas co-premiers sur E. D'après le lemme 2.5.4, f et $D(f)$ ne sont pas co-premiers sur F.

Supposons réciproquement qu'il existe $d(x) \in F[x]$ non constant tel que $d|f$ et $d|D(f)$. Comme f est scindé sur E, $d(x)$ a une racine $\alpha \in E$. Alors $x-\alpha \,|\, f$ et $x-\alpha \,|\, D(f)$. Posons $f(x) = (x-\alpha)h(x)$ avec $h \in E[x]$. Alors $D(f) = h(x) + (x-\alpha)D(h)$. Comme $x-\alpha \,|\, D(f)$, on a $x-\alpha | h(x)$, et donc $(x-\alpha)^2 | f(x)$. Cela veut dire que f a une racine multiple. Ceci achève la démonstration.

2.6. Corps finis

2.6.1. Lemme. Soit F un corps avec $\mathrm{car}(F) = p > 0$. Alors pour tout $a, b \in F$, on a

$$(a \pm b)^p = a^p \pm b^p.$$

Démonstration. Soient $a, b \in F$. D'abord, $p \cdot a = (p \cdot 1_F)a = 0_F$, et $p \cdot b = 0_F$. Or

$$(a+b)^p = a^p + \sum_{i=1}^{p-1} \binom{p}{i} a^{p-i} b^i + b^p.$$

Comme p est premier, $p \,|\, \binom{p}{i}$, pour tout $1 \leq i \leq p-1$. Donc $(a+b)^p = a^p + b^p$. En outre, si p est impaire, alors $(-b)^p = -b^p$ et si $p = 2$, alors $(-b)^p = b^p = -b^p$. Donc $(-b)^p = -b^p$ en tous cas. Par conséquent, $(a-b)^p = [a + (-b)]^p = a^p + (-b)^p = a^p - b^p$. Ceci achève la démonstration.

Remarque. Si $\mathrm{car}(F) = p > 0$, alors l'application

$$\phi : F \to F : a \mapsto a^p$$

est un homomorphisme de corps, appelé l'*application de Frobenius*.

2.6.2. Lemme. Soit F un corps fini. Si E est une extension finie de F, alors E est fini avec $|E| = |F|^{[E:F]}$.

Démonstration. Prenons une base $\{\alpha_1, \ldots, \alpha_n\}$ de E sur F. Alors l'application

$$\theta : \overbrace{F \times \cdots \times F}^{n \quad \text{fois}} \to E : (a_1, \ldots, a_n) \mapsto a_1\alpha_1 + \cdots + a_n\alpha_n$$

est bijective. Par conséquent $|E| = |\overbrace{F \times \cdots \times F}^{n \text{ fois}}| = |F|^n$. Ceci achève la démonstration.

On sait que pour tout entier $n > 0$, il existe un groupe d'ordre n ainsi qu'un anneau d'ordre n. On se demande si c'est vrai aussi pour des corps finis. La réponse est non.

2.6.3. Proposition. Soit F un corps fini. Alors $|F| = p^n$, où $p = \text{car}(F)$ est un nombre premier et n est le degré de F sur son corps premier P.

Démonstration. D'abord, P est fini car F est fini. D'après le théorème 1.2.7, $\text{car}(F) = p$ est un nombre premier et $P \cong \mathbb{Z}_p$. Ainsi $|P| = p$. D'autre part, $n = [F : P]$ est fini car F est fini. Il suit maintenant du lemme 2.6.2 que $|F| = p^n$. Ceci achève la démonstration.

2.6.4. Lemme. Soient F un corps fini et P son corps premier. Si $|F| = q$, alors F est un corps de rupture de $x^q - x$ sur P.

Démonstration. Remarquons que $F^* = F\backslash\{0\}$ est un groupe d'ordre $q - 1$. Pour tout $\beta \in F^*$, on a $\beta^{q-1} = 1$, et donc $\beta^q = \beta$. Ainsi tout $\beta \in F$ est une racine de $x^q - x$. Posons $F = \{\beta_1, \ldots, \beta_q\}$ avec les β_j deux à deux distincts. Alors $x - \beta_i \,|\, x^q - q$, pour tout $1 \leq i \leq q$. Comme les $x - \beta_j$ sont deux à deux distincts, ils sont deux à deux co-premiers. Ainsi $(x - \beta_1) \cdots (x - \beta_q) \,|\, x^q - x$. Par conséquent, $x^q - x = (x - \beta_1) \cdots (x - \beta_q)$. En outre, on voit aisément que $F = P(\beta_1, \ldots, \beta_q)$. Donc F est un corps de rupture de $x^q - x$ sur P. Ceci achève la démonstration.

2.6.5. Théorème. Soient p un premier et n un entier. Alors il existe un corps de cardinal p^n qui est unique à isomorphisme près.

Démonstration. Prenons F un corps de rupture de $x^{p^n} - x$ sur $\mathbb{Z}_p$. Alors $\text{car}(F) = p$. D'après le lemme 2.6.1, $L = \{\alpha \in F \mid \alpha^{p^n} = \alpha\}$, l'ensemble des racines de $x^{p^n} - x$ dans F, est un sous-corps de F. Comme $D(x^{p^n} - x) = -1$ est premier à $x^{p^n} - x$, le polynôme $x^{p^n} - x$ n'a pas de racine multiple d'après la proposition 2.5.5. Par conséquent, $|L| = p^n$. Comme $x^{p^n} - x$ est scindé sur L et F est le corps de rupture de $x^{p^n} - x$ sur $\mathbb{Z}_p$, on a $L = F$. Donc $|F| = p^n$.

Soit E un corps avec $|E| = p^n$. D'après la proposition 2.6.3, $|E| = q^s$ avec $q = \text{car}(E)$. Comme $q^s = p^n$, on a $q = p$, et donc $s = n$. Soit P le corps premier de E. Alors $P \cong \mathbb{Z}_p$. D'après le lemme 2.6.4, E est un corps de rupture de $x^{p^n} - x$ sur P. D'après le théorème 2.3.10, $L \cong F$. Ceci achève la démonstration.

Pour $a \in G$, désignons par $o(a)$ l'ordre de a.

2.6.6. Lemme. Soit G un groupe abélian fini ayant pour identité e.
(1) Si $a \in G$ avec $o(a) = n$, alors $o(a^r) = \frac{n}{(n,r)}$ pour tout $r \geq 1$.

(2) Si $a, b \in G$ tels que $(o(a), o(b)) = 1$, alors $o(ab) = o(a)o(b)$.

(3) Soit $n = \max\{o(a) \mid a \in G\}$. Alors $b^n = e$, pour tout $b \in G$.

Démonstration. (1) Posons $d = (n, r)$. Alors $n = n_1 d, r = r_1 d$ avec $(n_1, r_1) = 1$. Posons $o(a^r) = t$. Comme $(a^r)^{n_1} = a^{nr_1} = e$, on a $t \mid n_1$. D'autre part, comme $a^{rt} = (a^r)^t = e$, on a $n \mid rt$. D'où, $n_1 \mid r_1 t$. Ainsi $n_1 \mid t$ car $(n_1, r_1) = 1$. Par conséquent, $t = n_1$.

(2) Posons $o(a) = r$, $o(b) = s$, et $o(ab) = t$. Comme $(ab)^{rs} = (a^r)^s(b^s)^r = e$, on a $t \leq rs$. En outre, comme $(ab)^t = e$, on a $a^t = b^{-t}$, et donc $a^{st} = (b^s)^{-t} = e$. Ainsi $r \mid st$, et donc $r \mid t$ car r et s sont co-premiers. De même, $s \mid t$. D'où $rs \mid t$ car $(r, s) = 1$. Ainsi $rs \leq t$, et donc $rs = t$.

(3) Supposons $o(a) = n$. Supposons qu'il existe $b \in G$ tel que $o(b) = m \not| n$, alors il existe un premier q tel que $n = q^r n_1$ et $m = q^s m_1$, où $0 \leq r < s$ et $q \not| n_1$ et $q \not| m_1$. Posons $a_1 = a^{q^r}$ et $b_1 = b^{m_1}$. D'après (1), $o(a_1) = n_1$ et $o(b_1) = q^s$. D'après (2), $o(a_1 b_1) = q^s n_1 > q^r n_1 = n$, une contradiction à la maximalité de n. Ceci achève la démonstration.

2.6.7. Théorème. Si F est un corps fini, alors le groupe multiplicatif $F^* = F\backslash\{0\}$ de F est cyclique.

Démonstration. Soit $|F| = q$. Alors F^* est un groupe d'ordre $q-1$. Prenons $\alpha \in F^*$ tel que $n = o(\alpha)$ soit le plus grand parmi les ordres des éléments de F^*. Alors $n \leq |F^*| = q - 1$, et d'après 2.6.6(3), $\beta^n = 1$, pour tout $\beta \in F^*$. Donc $x^n - 1$ admet $q - 1$ racines distinctes dans F. Par conséquent, $q - 1 \leq n$, et donc $n = q - 1$. C'est-à-dire, $o(\alpha) = |F^*|$ et donc $< \alpha >= F^*$. Ceci achève la démonstration.

2.6.8. Corollaire. Toute extension finie d'un corps fini est simple.

Démonstration. Soient F un corps fini et E une extension finie de F. D'après le lemme 2.6.2, E est fini. D'après le théorème 2.6.7, il existe $\alpha \in E$ tel que $E^* =< \alpha >$. On voit aisément que $E = F(\alpha)$. Ceci achève la démonstration.

2.7. Extensions séparables

Partout dans cette section, on se fixe F un corps.

2.7.1. Définition. Soit $f(x) \in F[x]$ irréductible. On dit que $f(x)$ est *séparable* si $f(x)$ n'a pas de racine multiple; et *inséparable* sinon.

Exemple. Le polynôme $x^2+x+1 \in \mathbb{Z}_2[x]$ est séparable car $x^2+x+1 = (x-\alpha)(x-\alpha-1)$ sur le corps $L = \{0, 1, \alpha, \alpha + 1\}$.

2.7.2. Proposition. Soit $f(x) \in F[x]$ irréductible. Alors les conditions suivantes sont équivalentes:

(1) $f(x)$ est inséparable.

(2) $D(f) = 0$.

(3) $\mathrm{car}(F) = p > 0$ et il existe $g(x) \in F[x]$ tel que $f(x) = g(x^p)$.

Démonstration. D'abord, si $\mathrm{car}(F) = p > 0$ alors, pour tous $a \in F^*$ et $n \in \mathbb{Z}$, on a $na = 0$ si, et seulement si, $p \,|\, n$.

Supposons que $f(x)$ est inséparable, c'est-à-dire, f a une racine multiple. D'après la proposition 2.5.5, f et $D(f)$ ne sont pas co-premiers. Comme f est irréductible, on a $f \,|\, D(f)$. Ainsi $D(f) = 0$ puisque $\partial(D(f)) < \partial(f)$.

Posons $f(x) = a_0 + a_1 x + \cdots + a_n x^n$, où $n > 0$ et $a_n \in F^*$. Et supposons que $D(f) = 0$, c'est-à-dire, $ia_i = 0$, pour tout $1 \leq i \leq n$. Comme $a_n \neq 0$ et $n > 0$, on a $\mathrm{car}(F) = p > 0$ et $a_i = 0$ pour tout i tel que $p \not| i$. Cela veut dire que $f(x) = \sum_{0 \leq j \leq \frac{n}{p}} a_{jp}\, x^{pj}$. Ainsi

$$g(x) = \sum\nolimits_{0 \leq j \leq \frac{n}{p}} a_{jp}\, x^j \in F[x]$$

est tel que $f(x) = g(x^p)$.

Supposons enfin que (3) est valide. Alors $D(f) = 0$, et donc f et $D(f)$ ne sont pas co-premiers. D'après la proposition 2.5.5, f admet des racines multiples, c'est-à-dire, f est inséparable. Ceci achève la démonstration.

Remarque. Si $\mathrm{car}(F) = 0$, alors tout polynôme irréductible sur F est séparable.

2.7.3. Lemme. Supposons que $\mathrm{car}(F) = p > 0$. Posons $F^p = \{a^p \,|\, a \in F\}$. Si $a \in F \backslash F^p$, alors $x^p - a$ est irréductibe sur F, et donc inséparable.

Démonstration. Prenons E le corps de rupture de $x^p - a$ sur F. Alors il existe $\alpha \in E$ tel que $\alpha^p - a = 0$. Comme $\mathrm{car}(E) = \mathrm{car}(F) = p$, d'après le lemme 2.6.1, $x^p - a = x^p - \alpha^p = (x - \alpha)^p$. Supposons que $x^p - a$ est réductible sur F, c'est-à-dire, $x^p - a = f(x)g(x)$, où $f, g \in F[x]$ avec $0 < \partial(f) < p$. Sur le corps E, on a $f(x)g(x) = (x - \alpha)^p$. Donc $f(x) = (x - \alpha)^d$ avec $0 < d < p$. Ceci donne $\alpha^d \in F$. Comme p est premier, il existe $s, t \in \mathbb{Z}$ tels que $ps + dt = 1$. Donc $\alpha = \alpha^{ps+dt} = (\alpha^p)^s(\alpha^d)^t = a^s(\alpha^d)^t \in F$, puisque $\alpha^d \in F$. Donc $a = \alpha^p \in F^p$, une contradiction. Ceci achève la démonstration.

2.7.4. Définition. Soit $E : F$ une extension de corps.

(1) On dit que $\alpha \in E$ est *séparable* sur F si α est algébrique sur F et son polynôme minimal sur F est séparable.

(2) On dit que $E : F$ est *séparable* (ou bien, que E est *séparable* sur F) si tous les éléments de E sont séparables sur F.

Remarque. (1) Un corps F est séparable sur lui-même.

(2) Soient $F \subseteq L \subseteq E$ des corps. Si $E : F$ est séparable, alors $L : F$ l'est aussi.

Exemple. Toute extension algébrique de $\mathbb{Q}$ est séparable.

2.7.5. Théorème. Toute extension finie séparable de corps est simple.

Démonstration. Soit $E : F$ une extension finie et séparable de corps. Si F est fini, alors l'extension $E : F$ est simple d'après le corollaire 2.6.7.

Supposons maintenant que F est infini. On sait que $E = F(\alpha_1, \ldots, \alpha_n)$, où les $\alpha_i \in E$ sont algébriques sur F. Le résultat est trivial si $n = 1$. Supposons que $n > 1$ et l'énoncé est vrai pour $n - 1$. Remarquons que $F(\alpha_1, \ldots, \alpha_{n-1})$ est fini et séparable sur F. Par l'hypothèse de récurrence, $F(\alpha_1, \ldots, \alpha_{n-1}) = F(\beta)$ pour certain $\beta \in F(\alpha_1, \ldots, \alpha_{n-1})$. Donc $E = F(\beta, \alpha_n)$. Prenons $\bar{E}$ une clôture algébrique de E. Comme E est séparable sur F, on a

$$m_F^{\beta}(x) = (x - \beta_1) \cdots (x - \beta_s),\ \beta_1 = \beta,\ \beta_i \in \bar{E},\ \beta_i \neq \beta_j \text{ lorsque } i \neq j,$$

$$m_F^{\alpha_n}(x) = (x - \gamma_1) \cdots (x - \gamma_t),\ \gamma_1 = \alpha_n,\ \gamma_i \in \bar{E},\ \gamma_i \neq \gamma_j \text{ lorsque } i \neq j.$$

Comme F est infini, il existe $a \in F$ tel que $a \neq \frac{\beta_1 - \beta_i}{\gamma_1 - \gamma_j}$, pour tous $1 \leq i \leq s,\ 1 < j \leq t$. Posons $\alpha = \beta_1 - a\gamma_1 = \beta - a\alpha_n \in E$. Alors $F(\alpha) \subseteq E = F(\beta, \alpha_n)$.

Considérons $g(x) = m_F^{\beta}(\alpha + ax) \in F(\alpha)[x]$. Alors $g(\alpha_n) = m_F^{\beta}(\alpha + a\alpha_n) = m_F^{\beta}(\beta) = 0$. Donc $m_{F(\alpha)}^{\alpha_n}(x) |\ g(x)$. Pour tout $1 < j \leq t$, on a $\alpha + a\gamma_j \neq \beta_i$, pour tout $1 \leq i \leq s$. Donc $g(\gamma_j) = m_F^{\beta}(\alpha + a\gamma_j) \neq 0$. Donc $x - \gamma_j \nmid g(x),\ 1 < j \leq t$. Ceci implique $x - \gamma_j \nmid m_{F(\alpha)}^{\alpha_n}(x)$, pour tout $1 < j \leq t$. Or comme $m_{F(\alpha)}^{\alpha_n}(x) |\ m_F^{\alpha_n}(x)$, on a $m_{F(\alpha)}^{\alpha_n}(x) = x - \gamma_1 = x - \alpha_n$. Par conséquent, $\alpha_n \in F(\alpha)$, et donc $\beta = \alpha - a\alpha_n \in F(\alpha)$. Cela implique $E = F(\beta, \alpha_n) \subseteq F(\alpha)$, et donc $E = F(\alpha)$. Ceci achève la démonstration.

2.7.6. Défintion. On dit que F est *parfait* si tout polynôme irréductible sur F est séparable.

Exemple. Tout corps algébriquement clos est parfait.

2.7.7. Théorème. Soit F un corps.
(1) Si $\mathrm{car}(F) = 0$, alors F est parfait.
(2) Si $\mathrm{car}(F) = p > 0$, alors F est parfait si, et seulement si, $F = F^p$.

Démonstration. L'énoncé (1) suit immédiatement de la proposition 2.7.2. Considérons maintenant le cas où $\mathrm{car}(F) = p > 0$. Si $F \neq F^p$, alors il existe $a \in F \backslash F^p$. D'après le lemme 2.7.3, $x^p - a$ est irréductible sur F qui est inséparable. Donc F n'est pas parfait.

Supposons réciproquement que F n'est pas parfait. Alors il existe $f(x) \in F[x]$ qui est irréductible sur F et inséparable. D'après la proposition 2.7.2, $f(x) = g(x^p)$ avec $g(x) = \sum_{i=0}^{s} a_i x^i \in F[x]$. Si $F = F^p$, alors $a_i = b_i^p,\ b_i \in F$. Donc

$$f(x) = g(x^p) = \sum\nolimits_{i=0}^{s} b_i^p (x^p)^i = \sum\nolimits_{i=0}^{s} (b_i x^i)^p = \Big(\sum\nolimits_{i=0}^{s} b_i x^i\Big)^p$$

est réductible sur F, une contradiction. Donc $F \neq F^p$. Ceci achève la démonstration.

Exemple. Tout corps de nombres est parfait.

2.7.8. Corollaire. Tout corps fini est parfait.

Démonstration. Supposons que F est fini. Alors $\text{car}(F) = p > 0$ et $\phi : F \to F : a \mapsto a^p$ est un homomorphisme. Donc ϕ est injectif. Comme F est fini, ϕ est bijectif. Par conséquent, $F = F^p$. D'après le théorème 2.7.7, F est parfait. Ceci achève la démonstration.

Le résultat suivant suit immédiatement du théorème 2.7.5.

2.7.9. Théorème. Soit F un corps parfait. Alors toute extension finie de F est simple sur F.

Exemple. Toute extension finie de corps de nombres est simple.

2.8. Extensions normales

Partout dans cette section, on se fixe une extension de corps $E : F$.

2.8.1. Définition. On dit que l'extension $E : F$ est *normale* (ou bien, que E est *normal* sur F) si, pour tout polynôme irréductible $p(x)$ sur F, soit $p(x)$ n'a aucune racine dans E soit $p(x)$ est scindé sur E.

Remarque. Une extension normale n'est pas nécessairement algébrique.

Exemple. (1) F est normal sur lui-même.
(2) $\mathbb{C} : \mathbb{Q}$ est normale car tout polynôme irréductible sur $\mathbb{Q}$ est scindé sur $\mathbb{C}$.
(3) $\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}$ n'est pas normale. En effet, considérons le polynôme irréductible rationnel $f(x) = x^3 - 2$. On voit que $f(x)$ a une racine $\sqrt[3]{2}$ dans $\mathbb{Q}(\sqrt[3]{2})$, mais il n'est pas scindé sur $\mathbb{Q}(\sqrt[3]{2})$ (car les autres racines sont $-\frac{\sqrt[3]{2}}{2} - i\frac{\sqrt[3]{2}}{2}$ et $-\frac{\sqrt[3]{2}}{2} + i\frac{\sqrt[3]{2}}{2}$ qui ne sont pas réels).

2.8.2. Lemme. Soit $E : F$ normale. Si $\alpha \in E$ est algébrique sur F, alors $m_F^\alpha(x)$ est scindé sur E.

Démonstration. Le polynôme minimal $m_F^\alpha(x)$ de α sur F est irréductible sur F et admet une racine α dans E. D'après la définition de normalité, $m_F^\alpha(x)$ est scindé sur E. Ceci achève la démonstration.

2.8.3. Théorème. L'extension $E : F$ est normale et finie si, et seulement si, E est le corps de rupture d'un polynôme sur F.

Démonstration. Supposons que $E : F$ est normale et finie. Alors $E = F(\alpha_1, \ldots, \alpha_n)$, où les α_i sont algébrique sur F. D'après le lemme 2.8.2, $m_F^{\alpha_i}(x) = (x - \alpha_{i1}) \cdots (x - \alpha_{is_i})$, où $\alpha_{ij} \in E$ et $\alpha_{i1} = \alpha_i$. Alors

$$m_F^{\alpha_1}(x) \cdots m_F^{\alpha_n}(x) = (x - \alpha_{11}) \cdots (x - \alpha_{1s_1}) \cdots (x - \alpha_{n1}) \cdots (x - \alpha_{ns_n}),$$

et

$$E \supseteq F(\alpha_{11}, \ldots, \alpha_{1s_1}, \ldots, \alpha_{n1}, \ldots, \alpha_{ns_n}) \supseteq F(\alpha_1, \ldots, \alpha_n) = E.$$

D'où, $E = F(\alpha_{11}, \ldots, \alpha_{1s_1}, \ldots, \alpha_{n1}, \ldots, \alpha_{ns_n})$. Par conséquent, E est un corps de rupture de $m_F^{\alpha_1}(x) \cdots m_F^{\alpha_n}(x)$ sur F.

Supposons réciproquement qu'il existe $f(x) \in F[x]$ dont le corps de rupture sur F est E. D'après le corollaire 2.3.5, l'extension $E : F$ est finie. Soit $p(x)$ un polynôme irréductible monique sur F ayant une racine $\alpha \in E$. Soit L le corps de rupture de $p(x)f(x)$ sur E. Alors $p(x)$ est scindé sur L. Prenons $\beta \in L$ une racine de $p(x)$. Alors $m_F^{\beta}(x) = m_F^{\alpha}(x) = p(x)$. D'après le corollaire 2.3.9, il existe un F-isomorphisme $\phi : F(\alpha) \to F(\beta)$ tel que $\phi(\alpha) = \beta$.

Comme E est un corps de rupture de $f(x)$ sur F, $E(\alpha)$ et $E(\beta)$ sont des corps de rupture de $f(x)$ sur $F(\alpha)$ et sur $F(\beta)$, respectivement. Remarquons que $\phi(f(x)) = f(x)$. D'après le lemme 2.3.8, il existe un isomorphisme $\Phi : E(\alpha) \to E(\beta)$ tel que $\Phi|_{F(\alpha)} = \phi$. Par conséquent, $[E(\alpha) : F(\alpha)] = [E(\beta) : F(\beta)]$. Mais $[F(\beta) : F] = \partial p(x) = [F(\alpha) : F]$. Donc

$$[E(\beta) : F] = [E(\beta) : F(\beta)][F(\beta) : F] = [E(\alpha) : F(\alpha)][F(\alpha) : F] = [E(\alpha) : F],$$

c'est-à-dire, $[E(\beta) : E][E : F] = [E(\alpha) : E][E : F]$. Ainsi $[E(\beta) : E] = [E(\alpha) : E] = 1$ car $\alpha \in E$. Par conséquent, $\beta \in E$. Ceci montre que E contient toutes les racines de $p(x)$ dans L, c'est-à-dire, $p(x)$ est scindé sur E. Donc E est normal sur F. Ceci achève la démonstration.

2.8.4. Proposition. Si E est fini sur F, alors il existe une extension N de E telle que N est fini et normal sur F.

Démonstration. Comme $E : F$ est finie, $E = F(\alpha_1, \ldots, \alpha_n)$, où les α_i sont algébriques sur F. Posons $f(x) = m_F^{\alpha_1}(x) \cdots m_F^{\alpha_n}(x)$, et prenons N un corps de rupture de $f(x)$ sur E. Alors on peut écrire $m_F^{\alpha_i}(x) = (x - \alpha_{i1}) \cdots (x - \alpha_{is_i})$, $\alpha_{i1} = \alpha_i$, $i = 1, \ldots, n$, et

$$\begin{aligned} N &= E(\alpha_{11}, \ldots, \alpha_{1s_1}, \ldots, \alpha_{n1}, \ldots, \alpha_{ns_n}) \\ &= F(\alpha_1, \ldots, \alpha_n, \alpha_{11}, \ldots, \alpha_{1s_1}, \ldots, \alpha_{n1}, \ldots, \alpha_{ns_n}) \\ &= F(\alpha_{11}, \ldots, \alpha_{1s_1}, \ldots, \alpha_{n1}, \ldots, \alpha_{ns_n}). \end{aligned}$$

Donc N est un corps de rupture de $f(x)$ sur F. D'après le théorème 2.8.3, l'extension $N : F$ est finie et normale. Ceci achève la démonstration.

2.9. Exercices

1. Soit $E : F$ une extension de corps. Soit $m(x) \in F[x]$ monique dont $\alpha \in E$ est une racine. Si $\partial(m(x)) = [F(\alpha) : F]$, montrer que $m(x)$ est le polynôme minimal de α sur F.

2. Trouver le degré de chacune des extensions suivantes:

   (1) $\mathbb{Q}(3, \sqrt{5}, \sqrt{11}) : \mathbb{Q}$. (2) $\mathbb{Q}(\alpha) : \mathbb{Q}$ avec $\alpha \in \mathbb{C}$ tel que $\alpha^7 = 3$.

3. Montrer que les extensions de $\mathbb{Q}$ suivantes sont simples:

   (1) $\mathbb{Q}(\sqrt{5}, \sqrt{7})$; (2) $\mathbb{Q}(\sqrt{2}, \sqrt[3]{3})$.

4. Montrer qu'une extension de corps de degré premier est simple.

5. Trouver le polynôme minimal de $\alpha = \sqrt{2 + \sqrt[3]{2}}$ sur $\mathbb{Q}(\sqrt{2})$. *Indication*:

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

6. Considerer $\mathbb{Q}(\alpha)$, où $\alpha = \sqrt{2 + \sqrt[3]{2}}$. Trouver l'inverse $\alpha^4 - \alpha^2 + 2\alpha - 1$.

7. Montrer que $\sqrt{\pi}$ et $\pi^3 + \sqrt{\pi} + 1$ ne sont pas des nombres algébriques.

8. Trouver un corps de rupture de $x^2 - x - 1$ sur $\mathbb{Z}_3 = \{0, 1, -1\}$ en donnant les tables d'addition et de multiplication.

9. Trouver le corps de rupture de $x^6 - 16$ sur $\mathbb{Q}$.

10. Soient E, L, F des corps avec $F \subseteq L \subseteq E$. Montrer que l'extension $E : F$ est algébrique si, et seulement si, les extensions $E : L$ et $L : F$ sont toutes algébriques.

11. (1) Montrer, pour tout $n \geq 1$, qu'il existe un nombre complexe α dont le degré sur $\mathbb{Q}$ est égal à n.

    (2) Si A est le corps des nombres algébriques, montrer que A est de degré fini sur $\mathbb{Q}$. *Indication*: utiliser la première partie.

12. Soit $E : F$ une extension de corps avec E algébriquement clos. Si L est l'ensemble des éléments de E qui sont algébrique sur F, montrer que L est une clôture algébrique de F.

13. Soient F, E, L des corps avec $F \subseteq E \subseteq L$. Si E est un corps de rupture d'un polynôme $f(x)$ sur F, montrer que $E(S)$ avec $S \subseteq L$ est un corps de rupture de $f(x)$ sur $F(S)$.

14. Soit $E = F(\alpha)$ une extension simple d'un corps F avec α transcendant sur F. Montrer que $\beta \in E$ est algébrique sur F si et seulement si $\beta \in F$. *Indication*: Si $\beta = f(\alpha)/g(\alpha) \notin F$ est algébrique sur F, montrer que $[E : F(\beta)]$ est fini en consiérant $f(\alpha) = \beta g(\alpha)$.

15. Soit p un nombre premier. Soit E la clôture algébrique de $\mathbb{Z}_p$. Montrer les énoncés suivants.

    (1) Il existe, pour tout $n \geq 1$, exactement un sous-corps P_n de E de cardinal p^n tels que $E = \cup_{n=1}^{\infty} P_n$. *Indication*: Vérifier que P_n est l'ensemble des racines de $x^{p^n} - x$ dans E.

    (2) Il existe, pour tout $n \geq 1$, un polynôme irréductible sur $\mathbb{Z}_p$ de degré n. *Indication*: Appliquer le corollaire 2.6.8 au corps P_n trouvé en partie (1).

16. Soit $f(x)$ un polynôme non constant de degré n sur un corps F. Si E est un corps de rupture de $f(x)$ sur F, montrer que $[E : F]$ divise $n!$. *Indication*: Procécéder par recurrence. Soit $p(x)$ un facteur monique irréductible de $f(x)$ de degré r. Au cas où $r < n$, considérer le corps de rupture E_1 de $p(x)$ sur F contenu dans E et vérifier que E est le corps de rupture de $f(x)p(x)^{-1}$ sur E_1. Appliquer l'hypothèse de réccurence deux fois à ces corps de rupture. Remarquer que $\binom{n}{m}$ est un entier.

17. Soit $F(\alpha)$ une extension algébrique simple d'un corps F.

    (1) Montrer que tout corps intermédiaire M compris entre F et $F(\alpha)$ est engendré par les coefficients du polynône minimal de α sur M.

    (2) Montrer qu'il n'y a qu'un nombre fini des corps intermédiaire compris entre F et $F(\alpha)$.

18. Soit F un corps. Trouver la condition sur un entier positif n pour que $x^n - 1$ n'ait pas de racine multiple. *Indication*: Considérer séparément les cas où la caractéristique de F est nulle et non nulle.

19. Si f, g sont des polynômes sur un corps F, montrer que $D(fg) = D(f)g + fD(g)$.

20. Parmi les polynômes $x^3 + 1$, $x^2 + 2x - 1$, $x^6 + x^5 + x^4 + x^3 + x^2 + x + 1$, lesquels sont séparables si l'on les considère comme des polynômes sur $\mathbb{Q}$ et $\mathbb{Z}_2$, respectivement?

21. Si E est une extension finie et séparable d'un corps F, montrer le nombre de corps intermédiaires entre F et E est fini ou infini.

22. Soit F un corps de caractéristique $p > 0$. Si $a \in F \backslash F^p$, montrer que $x^{p^n} - a$ est irréductible sur F pour tout $n \geq 0$. *Indication*: Comparer avec le lemme 2.7.3.

23. Soit F un corps parfait. Montrer que toute extension algébrique E de F est parfaite. *Indication*: Si $\alpha \in E \backslash E^p$, considérer $x^p - \alpha$.

24. Soit $E : F$ une extension de corps avec E algébriquement clos de caractéristique $p > 0$. Montrer que

$$M = \{\alpha \in E \mid \alpha^{p^n} \in F \text{ pour un certain } n \geq 0\}$$

est le plus petit sous-corps parfait de E contenant F.

25. Soit F un corps de caractéristique $p > 0$. Montrer que le corps des fractions rationnelles $F(x)$ n'est pas parfait. *Indication*: Montrer qu'il n'existe pas $\alpha \in F(x)$ tel que $x = \alpha^p$.

26. Dans chacun des cas suivants, déterminer si l'extension est normale ou non:

(1) $\mathbb{Q}(\sqrt[7]{5}) : \mathbb{Q}$. (2) $\mathbb{Q}(\sqrt{5}, \sqrt[7]{5}) : \mathbb{Q}$.

(3) $\mathbb{Q}(\sqrt{-5}) : \mathbb{Q}$. (4) $\mathbb{Q}(x) : \mathbb{Q}$.

27. Montrer que toute extension de corps de degré 2 est normale.

Chapitre III: Théorie de Galois

3.1. Groupes de Galois

On se fixe $E : F$ une extension de corps partout dans cette section.

3.1.1. Proposition. Les F-automorphismes de E forment un groupe, appelé le *groupe de Galois* de l'extension $E : F$ et noté $G(E/F)$.

Démonstration. D'abord, $\mathbb{1}_E \in G(E/F)$. Soient $\phi, \psi \in G(E/F)$. Alors $\phi\psi$ et ϕ^{-1} sont des automorphismes de E tels que pour tout $a \in F$, $(\phi\psi)(a) = \phi(\psi(a)) = \phi(a) = a$ et $\phi^{-1}(a) = \phi^{-1}(\phi)(a)) = (\phi^{-1}\phi)(a) = \mathbb{1}_E(a) = a$. Donc $\phi\psi$ et $\phi^{-1} \in G(E/F)$. Ceci achève la démonstration.

Exemple. On a $G(F/F) = \{\mathbb{1}_F\}$.

3.1.2. Lemme. Soit $f(x) \in F[x]$ non constant. Alors chaque $\phi \in G(E/F)$ induit une permutation sur l'ensemble S (peut-être vide) des racines de $f(x)$ dans E.

Démonstration. Supposons $S \neq \emptyset$. Posons $f(x) = \sum_{i=0}^{n} a_i x^i$. Pour tout $\alpha \in S$, on a

$$f(\phi(\alpha)) = \sum_{i=0}^{n} a_i(\phi(\alpha))^i = \sum_{i=0}^{n} \phi(a_i)\phi(\alpha^i) = \phi(f(\alpha)) = \phi(0) = 0,$$

c'est-à-dire, $\phi(\alpha) \in S$. Comme ϕ est bijectif sur E et S est fini, ϕ est bijectif sur S. Ceci achève la démonstration.

Remarque. Si ρ est une permutation sur S, il n'y a pas nécessairement un $\phi \in G(E/F)$ tel que $\phi|_S = \rho$. Par exemple, les racines de $(x^2-2)(x^2-3)$ dans $E = \mathbb{Q}(\sqrt{2}, \sqrt{3})$ sont $\sqrt{2}, -\sqrt{2}, \sqrt{3}, -\sqrt{3}$, mais il n'y a pas $\phi \in G(E/\mathbb{Q})$ tel que $\phi(\pm\sqrt{2}) = \pm\sqrt{3}$ et $\phi(\pm\sqrt{3}) = \pm\sqrt{2}$ car $\sqrt{3}$ n'est pas racine de $x^2 - 2$.

Rappelons que si $E = F(\alpha_1, \ldots, \alpha_n)$, alors $\phi \in G(E/F)$ est déterminé par $\phi(\alpha_1), \ldots, \phi(\alpha_n)$.

Exemple. (1) Considérons l'extension $\mathbb{C} : \mathbb{R}$. On a $\mathbb{1}_C$ et $\sigma : \mathbb{C} \to \mathbb{C} : a + bi \mapsto a - bi$ sont dans $G(\mathbb{C}/\mathbb{R})$. Soit $\phi \in G(\mathbb{C}/\mathbb{R})$. D'après le lemme 3.1.2, $\phi(i) = \pm i$. Si $\phi(i) = i$, alors $\phi = \mathbb{1}_C$ et si $\phi(i) = -i$, alors $\phi = \sigma$. Ceci nous donne $G(\mathbb{C}/\mathbb{Q}) = \{\mathbb{1}_C, \sigma\}$.

(2) Considérons l'extension $\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}$. On sait que $\sqrt[3]{2}$ est la seule racine de $x^3 - 2$ dans $\mathbb{Q}(\sqrt[3]{2})$. Si $\phi \in G(\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q})$, alors $\phi(\sqrt[3]{2}) = \sqrt[3]{2}$, et donc $\phi = \mathbb{1}_{\mathbb{Q}(\sqrt[3]{2})}$. Par conséquent, $G(\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}) = \{\mathbb{1}_{\mathbb{Q}(\sqrt[3]{2})}\}$.

3.1.3. Proposition. Soit H un sous-groupe de $G(E/F)$. Alors

$$E^H = \{\alpha \in E \mid \phi(\alpha) = \alpha, \text{ pour tout } \phi \in H\}$$

est un corps intermédiaire entre F et E, appelé le *corps fixe* de H.

Démonstration. Si $a \in F$, alors $\phi(a) = a$, pour tout $\phi \in H$. D'où $F \subseteq E^H$. Si $\alpha, \beta \in E^H$, alors pour tout $\phi \in H$, $\phi(\alpha - \beta) = \phi(\alpha) - \phi(\beta) = \alpha - \beta$, et $\phi(\alpha\beta) = \phi(\alpha)\phi(\beta) = \alpha\beta$. En outre, $\phi(\alpha^{-1}) = (\phi(\alpha))^{-1}$ lorsque $\alpha \neq 0$. Donc $\alpha - \beta, \alpha\beta \in E^H$ et $\alpha^{-1} \in E^H$ si $\alpha \neq 0$. Par conséquent, E^H est un sous-corps de E. Ceci achève la démonstration.

Exemple. (1) $E^{\{\mathbb{1}_E\}} = E$.

(2) Considérons l'extension $\mathbb{C} : \mathbb{R}$ et $H = G(\mathbb{C}/\mathbb{R}) = \{\mathbb{1}_C, \sigma\}$. Alors $\alpha \in \mathbb{C}^H$ si, et seulement si, $\sigma(\alpha) = \alpha$ si, et seulement si, $\bar{\alpha} = \alpha$ si, et seulement si, $\alpha \in \mathbb{R}$. Donc $\mathbb{C}^{G(C/R)} = \mathbb{R}$.

(3) Considérons l'extension $\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}$. On a vu que $G(\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}) = \{\mathbb{1}_{Q(\sqrt[3]{2})}\}$. Donc

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

3.1.4. Lemme. Si H_1 et H_2 sont des sous-groupes de $G(E/F)$ avec $H_1 \subseteq H_2$, alors $E^{H_2} \subseteq E^{H_1}$.

Démonstration. Si $\alpha \in E^{H_2}$, alors $\phi(\alpha) = \alpha$, pour tout $\phi \in H_2$. En particulier, $\phi(\alpha) = \alpha$, pour tout $\phi \in H_1$. D'où $\alpha \in E^{H_1}$. Ceci achève la démonstration.

3.1.5. Proposition. (1) Si M est un corps intermédiaire entre F et E, alors $G(E/M)$ est un sous-groupe de $G(E/F)$.

(2) Si M_1 et M_2 sont des corps intermédiaire entre F et E avec $M_1 \subseteq M_2$, alors $G(E/M_2) \subseteq G(E/M_1)$.

Démonstration. (1) Soit $\phi \in G(E/M)$. Alors $\phi(\alpha) = \alpha$, pour tout $\alpha \in M$. En particulier, $\phi(a) = a$, pour tout $a \in F$. Donc $\phi \in G(E/F)$.

(2) Comme M_2 est un corps intermédiaire entre M_1 et E, d'après (1), $G(E/M_2)$ est un sous-groupe de $G(E/M_1)$. Ceci achève la démonstration.

3.1.6. Proposition. (1) Si M est un corps intermédiaire entre F et E, on a alors $M \subseteq E^{G(E/M)}$.

(2) Si H est un sous-groupe de $G(E/F)$, alors $H \subseteq G(E/E^H)$.

(3) Pour tout sous-groupe H de $G(E/F)$ et tout corps intermédiaire M entre F et E,

$$E^H = E^{G(E/E^H)},\ G(E/M) = G(E/E^{G(E/M)}).$$

Démonstration. (1) Soit $\alpha \in M$. Alors pour tout $\phi \in G(E/M)$, $\phi(\alpha) = \alpha$, c'est-à-dire, $\alpha \in E^{G(E/M)}$. Donc $M \subseteq E^{G(E/M)}$.

(2) Soit $\psi \in H$. Pour tout $\alpha \in E^H$, on a $\psi(\alpha) = \alpha$, c'est-à-dire, $\psi \in G(E/E^H)$. D'où, $H \subseteq G(E/E^H)$.

(3) D'après (2), on a $H \subseteq G(E/E^H)$, et donc $E^{G(E/E^H)} \subseteq E^H$ d'après la proposition 3.1.5(2). En outre, $E^H \subseteq E^{G(E/E^H)}$ d'après (1). Donc $E^H = E^{G(E/E^H)}$. De même, $G(E/M) = G(E/E^{G(E/M)})$. Ceci achève la démonstration.

Exemple. (1) Considérons l'extension $\mathbb{C} : \mathbb{Q}$. On sait $G(\mathbb{C}/\mathbb{R}) = \{\mathbb{1}_{\mathbb{C}}, \sigma\}$. On voit que $\mathbb{R} = \mathbb{C}^{G(\mathbb{C}/\mathbb{R})}$ et $\mathbb{C} = \mathbb{C}^{G(\mathbb{C}/\mathbb{C})}$.

(2) Considérons l'extension $E : \mathbb{Q}$ avec $E = \mathbb{Q}(\sqrt[3]{2})$. On sait $G(E/\mathbb{Q}) = \{\mathbb{1}\} = G(E/E)$. Donc $E^{G(E/\mathbb{Q})} = E$. Par conséquent, $\mathbb{Q} \subset E^{G(E/\mathbb{Q})}$.

3.2. Groupe de Galois de polynômes

Partout dans cette section, on se fixe F un corps. Soit $f(x) \in F[x]$ non constant dont E est le corps de rupture sur F. Alors le groupe $G(E/F)$ s'appelle le *groupe de Galois* de $f(x)$ sur F.

3.2.1. Définition. Soit $f(x) \in F[x]$ non constant. On dit que $f(x)$ est *séparable* sur F si tout facteur irréductible sur F de $f(x)$ n'a pas de racines multiples.

Exemple. Le polynôme rationnel $x^2 - 2x + 1$ est séparable sur $\mathbb{Q}$, bien qu'il ait une racine multiple.

Remarque. Si F est parfait, alors tout polynôme non constant sur F est séparable.

3.2.2. Lemme. Soit $f(x) \in F[x]$ séparable. Alors

(1) Tout facteur non constant de $f(x)$ sur F est séparable sur F.

(2) $f(x)$ est séparable sur toute extension E de F.

Démonstartion. L'énoncé (1) est trivial.

(2) Soit $d(x)$ un facteur irréductible de $f(x)$ sur E. Écrivons $f(x) = p_1(x) \cdots p_s(x)$ avec $p_i(x) \in F[x]$ irréductible. On a $d(x) \,|\, p_1(x) \cdots p_s(x)$ sur E. Étant irréductible sur E, $d(x) \,|\, p_i(x)$ pour un $1 \leq i \leq s$. Comme $p(x)$ n'a pas de racine multiples, $d(x)$ n'en a pas non plus. Ceci achève la démonstration.

3.2.3. Théorème. Soit $\phi : F \to L$ un isomorphisme de corps. Soient $f(x) \in F[x]$ dont E est un corps de rupture sur F et $g(x) = \phi(f(x)) \in L[x]$ dont M est un corps de rupture

sur L. Si $f(x)$ est séparable, alors le nombre d'isomorphismes $\Phi : E \to M$ tel que $\Phi|_F = \phi$ est égal à $[E : F]$.

Démonstration. Procédons sur $n = [E : F]$. Si $n = 1$, alors on n'a qu'un seul choix $\Phi = \phi$. Supposons que $n > 1$ et que l'énoncé est vrai pour $n-1$. Remarquons qu'il existe une racine α de $f(x)$ dans E qui n'est pas dans F. Alors $m_F^\alpha(x)$ est séparable car $m_F^\alpha(x)|f(x)$; et $\partial(m_F^\alpha(x)) = s > 1$ car $\alpha \notin F$. En outre, $l(x) = \phi(m_F^\alpha(x))$ est un facteur monique irréductible séparable de $g(x)$. Donc $l(x) = (x - \beta_1) \cdots (x - \beta_s)$, où $\beta_i \in M$ sont tels que $\beta_i \neq \beta_j$ lorsque $i \neq j$.

On se fixe un j avec $1 \leq j \leq s$. Alors $m_{\beta_j}^L(x) = l(x) = \phi(m_F^\alpha(x))$. D'après le lemme 2.3.8, il existe un unique isomorphisme $\psi_j : F(\alpha) \to L(\beta_j)$ tel que $\psi_j|_F = \phi$ et $\psi_j(\alpha) = \beta_j$. Maintenant $f(x) = (x - \alpha)h(x)$ avec E un corps de rupture de $h(x)$ sur $F(\alpha)$. De même, $g(x) = (x - \beta_j)h_j(x)$ et M est un corps de rupture de $h_j(x)$ sur $L(\beta_j)$. Comme $f(x)$ est séparable sur F, d'après le lemme 3.2.2, $h(x)$ est séparable sur $F(\alpha)$. Comme $(x-\beta_j)h_j(x) = \phi(f(x)) = \psi_j(f(x)) = (x - \beta_j)\psi_j(h(x))$, on a $h_j(x) = \psi_j(h(x))$. Posant $t = [E : F(\alpha)]$, on a

$$t = \frac{[E : F]}{[F(\alpha) : F]} = \frac{n}{s} < n.$$

D'après l'hypothèse de récurrence, il existe exactement t isomorphismes $\psi_{j1}, \ldots, \psi_{jt} : E \to M$ tels que $\psi_{ji}|_{F(\alpha)} = \psi_j$, et donc $\psi_{ji}|_F = \psi_j|_F = \phi$, pour tout $1 \leq i \leq t$. Comme les β_j sont deux à deux distincts, les ψ_j sont 2 à 2 distincts. Par conséquent, les ψ_{ji} avec $1 \leq j \leq s$ et $1 \leq i \leq t$ sont n isomorphismes distincts qui prolongent ϕ.

D'autre part, soit $\Phi : E \to M$ un isomorphisme tel que $\Phi|_F = \phi$. En particulier, $\Phi(m_F^\alpha(x)) = l(x)$. Ainsi $\beta = \Phi(\alpha)$ est une racine de $l(x)$. Donc $\beta = \beta_j$ pour un certain j avec $1 \leq j \leq s$. Par conséquent, $\Phi|_{F(\alpha)} = \psi_j$. Donc $\Phi = \psi_{ji}$, pour un $1 \leq i \leq t$. Ceci achève la preuve.

3.2.4. Théorème. Soit $f(x)$ un polynôme séparable sur F et soit E un corps de rupture de $f(x)$ sur F.

(1) $|G(E/F)| = [E : F]$.

(2) $E^{G(E/F)} = F$.

Démonstration. En appliquant le théorème 3.2.3 au cas où $\phi = \mathbb{1}_F$, on voit que (1) est valid. Pour montrer (2), posons $M = E^{G(E/F)} \supseteq F$. D'après la proposition 3.1.6(3), on a $G(E/F) = G(E/E^{G(E/F)}) = G(E/M)$. Comme $f(x)$ est séparable sur M d'après le lemme 3.2.2(2), et E est un corps de rupture de $f(x)$ sur M, il suit de (1) que

$$[E : M] = |G(E/M)| = |G(E/F)| = [E : F] = [E : M][M : F].$$

D'où $[M : F] = 1$, c'est-à-dire, $F = M = E^{G(E/F)}$. Ceci achève la démonstration.

Remarque. Le résultat précedent n'est pas valid si $f(x)$ n'est pas séparable. Par exemple, supposons que $\text{car}(F) = p > 0$ et $a \in F \backslash F^p$. D'après le lemme 2.7.3, $x^p - a$ est irréductible. Soit E le corps de rupture de $x^p - a$ sur F. Alors $E = F(\alpha)$ et donc $[E : F] = p$. De l'autre côté, on a $G(E/F) = \{\mathbb{1}_E\}$ et $E^{G(E/F)} = E$.

Exemple. Trouver le groupe de Galois de $f(x) = (x^2 - 2)(x^2 - 3)$ sur $\mathbb{Q}$.

Solution. $E = \mathbb{Q}(\sqrt{2}, \sqrt{3})$ est un corps de rupture de $f(x)$ sur $\mathbb{Q}$. Comme $\sqrt{3} \notin \mathbb{Q}(\sqrt{2})$, on a $x^2 - 3$ est irréductible sur $\mathbb{Q}(\sqrt{2})$. Donc $m_{\sqrt{3}}^{\mathbb{Q}(\sqrt{2})}(x) = x^2 - 3$. D'où, $[\mathbb{Q}(\sqrt{2}, \sqrt{3}) : \mathbb{Q}(\sqrt{2})] = 2$. Ainsi $[E : \mathbb{Q}] = [\mathbb{Q}(\sqrt{2}, \sqrt{3}) : \mathbb{Q}(\sqrt{2})][\mathbb{Q}(\sqrt{2}) : \mathbb{Q}] = 4$. Comme $\mathbb{Q}$ est parfait, $f(x)$ est séparable sur $\mathbb{Q}$. D'après le théorème 3.2.4, on a $|G(E/\mathbb{Q})| = 4$.

Remarquons maintenant que $\sqrt{3}$ et $-\sqrt{3}$ ont même polynôme minimal $x^2 - 3$ sur $\mathbb{Q}(\sqrt{2})$. Donc il existe un $\mathbb{Q}(\sqrt{2})$-isomorphisme $\phi : \mathbb{Q}(\sqrt{2})(\sqrt{3}) \to \mathbb{Q}(\sqrt{2})(-\sqrt{3})$ tel que $\phi(\sqrt{3}) = -\sqrt{3}$. Mais $\mathbb{Q}(\sqrt{2})(\sqrt{3}) = \mathbb{Q}(\sqrt{2})(-\sqrt{3}) = E$. Donc $\phi \in G(E/\mathbb{Q})$ tel que $\phi(\sqrt{2}) = \sqrt{2}$ et $\phi(\sqrt{3}) = -\sqrt{3}$. De même, il existe $\psi \in G(E/\mathbb{Q})$ tel que $\psi(\sqrt{2}) = -\sqrt{2}$, $\psi(\sqrt{3}) = \sqrt{3}$. On a alors $\phi\psi \in G(E/\mathbb{Q})$ tel que $\phi\psi(\sqrt{2}) = -\sqrt{2}$ et $\phi\psi(\sqrt{3}) = -\sqrt{3}$. On en déduit $G(E/\mathbb{Q}) = \{\mathbb{1}, \phi, \psi, \psi\phi\}$.

3.3. Extensions de Galois

Partout dans cette section, on se fixe $E : F$ une extension de corps.

3.3.1. Définition. On dit que $E : F$ est une *extension galoisienne*, ou bien E est *galoisien* sur F, si elle est finie, normale et séparable.

Remarque. D'après le théorème 2.7.5, toute extension galoisienne est simple.

Exemple. (1) L'extension $F : F$ est galoisienne.
(2) L'extension $\mathbb{C} : \mathbb{R}$ est galoisienne.

3.3.2. Lemme. Une extension finie $E : F$ est galoisienne si, et seulement si, pour tout $\alpha \in E$, on a $m_F^\alpha(x) = (x - \alpha_1) \cdots (x - \alpha_n)$, avec $\alpha_1, \ldots, \alpha_n \in E$ deux à deux distincts.

Démonstration. Supposons que $E : F$ est normale et séparable. Si $\alpha \in E$, alors $m_F^\alpha(x)$ est irréductible ayant une racine $\alpha \in E$. D'après la normalité, $m_F^\alpha(x) = (x - \alpha_1) \cdots (x - \alpha_n)$, avec $\alpha_1, \ldots, \alpha_n \in E$. Il suit de la séparabilité que les α_i sont deux à deux distincts.

Supposons réciproquement la condition énoncée dans le lemme est vérifiée. Alors tout $\alpha \in E$ est séparable sur F, et donc E est séparable sur F. En outre, soit $p(x) \in F[x]$ irréductible et monique. Si $p(x)$ admet une racine $\alpha \in E$, alors $p(x) = m_F^\alpha(x)$ est scindé sur E par l'hypothèse. Ainsi E est normal sur F. Ceci achève la démonstration.

3.3.3. Lemme d'Artin. Soit G un groupe fini d'automorphismes de E, et considérons $E^G = \{a \in E \mid \phi(a) = a, \text{ pour tout } \phi \in G\}$, le corps fixe de G. Alors $[E : E^G] \leq |G|$.

Démonstration. Posons $G = \{\phi_1, \phi_2, \ldots, \phi_m\}$, où $\phi_1 = \mathbb{1}_E$. Soient $\alpha_1, \alpha_2, \ldots, \alpha_n \in E$ avec $n > m$. Considérons le système homogène d'équations linéaires sur E comme suit:

$$(*) \quad \begin{cases} \phi_1(\alpha_1)x_1 + \phi_1(\alpha_2)x_2 + \cdots + \phi_1(\alpha_n)x_n = 0_E \\ \phi_2(\alpha_1)x_1 + \phi_2(\alpha_2)x_2 + \cdots + \phi_2(\alpha_n)x_n = 0_E \\ \vdots \qquad\qquad \vdots \qquad\qquad\qquad \vdots \qquad \vdots \\ \phi_m(\alpha_1)x_1 + \phi_m(\alpha_2)x_2 + \cdots + \phi_m(\alpha_n)x_n = 0_E. \end{cases}$$

Comme $n > m$, le système $(*)$ a une solution non nulle $(a_1, a_2, \ldots, a_n)$ avec $a_i \in E$. On peut supposer que le nombre de composantes non nulles de $(a_1, a_2, \ldots, a_n)$ est le plus petit parmi les solutions non nulles et que $a_r = 1_E$ pour un certain r avec $1 \leq r \leq n$. On montrera que $a_1, \cdots, a_n \in E^G$. On se fixe un j avec $1 \leq j \leq m$. Remplaçant x_i par a_i dans le système $(*)$, et ensuite appliquant ϕ_j, on a

$$(**) \quad \begin{cases} \phi_j\phi_1(\alpha_1)\phi_j(a_1) + \phi_j\phi_1(\alpha_2)\phi_j(a_2) + \cdots + \phi_j\phi_1(\alpha_n)\phi_j(a_n) = 0_E \\ \phi_j\phi_2(\alpha_1)\phi_j(a_1) + \phi_j\phi_2(\alpha_2)\phi_j(a_2) + \cdots + \phi_j\phi_2(\alpha_n)\phi_j(a_n) = 0_E \\ \vdots \qquad\qquad\qquad\qquad \vdots \qquad\qquad\qquad\qquad \vdots \qquad \vdots \\ \phi_j\phi_m(\alpha_1)\phi_j(a_1) + \phi_j\phi_m(\alpha_2)\phi_j(a_2) + \cdots + \phi_j\phi_m(\alpha_n)\phi_j(a_n) = 0_E. \end{cases}$$

Comme G est un groupe, on a $\{\phi_j\phi_1, \phi_j\phi_2, \ldots, \phi_j\phi_m\} = \phi_j G = G = \{\phi_1, \phi_2, \ldots, \phi_m\}$. D'après les égalités dans $(**)$, on voit que $(\phi_j(a_1), \phi_j(a_2), \ldots, \phi_j(a_n))$ est une solution du système $(*)$. Donc $(a_1 - \phi_j(a_1), a_2 - \phi_j(a_2), \ldots, a_n - \phi_j(a_n))$ l'est également. Supposons que $(a_1 - \phi_j(a_1), a_2 - \phi_j(a_2), \ldots, a_n - \phi_j(a_n))$ est non nulle. Pour tout i avec $1 \leq i \leq n$, si $a_i - \phi_j(a_i) \neq 0_E$, alors $a_i \neq 0_E$. En outre, $a_r - \phi_j(a_r) = 1 - \phi_j(1) = 1 - 1 = 0$ mais $a_r \neq 0$. Ceci implique que le nombre de composantes non nulles de $(a_1 - \phi_j(a_1), a_2 - \phi_j(a_2), \ldots, a_n - \phi_j(a_n))$ est strictement plus petit que celui de $(a_1, a_2, \ldots, a_n)$, une contradiction. Donc $\phi_j(a_i) = a_i$, pour tous $1 \leq i \leq n,\ 1 \leq j \leq m$. C'est-à-dire, $a_1, a_2, \ldots, a_n \in E^G$. Comme $\phi_1 = \mathbb{1}_E$, on a $a_1\alpha_1 + a_2\alpha_2 + \cdots + a_n\alpha_n = 0_E$. Ceci montre $\dim_{E^G} E \leq m$, c'est-à-dire, $[E : E^G] \leq |G|$. La preuve s'achève.

3.3.4. Théorème. Soit $E : F$ une extension de corps. Les conditions suivantes sont équivalentes:

(1) $E : F$ est galoisienne.

(2) E est un corps de rupture d'un polynôme séparable sur F.

(3) Il existe un groupe fini G d'automorphismes de E tel que $F = E^G$.

Démonstration. Supposons que $E : F$ est finie, normale, et séparable. D'après le théorème 2.8.3, E est un corps de rupture sur F d'un polynôme $f(x) \in F[x]$. Soit $p(x)$ un

facteur irréductible monique de $f(x)$ sur F. Alors il existe $\alpha \in E$ tel que $p(\alpha) = 0$. Donc $p(x) = m_F^\alpha(x)$ est séparable car $E : F$ est séparable. Par conséquent, $f(x)$ est séparable.

Supposons que $f(x) \in F[x]$ est séparable dont E est un corps de rupture sur F. D'après le théorème 3.2.4, $|G(E/F)| = [E : F]$ est fini et $F = E^{G(E/F)}$.

Supposons que $G = \{\phi_1, \phi_2, \ldots, \phi_m\}$, où $\phi_1 = \mathbb{1}_E$, est un groupe fini d'automorphismes de E tel que $F = E^G$. Remarquons $G \leq G(E/F)$. D'après le lemme d'Artin, $[E : F] \leq |G| = m$, et donc E est fini sur F. Soit $\alpha \in E$. Comme α est racine de $m_F^\alpha(x)$, on voit que $\phi_1(\alpha), \phi_2(\alpha), \ldots, \phi_m(\alpha)$ sont aussi racine de $m_F^\alpha(x)$. Supposons que $\{\alpha_1, \ldots, \alpha_r\}$ avec $r \leq m$ est l'ensemble des éléments distincts de l'ensemble $\{\phi_1(\alpha), \phi_2(\alpha), \ldots, \phi_m(\alpha)\}$. Alors $\{\phi_i(\alpha_1), \phi_i(\alpha_2), \ldots, \phi_i(\alpha_r)\} = \{\alpha_1, \ldots, \alpha_r\}$, pour tout $\phi_i \in G$. Comme $m_F^\alpha(\alpha_i) = 0$, on a $x - \alpha_i \,|\, m_F^\alpha(x)$ sur E, pour tout $1 \leq i \leq r$. Ainsi $(x - \alpha_1) \cdots (x - \alpha_r) \,|\, m_F^\alpha(x)$ sur E car les α_i avec $1 \leq i \leq r$ sont deux à deux distincts. Posons $g(x) = (x - \alpha_1) \cdots (x - \alpha_r)$. Pour tout $\phi_i \in G$, on a $\phi_i(g(x)) = (x - \phi_i(\alpha_1)) \cdots (x - \phi_i(\alpha_r)) = (x - \alpha_1) \cdots (x - \alpha_r) = g(x)$. Par conséquent, $g(x) \in F[x]$. Ainsi $g(x) \,|\, m_F^\alpha(x)$ sur F, et donc $m_F^\alpha(x) = g(x)$ car $m_F^\alpha(x)$ est irrédictible sur F. D'après le lemme 3.3.2, l'extension $E : F$ est galoisienne. Ceci achève la démonstration.

Remarque. Si F est un corps parfait, alors un corps de rupture de n'importe quel polynôme sur F est une extension galosienne de F.

3.3.5. Corollaire. Soit $E : F$ une extension galoisienne. Alors
(1) $F = E^{G(E/F)}$ et $|G(E/F)| = [E : F]$.
(2) Pour tout corps intermédiaire M entre F et E, l'extension $E : M$ est galoisienne.

Démonstration. D'après le théorème 3.3.4, il existe $f(x) \in F[x]$ séparable tel que E est un corps de rupture de $f(x)$ sur F. Alors l'énoncé (1) suit immédiatement du théorème 3.2.4. Enfin soit M un corps intermédiaire entre F et E. Alors $f(x)$ est séparable sur M et E est un corps de rupture de $f(x)$ sur M. Donc E est galoisien sur M d'après le théorème 3.3.4. Ceci achève la démonstration.

Remarque. En partie (2), l'extension $M : F$ n'est pas nécessairement galoisienne. Par exemple, soit E le corps de rupture de $x^3 - 2$ sur $\mathbb{Q}$. Alors $E : \mathbb{Q}$ est galoisienne. Posons $M = \mathbb{Q}(\sqrt[3]{2})$. Remarquons que $x^3 - 2$ a une racine dans M, mais il n'est pas scindé sur M. Donc M n'est pas normal sur $\mathbb{Q}$. Par conséquent, M n'est pas galoisien sur $\mathbb{Q}$.

3.3.6. Lemme. Soient $E : F$ une extension galoisienne. Pour tous $\alpha, \beta \in E$, il existe $\phi \in G(E/F)$ tel que $\phi(\alpha) = \beta$ si, et seulement si, $m_F^\alpha(x) = m_F^\beta(x)$.

Démonstration. La nécessité suit du lemme 2.3.8. Supposons maintenant $m_F^\alpha(x) = m_F^\beta(x)$. D'après le lemme 2.3.8, il existe un F-isomorphisme $\psi : F(\alpha) \to F(\beta)$ tel que

$\psi(\alpha) = \beta$. Or comme $E : F$ est une extension galoisienne, d'après le théorème 3.3.4, E est un corps de rupture d'un polynôme $f(x)$ sur F. Remarquons que $\psi(f(x)) = f(x)$ et que E est un corps de rupture de $f(x)$ sur $F(\alpha)$ et sur $F(\beta)$. D'après le théorème 2.3.10, il existe un isomorphisme $\phi : E \to E$ tel que $\phi|_{F(\alpha)} = \psi$. Ainsi $\phi \in G(E/F)$ est tel que $\phi(\alpha) = \beta$. Ceci achève la démonstration.

3.3.7. Lemme. Soient $E : F$ une extension galoisienne avec M un corps intermédiaire entre F et E. Alors $M : F$ est galoisienne si, et seulement si, $\phi(M) = M$, pour tout $\phi \in G(E/F)$.

Démonstration. Remarquons d'abord que M est finie et séparable sur F. Donc M est galoisien sur F si, et seulement si, M est normal sur F.

Supposons que M est normal sur F. On se fixe $\phi \in G(E/F)$. Comme M et $\phi(M)$ sont F-isomorphes, $[M : F] = [\phi(M) : F]$. Pour tout $\alpha \in M$, $m_F^\alpha(x)$ est scindé sur M par la normalité. Et $\phi(\alpha)$ est une racine de $m_F^\alpha(x)$. Donc $\phi(\alpha) \in M$, c'est-à-dire, $\phi(M) \subseteq M$, et donc $\phi(M) = M$.

Supposons réciproquement que $\phi(M) = M$, pour tout $\phi \in G(E/F)$. Soit $p(x) \in F[x]$ irréductible monique, qui a une racine $\beta \in M$. Alors $p(x)$ est scindé sur E car l'extension $E : F$ est normale. Si $\gamma \in E$ est une racine de $p(x)$, alors $m_F^\beta(x) = p(x) = m_F^\gamma(x)$. D'après le lemme 3.3.6, il existe $\phi \in G(E/F)$ tel que $\gamma = \phi(\beta)$, et donc $\gamma \in M$ car $\phi(M) = M$. Cela veut dire que $p(x)$ est scindé sur M. Par conséquent, M est normal sur F. Ceci achève la démonstration.

3.3.8. Théorème fondamental de Galois. Soit $E : F$ une extension galoisienne de corps. Posons $\mathcal{F}$ l'ensemble des corps intemédiaires entre F et E; et $\mathcal{G}$ l'ensemble des sous-groupes de $G(E/F)$.

(1) L'application $\mathcal{F} \to \mathcal{G} : M \mapsto G(E/M)$ est une bijection qui renverse l'ordre d'inclusion et a pour l'inverse l'application $\mathcal{G} \to \mathcal{F} : H \mapsto E^H$.

(2) Pour tout $M \in \mathcal{F}$, $[E : M] = |G(E/M)|$ et $[M : F] = [G(E/F) : G(E/M)]$, l'indice de $G(E/M)$ dans $G(E/F)$.

(3) Pour tout $M \in \mathcal{F}$, l'extension $M : F$ est galoisienne si, et seulement si, $G(E/M)$ est normal dans $G(E/F)$. Dans ce cas, $G(M/F) \cong G(E/F)/G(E/M)$.

Démonstration. (1) Pour tout $M \in \mathcal{F}$, d'après le corollaire 3.3.5, E est galoisien sur M, et donc $M = E^{G(E/M)}$. D'autre part, pour tout $H \in \mathcal{G}, H \subseteq G(E/E^H)$. Comme $E : E^H$ est galoisienne, d'après lemme d'Artin, $|G(E/E^H)| = [E : E^H] \leq |H|$. Par conséquent, $H = G(E/E^H)$. Ainsi l'application $\mathcal{F} \to \mathcal{G} : M \mapsto G(E/M)$ est bijective ayant pour l'inverse l'application $\mathcal{G} \to \mathcal{F} : H \mapsto E^H$.

(2) Pour tout $M \in \mathcal{F}$, l'extension $E : M$ est galoisienne. Donc $[E : M] = |G(E/M)|$.

D'où,

$$[M : F] = \frac{[E : F]}{[E : M]} = \frac{|G(E/F)|}{|G(E/M)|} = [G(E/F) : G(E/M)].$$

(3) Soit $M \in \mathcal{F}$. Supposons que $M : F$ est galoisienne. Pour tout $\phi \in G(E/F)$, $\phi(M) = M$ d'après le lemme 3.3.7, et donc $\phi|_M \in G(M/F)$. Ceci donne un homomorphisme de groupes:

$$\Phi : G(E/F) \mapsto G(M/F) : \phi \mapsto \phi|_M.$$

Or $\phi \in \mathrm{Ker}(\Phi)$ si, et seulement si, $\phi|_M = \mathbb{1}_M$ si, et seulement si, $\phi \in G(E/M)$. Par conséquent, $G(E/M) = \mathrm{Ker}(\Phi)$ est un sous-groupe normal de $G(E/F)$. En outre, comme $E : F$ est galoisienne, E est un corps de rupture sur F d'un polynôme $f(x) \in F[x]$, et donc E est un corps de rupture de $f(x)$ sur M. Soit $\psi \in G(M/F)$. Comme $\psi(f(x)) = f(x)$, d'après le théorème 2.3.10, il existe un automorphisme $\phi : E \to E$ tel que $\phi|_M = \psi$, c'est-à-dire, $\phi \in G(E/F)$ est tel que $\Phi(\phi) = \psi$. Ainsi Φ est surjectif. Par conséquent, $G(M/F) \cong G(E/F)/G(E/M)$.

Supposons réciproquement que $G(E/M) \trianglelefteq G(E/F)$. On se fixe $\phi \in G(E/F)$ et $\alpha \in M$. Pour tout $\psi \in G(E/M)$, on a $\phi^{-1}\psi\phi \in G(E/M)$, et donc

$$\psi[\phi(\alpha)] = (\psi\phi)(\alpha) = (\phi\phi^{-1}\psi\phi)(\alpha) = \phi[(\phi^{-1}\psi\phi)(\alpha)] = \phi(\alpha).$$

D'où $\phi(\alpha) \in E^{G(E/M)} = M$. Donc $\phi(M) \subseteq M$, et ainsi $\phi(M) = M$. D'après le lemme 3.3.7, l'extension $M : F$ est galoisienne. Ceci achève la démonstration.

Exemple. Soit E le corps de rupture de $x^4 - 2$ sur $\mathbb{Q}$. On veut trouver les corps intermédiaires compris entre E et $\mathbb{Q}$. Comme $\mathbb{Q}$ est parfait, l'extension $E : \mathbb{Q}$ est galoisienne. Comme

$$x^4 - 2 = (x^2 - \sqrt{2})(x^2 + \sqrt{2}) = (x - \sqrt[4]{2})(x + \sqrt[4]{2})(x - \sqrt[4]{2}i)(x + \sqrt[4]{2}i),$$

on a $E = \mathbb{Q}(\sqrt[4]{2}, -\sqrt[4]{2}, \sqrt[4]{2}i, -\sqrt[4]{2}i) = \mathbb{Q}(\sqrt[4]{2}, i)$. Donc

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

Comme i est une racine de $x^2 + 1 \in \mathbb{Q}(\sqrt[4]{2})[x]$ et $i \notin \mathbb{Q}(\sqrt[4]{2})$, on a $[\mathbb{Q}(\sqrt[4]{2}(i) : \mathbb{Q}(\sqrt[4]{2}] = 2$. Ainsi $[E : \mathbb{Q}] = 8$, et donc $|G(E/\mathbb{Q})| = 8$.

D'autre part, comme $[E : \mathbb{Q}] = [\mathbb{Q}(i)(\sqrt[4]{2}) : \mathbb{Q}(i)][\mathbb{Q}(i) : \mathbb{Q}] = 2[\mathbb{Q}(i)(\sqrt[4]{2}) : \mathbb{Q}(i)]$, on en déduit $[\mathbb{Q}(i)(\sqrt[4]{2}) : \mathbb{Q}(i)] = 4$. Étant un polynôme de degré 4 sur $\mathbb{Q}(i)$ dont $\sqrt[4]{2}$ est une racine, $x^4 - 2$ est le polynôme minimal de $\sqrt[4]{2}$ sur $\mathbb{Q}(i)$. De même, $x^4 - 2$ est également le polynôme minimal de $\sqrt[4]{2}i$ sur $\mathbb{Q}(i)$. Comme $E : \mathbb{Q}(i)$ est galoisienne, d'après le lemme 3.3.6, il existe $\sigma \in G(E/\mathbb{Q}(i))$ tel que $\sigma(\sqrt[4]{2}) = \sqrt[4]{2}i$. En particulier, $\sigma \in G(E/\mathbb{Q})$ tel que

$\sigma(i) = i$ et $\sigma(\sqrt[4]{2}) = \sqrt[4]{2}i$. En outre, i et $-i$ ont même polynôme minimal x^2+1 sur $\mathbb{Q}(\sqrt[4]{2})$. Comme $E : \mathbb{Q}(\sqrt[4]{2})$ est galoisienne, d'après le lemme 3.3.6, il existe $\tau \in G(E/\mathbb{Q}(\sqrt[4]{2}))$ tel que $\tau(i) = -i$. En particulier, $\tau \in G(E/\mathbb{Q})$ tel que $\tau(\sqrt[4]{2}) = \sqrt[4]{2}$ et $\tau(i) = -i$. À partir de σ et τ, on obtient des éléments de $G(E/\mathbb{Q})$ comme suit:

	$\mathbb{1}$	σ	σ^2	σ^3	τ	$\sigma\tau$	$\sigma^2\tau$	$\sigma^3\tau$
i	i	i	i	i	$-i$	$-i$	$-i$	$-i$
$\sqrt[4]{2}$	$\sqrt[4]{2}$	$\sqrt[4]{2}i$	$-\sqrt[4]{2}$	$-\sqrt[4]{2}i$	$\sqrt[4]{2}$	$\sqrt[4]{2}i$	$-\sqrt[4]{2}$	$-\sqrt[4]{2}i$

Comme $|G(E/\mathbb{Q})| = 8$, on conclut $G(E/\mathbb{Q}) = \{\mathbb{1}, \tau, \sigma, \sigma^2, \sigma^3, \sigma\tau, \sigma^2\tau, \sigma^3\tau\}$ avec des relations: $\mathbb{1} = \tau^2 = \sigma^4,\ \tau\sigma = \sigma^3\tau,\ \tau\sigma^2 = \sigma^2\tau$, et $\tau\sigma^3 = \sigma\tau$. On calcule les sous-groupes de $G(E/\mathbb{Q})$ comme suit:

d'ordre 8: $H_0 = G(E/\mathbb{Q})$.

d'ordre 4:

$$\begin{aligned} H_1 &= \{\mathbb{1}, \sigma, \sigma^2, \sigma^3\} \\ H_2 &= \{\mathbb{1}, \sigma^2, \tau, \sigma^2\tau\} \\ H_3 &= \{\mathbb{1}, \sigma^2, \sigma\tau, \sigma^3\tau\} \end{aligned}$$

d'ordre 2:

$$\begin{aligned} H_4 &= \{\mathbb{1}, \sigma^2\} \\ H_5 &= \{\mathbb{1}, \tau\} \\ H_6 &= \{\mathbb{1}, \sigma\tau\} \\ H_7 &= \{\mathbb{1}, \sigma^2\tau\} \\ H_8 &= \{\mathbb{1}, \sigma^3\tau\} \end{aligned}$$

d'ordre 1: $H_9 = \{\mathbb{1}\}$.

D'après le théorème de Galois, les corps intermédiaires entre $\mathbb{Q}$ et E sont $M_j = E^{H_j},\ j = 0, 1, \ldots, 9$. On a aisément $M_0 = E^{G(E/\mathbb{Q})} = \mathbb{Q}$ et $M_9 = E^{\{\mathbb{1}\}} = E = \mathbb{Q}(\sqrt[4]{2}, i)$. On va calculer les autres corps. D'abord tout $\alpha \in E$ s'écrit

$$\alpha = a_0 + a_1\sqrt[4]{2} + a_2\sqrt[4]{4} + a_3\sqrt[4]{8} + a_4 i + a_5\sqrt[4]{2}i + a_6\sqrt[4]{4}i + a_7\sqrt[4]{8}i,\ a_j \in \mathbb{Q}.$$

On commence par M_1. On a $\alpha \in M_1 = E^{\{\mathbb{1}, \sigma, \sigma^2, \sigma^3\}}$ si, et seulement si, $\sigma(\alpha) = \alpha$ si, et seulement si, $\alpha = a_0 + a_1\sqrt[4]{2}i - a_2\sqrt[4]{4} - a_3\sqrt[4]{8}i + a_4 i - a_5\sqrt[4]{2} - a_6\sqrt[4]{4}i + a_7\sqrt[4]{8}$ si, et seulement si, $a_1 = -a_5, a_2 = -a_2, a_3 = a_7, a_5 = a_1, a_6 = -a_6, a_7 = -a_3$ si, et seulement si, $a_1 = a_2 = a_3 = a_5 = a_6 = a_7 = 0$ si, et seulement si, $\alpha = a_0 + a_4 i$ si, et seulement si, $\alpha \in \mathbb{Q}(i)$. Par conséquent, $M_1 = \mathbb{Q}(i)$. De même $M_2 = \mathbb{Q}(\sqrt[4]{4}) = \mathbb{Q}(\sqrt{2})$, et $M_3 = \mathbb{Q}(\sqrt[4]{4}i) = \mathbb{Q}(\sqrt{2}i)$.

Pour calculer M_8, on voit que $\alpha \in M_8 = E^{\{\mathbb{1}, \sigma^3\tau\}}$ si, et seulement si, $\alpha = (\sigma^3\tau)(\alpha)$ si, et seulement si, $\alpha = a_0 - a_1\sqrt[4]{2}i - a_2\sqrt[4]{4} + a_3\sqrt[4]{8}i - a_4 i - a_5\sqrt[4]{2} - a_6\sqrt[4]{4}i + a_7\sqrt[4]{8}$ si, et seulement

si, $a_1 = -a_5, a_2 = -a_2, a_3 = a_7, a_4 = -a_4, a_5 = -a_1, a_6 = -a_6, a_7 = a_3$ si, et seulement si, $a_1 = -a_5, a_3 = a_7, a_2 = a_4 = a_6 = 0$ si, et seulement si,

$$\alpha = a_0 + a_1\sqrt[4]{2} + a_3\sqrt[4]{8} - a_1\sqrt[4]{2}i + a_3\sqrt[4]{8}i = a_0 + a_1\sqrt[4]{2}(1-i) + a_3\sqrt[4]{8}(1+i)$$

si, et seulement si, $\alpha \in \mathbb{Q}(\sqrt[4]{2}(1-i))$ car $\sqrt[4]{8}(1+i) = -(\sqrt[4]{2}(1-i))^3/2 \in \mathbb{Q}(\sqrt[4]{2}(1-i))$. Donc $M_8 = \mathbb{Q}(\sqrt[4]{2}(1-i))$. De même, on trouve $M_4 = \mathbb{Q}(\sqrt{2}, i)$, $M_5 = \mathbb{Q}(\sqrt[4]{2})$, $M_6 = \mathbb{Q}(\sqrt[4]{2}(1+i))$, $M_7 = \mathbb{Q}(\sqrt[4]{2}i)$.

Remarquons que M_0, M_1, M_2, M_3, M_4 et M_9 sont des corps de rupture de $x-1$, de x^2+1, de x^2-2, de x^2+2, de $(x^2-2)(x^2+1)$, et de x^4-2 sur $\mathbb{Q}$, respectivement. Donc ils sont tous galoisiens sur $\mathbb{Q}$. Par conséquent, H_0, H_1, H_2, H_3, H_4 et H_9 sont des sous-groupes normaux de $G(E/\mathbb{Q})$. De plus, $\sigma(M_5) = M_7$ et $\pi(M_6) = M_8$. D'après le lemme 3.3.7, M_5, M_6, M_7 et M_8 ne sont pas normaux sur $\mathbb{Q}$. Par conséquent, H_4, H_5, H_6, H_7 et H_8 ne sont pas normaux dans $G(E/\mathbb{Q})$.

3.4. Exercices

1. Soient $E : F$ et $L : F$ des extensions finies de corps. S'il existe un F-isomorphisme de E sur L, montrer que $[E : F] = [L : F]$.

2. Soit $E : F$ une extension de corps finie. Montrer qu'un F-homomorphisme de E dans lui-même est un F-automorphisme.

3. Soit F un corps avec $f(x) \in F[x]$. Soit E un corps de rupture de $f(x)$ sur F. Si $\alpha, \beta \in E$ sont des racines de $f(x)$, montrer qu'il existe $\phi \in G(E/F)$ tel que $\phi(\alpha) = \beta$ si, et seulement si, α et β sont racines du même facteur irréductible de $f(x)$ sur F.

4. Soit $f(x)$ un polynôme monique sur un corps F avec G son groupe de Galois. Si l'action de G sur l'ensemble des racines de $f(x)$ est transitive (c'est-à-dire, pour toutes racines α, β de $f(x)$, il existe un $\phi \in G$ tel que $\phi(\alpha) = \beta$), montrer que $f(x)$ est une puissance d'un polynôme irréductible sur F.

5. Trouver le groupe de Galois de chacun des polynômes rationnels suivants:

   (1) $x^3 - 2$ (2) $(x^3 - 1)(x^2 - 3)$.

6. Si $E : F$ est une extension de corps finie, montrer que $G(E/F)$ est finie.

7. Soit $\alpha = \sqrt{2 + \sqrt{2}} \in \mathbb{R}$.

(1) Montrer que $\mathbb{Q}(\alpha)$ est un corps de rupture de $x^4 - 4x^2 + 2$ sur $\mathbb{Q}$. *Indication*: Vérifier que $2 - \sqrt{2} = \alpha^2(\alpha^2 - 3)^2$.

(2) Montrer que $\mathbb{Q}(\alpha) : \mathbb{Q}$ est une extension galoisienne.

(3) Trouver l'ordre du groupe de Galois $G(\mathbb{Q}(\alpha)/\mathbb{Q})$.

(4) Montrer que $G(\mathbb{Q}(\alpha)/\mathbb{Q})$ est cyclique. *Indication*: Montrer qu'il existe $\phi \in G(\mathbb{Q}(\alpha)/\mathbb{Q})$ tel que $\phi(\sqrt{2}) = -\sqrt{2}$ et $\phi(\alpha) = \sqrt{2 - \sqrt{2}}$ et calculer $o(\phi)$.

8. Montrer que l'extension $\mathbb{Q}(\sqrt{2}, \sqrt{5}) : \mathbb{Q}$ est galoisienne. Trouver les corps intermédiaires compris entre $\mathbb{Q}$ et $\mathbb{Q}(\sqrt{2}, \sqrt{5})$, et specifier ceux qui sont galoisiens sur $\mathbb{Q}$ en trouvant les sous-groupes de $G(\mathbb{Q}(\sqrt{2}, \sqrt{5})/\mathbb{Q})$.

9. Soit $E : F$ une extension de corps galoisienne. Si $p(x)$ est un polynôme irréductible sur F, montrer que les facteurs irréductibles de $p(x)$ sur E ont même degré. *Indication.* Soient α, β racines de facteurs irréductibles de $p(x)$ sur E. Remarquant E est le corps de rupture d'un polynôme $f(x)$ sur F, montrer qu'il existe un F-isomorphisme $\phi : F(\alpha) \to F(\beta)$ qui envoie α à β et $f(x)$ à $f(x)$.

10. Soit F un corps. Montrer, pour tout entier $n \geq 1$, que le corps de rupture de $x^n - 1$ sur F est une extension galoisienne de F.

Chapitre IV: Groupes finis

4.1. Groupes résolubles

partout dans cette section, on se fixe G un groupe fini ayant e pour identité. Rappelons que si H est un sous-groupe de G d'indice 2, alors H est normal dans G. De plus, si G est d'ordre premier, alors G est cyclique, et donc abélien.

4.1.1. Définition. Un groupe G est dit *résoluble* s'il existe une suite

$$\{e\} = G_0 \trianglelefteq G_1 \trianglelefteq \cdots \trianglelefteq G_{s-1} \trianglelefteq G_s = G$$

de sous-groupes de G telle que G_i/G_{i-1} est abélien, $i = 1, \cdots, s$.

Exemple. (1) Tout groupe abélien G est résoluble ayant une suite $\{e\} \trianglelefteq G$.

(2) Le groupe symétrique S_n avec $1 \leq n \leq 4$ est résoluble. En effet, $S_1 = \{(1)\}$ et $S_2 = \{(1), (12)\}$ sont abéliens. Considérons maintenant le cas où $3 \leq n \leq 4$. Posons A_n le groupe alterné, c'est-à-dire, le groupe des permutations paires de $\{1, 2, \ldots, n\}$. Alors $[S_n : A_n] = 2$, et donc $A_n \trianglelefteq S_n$ tel que S_n/A_n est abélien. Comme $A_3 = \{(1), (123), (132)\}$ est abélien, S_3 est résoluble pour la suite $\{(1)\} \trianglelefteq A_3 \trianglelefteq S_3$. Enfin,

$$A_4 = \{(1), (123), (132), (124), (142), (134), (143), (234), (243), (12)(34), (13)(24), (14)(23)\}.$$

Et on voit que $V_4 = \{(1), (12)(34), (13)(24), (14)(23)\}$ est un sous-groupe abélien normal de A_4 d'indice 3. Donc S_4 est résoluble pour la suite $\{(1)\} \trianglelefteq V_4 \trianglelefteq A_4 \trianglelefteq S_4$.

Le résultat suivant est bien connu dans la théorie des groupes.

4.1.2. Lemme. Soit H, N des sous-groupes de G avec N normal.

(1) $H \cap N$ est un sous-groupe normal de H tel que $H/H \cap N \cong HN/N$.

(2) Tout sous-groupe de G/N est de la forme H/N avec $N \subseteq H \leq G$. En outre, $H/N \trianglelefteq G/N$ si, et seulement si, $H \trianglelefteq G$. Dans ce cas, $(G/N)/(H/N) \cong G/H$.

4.1.3. Théorème. Soient H, N des sous-groupes de G avec N normal dans G.

(1) Si G est résoluble, alors H et G/N sont résolubles.

(2) Si N et G/N sont résolubles, alors G est résoluble.

Démonstration. (1) Supposons que G est résoluble avec une suite

$$\{e\} = G_0 \trianglelefteq G_1 \trianglelefteq \cdots \trianglelefteq G_{s-1} \trianglelefteq G_s = G$$

telle que G_i/G_{i-1} est abélien, pour tout $0 < i \leq s$. Posant $H_i = H \cap G_i$, on a une suite

$$\{e\} = H_0 \trianglelefteq H_1 \trianglelefteq \cdots \trianglelefteq H_{s-1} \trianglelefteq H_s = H$$

telle que, pour tout $0 < i \leq s$, $H_i/H_{i-1} = (H \cap G_i)/(H \cap G_i) \cap G_{i-1} \cong (H \cap G_i)G_{i-1}/G_{i-1}$ est un sous-groupe de G_i/G_{i-1}, et donc abélien. Ainsi H est résoluble. En outre, on a une suite $\{e\} = G_0N/N \trianglelefteq G_1N/N \trianglelefteq \cdots \trianglelefteq G_{s-1}N/N \trianglelefteq G_sN/N = G/N$ telle que

$$\frac{G_iN/N}{G_{i-1}N/N} \cong \frac{G_iN}{G_{i-1}N} = \frac{G_i(G_{i-1}N)}{G_{i-1}N} \cong \frac{G_i}{G_i \cap G_{i-1}N} \cong \frac{G_i/G_{i-1}}{(G_i \cap G_{i-1}N)/G_{i-1}}.$$

Ce dernier est un quotient du groupe abélien G_i/G_{i-1}, et donc abélien. Par conséquent, G/N est résoluble.

(2) Supposons que N et G/N sont tous résolubles. Alors il existe une suite

$$\{e\} = N_0 \trianglelefteq N_1 \trianglelefteq \cdots \trianglelefteq N_{s-1} \trianglelefteq N_s = N$$

telle que N_i/N_{i-1} est abélien pour tout $0 < i \leq s$, et une suite

$$\{e\} = L_0/N \trianglelefteq L_1/N \trianglelefteq \cdots \trianglelefteq L_{t-1}/N \trianglelefteq L_t/N = G/N$$

telle que $(L_j/N)/(L_{j-1}/N)$ est abélien, pour tout $0 < j \leq t$. On a donc une suite

$$N = L_0 \trianglelefteq L_1 \trianglelefteq \cdots \trianglelefteq L_{r-1} \trianglelefteq L_r = G$$

telle que L_j/L_{j-1} est abélien, pour tout $0 < j \leq t$. Ainsi, G est résoluble pour la suite

$$\{e\} = N_0 \trianglelefteq N_1 \trianglelefteq \cdots \trianglelefteq N_{s-1} \trianglelefteq N_s = N = L_0 \trianglelefteq L_1 \trianglelefteq \cdots \trianglelefteq L_{r-1} \trianglelefteq L_r = G.$$

Ceci achève la démonstration.

4.1.4. Définition. Un groupe G est dit *simple* si G est non trivial n'ayant que deux sous-groupes normaux $\{e\}$ et G.

Exemple. Si $|G|$ est premier, alors G est simple.

On accepte le théorème suivant sans démonstration.

4.1.5. Théorème. Si $n \geq 5$, alors le groupe alterné A_n est simple.

4.1.6. Proposition. Un groupe fini G est résoluble et simple si, et seulement si, G est d'ordre premier.

Démonstration. La suffisance est triviale. Supposons maintenant que G est résoluble et simple. Alors il existe une suite

$$\{e\} = G_0 \triangleleft G_1 \triangleleft \cdots \triangleleft G_{s-1} \triangleleft G_s = G$$

telle que G_i/G_{i-1} est abélien, pour tout $0 < i \leq s$. Comme G est simple, on a $G_{s-1} = \{e\}$, et donc G est abélien. Prenons $e \neq g \in G$. Alors $o(g) > 1$. Posons $o(g) = pq$ avec p premier et $q \geq 1$. Posons $h = g^q$. Alors $o(h) = p$. Donc $\{e\} \subset < h > \trianglelefteq G$, car G est abélien. Par conséquent, $G =< h >$ est d'ordre p car G est simple. Ceci achève la démonstration.

4.1.7. Théorème. Le groupe symétrique S_n est résoluble si, et seulement si, $1 \leq n \leq 4$.

Démonstration. On sait que S_n est résoluble pour $1 \leq n \leq 4$. Supposons que $n \geq 5$ et que S_n est résoluble. D'après le théorème 4.1.3(1), A_n est également résoluble. D'après le théorème 4.1.5, A_n est simple. D'après le théorème 4.1.6, A_n est d'ordre premier, qui contredit le fait que $|A_n| = \frac{n!}{2} = 3 \times 4 \times \cdots \times n$. Ceci achève la démonstration.

4.2. Groupes p-primaires

Partout dans cette section, on se fixe G un groupe fini ayant e pour identité. Rappelons que

$$C(G) = \{h \in G \,|\, hg = gh, \text{ pour tout } g \in G\}$$

est un sous-groupe normal de G, appelé le *centre* de G. On voit aisément que G est abélien si, et seulement si, $C(G) = G$.

4.2.1. Définition. On dit que $g_1, g_2 \in G$ sont *conjugués*, noté $g_1 \sim g_2$, s'il existe $h \in G$ tel que $g_1 = hg_2h^{-1}$.

4.2.2. Lemme. La relation de conjugué est une relation d'équivalence.

Démonstration. D'abord, pour tout $g \in G$,, comme $g = ege^{-1}$, on a $g \sim g$.

Supposons maintenant que $g_1 \sim g_2$. Alors il existe $h \in G$ tel que $g_1 = hg_2h^{-1}$. D'où, $g_2 = h^{-1}g_1(h^{-1})^{-1}$, et donc $g_2 \sim g_1$.

Supposons enfin que $g_1 \sim g_2$ et $g_2 \sim g_3$. Alors il existe $h_1, h_2 \in G$ tels que $g_1 = h_1g_2h_1^{-1}$ et $g_2 = h_2g_3h_2^{-1}$. Or $g_1 = (h_1h_2)g_3(h_1h_2)^{-1}$, c'est-à-dire, $g_1 \sim g_3$. Ceci achève la démonstration.

Pour $g \in G$, posons $C_g = \{hgh^{-1} \,|\, h \in G\}$, la classe de conjugué de g dans G. En outre, on voit aisément que

$$C_G(g) = \{h \in G \,|\, gh = hg\}$$

est un sous-groupe de G, appelé le *centralisateur* de g dans G.

4.2.3. Lemme. Soit $g \in G$.

(1) On a $|C_g| = [G : C_G(g)]$. En particulier, $|C_g|$ est un facteur de $|G|$.

(2) On a $g \in C(G)$ si, et seulement si, $|C_g| = 1$.

Démonstration. (1) Posons $[G : C_G(g)] = s$. Soient $h_1C_G(g), \ldots, h_sC_G(g)$ les classes à gauche de G modulo $C_G(g)$. Pour tout $h \in G$, on a $h = h_ic$, pour certain $1 \leq i \leq s$ et certain $c \in C_G(g)$. Donc $hgh^{-1} = h_icgc^{-1}h_i^{-1} = h_igh_i^{-1}$. Cela implique $C_g = \{h_1gh_1^{-1}, \ldots, h_sgh_s^{-1}\}$. En outre, si $i \neq j$, alors $h_i^{-1}h_j \notin C_G(g)$. D'où, $gh_i^{-1}h_j \neq h_i^{-1}h_jg$, et donc $h_igh_i^{-1} \neq h_jgh_j^{-1}$. Ceci montre $|C_g| = s$.

(2) On voit que $g \in C(G)$ si, et seulement si, $hg = gh$ pour tout $h \in G$ si, et seulement si, $hgh^{-1} = g$ pour tout $h \in G$ si, et seulement si, $C_g = \{g\}$ si, et seulement si, $|C_g| = 1$. Ceci achève la démonstration.

4.2.4. Lemme. Soit G un groupe abélien fini. Alors pour tout facteur premier p de $|G|$, il existe $g \in G$ avec $o(g) = p$.

Démonstration. Procédons par récurrence sur $n = |G|$. Si $n = 1$, il n'y a rien à prouver. Supposons que $n > 1$ et que l'énoncé est vrai pour les groupes abéliens d'ordre $< n$. Soit M un sous-groupe maximal de G. Soit $H =< h >$ avec $h \in G \backslash M$. Alors $G = MH$ par la maximalité de M. Comme G est abélien, on a $H \trianglelefteq MH$ et $MH/H \cong M/M \cap H$. Ainsi

$$|G| = |MH| = \frac{|MH|}{|H|}|H| = \left|\frac{MH}{H}\right| \cdot |H| = \frac{|M||H|}{|M \cap H|}.$$

Soit p un facteur premier de $|G|$. Alors $p \mid |H||M|$, et donc $p \mid |M|$ ou $p \mid |H|$. Si $p \mid |M|$, alors il existe $g \in M$ avec $o(g) = p$ par l'hypothèse de récurrenec. Si $p \,|\, |H|$, alors $o(h) = pq$ avec $q \geq 1$. Dans ce cas, $o(h^q) = p$. Ceci achève la démonstration.

4.2.5. Définition. Soit p un premier. Un groupe G est dit *p-primaire* si $|G| = p^n$ avec $n \geq 0$.

Remarque. Si G est p-primaire, alors tous les sous-groupes et tous les quotients de G sont p-primaires.

Exemple. (1) Le groupe $K = \{e, a, b, ab \mid ab = ba, a^2 = b^2 = e\}$ est un groupe 2-primaire, appelé le *groupe de Klein*.

(2) Soit $E = \mathbb{Q}(\sqrt[4]{2}, i)$, le corps de rupture de $x^4 - 2$ sur $\mathbb{Q}$. On a vu que $G(E/\mathbb{Q})$ est d'ordre 8 et donc 2-primaire.

4.2.6. Proposition. Soit p un nombre premier. Si G est un groupe p-primaire non trivial, alors le centre $C(G)$ est non trivial.

Démonstration. Supposons que $|G| = p^n$ avec $n > 0$. Soient $C_1, C_2, \ldots, C_r$ les classes de conjugué de G, où $C_1 = \{e\}$. Alors

$$p^n = |G| = \sum_{i=1}^{r} |C_i| = 1 + \sum_{\imath=2}^{r} |C_i|.$$

D'après le lemme 4.2.3(1), $|C_i| = p^{n_i}$ avec $n_i \geq 0$. Si $n_i > 0$ pour tout i avec $2 \leq i \leq r$, alors $p \,|\, 1$, une contradiction. Donc il existe certain i_0 avec $2 \leq i_0 \leq r$ tel que $n_{i_0} = 0$, c'est-à-dire, $C_{i_0} = \{g_0\}$. Alors $g_0 \neq e$, et d'après le lemme 4.2.3(2), $g_0 \in C(G)$. Ceci achève la démonstration.

4.2.7. Théorème. Soient p un nombre premier et G un groupe p-primaire.

(1) G est résoluble.

(2) Si G est non trivial, alors G admet un sous-groupe normal d'indice p.

Démonstration. (1) Soit $|G| = p^n$ avec $n \geq 0$. Si $n = 0$, alors G est évidemment résoluble. Supposons que $n > 0$ et l'énoncé est vrai pour les p-groupes d'ordre $< p^n$. D'après la proposition 4.2.6, $|C(G)| = p^s$ avec $s > 0$. Étant d'ordre p^{n-s}, le groupe $G/C(G)$ est résoluble par l'hypothèse de récurrence. Comme $C(G)$ est abélien et donc résoluble, G est résoluble d'après le théorème 4.1.3(2).

(2) Prenons un sous-groupe normal maximal H de G. Alors G/H est simple. Comme G est résoluble par (1), G/H l'est aussi d'après le théorème 4.1.3(1). Il suit maintenant de la proposition 4.1.6 que G/H est d'ordre premier. Donc $|G/H| = p$, c'est-à-dire, $[G : H] = p$. Ceci achève la démonstration.

Question. Pour quel facteur d de $|G|$, le groupe G admet un sous-groupe d'ordre d?

4.2.8. Théorème de Sylow. Soient G un groupe fini et p un nombre premier. Si n est le plus grand exposant tel que p^n divise $|G|$, alors G admet un sous-groupe d'ordre p^n, appelé un *p-groupe de Sylow* de G.

Démonstration. Si $|G| = 1$, il n'a y rien à prouver. Supposons que $|G| > 1$ et que l'énoncé est vrai pour les groupes d'ordre $< |G|$. Supposons que $|G| = p^n q$ avec $(p, q) = 1$. Soient $g_1, g_2, \ldots, g_r \in G$ tels que $C_{g_1}, C_{g_2}, \ldots, C_{g_s}$ soient les classes de conjugué de G. Pour tout $1 \leq i \leq s$, d'après le lemme 4.2.3(1), $[G : C_G(g_i)] = |C_{g_i}|$, et donc

$$p^n q = |G| = |C_G(g_i)|[G : C_G(g_i)] = |C_G(g_i)||C_{g_i}|.$$

Supposons premièrement qu'il existe $1 \leq j \leq s$ tel que $|C_{g_j}| > 1$ et $p \not| \, |C_{g_j}|$. Alors $p^n \mid |C_G(g_j)|$ avec $|C_G(g_j)| < |G|$. Par l'hypothèse de récurrence, $C_G(g_j)$, ainsi que G, admet un sous-groupe d'ordre p^n.

Supposons maintenant que pour tout $1 \leq i \leq s$, soit $|C_{g_i}| = 1$ soit $p \mid |C_{g_i}|$. Alors

$$p^n q = |G| = \sum_{i=1}^{s} |C_{g_i}| = \sum_{|C_{g_i}|=1} |C_{g_i}| + \sum_{|C_{g_i}|>1}^{s} |C_{g_i}| = \sum_{g_i \in C(G)} 1 + \sum_{p \,|\, |C_{g_i}|} |C_{g_i}| = |C(G)| + pm.$$

Par conséquent, $p \,|\, C(G)$. D'après le lemme 4.2.4, $C(G)$ admet un sous-groupe H d'ordre p. Remarquons $H \trianglelefteq G$ tel que $|G/H| = p^{n-1}q$. Ainsi $n - 1$ est le plus grand exposant tel que

p^{n-1} divise $|G/H|$. Par l'hypothèse de récurrence, G/H admet un sous-groupe M/H, avec $H \leq M \leq G$, d'ordre p^{n-1}. Alors M est un sous-groupe de G tel que $|M| = |H||M/H| = p^n$. Ceci achève la démonstration.

Pour conclure, on appliquera la théorie de Galois pour montrer que $\mathbb{C}$ est un corps algébriquement clos.

4.2.9. Lemme. (1) Tout polynôme réel de degré impaire a au moins une racine réelle.

(2) Tout polynôme complexe de dgeré 2 a une racine complexe.

Démonstration. (1) Soit $f(x) = a_0 + a_1x + \cdots + a_nx^n \in \mathbb{R}[x]$. On peut supposer que $a_n > 0$. Considérons la fonction réelle

$$f : \mathbb{R} \to \mathbb{R} : t \mapsto f(t) = \sum_{i=0}^{n} a_i t^i.$$

Comme $a_n > 0$ et n est impaire, il existe $a < 0$ tel que $f(a) < 0$ et un $b > 0$ tel que $f(b) > 0$. Comme f est continue, il existe c avec $a < c < b$ tel que $f(c) = 0$.

(2) Il est connu que pour tout $\alpha \in \mathbb{C}$, il existe $\beta \in \mathbb{C}$ tel que $\beta^2 = \alpha$, c'est-à-dire, $\sqrt{\alpha} \in \mathbb{C}$. Or tout polynôme $\alpha x^2 + \beta x + \gamma$ sur $\mathbb{C}$ avec $\alpha \neq 0$ admet deux racines dans $\mathbb{C}$ suivantes:

$$\delta_1 = \frac{-\beta + \sqrt{\beta^2 - 4\alpha\gamma}}{2\alpha},\ \delta_2 = \frac{-\beta - \sqrt{\beta^2 - 4\alpha\gamma}}{2\alpha}.$$

Ceci achève la démonstration.

4.2.10. Corollaire. (1) Si E est une extension finie de $\mathbb{R}$ de degré impaire, alors $E = \mathbb{R}$.

(2) Si N est une extension galoisienne de $\mathbb{C}$ de degré 2^n avec $n \geq 0$, alors $N = \mathbb{C}$.

Démonstration. (1) Comme $\mathbb{R}$ est parfait, $E = \mathbb{R}(\alpha)$. Comme $\partial(m^\alpha_{\mathbb{R}}(x)) = [E : \mathbb{R}]$, le polynôme $m^\alpha_{\mathbb{R}}(x)$ est de degré impaire. D'après lemme 4.2.9(1), $m^\alpha_{\mathbb{R}}(x)$ admet une racine réelle. Par conséquent, $\partial(m^\alpha_{\mathbb{R}}(x)) = 1$, c'est-à-dire, $\alpha \in \mathbb{R}$. Cela implique que $E = \mathbb{R}$.

(2) Supposons que $[N : \mathbb{C}] = 2^n$ avec $n > 0$. Comme N est galoisien sur $\mathbb{C}$, d'après le théorème 3.3.8(2), $|G(N/\mathbb{C})| = [N : \mathbb{C}] = 2^n$. D'après le théorème 4.2.7, $G(N/\mathbb{C})$ admet un sous-groupe H d'indice 2. D'après le théorème 3.3.8(2), $[N^H : \mathbb{C}] = [G(N/\mathbb{C}) : H] = 2$. Prenons $\alpha \in N^H$ et $\alpha \notin \mathbb{C}$. Alors $N^H = \mathbb{C}(\alpha)$. Donc $\partial(m^\alpha_{\mathbb{C}}(x)) = [\mathbb{C}(\alpha) : \mathbb{C}] = 2$. D'après le lemme 4.2.9(2), $m^\alpha_{\mathbb{C}}(x)$ admet une racine dans $\mathbb{C}$, une contradiction à l'irréductibilité de $m^\alpha_{\mathbb{C}}(x)$. Ceci achève la démonstration.

4.2.11. Théorème fondamental d'algèbre. Le corps $\mathbb{C}$ est algébriquement clos.

Démonstration. Soit $f(x) \in \mathbb{C}[x]$ ayant E pour un corps de rupture sur $\mathbb{C}$. Alors $E : \mathbb{R}$ est finie. D'après la proposition 2.2.8, E est contenu dans un corps N qui est normal et fini sur $\mathbb{R}$. Ainsi $N : \mathbb{R}$ est galoisienne, puisque $\mathbb{R}$ est parfait. Comme $\mathbb{C} \subseteq N$, on a $[\, N : \mathbb{R}\,] = 2^n q$

avec $n > 0$ et $(2, q) = 1$. D'après le théorème 3.3.8, $|G(N/\mathbb{R})| = [N : \mathbb{R}] = 2^n q$. D'après le théorème 4.2.8, $G(N/\mathbb{R})$ a un sous-groupe H d'ordre 2^n. D'après le théorème 3.3.8(2), $[N^H : \mathbb{R}] = [G(N/\mathbb{R}) : H] = q$ est impaire. D'après le corollaire 4.2.10(1), on a $q = 1$. Ainsi $2^n = [N : \mathbb{R}] = 2[N : \mathbb{C}]$, et donc $[N : \mathbb{C}] = 2^{n-1}$. Comme $N : \mathbb{C}$ est galoisienne, d'après le corollaire 4.2.10(2), $N = \mathbb{C}$. En particulier $f(x)$ est sindé sur $\mathbb{C}$. Ceci achève la démonstration.

4.3. Exercices

1. Montrer, d'après la définition, que le groupe dièdre suivant est résoluble:

$$D_{2n} = \{e, a, a^2, \ldots, a^{n-1}, b, ba, ba^2, \ldots, ba^{n-1} \,|\, a^n = b^2 = e,\ ab = ba^{-1}\}.$$

2. Soient G un groupe fini et p un nombre premier. Montrer les énoncés suivants.
   (1) Si G est p-primaire, alors G admet un sous-groupe d'ordre d pour tout $d \,|\, |G|$.
   (2) Si $p^r \mid |G|$ avec $r \geq 0$, alors G admet un sous-groupe d'ordre p^r.

3. Soit G un groupe résoluble fini. Montrer qu'il existe une suite de sous-groupes

$$\{e\} = G_0 \lhd G_1 \lhd \cdots \lhd G_{r-1} \lhd G_r = G$$

   telle que G_i/G_{i-1} est d'ordre premier, $i = 1, \cdots, r$. *Indication*: Établir premièrement l'énoncé pour les groupes abéliens à l'aide du lemme 4.2.4.

4. Soit $E : F$ une extension de corps galoisienne. Si $G(E/F)$ est abélien et non trivial, montrer qu'il existe une suite $F = F_0 \subset F_1 \subset \cdots \subset F_r = E$ de sous-corps de E telle que $[F_i : F_{i-1}] = p$, $i = 1, \cdots, r$.

5. Soit $E : F$ une extension de corps galoisienne. Si $G(E/F)$ est p-primaire et non trivial, montrer qu'il y a une suite $F = F_0 \subset F_1 \cdots \subset F_{n-1} \subset F_n = F$ de sous-corps de E telle que $[F_i : F_{i-1}] = p$, $i = 1, \cdots, n$.

6. Soit $E : F$ une extension de degré premier p de corps de caractéristique zéro telle que (1) $F : F$ est la seule extension dont le degré n'est pas divisible par p et (2) E n'a aucune extension de degré p. Montrer que E est une clôture algébrique de F. *Indication*: Comparer avec 4.2.10 et 4.2.11.

Chapitre V: Résolution d'équations par radicaux

Partout dans ce chapitre, on se fixe $E : F$ une extension de corps de caractéristique zéro. Comme F est parfait, E est galoisien sur F si, et seulement si, E est un corps de rupture d'un polynôme sur F.

5.1. Définition. On dit que l'extension $E : F$ est *radicale*, ou bien E est *radical* sur F, s'il existe une suite

$$F = F_0 \subseteq F_1 \subseteq \cdots \subseteq F_r = E$$

de sous-corps de E telle que $F_i = F_{i-1}(\alpha_i)$, où $\alpha_i \in F_i$ tel que $\alpha_i^{n_i} \in F_{i-1}$ pour un certain $n_i > 0$, $i = 1, \ldots, r$.

Remarque. Dans le cas ci-dessus, on a $F_i = F(\alpha_1, \ldots, \alpha_i)$, $i = 1, \ldots, r$. Posant $a_i = \alpha_i^{n_i} \in F_{i-1}$, $i = 1, \cdots, r$, on voit que $\alpha_1 = \sqrt[n_1]{a_0}$ avec $a_0 \in F$ et

$$\alpha_2 = \sqrt[n_2]{a_1} = \sqrt[n_2]{b_0 + b_1 \sqrt[n_1]{a_0} + \cdots + b_{n_1-1}(\sqrt[n_1]{a_0})^{n_1-1}}, \quad a_0, b_0, b_1, \ldots, b_{n_1-1} \in F.$$

Par conséquent, tout élément E admet une expression radicale des éléments de F.

Exemple. (1) $\mathbb{C} : \mathbb{R}$ est radicale car $\mathbb{R} \subset \mathbb{C} = \mathbb{R}(i)$ avec $i^2 \in \mathbb{R}$.

(2) Soit $\alpha = \sqrt[5]{5 + \sqrt[3]{3 + \sqrt{2}}} \in \mathbb{R}$. Alors $\mathbb{Q}(\alpha) : \mathbb{Q}$ est radicale. En effet, posons $\beta = \sqrt[3]{3 + \sqrt{2}}$ et $\gamma = \sqrt{2}$. Alors $\beta = \alpha^5 - 5$, $\gamma = (\alpha^5 - 5)^3 - 3 \in \mathbb{Q}(\alpha)$. Ainsi on a une suite

$$\mathbb{Q} \subset \mathbb{Q}(\gamma) \subset \mathbb{Q}(\gamma, \beta) \subset \mathbb{Q}(\gamma, \beta, \alpha) = \mathbb{Q}(\alpha)$$

de sous-corps de $\mathbb{Q}(\alpha)$ avec $\gamma^2 \in \mathbb{Q}$, $\beta^3 = 2 + \gamma \in \mathbb{Q}(\gamma)$, et $\alpha^5 = 5 + \beta \in \mathbb{Q}(\gamma, \beta)$.

Le résultat suivant se découle immédiatement de la définition.

5.2. Lemme. (1) Si $E : F$ est radicale, alors $E : F$ est finie.

(2) S'il existe un corps intermédiaire L entre E et F tel que $E : L$ et $L : F$ sont toutes radicales, alors $E : F$ est radicale.

5.3. Proposition. Si $E : F$ est radicale, alors il existe une extension galoisienne et radicale $L : F$ telle que $E \subseteq L$.

Démonstration. Supposons qu'il existe une suite

$$F = F_0 \subseteq F_1 \subseteq \cdots \subseteq F_r = E$$

de sous-corps de E telle que $F_i = F_{i-1}(\alpha_i)$ avec $\alpha_i^{n_i} \in F_{i-1}$ où $n_i > 0$, $i = 1, \cdots, r$. En particulier, $F_i = F(\alpha_1, \cdots, \alpha_i)$, $i = 1, \ldots, r$.

Prenons $\bar{E}$ la clôture algébrique de E. Soit $V_i = \{\beta_{i1}, \ldots, \beta_{i,t_i}\}$ avec $\beta_{i1} = \alpha_i$ l'ensemble des racines de $m_F^{\alpha_i}(x)$ dans $\bar{E}$, $i = 1, \ldots, r$. Posons $E_0 = F$, et $E_i = F(V_1, \ldots, V_i) = E_{i-1}(V_i)$, $i = 1, \ldots, r$. Ceci nous donne une suite de corps

$$F = E_0 \subseteq E_1 \subseteq \cdots \subseteq E_{r-1} \subseteq E_r,$$

où E_i est une extension galoisienne sur F contenant F_i, $i = 1, \ldots, r$. En effet, E_i est un corps de rupture de $m_F^{\alpha_1}(x) \cdots m_F^{\alpha_i}(x)$ sur F. En particulier, E_r est une extension galoisienne de F contenant E.

Il reste à montrer que E_r est radical sur F. Il suffit, d'après le lemme 5.2(2), de montrer que $E_i : E_{i-1}$ est radicale, pour tout $1 \leq i \leq r$. En effet, on a une suite

$$E_{i-1} \subseteq E_{i-1}(\beta_{i1}) \subseteq E_{i-1}(\beta_{i1}, \beta_{i2}) \subseteq \cdots \subseteq E_{i-1}(\beta_{i1}, \ldots, \beta_{i,t_i}) = E_i$$

de sous-corps de E_i. Pour tout $1 \leq j \leq t_i$, on a $m_F^{\beta_{ij}}(x) = m_F^{\alpha_i}(x)$. Comme $E_i : F$ est galoisienne, d'après le lemme 3.3.6, il existe $\phi \in G(E_i/F)$ tel que $\beta_{ij} = \phi(\alpha_i)$. Donc $\beta_{ij}^{n_i} = \phi(\alpha_i^{n_i}) \in \phi(F_{i-1}) \subseteq \phi(E_{i-1}) = E_{i-1}$, cette dernière égalité suit du fait que E_{i-1} est galoisien sur F. Cela donne $\beta_{ij}^{n_i} \in E_{i-1} \subseteq E_{i-1}(\beta_{i1}, \ldots, \beta_{i,j-1})$. Par conséquent, E_i est radical sur E_{i-1} pour tout $1 \leq i \leq r$. Ceci achève la démonstration.

5.4. Définition. Soit $f(x) \in F[x]$. On dit que $f(x)$ est *résoluble par radicaux* sur F s'il existe une extension radicale $E : F$ telle que $f(x)$ est scindé sur E.

Remarque. Si $f(x)$ est résoluble par radicaux sur F, alors ses racines s'obtiennent à partir d'éléments de F par un nombre fini d'opérations de l'addition, de la soustraction, de la multiplication, de la division et de l'extraction de la racine.

Exemple. (1) Soit $a \in F$. Alors $x^n - a$ est résoluble par radicaux sur F.

(2) Le polynôme rationnel $f(x) = x^6 - 4x^3 + 1$ est résoluble par radicaux sur $\mathbb{Q}$. En effet, $f(x) = (x^3 - 2)^2 - 3$. Posons $\omega = -\frac{1}{2} + \frac{\sqrt{3}}{2}i$. Alors $\omega^2 = -\frac{1}{2} - \frac{\sqrt{3}}{2}i$ et $\omega^3 = 1$. Donc les racines de $f(x)$ sont comme suit:

$$\sqrt[3]{2+\sqrt{3}},\ \ \omega\sqrt[3]{2+\sqrt{3}},\ \ \omega^2\sqrt[3]{2+\sqrt{3}},\ \ \sqrt[3]{2-\sqrt{3}},\ \ \omega\sqrt[3]{2-\sqrt{3}},\ \ \omega^2\sqrt[3]{2-\sqrt{3}}.$$

Ainsi le corps de rupture de $f(x)$ sur $\mathbb{Q}$ est $E = \mathbb{Q}(\sqrt{3}, \sqrt[3]{2+\sqrt{3}}, \sqrt[3]{2-\sqrt{3}},\ \omega)$. On voit que E est radical sur $\mathbb{Q}$ pour la suite suivante:

$$\mathbb{Q} \subset \mathbb{Q}(\sqrt{3}) \subset \mathbb{Q}(\sqrt{3}, \sqrt[3]{2+\sqrt{3}}) \subset \mathbb{Q}(\sqrt{3}, \sqrt[3]{2+\sqrt{3}}, \sqrt[3]{2-\sqrt{3}}) \subset E.$$

On prouvera que $f(x)$ est résoluble par radicaux sur F si, et seulement si, le groupe de Galois de $f(x)$ est résoluble.

5.5. Lemme. Soit $n \geq 1$. Si $x^n - 1$ est scindé sur F, alors ses racines dans F forment un groupe cyclique d'ordre n.

Démonstration. Supposons que $x^n - 1$ est scindé sur F. Alors $\Sigma_n = \{a \in F \mid a^n = 1\}$ est évidemment un sous-groupe de F^*. Comme $\text{car}(F) = 0$, $D(x^n - 1) = nx^{n-1} \neq 0$. Ainsi $x^n - 1$ et $D(x^n - 1)$ sont co-premières. D'après la proposition 2.5.5, $x^n - 1$ n'a pas de racines multiples. D'où, $|\Sigma_n| = n$. Prenons $\zeta \in \Sigma_n$ d'ordre maximal d. D'après le lemme 2.6.6, $a^d = 1$, pour tout $a \in \Sigma_n$. Cela implique que $x^d - 1$ admet n racines distinctes. Par conséquen, $n \leq d$, et donc $d = n$. Cela veut dire $\Sigma_n =< \zeta >$. Ceci achève la démonstration.

Remarque. On dit que ζ est une racine n-ième primitive de l'unité de F si $< \zeta >= \Sigma_n$. Par exemple,

$$\zeta = \cos\frac{2\pi}{n} + i\sin\frac{2\pi}{n}$$

est une racine n-ième primitive de l'unité de $\mathbb{C}$.

5.6. Lemme. Pour tout $n \geq 1$, le groupe de Galois de $x^n - 1$ sur F est abélien.

Démonstration. Soit E un corps de rupture de $x^n - 1$. On veut montrer que $G(E/F)$ est abélien. Prenons $\zeta \in E$ une racine n-ième primitive de l'unité. Alors $E = F(\zeta)$. Soient $\phi, \psi \in G(E/F)$. Comme $\phi(\zeta), \psi(\zeta)$ sont racines de $x^n - 1$, on a $\phi(\zeta) = \zeta^i$ et $\psi(\zeta) = \zeta^j$ avec $0 \leq i, j < n$. Donc $(\phi\psi)(\zeta) = \zeta^{ij} = (\psi\phi)(\zeta)$. D'où, $\phi\psi = \psi\phi$. Ceci achève la démonstration.

5.7. Lemme. Soit $E = F(\alpha)$ avec $\alpha^n = a \in F$. Si $x^n - 1$ est scindé sur F, alors E est un corps de rupture de $x^n - a$ sur F avec $G(E/F)$ abélien.

Démonstration. Soit $\zeta \in F$ une racine n-ième primitive de l'unité. Pour tout $0 \leq i < n$, $(\zeta^i\alpha)^n - a = (\zeta^n)^i\alpha^n - a = 0$. Donc $\alpha, \zeta\alpha, \cdots, \zeta^{n-1}\alpha$ sont les racines de $x^n - a$. Comme $\zeta \in F$, $E = F(\alpha, \zeta\alpha, \ldots, \zeta^{n-1}\alpha)$ est un corps de rupture de $x^n - a$ sur F.

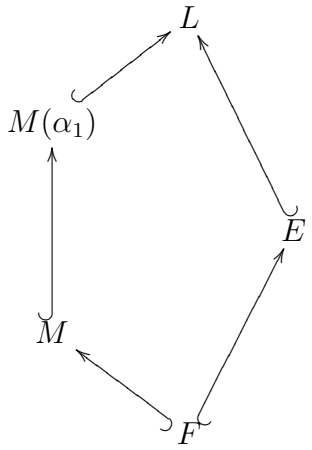
Soient $\phi, \psi \in G(E/F)$. Alors $\phi(\alpha), \psi(\alpha)$ sont des racines de $x^n - a$. Donc $\phi(\alpha) = \zeta^i\alpha$ et $\psi(\alpha) = \zeta^j\alpha$ avec $0 \leq i, j < n$. Ainsi $(\phi\psi)(\alpha) = \phi(\zeta^j\alpha) = \zeta^j\phi(\alpha) = \zeta^{j+i}\alpha = (\psi\phi)(\alpha)$. D'où, $\phi\psi = \psi\phi$. Ceci achève la démonstration.

5.8. Lemme. Soit E un corps de rupture d'un polynôme $f(x)$ sur F. Si E est radical sur F, alors $G(E/F)$ est résoluble.

Démonstration. Supposons $E = F(\alpha_1, \alpha_2, \ldots, \alpha_r)$, $\alpha_1^{n_1} \in F$, $\alpha_i^{n_i} \in F(\alpha_1, \ldots, \alpha_{i-1})$, $i = 2, \cdots, r$. Si $r = 0$, alors $E = F$. Donc $G(E/F)$ est trivial, et donc résoluble. Supposons que $r > 0$ et que l'énoncé est vrai pour $r - 1$.

Soit $\bar{E}$ la clôture algébrique de E. Prenons $\zeta \in \bar{E}$ une racine n_1-ième primitive de l'unité. Soit V l'ensemble des racines de $f(x)$ dans E. Posons $L = E(\zeta) = F(V,\ \zeta)$, $M = F(\zeta)$.

Considérons le diagramme



de sous-corps de L. Comme $L : F$ et $E : F$ sont galoisiennes, il suit du théorème 3.3.8(3) que $G(L/E)$ est normal dans $G(L/F)$ tel que $G(E/F) \cong G(L/F)/G(L/E)$. D'après le théorème 4.1.3(1), il suffit de montrer que $G(E/F)$ est résoluble. En effet, étant le corps de rupture de $x^{n_1} - 1$ sur F, M est galoisien sur F. De plus, d'après le lemme 5.7, $M(\alpha_1)$ est un corps de rupture de $x^{n_1} - \alpha_1^{n_1}$ sur M, et ainsi l'extension $M(\alpha_1) : M$ est galoisienne. D'après le théorème 3.3.8(3), on a une suite $G(L/M(\alpha_1)) \trianglelefteq G(L/M) \trianglelefteq G(L/F)$ avec

$$\frac{G(L/M)}{G(L/M(\alpha_1))} \cong G(M(\alpha_1)/M), \qquad \frac{G(L/F)}{G(L/M)} \cong G(M/F).$$

D'après les lemmes 5.6 et 5.7, $G(M(\alpha_1)/M)$ et $G(M/F)$ sont tous abéliens. Ainsi il suffit de montrer que $G(L/M(\alpha_1))$ est résoluble. En effet,

$$M(\alpha_1) \subseteq M(\alpha_1, \alpha_2) \subseteq \cdots \subseteq M(\alpha_1, \alpha_2, \ldots, \alpha_r) = F(\zeta, \alpha_1, \ldots, \alpha_r) = E(\zeta) = L$$

avec $\alpha_i^{n_i} \in F(\alpha_1, \ldots, \alpha_{i-1}) \subseteq M(\alpha_1, \ldots, \alpha_{i-1})$, $i = 2, \cdots, r$. Donc L est radical sur $M(\alpha_1)$. De plus, L est un corps de rupture de $(x^{n_1} - 1)f(x)$ sur $M(\alpha_1)$. D'après l'hypothèse de récurrence, $G(L/M(\alpha_1))$ est résoluble. Ceci achève la démonstration.

5.9. Lemme. Si $E : F$ est galoisienne alors, pour tout $\alpha \in E$,

$$N(\alpha) = \Pi_{\phi \in G(E/F)}\, \phi(\alpha) \in F,$$

appelé la *norme* de α.

Démonstration. Comme E est galoisien sur F, d'après le corollaire 3.3.5(1), on a $E^{G(E/F)} = F$. On se fixe $\psi \in G(E/F)$. Lorsque ϕ parcourt $G(E/F)$, $\psi\phi$ le parcourt aussi. Donc

$$\psi(N(\alpha)) = \Pi_{\phi \in G(E/F)}\, \psi(\phi(\alpha)) = \Pi_{\phi \in G(E/F)}\, (\psi\phi)(\alpha) = N(\alpha).$$

D'où, $N(\alpha) \in E^{G(E/F)}$. Ceci achève la démonstration.

Exemple. Considérons l'extension $\mathbb{C} : \mathbb{R}$. On sait que $G(\mathbb{C}/\mathbb{R}) = \{\mathbb{1}, \sigma\}$, où σ est la conjugaison. Ainsi la norme de $z = a + bi$ est $z\bar{z} = a^2 + b^2$.

5.10. Lemme. Soit $E : F$ une extension galoisienne avec $G(E/F)$ cyclique engendré par ϕ. Si $\alpha \in E$, alors $N(\alpha) = 1$ si, et seulement si, $\alpha = \phi(\beta)^{-1}\beta$ pour un certain $\beta \in E^*$.

Démonstration. La suffisance est évidente. Soit $\alpha \in E$ avec $N(\alpha) = 1$. En particulier, $\alpha \neq 0$. Posons $G(E/F) = \{\phi^0, \phi, \ldots, \phi^{n-1}\}$, et $\lambda_i = \phi^0(\alpha)\cdots\phi^i(\alpha) \in E$, $i = 0, \cdots n-1$. D'après la proposition 1.2.9, il existe $\gamma \in E$ tel que

$$\lambda_0\phi^0(\gamma) + \lambda_1\phi(\gamma) + \cdots + \lambda_{n-1}\phi^{n-1}(\gamma) \neq 0.$$

Posons $\delta_i = \lambda_i\phi^i(\gamma)$, $i = 0, \cdots n-1$, et $\beta = \sum_{i=0}^{n-1}\delta_i$. Alors $\beta \neq 0$, $\delta_0 = \alpha\gamma$, $\delta_{i+1} = \alpha\phi(\delta_i)$, $i = 0, \cdots n-1$, et $\delta_{n-1} = N(\alpha)\phi^{n-1}(\gamma) = \phi^{n-1}(\gamma)$. Or

$$\phi(\beta) = \sum_{i=0}^{n-1}\phi(\delta_i) = \alpha^{-1}\left(\sum_{i=0}^{n-2}\alpha\phi(\delta_i)\right) + \phi^n(\gamma) = \alpha^{-1}\sum_{i=1}^{n-1}\delta_i + \alpha^{-1}\delta_0 = \beta\alpha^{-1}.$$

D'où le résultat. La preuve s'achève.

5.11. Lemme. Soit $E : F$ une extension galoisienne de degré premier p. Si F contient une racine p-ième primitive de l'unité, alors $E = F(\beta)$ avec $\beta^p \in F$.

Démonstration. Soit $\zeta \in F$ une racine p-ième primitive de l'unité. En particulier $\zeta \neq 1$. Par l'hypothèse, $G(E/F) =< \phi >$ avec $o(\phi) = p$. Or

$$N(\zeta) = \Pi_{i=0}^{p-1}\,\phi^i(\zeta) = \Pi_{i=0}^{p-1}\,\zeta = \zeta^p = 1.$$

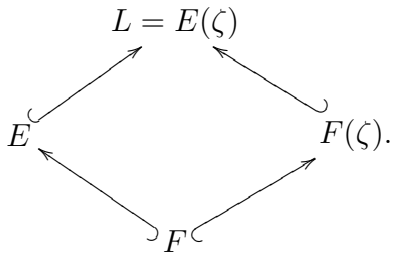
D'après le lemme 5.10, il existe $\beta \in E$ non nul tel que $\zeta = \beta\phi(\beta)^{-1}$. Ainsi $\phi(\beta) = \zeta^{-1}\beta$, et donc $\phi(\beta^p) = \zeta^{-p}\beta^p = \beta^p$. D'où, $\beta^p \in E^{G(E/F)} = F$. Si $\beta \in F$, alors $\zeta = \phi(\beta)^{-1}\beta = \beta^{-1}\beta = 1$, une contradiction. Donc $[F(\beta) : F] > 1$. Comme $[E : F] = p$, on a $E = F(\beta)$. Ceci achève la démonstration.

5.12. Théorème. Si $f(x) \in F[x]$ est non constant, alors $f(x)$ est résoluble par radicaux sur F si, et seulement si, le groupe de Galois de $f(x)$ est résoluble.

Démonstration. Soit E un corps de rupture de $f(x)$ sur F. En particulier, $E : F$ est galoisienne. Supposons d'abord qu'il existe un corps R contenant E tel que l'extension $R : F$ est radicale. D'après le lemme 5.3, il existe un corps N contenant R tel que $N : F$ est galoisienne et radicale. D'après le théorème 3.3.4, N est un corps de rupture d'un polynôme sur F, et donc $G(N/F)$ est résoluble d'après le lemme 5.8. Comme E est galoisien sur F, d'après le théorème 3.3.8, $G(N/E) \trianglelefteq G(N/F)$ tel que $G(E/F) \cong G(N/F)/G(N/E)$. Ainsi $G(E/F)$ est résoluble.

Supposons réciproquement que $G(E/F)$ est résoluble. On procède par récurrence sur $n = [E : F] = |G(E/F)|$. Si $n = 1$, alors $E = F$ est radical sur F. Supposons que $n > 1$

et la suffisance est vraie pour les extensions de degré $< n$. Prenons un sous-groupe normal maximal H de $G(E/F)$. Alors $G(E/F)/H$ est simple et résoluble. D'après la proposition 4.1.6, $G(E/F)/H$ est d'ordre premier p. Soit L un corps de rupture de $x^p - 1$ sur E. Alors $L = E(\zeta)$, où ζ est une racine p-ième primitive de l'unité. D'après le lemme 5.6, $G(L/E)$ est abélien. Considérons le diagramme de sous-corps de L suivant:



Remarquons que L est un corps de rupture de $(x^p - 1)f(x)$ sur F. Donc L est galoisien sur F. Comme E est galoisien sur F, d'après le théorème 3.3.8(3), $G(L/E) \trianglelefteq G(L/F)$ tel que $G(L/F)/G(L/E) \cong G(E/F)$, qui est résoluble par l'hypothèse. Comme $G(L/E)$ est abélien, $G(L/F)$ est résoluble. Si $\sigma \in G(L/F(\zeta)) \subseteq G(L/F)$, alors $\sigma(E) = E$ d'après le lemme 3.3.7. Ainsi

$$\Phi : G(L/F(\zeta)) \to G(E/F) : \sigma \mapsto \sigma|_E$$

est un homomorphisme de groupes. Si $\sigma|_E = \mathbb{1}_E$, alors $\sigma \in G(L/E)$ tel que $\sigma(\zeta) = \zeta$, et donc $\sigma = \mathbb{1}_L$. Cela veut dire que Φ est injectif. Comme $G(E/F)$ est résoluble par l'hypothèse, d'après le théorème 4.1.3(1), $G(L/F(\zeta))$ est résoluble. On considérera séparément les deux cas suivants.

(1) Supposons que Φ n'est pas surjectif. Alors $|G(L/F(\zeta))| < |G(E/F)|$. Remarquons que L est un corps de rupture de $f(x)$ sur $F(\zeta)$. Par hypothèse de récurrence, il existe un corps R contenant L tel que $R : F(\zeta)$ soit radicale. Or $F(\zeta) : F$ est radicale car $\zeta^p = 1 \in F$. Donc $R : F$ est radicale avec $E \subseteq R$, c'est-à-dire, $f(x)$ est résoluble par radicaux.

(2) Supposons que Φ est surjectif, et donc un isomorphisme. Alors $H^* = \Phi^{-1}(H)$ est un sous-groupe normal de $G(L/F(\zeta))$ d'indice p, puisque H est un sous-groupe normal de $G(E/F)$ d'indice p. Posons $M = L^{H^*}$, et considérons la suite

$$F \subset F(\zeta) \subset M \subset L$$

de sous-corps de L. D'après le théorème 3.3.8(3), M est galoisien sur $F(\zeta)$ et

$$|G(M/F(\zeta))| = [M : F(\zeta)] = [G(L/F(\zeta)) : H^*] = p.$$

Il suit du lemme 5.11 que $M = F(\zeta)(\beta)$ avec $\beta^p \in F(\zeta)$. Par conséquent, $M : F$ est radicale car $F(\zeta)$ est radical sur F.

Enfin, L est un corps de rupture de $f(x)$ sur M et $G(L/M) = H^*$ est résoluble d'ordre $< |G(L/F(\zeta))| = |G(E/F)|$. Par l'hypothèse de récurrence, il existe un corps R contenant L tel que $R : M$ soit radicale. Donc $R : F$ est radicale avec $E \subseteq R$. C'est-à-dire $f(x)$ est résoluble par radicaux sur F. Ceci achève la démonstration.

5.13. Théorème. Si F est un corps de caractéristique zéro, alors tout polynôme non constant sur F de degré < 5 est résoluble par radicaux sur F.

Démonstration. Soit $f(x) \in F[x]$ de degré < 5. Prenons E un corps de rupture de $f(x)$ sur F et V l'ensemble des racines distinctes de $f(x)$ dans E. Posons $n = |V|$, alors $n < 5$. Pour tout $\phi \in G(E/F)$, $\phi|_V$ est une permutation de V. Ceci donne un homomorphisme de groupes:

$$\Phi : G(E/F) \mapsto S_n : \phi \mapsto \phi|_V.$$

Comme $E = F(V)$, Φ est injectif. Par conséquent, $G(E/F)$ est isomorphe à un sous-groupe de S_n. D'après les théorèmes 4.1.7 et 4.1.3, $G(E/F)$ est résoluble. Ainsi $f(x)$ est résoluble par radicaux d'après le théorème 5.12. Ceci achève la démonstration.

Soit $n \geq 1$. On dit que $\alpha_1, \ldots, \alpha_n \in \mathbb{R}$ sont *algébriquement indépendants* sur $\mathbb{Q}$ si $f(\alpha_1, \ldots, \alpha_n) \neq 0$, pour tout $f \in \mathbb{Q}[x_1, \ldots, x_n]$ non nul.

5.14. Proposition. Pour tout entier $n \geq 1$, il existe des nombres réels $\alpha_1, \ldots, \alpha_n$ qui sont algébriquement indépendants sur $\mathbb{Q}$.

Démonstration. Si $n = 1$, le résultat est vrai car il existe des nombres réels transcendants. Supposons que $n > 1$ et il existe des nombres réels $\alpha_1, \ldots, \alpha_{n-1}$ qui sont algébriquement indépendants sur $\mathbb{Q}$. Si $f(x_1, \ldots, x_{n-1}, x_n)$ est un polynôme non nul sur $\mathbb{Q}$ à n variables, alors $f(\alpha_1, \ldots, \alpha_{n-1}, x)$ est un polynôme non nul sur $\mathbb{Q}[x]$. Ainsi l'ensemble $Z(f) = \{\alpha \in \mathbb{R} \mid f(\alpha_1, \ldots, \alpha_{n-1}, \alpha) = 0\}$ est fini. Comme $\mathbb{Q}[x_1, \ldots, x_{n-1}]^*$ est dénombrable, l'ensemble $\cup_{f \in \mathbb{Q}[x_1, \ldots, x_{n-1}]^*} Z(f)$ l'est aussi. Comme $\mathbb{R}$ est non dénombrable, il existe $\alpha_n \in \mathbb{R}$ n'appartenant pas à $\cup_{f \in \mathbb{Q}[x_1, \ldots, x_{n-1}]^*} Z(f)$. C'est-à-dire, $\alpha_1, \ldots, \alpha_{n-1}, \alpha_n$ sont algébriquement indépendants sur $\mathbb{Q}$. Ceci achève la démonstration.

5.15. Théorème. Soient $\alpha_1, \ldots, \alpha_n \in \mathbb{R}$ algébriquement indépendants sur $\mathbb{Q}$. Soit $G(x) = (x - \alpha_1) \cdots (x - \alpha_n)$ un polynôme sur $\mathbb{Q}(s_1, \ldots, s_n)$ où $s_i = \sum_{r_1 + \cdots r_n = i} \alpha_1^{r_1} \cdots \alpha_n^{r_n}$.

(1) Le groupe de Galois de $G(x)$ sur $\mathbb{Q}(s_1, \ldots, s_n)$ est S_n.

(2) Pour tout $n \geq 5$, $G(x)$ n'est pas résoluble par radicaux sur $\mathbb{Q}(s_1, \ldots, s_n)$.

Démonstration. Posons $F = \mathbb{Q}(s_1, \ldots, s_n)$. Alors $E = F(\alpha_1, \ldots, \alpha_n)$ est le corps de rupture de $G(x)$ sur F. Pour tout $1 \leq i \leq n$, posons $g_i(x) = (x - \alpha_i) \cdots (x - \alpha_n)$ un polynôme sur $F(\alpha_1, \ldots, \alpha_{i-1})$. Si $i < n$, on voit aisément que $\alpha_j \notin F(\alpha_1, \ldots, \alpha_{i-1})$ pour tout j avec $i \leq j \leq n$. On prétend que g_i est irréductible sur $F(\alpha_1, \ldots, \alpha_{i-1})$. C'est évident pour $i = n$.

Supposons que $i < n$. Si $\alpha_{i+1} + \cdots + \alpha_n \in F(\alpha_1, \ldots, \alpha_{i-1})$, alors $\alpha_i \in F(\alpha_1, \ldots, \alpha_{i-1})$, une contradiction. Ainsi $(x - \alpha_{i+1}) \cdots (x - \alpha_n) \notin F(\alpha_1, \ldots, \alpha_{i-1})[x]$. De même, on voit que tous les facteurs propres de $g_i(x)$ n'appartient pas à $F(\alpha_1, \ldots, \alpha_{i-1})[x]$. On en déduit que $g_i(x)$ est le polynôme minimal de α_i sur $F(\alpha_1, \ldots, \alpha_{i-1})$. Ceci nous donne $[E : F] = n!$. Donc $G(E/F)$ est isomorph à S_n. D'où, on a l'énoncé (1). Or la partie (2) suit immédiatement des théorèmes 5.12 et 4.1.5. Ceci achève la démonstration.

5.14. Exercices

1. Pour chacun des nombres suivants, trouver une extension radicale de $\mathbb{Q}$ qui le contient:

   (1) $\frac{\sqrt{11} - \sqrt[7]{23}}{\sqrt[4]{5}}$. (2) $(\sqrt{6} + 2\sqrt[3]{5})^4$.

   (3) $\frac{2\sqrt[5]{5} - 4}{\sqrt{1+\sqrt{99}}}$. (4) $\sqrt[3]{11}\sqrt[5]{\frac{7+\sqrt{3}}{2}} + \sqrt[4]{1 + \sqrt[3]{4}}$.

2. Montrer que $f(x) = x^6 - 10x^4 + 31x^2 - 30$ est résoluble par radicaux sur $\mathbb{Q}$.

3. Soit p un nombre premier et soit F un corps sur lequel le polynôme $x^p - 1$ est scindé. Montrer, pour tout $a \in F$, que $x^p - a$ est soit scindé soit irréductible sur F.

4. Soit F un corps de caractéristique zéro. Si $f(x) \in F[x]$ est non constant et résoluble par radicaux sur F, montrer qu'il existe une suite de corps

   $$F = F_0 \subset F_1 \subset \cdots \subset F_{s-1} \subset F_s$$

   telle que $f(x)$ est scindé sur F_s et $[F_i : F_{i-1}]$ est premier pour tout $1 \leq i \leq n$. *Indication*: Utiliser le numéro 3 de l'Exercices 4.3.

5. Soit E un corps fini ayant P pour corps premier. Montrer que $G(E/P)$ est un groupe cyclique d'ordre $[E : P]$. *Indication*: Considérer l'application de Frobenius.

6. Soit p un nombre premier, et soit F un corps sur lequel $x^p - 1$ est scindé. Si $E = F(\alpha)$ avec $\alpha^p \in F$ est une extension de F de degré p, montrer que $G(E/F)$ est cyclique d'ordre p ou 1.

7. Soit $\zeta = e^{\frac{2\pi i}{p}} \in \mathbb{C}$, où p est un premier. Montrer que $G(\mathbb{Q}(\zeta)/\mathbb{Q})$ est cyclique d'ordre $p - 1$.

8. Soit F un corps de caractéristique non divisant n sur lequel $x^n - 1$ est scindé. Soit E le corps de rupture de $x^n - a$ sur F. Donner un homomorphisme injectif $\phi : G(E/F) \to \mathbb{Z}_n$ et montrer que cette application est surjective si et seulement si $x^n - a$ est irréductible.

Chapitre VI: Construction géométrique à la règle et au compas

Posons $P_0 = \{(0,0),(1,0)\}$ deux points du plan $\mathbb{R}^2$. Supposons que $n \geq 0$ et qu'on a défini P_n. Désignons par D_n l'ensemble des droites passant par deux points distincts de P_n, et par C_n l'ensemble des cercles de centre d'un point de P_n ayant comme rayon la distance de deux points distincts de P_n. On définit alors P_{n+1} comme étant l'ensemble des points p qui est (1) soit dans P_n,

soit (2) l'intersection de deux droites distinctes de D_n,

soit (3) une intersections de deux cercles distincts de C_n,

soit (4) une intersection d'une droite de D_n et d'un cercle de C_n.

Par récurrence, on obtient une suite infinie d'ensembles de points de $\mathbb{R}^2$ comme suit:

$$P_0 \subseteq P_1 \subseteq \cdots \subseteq P_n \subseteq \cdots .$$

Exemple. $P_1 = \{(0,0),(1,0),(-1,0),(2,0),(\frac{1}{2},\frac{\sqrt{3}}{2}),(\frac{1}{2},-\frac{\sqrt{3}}{2})\}$.

6.1. Définition. (1) Un point (a,b) de $\mathbb{R}^2$ est dit *constructible* si $(a,b) \in \cup_{n=0}^{\infty} P_n$.

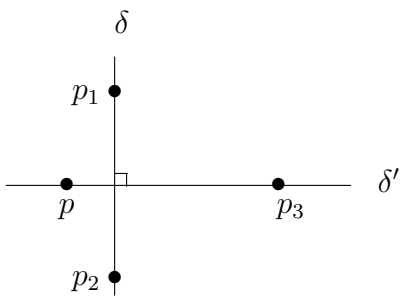
(2) Une droite dans $\mathbb{R}^2$ est dite *constructible* si elle appartient à $\cup_{n=0}^{\infty} D_n$.

(3) Un cercle dans $\mathbb{R}^2$ est dit *constructible* s'il appartient à $\cup_{n=0}^{\infty} C_n$.

Remarque. Les intersections de deux droites constructibles (respectivement, de deux cercles constructibles, d'une droite constructible et d'un cercle constructible) sont constructibles.

6.2. Lemme. Soit p un point constructible et δ une droite constructible. Alors la perpendiculaire, ainsi que la parallèle, à δ passant par p est constructible.

Démonstration. On sait que δ contient un point constructible p_1 ($\neq p$). On peut supposer que $p, p_1 \in P_n$ pour un certain $n \geq 1$. Soit p_2 ($\neq p$) une intersection de δ et le cercle de centre p de rayon $\overline{pp_1}$. Alors $p_2 \in P_{n+1}$. Soit p_3 une intersection des cercles de rayon $\overline{p_1p_2}$ et de centre p_1 et de centre p_2, respectivement. Alors $p_3 \in P_{n+2}$. Or la droite δ' passant par p et p_3 appartient à D_{n+2} et est perpendiculaire à δ. Ceci est illustré par le diagramme suivant:



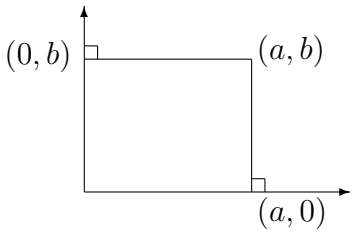
La preuve s'achève.

6.3. Définition. Un complexe $z = a + bi$ est dit *constructible* si le point $(a, b) \in \mathbb{R}^2$ est constructible.

Remarque. Un nombre réel a est constructible si le point $(a, 0)$ est constructible.

6.4. Lemme. Un complexe $z = a + bi$ est constructible si, et seulement si, les réels a et b le sont.

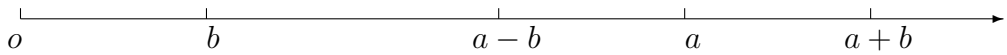
Démonstration. L'énoncé suit immédiatement du diagramme suivant:



La preuve s'achève.

6.5. Lemme. Si $a, b \in \mathbb{R}$ sont constructibles, alors $a \pm b$ le sont.

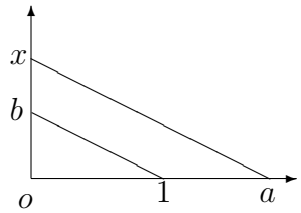
Démonstration. L'énoncé suit immd́eatement du diagramme suivant:



La preuve s'achève.

6.6. Lemme. Si $a, b \in \mathbb{R}$ sont constructibles, alors ab l'est.

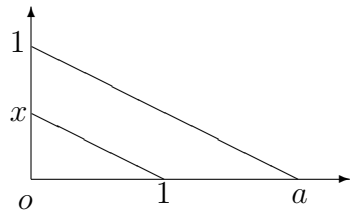
Démonstration. Considérons le diagramme suivant:



où $b1//xa$. Donc $\triangle bo1 \sim \triangle xoa$. Par conséquent, $\dfrac{x}{b} = \dfrac{a}{1}$, c'est-à-dire, $x = ab$. Ceci achève la démonstration.

6.7. Lemme. Si $a \in \mathbb{R}^*$ est constructible, alors a^{-1} l'est.

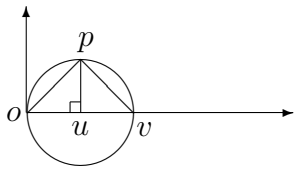
Démonstration. Considérons le diagramme suivant:



où $x1//1a$. Donc $\triangle xo1 \sim \triangle 1oa$. Par conséquent, $\frac{1}{a} = \frac{x}{1} = x$. Ceci achève la démonstration.

6.8. Lemme. Si $a \in \mathbb{R}^+$ est constructible, alors $\sqrt{a}$ l'est.

Démonstration. Considérons le diagramme suivant:



où $u = (1, 0)$, $v = (1 + a, 0)$, et $p = (1, x)$. Comme $\triangle oup \sim \triangle puv$, on a $\frac{x}{a} = \frac{1}{x}$, c'est-à-dire, $x = \sqrt{a}$. Ceci achève la démonstration.

6.9. Théorème. Les complexes constructibles forment un sous-corps de $\mathbb{C}$ qui est le plus petit parmi les sous-corps fermés pour les racines carrées et pour la conjugaison.

Démonstration. Il suit facilement des lemmes 6.4, 6.5, 6.6, 6.7, 6.8 et 6.9 que les complexes constructibles forment un sous-corps de $\mathbb{C}$ qui est fermé pour les racines carrées et pour la conjugaison. Soit E un sous-corps de $\mathbb{C}$ qui est fermé pour les racines carrées et pour la conjugaison. En particulier, $i \in E$. Si $a + bi \in E$, comme $a - bi \in E$, on a $a \in E$, et donc $b \in E$. Ceci montre que $a + bi \in E$ si et seulement si $a, b \in E$. En outre, si $a, b, c \in E$ avec $a \neq 0$, alors les racines du polynôme $ax^2 + bx + c$ appartiennent à E.

On se fixe un nombre constructible $z = a + bi$. Alors $(a, b) \in \cup_{n\geq 0} P_n$. Il est évident que $z \in E$ lorsque $(a, b) \in P_0$. Supposons que $n > 0$ et $z \in E$ lorsque $(a, b) \in P_i$ avec $0 \leq i < n$. Soient $(c_1, d_1), (c_2, d_2) \in P_{n-1}$. It suit de l'hypothèse de récurence que $c_i, d_i \in E$, $i = 1, 2$. Comme E est fermé pour les racinces carrées, la distance entre (c_1, d_1) et (c_2, d_2) appartient à E. Supposons maintenant que $(a, b) \in P_n \backslash P_{n-1}$. Considérons les cas suivants.

(1) Le point (a, b) est l'intersection de deux droites L_1 et L_2 dans D_{n-1}. Par définition, L_i passe par deux points distincts (a_i, b_i) et (c_i, d_i) appartenant à P_{n-1}. Donc

$$(a - a_i)(d_i - b_i) = (c_i - a_i)(b - b_i), i = 1, 2.$$

En résolvant le système, on trouve que $a, b \in E$ puisque $a_i, b_i, c_i, d_i \in E$, $i = 1, 2$. Ainsi $z = a + bi \in E$.

(2) Le point (a, b) est l'intersection d'une droite L passant par deux points distincts (a_1, b_1) et (a_2, b_2) dans P_{n-1} et d'un cercle de centre $(c, d) \in P_{n-1}$ et de rayon r, la distance entre deux points dans P_{n-1}. Donc $(a-a_1)(b_2-b_1) = (a_2-a_1)(b-b_1)$ et $(a-c)^2+(b-d)^2 = r^2$. Comme $a_2 \neq a_1 \neq 0$ ou $b_2 - b_1 \neq 0$ et $a_i, b_i, c, d, r \in E$, $i = 1, 2$, on voit que $a, b \in E$. Donc $z = a + bi \in E$.

(3) Le point (a, b) est l'intersection de deux cercles respectivement de centres $(a_i, b_i) \in P_{n-1}$ et de rayons $r_i \in E$, $i = 1, 2$. Alors $(a - a_i)^2 + (b - b_i)^2 = r_i^2$, $i = 1, 2$. Ceci nous donne $(a_2 - a_1)(2a - (a_1 + a_2)) + (b_2 - b_1)(2b - (b_1 + b_2)) = r_1^2 - r_2^2$. Comme $a_2 - a_1 \neq 0$ ou $b_2 - b_1 \neq 0$ et $a_i, b_i, r_i \in E$, $i = 1, 2$, on trouve $a, b \in E$. Par conséquent, $z = a + bi \in E$. Ceci achève la démontsration.

Remarque. Tous les nombres rationnels sont constructibles.

6.10. Théorème. Un complexe z est constructible si, et seulement si, z appartient à un sous-corps de $\mathbb{C}$ de la forme $\mathbb{Q}(\alpha_1, \alpha_2, \ldots, \alpha_r)$ avec $\alpha_i^2 \in \mathbb{Q}(\alpha_1, \ldots, \alpha_{i-1})$, $i = 1, \cdots, r$.

Démonstration. Soit F le corps des nombres constructibles. Posons E l'ensemble des complexes satisfaisant à la condition énoncée dans le théorème. On se fixe un nombre $z \in E$, qui appartient à $\mathbb{Q}(\alpha_1, \alpha_2, \ldots, \alpha_r)$, où $\alpha_i^2 \in \mathbb{Q}(\alpha_1, \ldots, \alpha_{i-1})$, $i = 1, \cdots, r$.

(1) D'abord, $\mathbb{Q} \subseteq F$. Supposons que $\mathbb{Q}(\alpha_1, \ldots, \alpha_{i-1}) \subseteq F$. Alors $\alpha_i^2 = a_{i-1} \in F$, c'est-à-dire, $\alpha_i = \sqrt{a_{i-1}}$ avec a_{i-1} constructible. D'après le théorème 6.9, α_i est constructible. Par conséquent, $\mathbb{Q}(\alpha_1, \ldots, \alpha_{i-1}, \alpha_i) \subseteq F(\alpha_i) \subseteq F$. Ceci montre que $\mathbb{Q}(\alpha_1, \ldots, \alpha_r) \subseteq F$. En particulier, $z \in F$. Ainsi $E \subseteq F$.

(2) On a $\bar{z} \in \overline{\mathbb{Q}(\alpha_1, \alpha_2, \ldots, \alpha_r)} = \mathbb{Q}(\bar{\alpha_1}, \ldots, \bar{\alpha_r})$, où $\bar{\alpha_i}^2 = \overline{\alpha_i^2} \in \overline{\mathbb{Q}(\alpha_1, \ldots, \alpha_{i-1})} = \mathbb{Q}(\bar{\alpha_1}, \ldots, \bar{\alpha}_{i-1})$, $i = 1, \cdots, r$. D'où, $\bar{z} \in E$. Donc E est fermé pour la conjugaison.

(3) On a $\sqrt{z} \in \mathbb{Q}(\alpha_1, \alpha_2, \ldots, \alpha_r, \sqrt{z})$, où $\alpha_i^2 \in \mathbb{Q}(\alpha_1, \ldots, \alpha_{i-1})$ pour tout $1 \leq i \leq r$, et $(\sqrt{z})^2 = z \in \mathbb{Q}(\alpha_1, \alpha_2, \ldots, \alpha_r)$. D'où, $\sqrt{z} \in E$. Donc E est fermé pour les racines carrées.

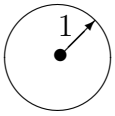
(4) Soit $y \in E$ appartenant à $\mathbb{Q}(\beta_1, \beta_2, \ldots, \beta_t)$, où $\beta_i^2 \in \mathbb{Q}(\beta_1, \ldots, \beta_{j-1})$, $j = 1, \cdots, t$. Posant $\alpha_{i+j} = \beta_j$, $j = 1, \cdots, t$, on a $y \pm z, yz, yz^{-1} \in \mathbb{Q}(\alpha_1, \alpha_2, \ldots, \alpha_{r+t})$ avec $\alpha_i^2 \in \mathbb{Q}(\alpha_1, \ldots, \alpha_{i-1})$, $i = 1, \cdots, r + t$. Donc $y \pm z, yz, yz^{-1} \in E$. Ainsi E est un sous-corps de $\mathbb{C}$. D'après le théorème 6.9, $F \subseteq E$. Ainsi $E = F$. Ceci achève la démonstration.

6.11. Corollaire. Si $z \in \mathbb{C}$ est constructible, alors $[\mathbb{Q}(z) : \mathbb{Q}] = 2^n$ avec $n \geq 0$.

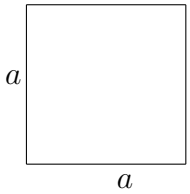
Démonstration. Supposons que z est constructible. D'après le théorème 6.10, $z \in \mathbb{Q}(\alpha_1, \alpha_2, \ldots, \alpha_r)$ avec $\alpha_1^2 \in \mathbb{Q}$, et $\alpha_i^2 \in \mathbb{Q}(\alpha_1, \ldots, \alpha_{i-1})$, pour tout $1 \leq i \leq r$. On voit aisément que $[\mathbb{Q}(\alpha_1, \ldots, \alpha_{i-1}, \alpha_i) : \mathbb{Q}(\alpha_1, \alpha_2, \ldots, \alpha_{i-1})] = 1$ ou 2. Donc $[\mathbb{Q}(\alpha_1, \ldots, \alpha_r) : \mathbb{Q}] = 2^s$ avec $0 \leq s \leq r$. Par conséquent, $[\mathbb{Q}(z) : \mathbb{Q}] = 2^n$ avec $0 \leq n \leq s$. Ceci achève la démonstration.

6.12. Théorème. La quadrature du cercle (c'est-à-dire, la construction d'un carré ayant même aire qu'un cercle donné) à la règle et au compas est impossible.

Démonstration. Considérons le cercle



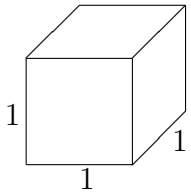
d'aire π. Supposons que l'on peut construire un carré



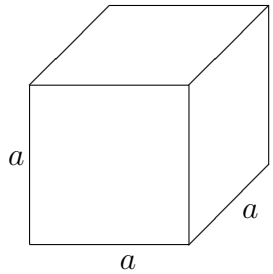
d'aire π, c'est-à-dire, $a^2 = \pi$. Alors $\sqrt{\pi} = a$ est un nombre constructible. D'après le corollaire 6.11, $[\mathbb{Q}(\sqrt{\pi}) : \mathbb{Q}] = 2^n$ avec $n \geq 0$, qui est impossible car $\sqrt{\pi}$ est transcendant sur $\mathbb{Q}$. La preuve s'achève.

6.13. Théorème. La duplication du cube (c'est-à-dire, la construction d'un cube de volume double d'un cube donné) à la règle et au compas est impossible.

Démonstration. Considérons le cube



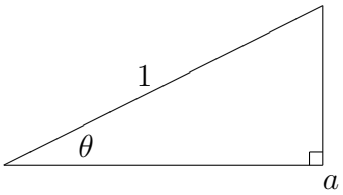
de volume 1. Supposons que l'on peut construire un cube



de volume 2, c'est-à-dire, $a^3 = 2$. Alors $\sqrt[3]{2}$ est un nombre constructible. Mais $[\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}] = 3$, qui contredit le corollaire 6.11. La preuve s'achève.

6.14. Théorème. La trisection de l'angle à la règle et au compas est impossible.

Démonstration. Considérons le triangle



où $a = \cos\theta$. On voit que l'angle θ est constructible si, et seulement si, le nombre $\cos\theta$ est constructible.

Or comme $\cos\frac{\pi}{3} = \frac{1}{2}$ est constructible, l'angle $\frac{\pi}{3}$ est constructible. Supposons que l'on peut triséquer $\frac{\pi}{3}$. Alors $b = \cos\frac{\pi}{9}$ est constructible. Comme $\cos 3\theta = 4\cos^3\theta - 3\cos\theta$, on a $4b^3 - 3b = \frac{1}{2}$. Ainsi b est une racine de $x^3 - \frac{3}{4}x - \frac{1}{8}$, ce qui est irréductible sur $\mathbb{Q}$. Par conséquent, $[\mathbb{Q}(b) : \mathbb{Q}] = 3$, une contradiction au corollaire 6.11. Ceci achève la démonstration.

6.15. Lemme. Si $z \in \mathbb{C}$ est tel que $\mathbb{Q}(z) : \mathbb{Q}$ soit galoisienne, alors z est constructible si, et seulement si, $[\mathbb{Q}(z) : \mathbb{Q}] = 2^n$ avec $n \geq 0$.

Démonstration. La nécessité suit du corollaire 6.11. Supposons maintenant que $[\mathbb{Q}(z) : \mathbb{Q}] = 2^n$ avec $n > 0$. Comme $\mathbb{Q}(z) : \mathbb{Q}$ est galoisienne, d'après le théorème 3.3.8, il existe une suite

$$\mathbb{Q} = F_0 \subset F_1 \subset \cdots \subset F_{r-1} \subset F_r = \mathbb{Q}(z)$$

de sous-corps de $\mathbb{Q}(z)$ telle que $[F_i : F_{i-1}] = 2$. Prenons $\beta \in F_i \backslash F_{i-1}$. Alors β est une racince d'un polynôme $x^2 + bx + c$ avec $b, c \in F_{i-1}$. Posons $\alpha_i = 2\beta + b$. Alors $\alpha_i \in F_i \backslash F_{i-1}$ et $\alpha_i^2 \in F_{i-1}$. Ainsi $F_i = F_{i-1}(\alpha_i)$. D'après le théorème 6.10, z est constructible. Ceci achève la démonstration.

6.16. Définition. La fonction d'Euler ϕ est définie pour $n \geq 1$ par

$$\phi(n) = |\{j \mid 0 < j < n,\ (j, n) = 1\}|.$$

Le résultat suivant est classique dans la théorie des nombres.

6.17. Proposition. Si $n = p_0^{e_0} p_1^{e_1} \cdots p_s^{e_s}$, où $e_i > 0$ et les p_i sont des nombres premiers deux à deux distincts, alors

$$\phi(n) = (p_0^{e_0} - p_0^{e_0 - 1})(p_1^{e_1} - p_1^{e_1 - 1}) \cdots (p_s^{e_s} - p_s^{e_s - 1}).$$

Exemple. $\phi(36) = \phi(2^2 3^3) = (2^2 - 2)(3^2 - 3) = 12$.

6.18. Lemme. Soit $n \geq 1$. Pour tout j avec $0 \leq j < n$, le complexe

$$\zeta_j = \cos\frac{2j\pi}{n} + i\sin\frac{2j\pi}{n}$$

est une racine n-ième primitive de l'unité si, et seulement si, $(n, j) = 1$. Par conséquent, il y a exactement $\phi(n)$ racines n-ième primitives de l'unité.

Démonstration. D'abord, les ζ_j avec $0 \leq j \leq n-1$ sont les racines de $x^n - 1$, qui forment un groupe cyclique d'ordre n engendré par ζ_1. Pour tout $0 \leq j < n$, on a $\zeta_j = (\zeta_1)^j$. D'après le lemme 2.6.6(1), $o(\zeta_j) = \frac{n}{(n,j)}$. Par conséquent, ζ_j est une racine n-ième primitive de l'unité si, et seulement si, $o(\zeta_j) = n$ si, et seulement si, $n = \frac{n}{(n,j)}$ si, et seulement si, $(n, j) = 1$. Ceci achève la démonstration.

6.19. Définition. Soit $n \geq 1$. Le polynôme

$$\Phi_n(x) = \Pi_{0<j<n;\ (j,\,n)=1}\ (x - \zeta_j)$$

s'appelle le *n-ième polynôme cyclotomique.*

Remarque. $\Phi_n(x)$ est de degré $\phi(n)$.

Exemple. $\Phi_4(x) = (x - \zeta_1)(x - \zeta_3) = (x - i)(x + i) = x^2 + 1$, qui est irréductible sur $\mathbb{Q}$.

6.20. Théorème. $\Phi_n(x)$ avec $n \geq 1$ est un polynôme rationnel irréductible.

Dḿonstration. D'abord, $E = \mathbb{Q}(\zeta)$ est le corps de rupture de $x^n - 1$. Ainsi $E : \mathbb{Q}$ est une extension galoisienne. Pour tout $1 \leq j < n$, il est évident que ζ_j est une racine n-ième primitive de l'unité si et seulement si $E = \mathbb{Q}(\zeta_j)$. Soit $\phi \in G(E/\mathbb{Q})$. Si ζ_j est une racine n-ième primitive de l'unité, alors $E = \phi(E) = \phi(\mathbb{Q}(\zeta_j)) = \mathbb{Q}(\phi(\zeta_j))$. D'où, $\phi(\zeta_j)$ est aussi une racine n-ième primitive de l'unité. Ceci implique que ϕ fixe le polynôme $\Phi_n(x)$. Comme $E : \mathbb{Q}$ est galoisienne, $\Phi_n(x)$ est un polynôme rationnel. Soient α, β des racines n-ième primitives de l'unité. Alors $\beta = \alpha^p$ pour un certain $p > 0$ et $E = \mathbb{Q}(\alpha) = \mathbb{Q}(\beta)$. Comme $\{1, \alpha, \cdots, \alpha^{n-1}\}$ et $\{1, \beta, \cdots, \beta^{n-1}\}$ sont des $\mathbb{Q}$-bases de E, il existe une bijection $\mathbb{Q}$-linéaire $\psi : E \to E$ tel que $\psi(\alpha^i) = \beta^i$, $i = 0, 1, \cdots, n-1$. Pour tous $i, j \geq 0$, posant $i + j = ns + r$ avec $0 \leq r < n$, on a

$$\psi(\alpha^i \alpha^j) = \psi(\alpha^{i+j}) = \psi(\alpha^r) = \beta^r = \beta^{i+j} = \psi(\alpha^i)\psi(\alpha^j).$$

On en déduit facilement que ψ est un homomorphism de corps. Donc $\psi \in G(E/\mathbb{Q})$. Ceci montre que l'action de $G(E/\mathbb{Q})$ sur les racines de $\Phi_n(x)$ est transitive. Ayant aucune racine multiple, $\Phi_n(x)$ est irréductibe sur $\mathbb{Q}$. Ceci achève la dḿonstration.

Remarque. Si $\zeta \in \mathbb{C}$ est une racine n-ième primitive de l'unité, alors $m_{\mathbb{Q}}^{\zeta}(x) = \Phi_n(x)$. Ainsi $[\mathbb{Q}(\zeta) : \mathbb{Q}] = \phi(n)$.

6.21. Définition. Pour $n \geq 0$, on dit que $F_n = 2^{2^n} + 1$ est le *n-ième nombre* de Fermat. Un nombre premier p s'appelle un *premier de Fermat* si p est un nombre de Fermat.

Exemple. Pour $n = 0, 1, 2, 3, 4$, on a des premiers de Fermat $3, 5, 17, 257$ et 65537. Mais les premiers $7, 11, 13, 19$ ne sont pas des nombres de Fermat.

Remarque. (1) Il est connu que F_5 n'est pas premier.

(2) Si $p = 2^n + 1$ avec $n \geq 0$ est premier, alors il est un premier de Fermat. En effet, si $n = mq$ avec $q > 1$ impaire et $m \geq 1$, alors $a = 2^m \geq 2$. Donc

$$p = a^q + 1 = (a+1)((a^{q-1} - a^{q-2}) + \cdots + (a^2 - a) + 1)$$

n'est pas premier.

6.22. Théorème de Gauss. Soit $n \geq 3$. Alors le n-polygone régulier est constructible à la régle et au compas si, et seulement si, $n = 2^r p_1 \cdots p_s$, où $r, s \geq 0$ et $p_1, \ldots, p_s$ des premiers de Fermat deux à deux distincts.

Démonstration. Posons $n = 2^r p_1^{e_1} \cdots p_s^{e_s}$, où $r, s \geq 0$, $e_j > 0$ et $p_1, \ldots, p_s$ sont des nombres premiers impaires distincts. Alors le n-polygone régulier est constructible si, et seulement si, l'angle $\frac{2\pi}{n}$ est constructible si, et seulement si, $\cos\frac{2\pi}{n}$ et $\sin\frac{2\pi}{n}$ sont constructibles si, et seulement si, $\zeta = \cos\frac{2\pi}{n} + i\sin\frac{2\pi}{n}$ est constructible. Comme $\mathbb{Q}(\zeta) : \mathbb{Q}$ est galoisienne, ceci est équivalent à $[\mathbb{Q}(\zeta) : \mathbb{Q}] = 2^t$ avec $t \geq 0$ si, et seulement si, $\phi(n) = 2^t$ avec $t \geq 0$ si, et seulement si, $2^{r-1} p_1^{e_1 - 1} \cdots p_s^{e_s - 1}(p_1 - 1) \cdots (p_s - 1) = 2^t$ si, et seulement si, $e_1 = \cdots = e_s = 1$ et $p_i - 1 = 2^{m_i}$, c'est-à-dire, chacun des p_i est un premier de Fermat. Ceci achève la démonstration.

Exemple. Le n-polygône régulier est constructible pour $n = 3, 5, 17$, et non constructible pour $n = 7, 11, 13, 19$.

6.23. Exercices

1. Montrer que les complexes constructibles forment un sous-corps de $\mathbb{C}$.
2. Vérifier que le polynôme $x^3 - \frac{3}{4}x - \frac{1}{8}$ est irréductible sur $\mathbb{Q}$.