# Cours de théorie des groupes

Denis Benois

Institut de Mathématiques, Université de Bordeaux, 351, cours de la Libération
33405 Talence, France
*Email address*: denis.benois@math.u-bordeaux.fr

# Tables des matières

CHAPITRE 1

# Groupes

## 1. Lois de composition

**Définition.** *Soit $X$ un ensemble. On appelle loi de composition interne sur $X$ (ou loi de composition sur $X$ tout court) une application*

$$X \times X \to X, \qquad (x, y) \mapsto x * y.$$

Un même ensemble peut être muni des lois de composition différentes.

**Exemples.** $(\mathbf{Z}, +)$, $(\mathbf{Z}, \cdot)$, $(\mathbf{Z}, -)$.

**Définition.** *1) Une loi de composition $*$ sur $X$ est dite*

- *associative si et seulement si*

$$\forall x, y, z \in X, \qquad (x * y) * z = x * (y * z).$$

- *commutative si et seulement si*

$$\forall x, y \in X, \qquad x * y = y * x.$$

*2) On dit que $e \in X$ est un élément neutre pour la loi $*$ si*

$$\forall x \in X, \qquad x * e = e * x = x.$$

**Proposition 1.1.** *Si $X$ possède un élément neutre pour $*$, il est unique.*

Preuve. Supposons que $e$ et $e'$ sont deux éléments neutres pour $*$. Alors

$$e' = e' * e = e.$$

■

**Définition.** *Supposons que $(X, *)$ possède un élément neutre $e \in X$. On dit que deux élément $x$ et $x' \in X$ sont inverses si*

$$x * x' = x' * x = e.$$

**Proposition 1.2.** *Supposons la loi associative. Si $x$ admet un inverse, celui-ci est unique.*

Preuve. Supposons que $x'$ et $x''$ sont deux inverses de $x$. Alors

$$x' = x' * e = x' * (x * x'') = (x' * x) * x'' = e * x'' = x''.$$

■

Nous adoptons la notation suivante:

$$x^{-1} \text{ désigne l'inverse de } x.$$

**Exemples.** 1) 0 est l'element neutre de $(\mathbf{Z}, +)$. Pour tout $x \in \mathbf{Z}$, $-x$ est l'inverse de $x$ pour l'addition.

2) 1 est l'élément neutre de $(\mathbf{Z}, \cdot)$. Dans $(\mathbf{Z}, \cdot)$, seuls 1 et $-1$ ont un inverse:

$$1 \cdot 1 = 1, \qquad (-1) \cdot (-1) = 1.$$

## 2. Groupes

**Définition.** *On appelle groupe un ensemble non vide $(G, \cdot)$ muni d'une loi de composition vérifiant les propriétés suivantes, les axiomes de groupe :*

1) *(associativité) $*$ est associative ;*
2) *(élément neutre) $*$ possède un élément neutre (dans $G$) ;*
3) *(élément inverse) tout élément $x \in G$ est inversible.*

*Si, en plus, la loi est commutative, on dit que $G$ est commutatif ou abélien.*

Si $G$ est fini, on appelle ordre de $G$ son cardinal $|G|$.
Pour simplifier la notation on va écrire $(G, \cdot)$ plutôt que $(G, *)$.

**Exemples.** 1) $(\mathbf{Z}, +)$ est un groupe abélien.
2) $(\mathbf{Z}, \cdot)$ n'est pas un groupe.
3) $(\mathbf{Q}^*, \cdot)$ est un groupe abélien.

**Exercice 1.** Soit $K$ un corps. On note $\mathrm{M}_n(K)$ l'ensemble des matrices carrées de taille $n$ à coefficients dans $K$. On pose

$$\mathrm{GL}_n(K) = \{X \in \mathrm{M}_n(K) \mid \det(X) \neq 0\}.$$

Alors $\mathrm{GL}_n(K)$ est un groupe pour la multiplication matricielle, appelé le groupe général linéaire de degré $n$. Si $n \geqslant 2$, ce groupe n'est pas abélien.

**Exercice 2.** Soit $X$ un ensemble et soit $S(X) = \{f : X \to X \mid f \text{ bijection}\}$. $fg(x) = f(g(x))$. Montrer les assertions suivantes :
a) le produit est associatif ;
b) $\mathrm{id}_X$ est un élément neutre ;
c) l'inverse de $f$ est l'application réciproque $f^{-1}$.
On en déduit que $S(X)$ est un groupe. On l'appelle le groupe symétrique de $X$.

**Définition.** *Soir $G$ un groupe. On dit qu'une partie non vide $H \subset G$ est un sous-groupe de $G$ si elle possède les propriétés suivantes :*

1) $e \in H$;
2) $x, y \in H \Rightarrow xy \in H$;
3) $x \in H \Rightarrow x^{-1} \in H$.

L'ensemble $H \subset G$ avec la loi de composition induite par celle de $G$ est un groupe.

**Exemples.** 1) Pour tout groupe $G$, $\{e\}$ et $G$ sont des sous-groupes de $G$. On dit qu'un sous-groupe $H$ est propre si $H \neq \{0\}, G$.
2) $(\mathbf{Z}, +) \subset (\mathbf{R}, +)$.
3) Soit $K$ un corps et soit

$$\mathrm{SL}_n(K) = \{X \in \mathrm{M}_n(K) \mid \det(X) = 1\}.$$

Alors $\mathrm{SL}_n(K)$ est un sous-groupe de $\mathrm{GL}_n(K)$. On l'appelle le groupe spécial linéaire de rang $n$.

**Propriétés 2.1.** 1) *Soit $H$ une partie non-vide de $G$. Les conditions suivantes sont équivalentes:*
   *a) $H$ est un sous-groupe de $G$*
   *b) $x \in G$, $y \in G \Rightarrow xy^{-1} \in G$.*
2) *Soit $(H_i)_{i\in I}$ une famille de sous-groupes de $G$. Montrer que $\cap_{i\in I} H_i$ est un sous-groupe de $G$.*
3) *Soient $H_1$ et $H_2$ deux sous-groupes de $G$. Montrer que $H_1 \cup H_2$ est un sous-groupe de $G$ si et seulement si soit $H_1 \subset H_2$ soit $H_2 \subset H_1$.*

**Définition.** *Soit $S \subset G$. On appelle sous-groupe engendré par $S$ et l'on note $< S >$ le plus petit sous-groupe de $G$ contenant $S$ :*

$$< S >= \cap_{S\subset H} H.$$

**Exercice 3.** Soit $S^{-1} = \{s^{-1} \mid s \in S\}$. Montrer que

$$< S >= \{g_1 \cdot g_2 \cdots g_{m-1} \cdot g_m \mid \text{où } m \geqslant 1 \text{ et } g_i \in S \cup S^{-1} \text{ pour tout } 1 \leqslant i \leqslant m\}.$$

**Définition.** *Soit $x \in G$. On appelle sous-groupe monogène engendré par $x$ le groupe $< x >$ . On dit que $G$ est monogène s'il existe $x \in G$ tel que $G =< x >$ . Un groupe cyclique est un groupe qui est à la fois monogène et fini.*

**Définition.** *On appelle ordre de $x$ et l'on note* $\mathrm{ord}(x)$ *le plus petit $n \geqslant 1$ tel que $x^n = e$. Si $x^n \neq e$ pour tout $n \geqslant 1$, on pose* $\mathrm{ord}(x) = +\infty$.

**Propriété 2.2.** *Soit $x$ un élément d'ordre fini $n$. Si $x^m = e$, alors $n \mid m$.*

Preuve. Supposons que $\mathrm{ord}(x) = n < \infty$. Alors pour tout $m \in \mathbf{Z}$ on peut effectuer la division euclidienne par $n$ :

$$m = nq + r, \qquad q, r \in \mathbf{Z}, \quad 0 \leqslant r \leqslant n-1.$$

Donc

$$\boxed{x^m = x^{nq}x^r = x^r, \qquad \text{où } r \text{ est un entier } 0 \leqslant r \leqslant n-1.} \tag{1}$$

Supposons maintenant que $x^m = e$. Alors $x^r = e$ avec $0 \leqslant r \leqslant n-1$, d'où $r = 0$. Nous avons donc prouvé que $n \mid m$. ∎

**Théorème 2.3.** *Soit $x \in G$.*

i) *Si* $\mathrm{ord}(x) = n < \infty$, *alors $< x >$ est un sous-groupe d'ordre $n$:*

$$< x >= \{e, x, x^2, \ldots, x^{n-1}\}.$$

ii) *Si* $\mathrm{ord}(x) = +\infty$, *alors*

$$< x >= \{\ldots, x^{-2}, x^{-1}, e, x, x^2, \ldots\},$$

*où les éléments $x^m$ ($m \in \mathbf{Z}$) sont deux à deux distincts.*

PREUVE. a) Il découle de l'exercice 3 que dans les deux cas on a :

$$< x >= \{x^m \mid m \in \mathbf{Z}\}.$$

Supposons d'abord que $\text{ord}(x) = +\infty$. Montrons que les éléments $x^m$ sont deux à deux distincts. En effet, si $x^m = x^k$ avec $m \geqslant k$, alors $x^{m-k} = e$. Comme $\text{ord}(x) = +\infty$, on en déduit que $m - k = 0$, d'où $m = k$.

b) Supposons que $\text{ord}(x) = n < \infty$. La formule (1)) montre que pour tout $m \in \mathbf{Z}$, on a $x^m = x^r$ avec $0 \leqslant r \leqslant n-1$. Donc

$$< x >= \{\ldots, x^{-2}, x^{-1}, e, x, x^2, \ldots\},$$

Pour montrer que les éléments $x^r$ $(0 \leqslant r \leqslant n-1)$ sont deux à deux distincts, supposons que

$$x^r = x^\ell, \qquad \text{pour } 0 \leqslant r \leqslant \ell \leqslant n-1.$$

Alors $x^{\ell-r} = e$, d'où $n \mid (\ell - r)$ par la propriété 2.2. Comme $0 \leqslant \ell - r \leqslant n-1$, on en déduit que $\ell = r$. ∎

## 3. Classes suivant un sous-groupe

Soit $G$ un groupe. Pour chaque $g \in G$, on note $L_g$ l'application multiplication à gauche par $g$ :

$$\begin{aligned} L_g : & G \to G, \\ & x \mapsto gx. \end{aligned}$$

De même, on note $R_g$ l'application multiplication à droite par $g$ :

$$\begin{aligned} R_g : & G \to G, \\ & x \mapsto xg. \end{aligned}$$

**Propriété 3.1.** *Les applications $L_g$ et $R_g$ sont bijectives.*

PREUVE. Soit $y \in G$. En multipliant à gauche par $g^{-1}$ les deux membres de l'équation $gx = y$, on trouve que $x = g^{-1}y$ est une solution de cette équation et une seule. Donc $L_g$ est bijective. Le même argument montre que $R_g$ est bijective. ∎

Pour désigner que $H$ est un sous-groupe de $G$, on écrit :

$$H \leqslant G.$$

**Définition.** *Soit $H \leqslant G$. Pour tout $x \in G$, on appelle classe à gauche de $x$ suivant $H$ l'ensemble*

$$xH = \{xh \mid h \in H\}.$$

*On appelle classe à droite de $x$ suivant $H$ l'ensemble*

$$Hx = \{hx \mid h \in H\}.$$

On note $x \underset{H}{\sim} y$ et $x \overset{H}{\sim} y$ les relation sur $G$ définies comme suit :

$$\begin{aligned} x \underset{H}{\sim} y \quad & \Leftrightarrow x^{-1}y \in H, \\ x \overset{H}{\sim} y \quad & \Leftrightarrow xy^{-1} \in H. \end{aligned}$$

**Théorème 3.2.** i) *Les relations* $\underset{H}{\sim}$ *et* $\overset{H}{\sim}$ *sont des relations d'équivalence.*

ii) *La classe de* $x$ *suivant la relation* $\underset{H}{\sim}$ *est* $xH$. *La classe de* $x$ *suivant la relation* $\overset{H}{\sim}$ *est* $Hx$.

iii) *Pour tout* $x \in G$, *l'application* $L_x$ *induit la bijection*

$$H \to xH,$$
$$h \mapsto xh.$$

*De même, pour tout* $x \in G$, *l'application* $R_x$ *induit la bijection*

$$H \to Hx,$$
$$h \mapsto hx.$$

Preuve. i) On montre que $\underset{H}{\sim}$ est un relation d'équivalence.

*Réflexivité.* Comme $x^{-1}x = e \in H$, on a $x \underset{H}{\sim} x$.

*Symétrie.* Supposons que $x \underset{H}{y}$. Alors $x^{-1}y \in H$. Comme $H$ est un sous-groupe de $G$, on en déduit que $\left(x^{-1}y\right)^{-1} \in H$. Donc

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

ce qui montre que $y \underset{H}{\sim} x$.

*Transitivité.* Supposons que $x \underset{H}{y}$ et $y \underset{H}{z}$. Alors $x^{-1}y \in H$ et $y^{-1}z \in H$. Donc

$$x^{-1}z = (x^{-1}y) \cdot (y^{-1}z) \in H,$$

ce qui montre que $x \underset{H}{\sim} z$.

Donc $\underset{H}{\sim}$ est une relation d'équivalence. La preuve que $\overset{H}{\sim}$ est un relation d'équivalence est analogue.

ii) On a

$$x \underset{H}{\sim} y \quad \Leftrightarrow x^{-1}y \in H \quad \Leftrightarrow y = xh, \quad \text{où } h \in H.$$

Donc la classe de $x$ suivant la relation $\underset{H}{\sim}$ est :

$$\mathrm{cl}_H(x) := \{y \in G \mid x \underset{H}{\sim} y\} = \{xh \mid h \in H\} = xH.$$

Un calcul analogue montre que la classe de $x$ suivant la relation $\overset{H}{\sim}$ est :

$$\mathrm{cl}^H(x) := \{y \in G \mid x \overset{H}{\sim} y\} = \{hx \mid h \in H\} = Hx.$$

iii) Clair. ∎

L'ensemble des classes d'équivalence pour la relation $\underset{H}{\sim}$ donne une partition de $G$ :

(2) $$\boxed{G = \bigcup_{i \in I} x_i H \qquad \text{(réunion disjointe des classes à gauche).}}$$

De même, l'ensemble des classes d'équivalence pour la relation $\overset{H}{\sim}$ donne une partition

$$\boxed{G = \bigcup_{j\in J} Hy_j \qquad \text{(réunion disjointe des classes à droite).}} \tag{3}$$

En général, ces partitions ne coïncident pas.

L'application

$$\begin{aligned} i : G &\to G, \\ g &\mapsto g^{-1} \end{aligned}$$

est un bijection (il suffit de remarquer que $i \circ i = \mathrm{id}_G$, donc $i^{-1} = i$). On peut facilement voir que $i(xH) = Hx^{-1}$ pour tout $x \in G$. Donc

$$G = \bigcup_{i\in I} Hx_i^{-1}$$

est une partition de $G$ en classes à droites disjointes. Donc cette partition coïncide avec (3). On en déduit que l'application $xH \mapsto Hx^{-1}$ établit une bijection entre l'ensemble des classes à gauche et l'ensemble des classes à droite suivant $H$. En particulier, les ensembles $I$ et $J$ ont même cardinal :

$$|I| = |J|.$$

**Définition.** *On pose* $(G : H) = |I|$ *et on l'appelle indice de* $H$ *dans* $G$.

Dans ce cours, nous allons utiliser cette notation uniquement pour les sous-groupes d'indice fini. On a le théorème important suivant :

**Théorème 3.3** (théorème de Lagrange)**.** *Soit* $G$ *un groupe fini. Alors*

$$|G| = (G : H) \cdot |H|.$$

Preuve. Le théorème découle de la partition (2) et du fait que $|xH| = |H|$ pour tout $x \in G$. ∎

**Corollaire 3.4.** *Si* $G$ *est fini, alors* $|H|$ *divise* $|G|$.

**Corollaire 3.5.** *Soit* $G$ *un groupe fini et soit* $x \in G$. *Alors* $\mathrm{ord}(x)$ *divise* $|G|$.

Preuve. D'après le théorème 2.3, on a

$$\left|\langle x\rangle\right| = \mathrm{ord}(x).$$

Il suffit d'appliquer le corollaire précédent. ∎

**Corollaire 3.6.** *Soit* $p$ *un nombre premier. Tout groupe d'ordre* $p$ *est cyclique.*

Preuve. Soit $G$ un groupe d'ordre $p$. On choisit un élément $x \in G$ tel que $x \neq e$. Comme $\mathrm{ord}(x)$ divise $p$ et $p$ est un nombre premier, on en déduit que $\mathrm{ord}(x) = p$. Donc $< x >$ est un sous-groupe de $G$ d'ordre $p$, d'où $G =< x >$ . ∎

**Exercice 4.** *Soient* $K \subset H \subset G$ *deux sous-groupes d'un groupe* $G$. *Supposons que* $(G : K) < +\infty$. *Montrer que* $(G : H)$ *et* $(H : K)$ *sont finis et que*

$$(G : K) = (G : H)(H : K).$$

## 4. Groupe quotient

Soient $G$ un groupe et $H \leqslant G$.

**Définition.** *On dit que $H$ est distingué ou normal dans $G$ et l'on note $H \trianglelefteq G$ si*

$$xH = Hx, \qquad \forall x \in H.$$

**Propriété 4.1.** *$H \trianglelefteq G$ si et seulement si*

$$x^{-1}Hx \subseteq H, \qquad \forall x \in G.$$

Preuve. Il est clair que si $H \trianglelefteq G$, alors $x^{-1}Hx = H \subseteq H$. Réciproquement, supposons que

$$x^{-1}Hx \subset H, \qquad \forall x \in G. \tag{4}$$

En remplaçant $x$ par $x^{-1}$, on trouve que

$$xHx^{-1} \subseteq H, \qquad \forall x \in G,$$

d'où

$$H = x^{-1}(xHx^{-1})x \subseteq x^{-1}Hx, \qquad \forall x \in G. \tag{5}$$

Les inclusions réciproques (4) et (5) montrent que $x^{-1}Hx = H$, d'où $Hx = Hx$ pour tout $x \in G$. ∎

**Exemples.** 1) $G$ abélien. Tout sous-groupe est normal.
2) $(G : H) = 2$. Alors $H$ est normal (exercice).

**Exercice 5.** Montrer que $\mathrm{SL}_n(K) \trianglelefteq \mathrm{GL}_n(K)$.

**Remarques 4.2.** 1) Si $K \leqslant H \leqslant G$ et $K \trianglelefteq G$, alors $K \trianglelefteq H$. Remarquons que $K \trianglelefteq H$ et $H \trianglelefteq G$ n'implique pas que $K \trianglelefteq G$.

2)$H \trianglelefteq G$ si et seulement si les relations d'équivalence $\underset{H}{\sim}$ et $\overset{H}{\sim}$ coïncident. Cela découle du fait que $\mathrm{cl}_H(x) = \mathrm{cl}^H(x)$ pour tout $x \in G$.

**Propriété 4.3.** *Si $x' \underset{H}{\sim} x$ et $y' \underset{H}{\sim} y$, alors $x'y' \underset{H}{\sim} xy$.*

Preuve. Si $x' \underset{H}{\sim} x$ et $y' \underset{H}{\sim} y$, alors il existe $h, k \in H$ tels que $x' = xh$ et $y' = yk$. On a:

$$x'y' = (xh)(yk) = x(hy)k.$$

Comme $hy \in Hy = yH$, il existe $h' \in H$ tel que $hy = yh'$. Donc

$$x'y' = x(yh')k = (xy)(h'k) \in xyH.$$

On en déduit que $x'y' \underset{H}{\sim} xy$. ∎

Soit $H \trianglelefteq G$. On note

$$G/H = G/\underset{H}{\sim} = \{\mathrm{cl}_H(x) \mid x \in G\}$$

le quotient de $G$ par la relation $\underset{H}{\sim}$. Rappelons que $\mathrm{cl}_H(x) = xH = Hx = \mathrm{cl}^H(x)$. On munit $G/H$ d'une loi de composition en posant :

$$\mathrm{cl}_H(x) \cdot \mathrm{cl}_H(y) = \mathrm{cl}_H(xy). \tag{6}$$

On déduit de la propriété 4.3 que cette loi de composition est bien définie.

**Théorème 4.4.** *La loi de composition* (6) *munit $G/H$ d'une structure de groupe.*

PREUVE. *Associativité.* Soient $x, y, z \in G$. Alors

$$(\mathrm{cl}_H(x)\cdot\mathrm{cl}_H(y))\cdot\mathrm{cl}_H(z) = \mathrm{cl}_H(xy)\cdot\mathrm{cl}_H(z) = \mathrm{cl}_H((xy)z) = \\ \mathrm{cl}_H(x(yz)) = \mathrm{cl}_H(x)\cdot\mathrm{cl}_H(yz) = \mathrm{cl}_H(x)\cdot(\mathrm{cl}_H(y)\cdot\mathrm{cl}_H(z)).$$

■

**Définition.** *Le groupe $G/H$ est appelé le groupe quotient de $G$ par $H$.*

**Exemples.** Pour tout entier $n \geqslant 1$, on a $n\mathbf{Z} \subset\trianglelefteq \mathbf{Z}$. Alors

$$x \underset{n\mathbf{Z}}{\sim} y \Leftrightarrow x - y \in n\mathbf{Z} \Leftrightarrow x \equiv y \pmod{n}.$$

Donc $\mathrm{cl}_{n\mathbf{Z}}(x)$ coïncide avec la classe résiduelle de $x$ modulo $n$ :

$$\mathrm{cl}_{n\mathbf{Z}}(x) = \overline{x} = \{y \in \mathbf{Z} \mid y \equiv x \pmod{n}\}.$$

Le groupe quotient est le groupe $\mathbf{Z}/n\mathbf{Z}$ des classes de résidu modulo $n$. C'est un groupe cyclique d'ordre $n$, il est engendré, par exemple, par la classe $\overline{1}$.

## 5. Homomorphismes

Un homomorphisme de groupes (ou morphisme de groupes tout court) est une application entre deux groupes qui respecte la structure de groupe.

**Définition.** *i) Soient $(G, *)$ et $(G', \star)$ deux groupes munis des lois de composition $*$ et $\star$ respectivement. Un morphisme de $G$ dans $G'$ est une application $f : G \to G'$ telle que*

$$f(x_1 * x_2) = f(x_1) \star f(x_2), \qquad \forall x_1, x_2 \in G.$$

*ii) On dit qu'un morphisme $f$ est un monomorphisme s'il est injectif, un épimorphisme s'il est surjectif, un isomorphisme s'il est bijectif.*

*iii) Un morphisme d'un groupe dans lui-même est appelé un endomorphisme. Un automorphisme de $G$ est un morphisme qui est à la fois un isomorphisme et un endomorphisme.*

**Exemples.** 1) Soit $(\mathbf{R}_+^*, \cdot)$ l'ensemble des réels strictement positifs $\mathbf{R}_+^* = \{x \in \mathbf{R} \mid x > 0\}$ muni de la multiplication usuelle. On vérifie facilement que $(\mathbf{R}_+^*, \cdot)$ est un groupe. Soit $(\mathbf{R}, +)$ le groupe des nombres réels pour l'addition usuelle. L'application

$$\log : \mathbf{R}_+^* \to \mathbf{R},$$
$$x \mapsto \log(x)$$

est un morphisme de groupes :

$$\log(x_1 x_2) = \log(x_1) + \log(x_2).$$

En outre, log est une bijection. Donc c'est un isomorphisme entre $(\mathbf{R}_+^*, \cdot)$ et $(\mathbf{R}, +)$.

2) Soit $K$ un corps. On note $K^*$ le groupe multiplicatif de $K$. L'application

$$\det : \mathrm{GL}_n(K) \to K^*$$
$$X \mapsto \det(X)$$

est un morphisme de groupes. En effet,

$$\det(XY) = \det(X)\det(Y).$$

**Convention.** Pour simplifier la rédaction, on va remplacer les lois de composition $*$ et $\star$ par la loi multiplicative.

**Exercice 6.** *Montrer que si $f : G \to G'$ et $\varphi : G' \to G''$ sont des homomorphismes, alors la composition $\varphi f : G \to G''$ l'est aussi. Si $f$ et $\varphi$ sont des isomorphismes, alors $\varphi f$ l'est.*

**Exercice 7.** *Soit $G$ un groupe.*

*1) Montrer que l'ensemble* $\mathrm{Aut}(G)$ *des automorphismes de $G$ est un sous-groupe de $S(G)$.*

*2)Pour tout $g \in G$, on définit l'application $c_g : G \to G$ en posant $c_g(x) = gxg^{-1}$. Montrer que $c_g$ est un automorphisme de $G$. On appelle $c_g$ l'automorphisme intérieur associé à $g$.*

*3) Montrer que l'application $g \mapsto c_g$ est un homomorphisme $G \to \mathrm{Aut}(G)$.*

*4) On note* $\mathrm{Int}(G)$ *l'ensemble des automorphismes intérieurs de $G$. Montrer que* $\mathrm{Int}(G) \trianglelefteq \mathrm{Aut}(G)$.

**Propriétés 5.1.** *Soit $f : G \to G'$ un morphisme de groupes. Alors :*

1) $f(e) = e'$.
2) $f(x^{-1}) = f(x)^{-1}$.

Preuve. 1) Comme $e = e \cdot e$, on a :

$$f(e) = f(e \cdot e) = f(e)f(e).$$

En multipliant à gauche par $f(e)^{-1}$ les deux membres de cette équation, on obtient que $e' = f(e)$.

2) Soit $x \in G$. Comme $x \cdot x^{-1} = e$, on a :

$$f(x)f(x^{-1}) = f(x \cdot x^{-1}) = f(e) = e'.$$

De même, $f(x^{-1})f(x) = e'$. Donc $f(x^{-1}) = f(x)^{-1}$. ∎

**Définition.** *Si $f : G \to G'$ est un morphisme de groupes, alors le noyau et l'image de $f$ sont définis par*

$$\ker(f) = \{x \in G \mid f(x) = e_{G'}\} \qquad \textit{(noyau } f\textit{)},$$
$$\mathrm{Im}(f) = f(G) \qquad \textit{(image de } f\textit{)},$$

**Exemples.** *1) Soit $H \trianglelefteq G$ et soit $p : G \to G/H$ l'application $p(x) = \mathrm{cl}_H(x)$. Alors $p$ est un epimorphism et* $\ker(p) = H$.

Dans le théorème suivant, nous résumons les principales propriétés du noyau et de l'image d'un morphisme.

**Théorème 5.2.** *Soit $f : G \to G'$ un morphisme. Alors :*

i) $\ker(f)$ *est un sous-groupe distingué de* $G$*;*
ii) $\mathrm{Im}(f) = f(G)$ *est un sous-groupe de* $G'$*;*
iii) $f$ *est un monomorphisme si et seulement si* $\ker(f) = \{e\}$.

Preuve. i) Soient $x, y \in \ker(f)$. Alors

$$f(xy^{-1}) = f(x)f(y^{-1}) = f(x)f(y)^{-1} = e' \cdot e' = e'.$$

Donc $xy^{-1} \in \ker(f)$ si $x, y \in \ker(f)$. On en déduit que $\ker(f) < G$.

Soient $g \in G$ et $x \in \ker(f)$. Alors

$$f(g^{-1}xg) = f(g^{-1})f(x)f(g) = f(g^{-1}) \cdot e' \cdot f(g) = f(g^{-1})f(g) = f(g^{-1}g) = f(e) = e'.$$

On en déduit que $g^{-1}xg \in \ker(f)$. Donc $g \cdot \ker(f) \cdot g^{-1} \subseteq \ker(f)$ pour tout $g \in G$, ce qui montre que $\ker(f) \trianglelefteq G$.

ii) Soient $y_1, y_2 \in \mathrm{Im}(f)$. Alors il existe $x_1, x_2 \in G$ tels que $f(x_1) = y_1$ et $f(x_2) = y_2$. On a:

$$y_1 y_2^{-1} = f(x_1)f(x_2)^{-1} = f(x_1)f(x_2^{-1}) = f(x_1 x_2^{-1}) \in \mathrm{Im}(f).$$

Donc $\forall y_1, y_2 \in \mathrm{Im}(f)$, $y_1 y_2^{-1} \in \mathrm{Im}(f)$. On en déduit que $\mathrm{Im}(f) \leqslant G'$.

iii) Il est clair que si $f$ est un monomorphisme, alors $\ker(f) = \{e\}$. Réciproquement, supposons que $\ker(f) = \{e\}$. Alors :

$$f(x_1) = f(x_2) \;\Rightarrow\; f(x_1 x_2^{-1}) = f(x_1)f(x_2)^{-1} = e' \;\Rightarrow\; x_1 x_2^{-1} = e \;\Rightarrow\; x_1 = x_2.$$

On en déduit que $f$ est injectif. ∎

Soit $f$ une application d'un ensemble $E$ dans un ensemble $E'$:

$$f : E \to E'.$$

Alors $f$ induit la relation d'équivalence "avoir même image par $f$" sur l'ensemble $E$:

$$x_1 \mathcal{R} x_2 \quad \Leftrightarrow \quad f(x_1) = f(x_2).$$

Pour tout $x \in E$, on note $\bar{x}$ la classe de $x$ pour la relation $R$. Soit

$$E/\mathcal{R} = \{\bar{x} \mid x \in E\}$$

l'ensemble quotient de $E$ par la relation $\mathcal{R}$. Alors l'application

$$\begin{aligned} \bar{f} \; &: E/\mathcal{R} \to E', \\ &\bar{x} \mapsto f(x) \end{aligned}$$

est bien définie, injective, et induit une bijection de $E/\mathcal{R}$ sur $\mathrm{Im}(f) := f(E)$. On a donc un diagramme

$$\begin{array}{ccc} E & \xrightarrow{\;f\;} & E' \\ \downarrow{\scriptstyle p} & & \uparrow{\scriptstyle i} \\ E/\mathcal{R} & \xrightarrow{\;\bar{f}\;} & \mathrm{Im}(f), \end{array}$$

où $p : E \to E/\mathcal{R}$ est l'application $p(x) = \bar{x}$ et $i$ désigne l'inclusion de $\mathrm{Im}(f)$ dans $E'$. Ce diagramme est commutatif, à savoir:

$$f = i \circ \bar{f} \circ p.$$

On remarque que l'application $p$ est surjective.

Soit maintenant $f : G \to G'$ un morphisme de groupes. On considère la relation $\mathcal{R}$ sur $G$. Alors :

$$x_1 \mathcal{R} x_2 \quad \Leftrightarrow \quad f(x_1) = f(x_2) \quad \Leftrightarrow \quad f(x_1^{-1}x_2) = e' \quad \Leftrightarrow \quad x^{-1}y \in \ker(f).$$

Donc la relation $\mathcal{R}$ coïncide avec la relation $\underset{\ker(f)}{\sim}$ associée au sous-groupe distingué $\ker(f)$ de $G$. La classe $\bar{x}$ pour la relation $\mathcal{R}$ coïncide avec la classe de $x$ suivant $\ker(f)$ :

$$\bar{x} = x \cdot \ker(f) = \ker(f) \cdot x.$$

En particulier, $G/\mathcal{R} = G/\ker(f)$, et l'on a un diagramme :

$$\begin{array}{ccc} G & \xrightarrow{\ f\ } & G' \\ \downarrow{\scriptstyle p} & & \uparrow{\scriptstyle i} \\ G/\ker(f) & \xrightarrow{\ \bar{f}\ } & \mathrm{Im}(f), \end{array}$$

On remarque que dans ce diagramme, $p : G \to /\ker(f)$ est un epimorphisme.

**Théorème 5.3** (Premier théorème d'isomorphisme)**.** *L'application $\bar{f}$ est un isomorphisme de groupes:*

$$\bar{f} \ : \ G/\ker(f) \simeq \mathrm{Im}(f).$$

Preuve. On sait déjà que $\bar{f}$ est une bijection. Soient $x_1, x_2 \in G$. Alors

$$\bar{f}(\bar{x}_1\bar{x}_2) = \bar{f}(\overline{x_1x_2}) = f(x_1x_2) = f(x_1)f(x_2) = \bar{f}(\bar{x}_1)\bar{f}(\bar{x}_2).$$

Donc $\bar{f}$ est un morphisme de groupes. ∎

**Exemples.** *Soit $K$ un corps. Le morphisme*

$$\det \ : \ \mathrm{GL}_n(K) \to K^*, \qquad X \mapsto \det(X)$$

*est un momorphisme surjectif et* $\ker(\det) = \mathrm{SL}_n(K)$ *est un sous-groupe distingué de* $\mathrm{GL}_n(K)$. *On a un isomorphisme :*

$$\mathrm{GL}_n(K)/\mathrm{SL}_n(K) \simeq K^*.$$

Soient $X, Y \subseteq G$ deux parties d'un groupe $G$. On pose

$$XY := \{xy \mid x \in X,\ y \in Y\}.$$

**Propriété 5.4.** *Soient $N \trianglelefteq G$ et $H \leqslant G$. Alors $HN$ est un sous-groupe de $G$.*

Preuve. a) Soient $x_1 = h_1n_1$ et $x_2 = h_2n_2$ ($h_1, h_2 \in H$, $n_1, n_2 \in N$) deux éléments de $HN$. Alors

$$x_1x_2 = (h_1n_1) \cdot (h_2n_2) = h_1(n_1h_2)n_2.$$

Comme $N \trianglelefteq G$, on a $Nh_2 = h_2N$ et il existe $n_1' \in N$ tel que $n_1h_2 = h_2n_1'$. Donc

$$x_1x_2 = h_1(h_2n_1')n_2 = (h_1h_2) \cdot (n_1'n_2), \qquad h_1h_2 \in H, \quad n_1'n_2 \in N.$$

On en déduit que $x_1 x_2 \in HN$.

b) Soit $x = hn \in HN$. Alors

$$x^{-1} = (hn)^{-1} = n^{-1}h^{-1}.$$

Comme $Nh^{-1} = h^{-1}N$, il existe $n' \in N$ tel que $n^{-1}h^{-1} = h^{-1}n'$, et on obtient que $x^{-1} = h^{-1}n' \in HN$.

Il en découle que $HN \leqslant G$. ∎

**Théorème 5.5** (Deuxième théorème d'isomorphisme)**.** *Soient $N \trianglelefteq G$ et $H \leqslant G$. Alors $N \cap H \trianglelefteq H$ et il existe un isomorphisme*

$$H/(H \cap N) \simeq HN/N\,.$$

Preuve. On considère le morphisme

$$\begin{aligned} f\ &: H \to HN/N, \\ &h \mapsto hN. \end{aligned}$$

a) On calcule le noyau de $f$ :

$$h \in \ker(f) \quad \Leftrightarrow \quad f(h) = 0 \quad \Leftrightarrow \quad hN = N \quad \Leftrightarrow \quad h \in H \cap N.$$

Donc $\ker(f) = H \cap N$.

b) Montrons que $f$ est surjectif. Soit $yN \in HN/N$. Alors $y$ s'écrit sous la forme $y = hn$, où $h \in H$ et $n \in N$. Donc

$$yN = hnN = hN = f(h).$$

c) En appliquant le premier théorème d'isomorphisme au morphisme $f$ on obtient que $H/(H \cap N) \simeq HN/N$. Le théorème est démontré. ∎

**Théorème 5.6** (Troisième théorème d'isomorphisme)**.** *Soit $G$ un groupe et soient $H$ et $K$ deux sous-groupes distingués de $G$. Supposons que $K \subset H$. Alors $H/K \trianglelefteq G/K$ et l'on a un isomorphisme*

$$(G/K)/(H/K) \simeq G/H.$$

Preuve. On considère l'application

$$\begin{aligned} f\ &: G/K \to G/H, \\ &xK \mapsto xH. \end{aligned}$$

On vérifie facilement que $f$ est un morphisme surjectif. En outre,

$$xK \in \ker(f) \quad \Leftrightarrow \quad xH = H \quad \Leftrightarrow \quad x \in H.$$

Donc $\ker(f) = H/K$. En appliquant le premier théorème d'isomorphisme, on en déduit le théorème. ∎

## 6. Centre. Groupe dérivé

Soit $G$ un groupe. On dit que deux éléments $x, y \in G$ commutent si $xy = yx$.

**Définition.** *Soit $G$ un groupe. On appelle centre de $G$ l'ensemble des éléments de $G$ qui commutent avec tous les éléments de $G$ :*

$$Z(G) = \{x \in G \mid xy = yx, \quad \forall y \in G\}.$$

**Théorème 6.1.** *$Z(G)$ est un sous-groupe abélien et distingué de $G$.*

Preuve. a) Soit $x \in Z(G)$ et soit $y \in G$. Alors

$$xy = yx.$$

En multipliant les deux membres de cette équation à gauche et à droite par $x^{-1}$ on obtient :

$$yx^{-1} = x^{-1}(xy)x^{-1} = x^{-1}(yx)x^{-1} = x^{-1}y.$$

Donc $x^{-1} \in Z(G)$.

b) Soient $x_1, x_2 \in Z(G)$. Alors pour tout $y \in Z(G)$ on a :

$$y(x_1x_2) = (yx_1)x_2 = (x_1y)x_2 = x_1(yx_2) = x_1(x_2y) = (x_1x_2)y.$$

Donc $x_1x_2 \in Z(G)$. Comme $e \in Z(G)$, on déduit des parties a) et b) que $Z(G)$ est un sous-groupe.

c) $Z(G)$ est clairement abélien. Soit $y \in G$. Alors $yx = xy$ pour tout $x \in Z(G)$. Donc $yZ(G) = Z(G)y$. On en déduit que $Z(G) \trianglelefteq G$.

■

**Exercice 8.** *1) Soit $K$ un corps. Montrer que*

$$Z(\mathrm{GL}_n(K)) = \{\alpha I_n \mid \alpha \in K^*\}.$$

**Exercice 9.** *On reprend l'exercice 7. Montrer que $Z(G)$ est le noyau du morphisme*

$$G \to \mathrm{Aut}(G),$$
$$g \to c_g.$$

*En déduire que* $\mathrm{Int}(G) \simeq G/Z(G)$.

**Exercice 10.** *On dit que $H \leqslant G$ est un sous-groupe caractéristique si $f(H) \subseteq H$ pour tout $f \in \mathrm{Aut}(G)$.*

*a) Montrer que tout sous-groupe caractéristique est distingué.*

*b) Montrer que $Z(G)$ est un sous-groupe caractéristique.*

Pour tous $x, y \in G$ on appelle commutateur de $x$ et $y$ l'élément

$$[x, y] := xyx^{-1}y^{-1}.$$

Donc $[x, y] = e$ si et seulement si $x$ et $y$ commutent.

**Définition.** *On appelle groupe dérivé de $G$ et l'on note $[G, G]$ ou $D(G)$ le sous-groupe de $G$ engendré par les commutateurs $[x, y]$, où $x, y \in G$ :*

$$[G, G] := \langle [x, y] \mid x, y \in G \rangle.$$

**Théorème 6.2.** *Soit $G$ un groupe.*

i) $[G,G] \trianglelefteq G$;
ii) $G/[G,G]$ *est abélien.*
iii) *Soit* $H \trianglelefteq G$. *Alors*

$$G/H \text{ est abélien} \Leftrightarrow [G,G] \subseteq H.$$

Preuve. i) Un calcul direct montre les formules suivantes :

$$x[y,z]x^{-1} = [xyx^{-1}, xzx^{-1}], \tag{7}$$

$$[y,z]^{-1} = [z,y]. \tag{8}$$

En utilisant la formule (8) et l'énoncé de l'exercice 3, on obtient que tout $h \in [G,G]$ s'écrit sous la forme

$$h = h_1 h_2 \cdots h_n, \qquad \text{où } h_i = [y_i, z_i].$$

On a

$$xhx^{-1} = (xh_1x^{-1}) \cdots (xh_nx^{-1}).$$

La formule (7) montre que $xh_ix^{-1} \in [G,G]$ pour tout $i$. Donc $xhx^{-1} \in [G,G]$. On en déduit que $[G,G] \trianglelefteq G$.

ii) Pour simplifier la notation, on note $\overline{x} \in G/[G,G]$ la classe de $x$ suivant $[G,G]$. Alors $\overline{x} \cdot \overline{y} = \overline{xy}$ pour tous $x, y \in G$. Donc

$$[\overline{x}, \overline{y}] = \overline{[x,y]} = \overline{e}.$$

On en déduit que $G/[G,G]$ est abélien.

iii) Soit $[G,G] \leqslant H \leqslant G$.

Réciproquement, supposons que $H \trianglelefteq G$ et $G/H$ est abélien. Pour tout $x \in G$, on pose $\overline{x} = \mathrm{cl}_H(x)$. Alors pour tous $x, y \in G$ on a

$$\overline{[x,y]} = [\overline{x}, \overline{y}] = \overline{e}.$$

Donc $[x,y] \in H$ pour tous $x, y \in G$. On en déduit que $[G,G] \subseteq H$. ∎

**Exemple.** $G$ abélien ssi $Z(G) = G$ ssi $[G,G] = \{e\}$.

CHAPITRE 2

# Action de groupe

## 1. Action d'un groupe sur un ensemble

Soient $G$ un groupe et $X$ un ensemble. On note $e$ l'élément neutre de $G$.

**Définition.** *On appelle action à gauche de $G$ sur $X$ une application*

$$f : G \times X \to X$$

*vérifiant les propriétés suivantes :*

1) $f(e,x) = x, \qquad \forall x \in X.$
2) $f(g_1g_2,x) = f(g_1,f(g_2,x)), \qquad \forall g_1,g_2 \in G \text{ et } \forall x \in X.$

Pour alléger la notation on pose $gx := f(g,x)$. Alors les propriétés 1-2) s'écrivent :

1) $ex = x, \qquad \forall x \in X.$
2) $(g_1g_2)x = g_1(g_2x), \qquad \forall g_1,g_2 \in G \text{ et } \forall x \in X.$

De manière analogue, on définit une action *à droite* de $G$ sur $X$ comme étant une application

$$X \times G \to X,$$
$$(x,g) \mapsto xg$$

vérifiant les propriétés suivantes :

1*) $xe = x, \qquad \forall x \in X.$
2*) $x(g_1g_2) = (xg_1)g_2, \qquad \forall g_1,g_2 \in G \text{ et } \forall x \in X.$

**Exemple.** Soit $X$ un ensemble et soit $S(X)$ le groupe symétrique de $X$ (cf. Exercice 2). On considère l'application

$$f : S(X) \times X \to X,$$
$$f(\sigma,x) := \sigma(x), \qquad \forall \sigma \in S(X), \forall x \in X.$$

Il est facile de voir que $f$ définit une action à gauche de $S(X)$ sur $X$.

Nous allons prouver que toute action de $G$ sur $X$ se factorise à travers $S(X) \times X$.

**Théorème 1.1.** *1) Soit $f : G \times X \to X$ une action à gauche de $G$ sur $X$. Pour tout $g \in G$, on pose:*

$$f_g : X \to X,$$
$$f_g(x) = f(g,x) = gx.$$

*Alors $f_g \in S(X)$, et l'application*

$$\varphi : G \to S(X),$$
$$\varphi(g) = f_g$$

*est un morphisme de groupes.*

*2) Réciproquement soit $\varphi : G \to S(X)$ un morphisme de groupes. Alors l'application*

$$f : G \times X \to X,$$
$$f(g,x) = \varphi(g)(x)$$

*définit une action de $G$ sur $X$.*

PREUVE. 1) Soit $f : G \times X \to X$ une action à gauche de $G$ sur $X$. On fixe $g \in G$ et on considère l'application $f_g : X \to X$.

a) Supposons que $f_g(x_1) = f_g(x_2)$. Alors $gx_1 = gx_2$, d'où :

$$x_1 = g^{-1}(gx_1) = g^{-1}(gx_2) = (g^{-1}g)x_2 = ex = x_2$$

Donc $f_g$ est injective.

Soit $y \in X$ un élément de $X$ et soit $x = g^{-1}y$. Alors

$$f_g(x) = g(g^{-1}y) = (gg^{-1})y = ey = y.$$

On en déduit que $f_g$ est surjective. Donc $f_g \in S(X)$.

b) Soient $g_1, g_2 \in G$. Pour tout $x \in X$, on a

$$f_{g_1g_2}(x) = (g_1g_2)x = g_1(g_2x) = f_{g_1}(g_2x) = f_{g_1}(f_{g_2}(x)) = f_{g_1} \circ f_{g_2}(x).$$

Donc $f_{g_1g_2} = f_{g_1} \circ f_{g_2}$, d'où

$$\varphi(g_1g_2) = f_{g_1g_2} = f_{g_1} \circ f_{g_2} = \varphi(g_1)\varphi(g_2).$$

On en déduit que $\varphi$ est un morphisme de groupes.

2) Soit $\varphi : G \to S(X)$ un morphisme de groupes. On pose :

$$f(g,x) = \varphi(g)(x), \quad \forall g \in G, x \in X.$$

Alors :

a) $f(e,x) = \varphi(e)(x) = \mathrm{id}_X(x) = x$.

b) Pour tous $g_1, g_2 \in G$ et $x \in X$ on a :

$$f(g_1g_2,x) = \varphi(g_1g_2)(x) = \varphi(g_1) \circ \varphi(g_2)(x) = f(g_1,\varphi(g_2)(x)) = f(g_1,f(g_2,x)).$$

Donc $f$ définit une action de $G$ sur $X$. ∎

**Exemple.** Soit $G$ un groupe. On considère l'application

$$f : G \times G \to G,$$
$$f(g,x) = gx.$$

Il est facile de voir que $f$ définit une action à gauche de $G$ sur $G$. Pour tout $g \in G$, l'application $f_g$ coïncide avec l'application

$$L_g : G \to G, \qquad L_g(x) = gx.$$

Par le théorème précédent, on a un morphisme de groupes

$$\varphi : G \to S(G), \qquad \varphi(g) = L_g.$$

Si $g \in \ker(\varphi)$, alors $L_g = \mathrm{id}_G$, i.e. $L_g(x) = gx = x$ pour tout $x \in G$. Donc $g = e$ et $\ker(\varphi) = \{e\}$. On en déduit que $\varphi$ est un monomorphisme.

Supposons de plus que $G$ est fini et posons $n = |G|$. Alors $S(G) \simeq S_n$ et l'injectivité du morphisme $\varphi : G \to S_n$ implique le théorème suivant :

**Théorème 1.2** (Cayley)**.** *Soit $G$ un groupe fini d'ordre $n$. Alors $G$ est isomorphe à un sous-groupe de $S_n$.*

## 2. Formule des classes

**2.1.** Soit $G$ un groupe opérant sur un ensemble $X$.

**Définition.** *Soit $x \in X$.*
*1) On appelle orbite de $x \in X$ sous l'action de $G$ et l'on note $Gx$ ou* $\mathrm{Orb}(x)$ *l'ensemble*

$$\{gx \mid g \in G\}.$$

*2) On appelle stabilisateur de $x \in X$ dans $G$ et l'on note $G_x$ ou* $\mathrm{Stab}(x)$ *l'ensemble*

$$\{g \in G \mid gx = x\}.$$

*3) On dit que $x \in X$ est un point fixe de l'action de $G$ si $G_x = G$.*

On note $X^G$ l'ensemble des points fixes de $X$. Il découle des définitions que

$$x \in X^G \quad \Leftrightarrow \quad Gx = \{x\} \quad \Leftrightarrow \quad G_x = G.$$

**Théorème 2.2.** *Soit $G$ un groupe opérant sur $X$. Alors :*
*1)Pour tout $x \in X$, on a $G_x \leqslant G$.*
*2) Les orbites de $X$ sous l'action de $G$ constituent une partition de $G$.*
*3) On note $G/G_x$ l'ensemble des classes à gauche de $G$ suivant $G_x$. L'application*

$$\alpha : G \to Gx,$$
$$\alpha(g) = gx$$

*induit un bijection entre $G/G_x$ et $Gx$.*

Preuve. 1) Si $g_1, g_2 \in G_x$, alors $g_1 x = g_2 x = x$. Alors

$$(g_1 g_2)x = g_1(g_2 x) = g_1 x = x,$$

d'où $g_1 g_2 \in G_x$. En outre,

$$g_1^{-1} x = g_1^{-1}(g_1 x) = (g_1^{-1} g_1)x = x,$$

d'où $g_1^{-1} \in G_x$. On en déduit que $G_x \leqslant G$.
2) On considère la relation $\sim$ sur $X$ définie par la formule

$$x \sim y \quad \Leftrightarrow \quad y \in Gx$$

et l'on montre que $\sim$ est une relation d'équivalence.

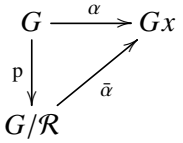
a) $x \sim x$ car $x = ex \in Gx$.
b) Si $x \sim y$, alors il existe $g \in G$ tel que $y = gx$. Donc $x = g^{-1}y \in Gy$, d'où $y \sim x$.
c) Si $x \sim y$ et $y \sim z$, alors il existe $g_1, g_2 \in G$ tels que $y = g_1 x$ et $z = g_2 y$. Donc $z = (g_2 g_1)x$ et $x \sim z$.

Par définition, la classe d'équivalence de $x$ pour la relation $\sim$ est l'orbite de $x$. Comme toute relation d'équivalence sur $X$ donne une partition de $X$ où les ensembles disjoints sont les classes d'équivalence, on en déduit le 2) du théorème.

3) Par le théorème de factorisation, l'application $\alpha : G \to Gx$ se factorise à travers de l'ensemble quotient $G/\mathcal{R}$, où la relation $\mathcal{R}$ est définie par :

$$g_1 \mathcal{R} g_2 \quad \Leftrightarrow \quad \alpha(g_1) = \alpha(g_2).$$

On a un diagramme :




où $\bar{\alpha}(\mathrm{p}(g)) = \alpha(x)$. L'application $\bar{\alpha}$ est une bijection. En outre :

$$g_1 \mathcal{R} g_2 \quad \Leftrightarrow \quad g_1 x = g_2 x \quad \Leftrightarrow \quad g_2^{-1} g_1 x = x \quad \Leftrightarrow \quad g_2^{-1} g_1 \in G_x.$$

Donc $\mathcal{R}$ coïncide avec la relation d'équivalence $\underset{G_x}{\sim}$ associée à $G_x$. On en déduit que $G/\mathcal{R}$ coïncide avec l'ensemble des classes à gauche suivant $G_x$, d'où le 3). ■

On choisit un représentant $s \in X$ de chaque orbite. On note $S$ l'ensemble des représentants choisis. L'orbite $Gs$ de $s \in S$ est ponctuelle (i.e. elle est réduite à un élément) si et seulement si $s \in X^G$. Donc nous pouvons écrire :

$$S = X^G \cup S',$$

où $S'$ est complémentaire de $X^G$ dans $S$. On note que $(G : G_s) \neq 1$ si $s \in S'$.

**Corollaire 2.3** (formule des classes)**.** *Supposons que $X$ est un ensemble fini. Alors*

$$\boxed{|X| = \sum_{s \in S} (G : G_s)}$$

Preuve. D'après le théorème précédent, on a :

$$|X| = \sum_{s \in S} |Gs| = \sum_{s \in S} (G : G_s).$$

■

On peut écrire la formule des classes sous la forme suivante :

$$\boxed{|X| = |X^G| + \sum_{s \in S'} (G : G_s).}$$

**2.4.** Rappelons (cf. Exercice 7) que l'application $g \mapsto c_g$ qui à tout $g \in G$ associe l'automorphisme intérieur $c_g$ donne un morphisme de groupes :

$$\varphi : G \to \mathrm{Aut(G)} \subseteq S(G).$$

Ce morphisme définit une action de $G$ sur $G$ qui n'est rien d'autre que l'action par conjugaison :

$$G \times G \to G,$$
$$(g, x) \mapsto gxg^{-1}.$$

**Définition.** *Pour tout $x \in G$, on appelle centralisateur de $x$ dans $G$ le sous-groupe*

$$C_G(x) := \{g \in G \mid gx = xg\}.$$

Alors :

$$G_x = \{g \in G \mid gxg^{-1} = x\} = \{g \in G \mid gx = xg\} = C_G(x).$$

En particulier,

$$x \in G^G \quad \Leftrightarrow \quad G_x = G \quad \Leftrightarrow \quad x \in Z(G).$$

Donc $S = Z(G) \cup S'$ où $S' = \{s \in S \mid s \notin Z(G)\}$.

Supposons que $G$ est fini. La formule des classes s'écrit :

$$\boxed{|G| = |Z(G)| + \sum_{s \in S'} (G : C_G(s)).}$$

On peut aussi écrire :

$$\boxed{|G| = |Z(G)| + \sum_{s \in S'} \frac{|G|}{|C_G(s)|}.}$$

Nous donnons maintenant une application de la formule des classes à l'étude des groupes finis.

**Définition.** *Soit $p$ un nombre premier. On dit qu'un groupe fini $G$ est un $p$-groupe si $|G| = p^n$, $n \geqslant 1$.*

**Théorème 2.5.** *Soit $G$ un $p$-groupe. Alors $Z(G) \neq \{e\}$.*

Preuve. On a :

$$s \in S' \quad \Rightarrow \quad (G : G_s) \neq 1 \quad \Rightarrow \quad p \text{ divise } (G : G_s).$$

Comme $p$ divise $|G| = p^n$, on déduit de la formule des classes que $p$ divise $Z(G)$ et donc $Z(G) \neq \{e\}$.

■

## 3. Théorèmes de Sylow

Dans cette section, $G$ désigne un groupe fini d'ordre $n = |G|$. Soit $p$ un nombre premier.

**Définition.** *Soit $p^a$ la plus grande puissance de $p$ divisant $n = |G|$. On appelle $p$-sous-groupe de Sylow un sous-groupe de $G$ dont l'ordre est $p^a$.*

**Théorème 3.1** (premier théorème de Sylow)**.** *Soit $p$ un nombre premier divisant $|G|$. Le groupe $G$ a au moins un $p$-sous-groupe de Sylow.*

Preuve. On montre le théorème par récurrence sur $n$.

1) Pour $n = 1$ l'assertion est évidente.

2) Soit $n > 1$. Admettons le résultat pour tous les goupes finis d'ordre $< n$. On considère 2 cas :

a) Il existe un sous-groupe propre (i.e. distinct de $G$) $H < G$ tel que $p^a$ divise $|H|$. Dans ce cas par l'hypothèse de récurrence $H$ admet un $p$-sous groupe de Sylow $P$. Alors $P$ est un $p$-sous-groupe de Sylow pour $G$.

b) Dans le second cas tous les sous-groupes stricts de $G$ ont un ordre non divisible par $p^a$, donc on a :

$$\forall H < G, \quad p \text{ divise } (G : H).$$

On applique la formule des classes :

$$|G| = |Z(G)| + \sum_{s \in S'} (G : C_G(s)).$$

Par l'hypothèse, $p$ divise $|G|$ et $(G : C_G(s))$ pour tout $s \in S'$ donc $p$ divise $|Z(G)|$. Nous avons besoin du lemme suivant :

**Lemme 3.2.** *Si $A$ est un groupe abélien fini et $p$ un nombre premier qui divise $|A|$, alors il existe un élément d'ordre $p$ dans $A$.*

Preuve du lemme. On montre le lemme par récurrence sur $m = |A|$. Si $m = p$, tout élément de $A$ est d'ordre $p$.

Supposons que $m > p$ et que l'assertion est vraie pour tous les groupes abélien d'ordre $< m$. Soit $y \neq e$ un élément de $A$. Si $\text{ord}(y) = pk$, alors $\text{ord}(y^k) = p$ et $x = y^k$ est un élément d'ordre $p$.

Sinon $\text{ord}(y) = k$ est premier à $p$. Soit $\bar{A} = A/ < y >$ . Comme $p$ divise $|\bar{A}|$, par l'hypothèse de récurrence il existe un élément $\bar{z} \in B$ d'ordre $p$. Soit $z \in A$ un représentant de $\bar{z}$ dans $A$. Alors $z^p \in < y >$, d'où $\text{ord}(z) = pk$ pour un certain entier $k$. En posant $x = z^k$, on trouve que $\text{ord}(x) = p$. ∎

Retour à la preuve du théorème. Par le lemme précédant, il existe un sous-groupe $H \subset Z(G)$ d'ordre $p$. Soit $G' = G/H$. Par l'hypothèse de récurrence, $G'$ possède un sous-groupe de Sylow $P'$ et $|P'| = p^{a-1}$. On considère le morphisme de projection $\pi : G \to G'$, $\pi(x) = \text{cl}_H(x)$. Alors l'image réciproque $P := \pi^{-1}(P')$ de $P'$ dans $G$ est un sous-groupe d'ordre $p^a$. Donc $P$ est un $p$-sous-groupe de Sylow de $G$. ∎

Soit $\mathrm{Syl}_p(G)$ l'ensemble des $p$-sous-groupes de Sylow de $G$ :

$$\mathrm{Syl}_p(G) := \{P \leqslant G \mid |P| = p^a\}.$$

Alors $G$ agit sur $\mathrm{Syl}_p(G)$ par conjugaison:

$$G \times \mathrm{Syl}_p(G) \to \mathrm{Syl}_p(G),$$
$$(g, P) \mapsto gPg^{-1}.$$

**Définition.** *Soit $H \leqslant G$. On appelle normalisateur de $H$ le sous-groupe*

$$N_G(H) := \{g \in G \mid gHg^{-1} \subseteq H\}.$$

*On remarque que $H \trianglelefteq N_G(H)$.*

Soit $P \in \mathrm{Syl}_p(G)$. Alors :

$$G_P = \{x \in G \mid xPx^{-1} \subseteq P\} = N_G(P).$$

La formule $|\mathrm{Orb}_G(P)| = (G : G_P)$ s'écrit :

$$|\mathrm{Orb}_G(P)| = (G : N_G(P)) = \frac{(G : P)}{(G : N_G(P))}.$$

Si on écrit $n = |G|$ sous la forme $n = p^a m$, $p \nmid m$, la dernière formule implique :

$$|\mathrm{Orb}_G(P)| \text{ divise } m. \tag{9}$$

En particulier, $|\mathrm{Orb}_G(P)|$ est premier à $p$.

Si $H$ est un $p$-groupe agissant sur un ensemble fini $X$, alors $p$ divise $(H : H_s)$ pour tout $s \in S'$ et la formule des classes donne :

$$|X| \equiv |X^H| \pmod{p}. \tag{10}$$

Soit maintenant $H$ un sous-groupe de $G$ dont l'ordre est une puissance de $p$:

$$|H| = p^b.$$

Soit $P$ un $p$-sous-groupe de Sylow de $G$. Alors $H$ agit par conjugaison sur $X := \mathrm{Orb}_G(P)$ et la congruence précédente s'écrit :

$$|\mathrm{Orb}_G(P)| \equiv |\mathrm{Orb}_G(P)^H| \pmod{p}.$$

Comme $|\mathrm{Orb}_G(P)|$ est premier à $p$, on en déduit que

$$|\mathrm{Orb}_G(P)^H| \neq 0,$$

et donc que l'ensemble $\mathrm{Orb}_G(P)^H$ est non vide.

Soit $P' \in \mathrm{Orb}_G(P)^H$. Alors :

$$h^{-1}P'h \subset P', \qquad \text{pour tout} \quad h \in H.$$

Donc $HP' := \{hx | h \in H, x \in P'\}$ est un sous-groupe de $G$ et par le deuxième théorème d'isomorphisme on a :

$$(HP' : P') = (H : H \cap P').$$

Comme $H$ et $P'$ sont des $p$-groupes, on en déduit que $HP'$ est un $p$-sous-groupe de $G$ contenant $P'$. Or $P'$ est un $p$-sous-groupe de Sylow, d'où $HP' = P'$. Donc $H \subseteq P'$.

Nous avons démontré la première partie du théorème suivant :

**Théorème 3.3** (deuxième théorème de Sylow)**.** *i) Tout sous-groupe $H$ dont l'ordre est une puissance de $p$ est contenu dans un $p$-sous-groupe de Sylow.*

*ii) Deux $p$-sous-groupes de Sylow sont conjugués entre eux.*

Preuve. Le i) est déjà démontré.

ii) Soit $Q$ un $p$-sous-groupe de Sylow. En posant $H = Q$ dans le raisonnement précédent on trouve que pour tout sous-groupe de Sylow $P$, il existe $P' = xPx^{-1}$, $x \in G$ tel que $Q \subseteq P'$. Donc $Q = P' = xPx^{-1}$. ∎

On note $n_p$ le nombre des $p$-sous groupes de Sylow de $G$ :

$$n_p := \left|\mathrm{Syl}_p(G)\right|.$$

**Théorème 3.4** (troisième théorème de Sylow)**.** *On a :*

$$\boxed{n_p \equiv 1 \pmod{p}.}$$

Preuve. On fixe un sous-groupe de Sylow $P$ de $G$ et on considère l'action par conjugaison de $P$ sur $\mathrm{Syl}_p(G)$. L'orbite de $P$ est réduite à $P$, donc $P \in \mathrm{Syl}_p(G)^P$.

Supposons que $P' \in \mathrm{Syl}_p(G)^P$. Alors $xP'x^{-1} = P'$ pour tout $x \in P$. Exactement comme dans la preuve du théorème précédent on en déduit que $PP'$ est un $p$-sous-groupe de $G$. Comme $P \subseteq PP'$ et $P' \subseteq PP'$ sont des $p$-sous-groupes de Sylow de $G$, on conclut que $P = PP' = P'$. Donc

$$\mathrm{Syl}_p(G)^P = \{P\}$$

et la formule (10) donne :

$$|\mathrm{Syl}_p(G)| \equiv \left|\mathrm{Syl}_p(G)^P\right| \equiv 1 \pmod{p}.$$

**Remarque 3.5.** Comme tous les $p$-sous-groupes Sylow de $G$ sont conjugués entre eux, on a $\mathrm{Syl}_p(G) = \mathrm{Orb}_G(P)$ pour tout $p$-Sylow $P$. On déduit de la formule (9) que

$$\boxed{n_p \mid m, \qquad \text{où} \quad n = p^a m.}$$

**Exemple.** Soit $G$ un groupe d'ordre $n = pq$, où $p$ et $q$ sont deux nombres premiers. Supposons que $p < q$ et que $q \not\equiv 1 \pmod{p}$. Alors $n_q \in \{1, p\}$ et $n_q \equiv 1 \pmod{q}$, d'où $n_q = 1$. Soit $Q$ le $q$-sous-groupe de Sylow. Alors pour tout $g \in G$ on a $gQg^{-1} = Q$. On en déduit que $Q \trianglelefteq G$. De même, $n_p \in \{1, q\}$ et $n_p \equiv 1 \pmod{p}$. Comme $q \not\equiv 1 \pmod{p}$, on en déduit que $n_p = 1$ et $P \trianglelefteq G$. Les groupes $P$ et $Q$ sont cycliques d'ordres $p$ et $q$ respectivement. Soient $P = \langle x \rangle$ et $Q = \langle y \rangle$. Comme $Q \trianglelefteq G$, on a $xyx^{-1} \in Q$, d'où

$$[x, y] = xyx^{-1}y^{-1} = (xyx^{-1})y \in Q.$$

De même, $[x, y] \in P$. Donc $[x, y] \in P \cap Q = \{e\}$ et nous avons prouvé que $G$ est un groupe abélien. On pose $z = xy$. Il est facile de voir que $\mathrm{ord}(z) = pq$, d'où $G = \langle z \rangle \simeq \mathbf{Z}/pq\mathbf{Z}$.

∎

CHAPITRE 3

# Exemples et constructions

## 1. Groupes symétriques

Ce chapitre commence par un bref rappel sur les groupes symétriques. Soit $n \geqslant 1$ un entier positif. On pose $E_n := \{1, 2, \ldots, n\}$ et l'on note $S_n$ le groupe $S(E_n)$ des bijections $\sigma : E_n \to E_n$. Les éléments de $S_n$ sont appelés permutations de $E_n$. On peut écrire toute permutation $\sigma \in S_n$ sous la forme :

$$\sigma = \begin{pmatrix} 1 & 2 & \ldots & n \\ \sigma(1) & \sigma(2) & \ldots & \sigma(n) \end{pmatrix}.$$

On note que $\sigma(i) \neq \sigma(j)$ si $i \neq j$. Il est facile de prouver que

$$\boxed{|S_n| = n!.}$$

On appelle support de $\sigma \in S_n$ l'ensemble

$$\mathrm{Supp}(\sigma) = \{i \in E_n \mid \sigma(i) \neq i\}.$$

**Définition.** *1) On dit qu'un permutation $\sigma \in S_n$ est un cycle de longueur $k$ (ou un $k$-cycle) si et seulement s'il existe $\{i_1, i_2, \ldots i_k\} \subset \{1, \ldots n\}$ tels que*

a) $\mathrm{Supp}(\sigma) = \{i_1, i_2, \ldots, i_k\}$.

b) *On a $\sigma(i_1) = i_2$, $\sigma(i_2) = i_3$, $\ldots, \sigma(i_k) = i_1$.*

*Un tel cycle se note :*

$$\sigma = (i_1, i_2, \ldots, i_k).$$

*2) On appelle transposition un cycle de longueur 2. Toute transposition s'écrit sous la forme $(i, j)$, où $i \neq j$.*

Le théorème suivant résume quelques propriétés des cycles.

**Théorème 1.1.** *i) Tout élément de $S_n$ s'ecrit comme produit de cycles à supports disjoints. Deux permutations à supports disjoints commutent.*

*ii) Soit $\sigma$ un cycle de longueur $k$. Alors* $\mathrm{ord}(\sigma) = k$.

*iii) On a:*

$$(i_1, i_2, \cdots, i_k) = (i_1, i_2)(i_2, i_3) \cdots (i_{k-1}, i_k).$$

*iv) Le groupe $S_n$ est engendré par les transpositions.*

Preuve. i) Soit $\sigma \in S_n$. Considérons l'action du groupe cyclique $\langle \sigma \rangle$ sur $E_n$. Alors $E_n$ est l'union disjointe des orbites sous l'action de $\langle \sigma \rangle$, soient $O_1, \ldots O_s$ les orbites non ponctuelles. Soit $c_i$ la permutation qui agit comme $\sigma$ sur $O_i$ et comme l'identité sur $E_n \setminus O_i$. Alors il est facile de voir que $c_i$ est un cycle de longueur $k_i = |O_i|$ et $\sigma = c_1 c_2 \cdots c_s$.

Un calcul facile montre les points ii) et le iii).
Le i) et le iii) impliquent le point iv). ∎

**Exercice 11.** Montrer que $S_n$ est engendré par les familles suivantes :

- $\{(1,k) \mid 2 \leqslant k \leqslant n\}$;
- $\{(1,2),(1,2,\ldots,n)\}$.

**Définition.** *Soit $\sigma \in S_n$ et soient $i,j \in \{1,\ldots,n\}$ tels que $i<j$. On dit que $\sigma$ présente une inversion en $(i,j)$ si $\sigma(i) > \sigma(j)$.*

On appelle nombre d'inversions de $\sigma$ et l'on note $\nu(\sigma)$ le nombre des couples $(i,j)$ tels que $\sigma$ présente une inversion en $(i,j)$.

**Définition.** *On appelle signature de $\sigma \in S_n$ l'entier*

$$\varepsilon(\sigma) = (-1)^{\nu(\sigma)}.$$

**Théorème 1.2.** *i) L'application*

$$\varepsilon : S_n \to \{-1,1\}$$

*est un morphisme de groupes. De façon équivalente :*

$$\varepsilon(\sigma\tau) = \varepsilon(\sigma)\varepsilon(\tau).$$

*ii) Soit $\sigma = \tau_1\tau_2\cdots\tau_m$ une décomposition en produit de transpositions. Alors*

$$\varepsilon(\sigma) = (-1)^m.$$

*En particulier, si $\sigma$ est un k-cycle, alors*

$$\varepsilon(\sigma) = (-1)^{k-1}.$$

Preuve. i) On définit une action de $S_n$ sur l'anneau des polynômes en $n$ variables en posant :

$$\sigma \star f(X_1,\ldots,X_n) := f(X_{\sigma(1)},\ldots,X_{\sigma(n)}), \qquad \forall \sigma \in S_n, \quad f(X_1,\ldots,X_n) \in \mathbf{Q}[X_1,\ldots,X_n].$$

On vérifie facilement que

$$(\sigma\tau) \star f(X_1,\ldots,X_n) = \sigma \star (\tau \star f(X_1,\ldots,X_n)).$$

Soit $\Delta(X_1,\ldots,X_n) = \prod_{1\leqslant i<j\leqslant n} (X_i - X_j)$. Alors :

$$\sigma \star \Delta(X_1,\ldots,X_n) = (-1)^{\nu(\sigma)}\Delta(X_1,\ldots,X_n) = \varepsilon(\sigma)\Delta(X_1,\ldots,X_n).$$

Donc :

$$\varepsilon(\sigma\tau)\Delta = (\sigma\tau)\star\Delta = \sigma\star(\tau\star\Delta) = \varepsilon(\tau)\sigma\star\Delta = \varepsilon(\tau)\varepsilon(\sigma)\Delta.$$

On en déduit que $\varepsilon(\sigma\tau) = \varepsilon(\sigma)\varepsilon(\tau)$.

ii) Soit $\tau = (i,j)$ une transposition. On peut toujours supposer que $i<j$. Alors

$$\begin{pmatrix} 1 & 2 & \ldots & i & \ldots & j & \ldots & n \\ 1 & 2 & \ldots & j & \ldots & i & \ldots & n \end{pmatrix}.$$

Les inversions dans cette permutation sont les $(j-i)$ couples $(i,i+1),(i,i+2),\ldots,(i,j)$ et les $(j-i-1)$ couples $(i+1,j),(i+2,j),\ldots,(j-1,j)$. Donc $\nu(\tau) = 2(j-i)-1$ et $\varepsilon(\tau) = -1$.

En utilisant le i), on trouve que $\varepsilon(\sigma) = (-1)^m$ si $\sigma$ est produit de $m$ transpositions. La dernière formule découle du point iii) du théorème 1.1.

■

**Définition.** *On appelle groupe alterné de degré n et l'on note $A_n$ le noyau du morphisme $\varepsilon$.*

On a $A_n \trianglelefteq S_n$ et $(S_n : A_n) = 2$.

**Théorème 1.3.** *Le groupe $A_n$ est engendré par les 3-cycles.*

Preuve. Tout élément de $A_n$ s'écrit comme le produit d'un nombre pair de transpositions. Or on a :

$$(i,j)(j,k) = (j,k,i),$$
$$(ij)(lk) = (i,k,j)(i,k,l).$$

■

Nous aurons besoin du résultat suivant :

**Proposition 1.4.** *i) Pour tout $\sigma \in S_n$, on a:*

$$\sigma(i_1, i_2, \ldots, i_k)\sigma^{-1} = (\sigma(i_1), \sigma(i_2), \ldots, \sigma(i_k)).$$

*ii)Dans $S_n$, deux cycles de même longueur sont conjugués.*
*iii) Soit $n \geqslant 5$. Dans $A_n$, les 3-cycles sont conjugués.*

Preuve. i) Vérification directe.
ii) Soit $(j_1, j_2, \ldots, j_k)$ un autre $k$-cycle. On prend un élément $\sigma$ tel que $\sigma(i_s) = j_s$ pour $1 \leqslant s \leqslant k$ et l'on applique le i).
iii) Il suffit de prouver que tout 3-cycle $(i,j,k)$ est conjugué au cycle $(1,2,3)$. Le ii) implique qu'il existe $\sigma \in S_n$ tel que $(i,j,k) = \sigma(1,2,3)\sigma^{-1}$. Si $\sigma \in A_n$, le iii) est prouvé. Sinon on pose $\sigma' = \sigma(4,5)$ et l'on vérifie facilement que $\sigma' \in A_n$ et $(i,j,k) = \sigma'(1,2,3)\sigma'^{-1}$. ■

## 2. Groupes simples. Simplicité de $A_n$

**Définition.** *Un groupe G est simple s'il a exactement deux sous-groupes distingués: $\{e\}$ et G lui-même.*

**Exemple.** Soit $G$ un groupe abélien d'ordre $n$. Par le lemme 3.2, pour tout diviseur premier $p$ de $|G|$ le groupe $G$ admet un sous-groupe cyclique d'ordre $p$. On en déduit qu'un groupe abélien est simple si et seulement s'il est d'ordre premier $p$ (et donc isomorphe à $\mathbf{Z}/p\mathbf{Z}$).

**Théorème 2.1.** *Le groupe $A_n$ est simple pour $n \geqslant 5$.*

**Remarque 2.2.** Le groupe $A_2$ est trivial: $A_2 = \{e\}$. Le groupe $A_3 := \{e, (1,2,3), (1,3,2)\}$ est cyclique d'ordre 3, en particulier il est simple. Le groupe $A_4$ possède un sous-groupe distingué (le groupe de Klein $K$) :

$$K = \{e, (12)(34), (13)(24), (14)(23)\} \trianglelefteq A_4.$$

Donc $A_4$ n'est pas simple.

Preuve du théorème. a) On montre que le groupe $A_5$ est simple. On remarque que $|A_5| = 60 = 2^2 \cdot 3 \cdot 5$. On veut classifier les éléments de $A_5$:

• L'unique élément d'ordre 1 est l'élément neutre.

• Les éléments d'ordre 2 sont de la forme $(i,j)(k,l)$. On en déduit facilement que le nombre d'éléments de cette forme est égal à

$$\frac{\frac{5\cdot 4}{2}\cdot\frac{3\cdot 2}{2}}{2} = 15.$$

• Les éléments d'ordre 3 sont de la forme $(i,j,k)$. Le nombre d'éléments de cette forme est égal à

$$\frac{5\cdot 4\cdot 3}{3} = 20.$$

• Les éléments d'ordre 5 sont les 5 cycles. Le nombre de 5-cycles dans $A_5$ est égal à

$$\frac{5\cdot 4\cdot 3\cdot 2\cdot 1}{5} = 24.$$

Comme $1+15+20+24 = 60$, on a une liste complète des éléments de $A_5$.

Les éléments d'ordre 3 sont conjugués dans $A_5$. On voit facilement que les éléments d'ordre 2 sont également deux à deux conjugués. En effet, si $\tau_1 = (i,j)(k,l)$ et $\tau_2 = (a,b)(c,d)$, alors

$$\tau_2 = \sigma\tau_1\sigma^{-1}, \qquad \text{pour } \sigma = (i,a)(j,b)(k,c)(l,d) \in A_5.$$

Les éléments d'ordre 5 engendrent les 5-sous-groupes de Sylow de $A_5$, qui sont conjugués par le deuxième théorème de Sylow.

Soit $\{e\} \neq H \trianglelefteq A_5$. Alors $H$ contient un élément d'ordre $d \in \{2,3,5\}$. Comme $gHg^{-1} = H$ pour tout $G \in A_5$, on déduit des remarques précédentes que $H$ contient tous les éléments d'ordre $d$. On remarque ensuite que les entiers $15+1 = 16$, $20+1 = 21$ et $24+1 = 25$ ne divisent pas $|A_5|$. Donc $H$ contient également tous les éléments d'ordre $d' \neq d$. On en déduit facilement que $|H| > 30$, d'où $|H| = |A_5|$ et $H = A_5$.

b) On montre que $A_n$ est simple pour $n \geqslant 6$. Soit $\{e\} \neq H \trianglelefteq A_n$. On commence par prouver que $H$ contient un élément $g \neq e$ tel que $\big|\mathrm{Supp}(g)\big| \leqslant 5$. Soit $\tau \in H \setminus \{e\}$. Alors il existe $a \in E_n$ tel que $b := \tau(a) \neq a$. Soient $c \in E_n \setminus \{a,b\}$ et $\sigma = (a,c,b)$. On pose $g = [\sigma,\tau]$. Alors :

$$g = \sigma\tau\sigma^{-1}\tau^{-1} = \left(\sigma\tau\sigma^{-1}\right)\tau^{-1} \in H.$$

D'autre part, on a :

$$g = (a,c,b)\cdot\left(\tau(a,b,c)\tau^{-1}\right) = (a,c,b)\cdot(\tau(a),\tau(b),\tau(c)) = (a,c,b)\cdot(b,\tau(b),\tau(c)).$$

Donc $\mathrm{Supp}(g) \subset \{a,b,c,\tau(b),\tau(c)\}$, d'où $|\mathrm{Supp}(g)| \leqslant 5$. Finalement pour que $g \neq e$ il suffit de prendre $c \neq \tau(b)$.

Soit $E \subset E_n$ une partie de $E$ telle que $\mathrm{Supp}(g) \subseteq E$ et $|E| = 5$. Alors $S(E) \simeq S_5$ contient un sous-groupe $A(E) \simeq A_5$. On définit un monomorphisme

$$i : A(E) \to A_n$$

en posant $i(\sigma)|_E = \sigma$ et $i(\sigma)|_{E_n\setminus E} = \mathrm{id}$. Soit $H' = H \cap A(E)$. Comme $g \in H'$, on a $\{e\} \neq H' \trianglelefteq A(E) \simeq A_5$, d'où $H' = A(E)$. Alors $H' \subseteq H$ contient un 3-cycle. On en déduit que $H$ contient tous les 3-cycles, d'où $H = A_n$ par le théorème 1.3. ∎

**Remarque 2.3.** *1) Les groupes finis* $\mathrm{PSL}_n(\mathbb{F}_q) = \mathrm{SL}_n(\mathbb{F}_q)/Z$ *sont simples sauf si* $n = 2$, $q = 2, 3$.

*2) La classification exhaustive des groupes simples finis a été achevée en 1982. On peut les repartir en* 17 *familles infinies (comme* $A_n$, $\mathrm{PSL}_n$, *... auquels il faut ajouter* 26 *groupes exceptionnels (sporadiques). Le plus grand de ces groupes (le Monstre de Fischer-Griess) est d'ordre*

$$2^{46}3^{20}5^9 7^6 11^2 13^3 17 \cdot 19 \cdot 23 \cdot 29 \cdot 31 \cdot 41 \cdot 47 \cdot 59 \cdot 71.$$

## 3. Groupes résolubles

Soit $G$ un groupe. On pose $G^{(0)} = G$ et $G^{(i+1)} = [G^{(i)}, G^{(i)}]$ pour tout $i \geqslant 0$. Donc $G^{(1)} = [G, G]$, $G^{(2)} = [G^{(1)}, G^{(1)}]$ etc.

**Définition.** *On appelle* $(G^{(i)})_{i\in\mathbf{N}}$ *la suite dérivée de* $G$.

**Proposition 3.1.** *Soit* $G$ *un groupe.*
*i) Pour tout automorphisme* $\sigma \in \mathrm{Aut}(G)$, *on a* $\sigma(G^{(i)}) = G^{(i)}$.
*ii)* $G^{(i)} \trianglelefteq G$ *pour tout* $i \geqslant 0$.

Preuve. i) Nous prouvons le i) par récurrence sur $i$. Le cas $i = 0$ est clair ($\sigma(G^{(0)}) = G^{(0)}$). Supposons que $\sigma(G^{(i)}) = G^{(i)}$. Pour tous $x, y \in G^{(i)}$ on a :

$$\sigma([x, y]) = [\sigma(x), \sigma(y)] \in [G^{(i)}, G^{(i)}] = G^{(i+1)}.$$

Comme les éléments $[x, y]$, $(x, y \in G^{(i)})$ engendrent $G^{(i+1)}$, on en déduit que $\sigma(G^{(i+1)}) \subseteq G^{(i+1)}$. En remplaçant dans cette inclusion $\sigma$ par $\sigma^{-1}$ on obtient que $G^{(i+1)} \subseteq \sigma(G^{(i+1)})$. Donc $\sigma(G^{(i+1)}) = G^{(i+1)}$.

ii) Il suffit d'appliquer le i) aux automorphismes intérieurs $c_g$, $g \in G$. ∎

**Définition.** *On dit que* $G$ *est résoluble s'il existe* $i \in \mathbf{N}$ *tel que* $G^{(i)} = \{e\}$. *On appelle classe de résolubilité de* $G$ *et l'on note* $\mathrm{cl}(G)$ *le plus petit* $n$ *tel que* $G^{(n)} = \{e\}$.

**Proposition 3.2.** *Soit* $G$ *un groupe.*

*i) Si* $G$ *est résoluble de classe* $n$, *alors tout sous-groupe* $H \leqslant G$ *est résoluble de classe* $\leqslant n$.

*ii) Soit* $H \trianglelefteq G$. *Alors* $G$ *est résoluble si et seulement si* $H$ *et* $G/H$ *sont résolubles. En outre,*

$$\mathrm{cl}(G) \leqslant \mathrm{cl}(H) + \mathrm{cl}(G/H), \qquad \mathrm{cl}(H) \leqslant \mathrm{cl}(G), \qquad \mathrm{cl}(G/H) \leqslant \mathrm{cl}(G).$$

Preuve. i) Comme $H \subseteq G$, on a $H^{(i)} \subseteq G^{(i)}$ pour tout $i \geqslant 0$. Donc $H$ est résoluble et $\mathrm{cl}(H) \leqslant \mathrm{cl}(G)$.

ii) Soient $H \trianglelefteq G$ et $\pi : G \to \overline{G} := G/H$ la projection canonique. Alors :

$$[\pi(x), \pi(y)] = \pi([x, y]), \qquad \forall x, y \in G.$$

Comme les commutants $[\pi(x), \pi(y)]$, $x, y \in G$ engendrent $[\overline{G}, \overline{G}]$, on obtient que $\pi(G^{(1)}) = \overline{G}^{(1)}$. Une simple récurrence montre que $\pi(G^{(i)}) = \overline{G}^{(i)}$.

Supposons d'abord que $H$ et $G/H$ sont résolubles et posons $m = \mathrm{cl}(H)$, $n = \mathrm{cl}(G/H)$. Alors $\pi(G^{(n)}) = \overline{G}^{(n)} = \{\overline{e}\}$, d'où $G^{(n)} \subseteq H$. En utilisant le i), on obtient que $G^{(n+m)} = \left(G^{(n)}\right)^{(m)} = \{e\}$. Donc $G$ est résoluble et $\mathrm{cl}(G) \leqslant n+m$.

Réciproquement, si $G$ est résoluble, alors $\overline{G}^{(\mathrm{cl}(G))} = \pi(G^{(\mathrm{cl}(G))}) = \{\overline{e}\}$. Donc $G/H$ est résoluble de classe $\leqslant \mathrm{cl}(G)$. ∎

**Exemples.** 1) Tout groupe abélien non-trivial est résoluble de classe 1.

2) Le groupe $S_4$ est résoluble :

$$\{e\} \trianglelefteq K \trianglelefteq A_4 \trianglelefteq S_4;$$

$[S_4, S_4] = A_4$, $[A_4, A_4] = K$, $[K, K] = \{e\}$, où $K$ désigne le groupe de Klein. Si $n \geqslant 5$, on a $[A_n, A_n] = A_n$, ce qui montre que les groupes $S_n$ et $A_n$ ne sont pas résolubles.

3) Soit $p$ un nombre premier. Tout $p$-groupe fini est résoluble.

Preuve. On peut prouver cette assertion par récurrence sur $n$, où $p^n := |G|$. Si $n = 0$, alors $G = \{e\}$ et l'assertion est claire.

Supposons maintenant que $n \geqslant 1$. Par le théorème 2.5, $Z(G) \neq \{e\}$. Comme le groupe $Z(G)$ est abélien, il est résoluble. D'autre part, $|G/Z(G)| = p^m$, où $m < n$. Par l'hypothèse de récurrence, $G/Z(G)$ est abélien. On en déduit que $G$ est abélien. ∎

**Théorème 3.3.** *Les propriétés suivantes sont équivalentes :*
i) *$G$ est résoluble.*
ii) *Il existe une chaîne*

$$\{e\} = G_n \trianglelefteq G_{n-1} \trianglelefteq G_{n-2} \trianglelefteq \ldots \trianglelefteq G_1 \trianglelefteq G_0 = G$$

*de sous-groupes* **distingués dans $G$** *et tels que $G_i/G_{i+1}$ soit abélien pour tout $0 \leqslant i \leqslant n-1$.*
iii) *Il existe une chaîne*

$$\{e\} = G_n \trianglelefteq G_{n-1} \trianglelefteq G_{n-2} \trianglelefteq \ldots \trianglelefteq G_1 \trianglelefteq G_0 = G.$$

*telle que $G_i/G_{i+1}$ soit abélien pour tout $0 \leqslant i \leqslant n-1$.*

Preuve. i) ⇒ ii). Posons $G_i := G^{(i)}$. Par le théorème 6.2, $G_{i+1} \trianglelefteq G_i$ et les quotients $G_i/G_{i+1}$ sont abéliens et par la proposition 3.2, $G_i$ sont distingués même das $G$.

ii) ⇒ iii). C'est clair comme la condition ii) est plus forte que la condition iii).

iii) ⇒ i). On montre par récurrence que $G^{(i)} \subseteq G_i$. C'est clair pour $i = 0$. Supposons que $G^{(i)} \subseteq G_i$. Le deuxième théorème d'isomorphisme donne :

$$G^{(i)}/G^{(i)} \cap G_{i+1} \simeq G^{(i)}G_{i+1}/G_{i+1} \subseteq G_i/G_{i+1}$$

Comme $G_i/G_{i+1}$ est abélien, on en déduit que $G^{(i)}/G^{(i)} \cap G_{i+1}$ l'est aussi. En appliquant le théorème 6.2 on obtient que $G^{(i+1)} \subseteq G^{(i)} \cap G_{i+1} \subseteq G_{i+1}$, ce qui achève la démonstration. ∎

Nous donnons maintenant un exemple important de groupes résolubles.

**Proposition 3.4.** *Soit $K$ un corps et soit $T_n^+(K)$ le groupe multiplicatif des matrices triangulaires supérieures inversibles. Alors $T_n^+(K)$ est résoluble de classe $\leqslant n$.*

Preuve. a) Soit $\{e_1, e_2, \ldots, e_n\}$ la base canonique de l'espace vectoriel $V := K^n$. On considère le drapeau des sous-espaces vectoriels $V_k$ :

$$V_n = \{0\} \subset V_{n-1} \subset \ldots \subset V_1 \subset V_0 = V, \qquad V_k = \{e_1, e_2, \ldots, e_{n-k}\}, \qquad 0 \leqslant k \leqslant n.$$

Soit

$$B_i := \{g \in T_n^+(K) \mid (g-1)V_k \subset V_{k+i}, \quad 0 \leqslant k \leqslant n-i\}.$$

On vérifie facilement que $B_0 = T_n^+(K)$ et que pour tout $1 \leqslant i \leqslant n$ on a :

$$B_i = 1 + N_i, \qquad N_i = \{g = (a_{st}) \mid a_{st} = 0 \quad \text{si } s \geqslant t - i + 1\}.$$

En particulier, $B_n = \{1\}$.

b) On vérifiera la propriété suivante :

$$\text{si } g_j \in B_j \text{ et } g_i \in B_i, \text{ alors } [g_j, g_i] \in B_{\min\{i+j,n\}}.$$

Pour tout $v_k \in V_k$ on a :

$$g_j(v_k) = v_k + x_{k+j}, \qquad x_{k+j} \in V_{k+j},$$
$$g_i(v_k) = v_k + y_{k+i}, \qquad y_{k+i} \in V_{k+i}.$$

Donc

$$g_i g_j(v_k) = v_k + x_{k+j} + y_{k+i} \pmod{V_{k+i+j}},$$
$$g_j g_i(v_k) = v_k + x_{k+j} + y_{k+i} \pmod{V_{k+i+j}}.$$

On en déduit que $g_i g_j(v_k) \equiv g_j g_i(v_k) \pmod{V_{k+i+j}}$, d'où on a :

$$[g_i^{-1}, g_j^{-1}](v_k) = g_i^{-1} g_j^{-1} g_i g_j(v_k) \equiv v_k \pmod{V_{k+i+j}}.$$

Donc $[g_j, g_i]^{-1} = [g_i^{-1}, g_j^{-1}] \in B_{i+j}$. Comme $B_{i+j}$ est un groupe, $[g_j, g_i] \in B_{\min\{i+j,n\}}$.

c) Un calcul simple montre que $[B_0, B_0] \subseteq B_1$. En utilisant la propriété b), on obtient que $[B_i, B_j] \subseteq B_{\min\{i+j,n\}}$. En particulier, $[B_i, B_i] \subseteq B_{\min\{2i,n\}}$ pour $i \geqslant 1$. On en déduit la proposition. ∎

**Corollaire 3.5.** *$B_i \trianglelefteq T_n^+(K)$ pour tout $0 \leqslant i \leqslant n$.*

Preuve. La preuve est laissée en exercice. ∎

**Remarque 3.6.** 1) Un groupe fini d'ordre $p^a q^b$, où $p$ et $q$ sont des nombres premiers, est résoluble (Théorème de Burnside).

2) Tout groupe fini d'ordre impair est résoluble (théorème de Feit-Thompson).

**Définition.** *Soit $G$ un groupe. On appelle chaîne normale de sous-groupes de $G$ une suite finie de la forme*

$$\{e\} = G_n \trianglelefteq G_{n-1} \trianglelefteq G_{n-2} \trianglelefteq \ldots \trianglelefteq G_1 \trianglelefteq G_0 = G.$$

*On appelle $n$ la longueur de la chaîne.*

Soit $H \trianglelefteq G$. On pose $\overline{G} := G/H$ et l'on note $\pi : G \to \overline{G}$ le morphisme canonique. Soient

$$\{e\} = H_m \trianglelefteq H_{m-1} \trianglelefteq H_{m-2} \trianglelefteq \ldots \trianglelefteq H_1 \trianglelefteq H_0 = H$$

et

$$\{e\} = \overline{G}_n \trianglelefteq \overline{G}_{n-1} \trianglelefteq \ldots \trianglelefteq \overline{G}_1 \trianglelefteq \overline{G}_0 = \overline{G},$$

deux chaînes normales. Posons

$$G_i = \begin{cases} \pi^{-1}(\overline{G}_i), & \text{si } 0 \leqslant i \leqslant n, \\ H_{i-n}, & \text{si } n \leqslant i \leqslant m+n. \end{cases}$$

Remarquons que pour $i = n$ on a :

$$G_n = \pi^{-1}(\{\overline{e}\}) = H = H_0.$$

**Proposition 3.7.** *On a une chaîne normale de longueur $n+m$ :*

$$\{e\} = G_{n+m} \trianglelefteq G_{n+m-1} \trianglelefteq \ldots \trianglelefteq G_n \trianglelefteq \ldots \trianglelefteq G_1 \trianglelefteq G_0 = G.$$

*En outre,*

$$G_i/G_{i+1} := \begin{cases} \overline{G}_i/\overline{G}_{i+1}, & \textit{si } 0 \leqslant i \leqslant n-1, \\ H_{i-n}/H_{i-n+1}, & \textit{si } n \leqslant i \leqslant m+n-1. \end{cases}$$

Preuve. Pour tout $i$ tel que $0 \leqslant i \leqslant n$ posons $G_i = \pi^{-1}(\overline{G}_i)$. Comme le morphisme $\pi$ est surjectif, sa restriction sur $G_i$

$$\pi|_{G_i} : G_i \to \overline{G}_i$$

est surjective et $\ker(\pi|_{G_i}) = H$. Par définition, $G_{i+1}$ est le noyau du morphisme

$$G_i \to \overline{G}_i \to \overline{G}_i/\overline{G}_{i+1}.$$

On en déduit que $G_{i+1} \trianglelefteq G_i$, et par le troisième théorème d'isomorphisme, on a :

$$\overline{G}_i/\overline{G}_{i+1} \simeq (G_i/H)/(G_{i+1}/H) \simeq G_i/G_{i+1}, \qquad \text{pour tout } 0 \leqslant i \leqslant n-1.$$

■

**Théorème 3.8.** *Soit $G$ un groupe fini. Les propriétés suivantes sont équivalentes :*

*i) $G$ est résoluble.*

*ii) Il existe une chaîne normale telle que chaque groupe quotient soit cyclique.*

*iii) Il existe une chaîne normale telle que chaque groupe quotient soit d'ordre premier.*

Preuve. Il est clair que iii) $\Rightarrow$ ii) $\Rightarrow$ i). Il reste à montrer que i) $\Rightarrow$ iii).

a) Nous prouvons par récurrence que tout groupe abélien fini $A$ d'ordre $> 1$ admet une chaîne normale telle que chaque groupe quotient soit d'ordre premier. Si $A$ est d'ordre 2, c'est clair. Supposons que l'assertion est vraie pour les groupes d'ordre $< m$. Soit $|A| = m$. Par le lemme 3.2, $A$ admet un sous-groupe cyclique $C$ d'ordre premier. Par l'hypothèse de récurrence, $A/C$ admet une chaîne telle que tout groupe quotient soit d'ordre premier. En appliquant la proposition 3.7, on obtient une chaîne pour le groupe $A$ vérifiant la propriété voulue.

b) Nous montrons que i) $\Rightarrow$ iii) par récurrence sur l'ordre $n$ de $G$. Supposons que l'assertion est prouvée pour les groupes d'ordre $< n$. En vertu de a), nous pouvons supposer que $G$ n'est pas abélien. Alors il existe un sous-groupe non-trivial $H \trianglelefteq G$ tel que $G/H$ soit abélien. Par l'hypothèse de récurrence, $H$ et $G/H$ admettent des chaînes normales telles que chaque groupe quotient soit d'ordre premier. En appliquant la proposition 3.7, on obtient une chaîne pour le groupe $G$ vérifiant la propriété voulue. ■

CHAPITRE 4

# Théorie de Galois

## 1. Extensions de corps

Soit $K$ un corps. On note $1_K$ l'élément neutre pour multiplication de $K$ (l'élément unité). On appelle morphisme caractéristique le morphisme d'anneaux $\psi : \mathbf{Z} \to K$ défini par :

$$\psi(n) = \begin{cases} \underbrace{1_K + 1_K + \cdots + 1_K}_{n \text{ fois}}, & \text{si } n \geqslant 0, \\ -\psi(-n), & \text{si } n < 0. \end{cases}$$

Le noyau $\ker(\psi)$ est un idéal de $\mathbf{Z}$ et l'application $\psi$ induit un monomorphisme

$$\overline{\psi} : \mathbf{Z}/\ker(\psi) \hookrightarrow K.$$

On en déduit que $\mathbf{Z}/\ker(\psi)$ est un anneau intègre. Ceci implique que soit $\ker(\psi) = \{0\}$, soit $\ker(\psi) = p\mathbf{Z}$, où $p$ est un nombre premier.

- Si $\ker(\psi) = p\mathbf{Z}$, on dit que $K$ est de caractéristique $p$. Alors $K$ contient un sous-corps qui est isomorphe à $\mathbf{F}_p := \mathbf{Z}/p\mathbf{Z}$.
- Si $\ker(\psi) = \{0\}$, on dit que $K$ est de caractéristique 0. Alors $\psi : \mathbf{Z} \to K$ est un monomorphisme. On peut prolonger $\psi$ en morphisme de corps $\mathbf{Q} \to K$ en posant
$$\psi\left(\frac{a}{b}\right) = \frac{\psi(a)}{\psi(b)}, \qquad \frac{a}{b} \in \mathbf{Q}.$$
d'où on déduit que $K$ contient un sous-corps isomorphe à $\mathbf{Q}$.

**Définition.** *i) Si $L$ est un corps contenant $K$, on dit que $L$ est une extension de $K$ et l'on note $L/K$.*

*ii) Une extension $L/K$ est finie si en tant que $K$-espace vectoriel, $L$ est de dimension finie sur $K$, i.e. s'il existe $\omega_1, \ldots, \omega_n \in L$ tels que tout $x \in L$ s'écrit de façon unique sous la forme*

$$x = a_1\omega_1 + a_2\omega_2 + \cdots + a_n\omega_n, \qquad a_i \in K.$$

*On appelle degré de l'extension $L/K$ et l'on note $[L : K]$ la dimension n de $L$ sur $K$.*

**Théorème 1.1** (théorème de la base télescopique)**.** *Soient $L$ une extension de $K$ et $M$ une extension de $L$. Alors :*

i) *$M/K$ est finie si et seulement si $M/L$ et $L/K$ sont finies. Dan ce cas, on a :*

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

ii) *Plus précisément, si* $\{\omega_i\}_{i=1}^m$ *est une base de* $L/K$ *et* $\{\Omega_j\}_{j=1}^n$ *est une base de* $M/L$*, alors* $\{\Omega_j\omega_i\}_{1\leqslant i\leqslant m, 1\leqslant j\leqslant n}$ *est une base de* $M/K$.

Preuve. a) Supposons que $M/K$ est finie. Toute base de $M$ sur $K$ est une famille génératrice de $M$ sur $L$. On en déduit que $[M : L] \leqslant [M : K] < +\infty$. Le corps $L$ est un sous-$K$-espace vectoriel de $M$, d'où $[L : K] \leqslant [M : K]$. Donc $M/L$ et $L/K$ sont finies.

b) Supposons que $L/K$ et $M/L$ sont finies et posons $m = [L : K]$ et $n = [M : L]$. Soient $\{\omega_i\}_{i=1}^m$ une base de $L/K$ et $\{\Omega_j\}_{j=1}^n$ une base de $M/L$. Nous allons montrer que $\{\Omega_j\omega_i\}_{1\leqslant i\leqslant m, 1\leqslant j\leqslant n}$ est une base de $M/K$.

Soit $y \in M$. Alors il existe des éléments $x_1, \ldots, x_n \in L$ tels que

$$y = \sum_{j=1}^{n} x_j \Omega_j.$$

Par ailleurs, pour tout $j$ on a :

$$x_j = \sum_{i=1}^{m} a_{ij}\omega_i, \qquad a_{ij} \in K.$$

Donc on a :

$$y = \sum_{j=1}^{n}\sum_{i=1}^{m} a_{ij}(\omega_i\Omega_j), \qquad a_{ij} \in K.$$

On en déduit que $\{\Omega_j\omega_i\}_{1\leqslant i\leqslant m, 1\leqslant j\leqslant n}$ est une famille génératrice.

Montrons que la famille $\{\Omega_j\omega_i\}_{1\leqslant i\leqslant m, 1\leqslant j\leqslant n}$ est libre. Supposons que

$$\sum_{\substack{1\leqslant i\leqslant m\\ 1\leqslant j\leqslant n}} b_{ij}(\omega_i\Omega_j) = 0, \qquad b_{ij} \in K.$$

Cette relation s'écrit aussi :

$$\sum_{j=1}^{n}\left(\sum_{i=1}^{n} b_{ij}\omega_i\right)\Omega_j = 0.$$

Comme $\{\Omega_j\}_{j=1}^n$ est une base de $M/L$, on en déduit que

$$\sum_{i=1}^{n} b_{ij}\omega_i = 0, \qquad 1 \leqslant j \leqslant n.$$

Pour chaque $j$, comme $\{\omega_i\}_{i=1}^m$ est une base de $L/K$, on obtient que $b_{ij} = 0$. Donc la famille $\{\Omega_j\omega_i\}_{1\leqslant i\leqslant m, 1\leqslant j\leqslant n}$ est libre. ∎

**Définition.** *Soit* $L/K$ *une extension.*

*1) Un élément* $\alpha \in L$ *est algébrique sur* $K$ *s'il existe un polynôme non-nul* $f(X) \in K[X]$ *tel que* $f(\alpha) = 0$.

*2) Une extension* $L/K$ *est algébrique, si tout* $\alpha \in L$ *est algébrique sur* $K$.

**Théorème 1.2.** *Toute extension finie est algébrique.*

PREUVE. Soit $L/K$ une extension finie et soit $n = [L : K]$. Soit $\alpha$ un élément de $L$. Alors les éléments $1, \alpha, \alpha^2, \ldots, \alpha^n$ forment une famille de vecteurs de cardinal $n+1$ dans $L$. Cette famille est donc liée, i.e. il existe $a_0, a_1, \ldots, a_n$ qui ne sont pas tous nuls et tels que

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

On en déduit le théorème. ∎

**Théorème 1.3.** *Soit $\alpha \in L$ un élément algébrique sur $K$. Alors l'idéal*

$$I = \{f(X) \in K[X] \mid f(\alpha) = 0\}$$

*est un idéal principal dans $K[X]$ qui est engendré par un polynôme unitaire irréductible $P(X)$.*

*On dit que $P(X)$ est le polynôme minimal de $\alpha$ sur $K$.*

PREUVE. Comme l'anneau $K[X]$ est principal, il existe un polynôme unitaire $P(X)$ qui engendre $I$. Pour montrer qu'il est irréductible supposons que $P(X)$ se décompose en produit de deux facteurs de degré $< \deg(P)$ :

$$P(X) = f(X)g(X).$$

Alors $f(\alpha)g(\alpha) = P(\alpha) = 0$, d'où on tire que l'un au moins des facteurs est nul. Si, par exemple, $f(\alpha) = 0$, alors $f(X) \in I$, donc $P(X) \mid f(X)$. D'autre part, $\deg(f) < \deg(P)$, ce qui donne une contradiction. ∎

Soit $\alpha \in L$ un élément algébrique et soit $P$ le polynôme minimal de $\alpha$. On note $K[\alpha]$ la plus petite sous-extension de $L/K$ contenant $\alpha$. On pose $n = \deg(P)$. Alors :

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

Plus précisement, on a le résultat suivant.

**Théorème 1.4.** *Soit $\alpha \in L$ un élément algébrique et soit $P$ le polynôme minimal de $\alpha$. Alors :*

i) *L'application*

$$\varphi : K[X] \to L$$

*définie par $\varphi(f(X)) = f(\alpha)$ est un homomorphisme d'anneaux.*

ii) *$\ker(\varphi) = (P)$ est un idéal maximal de $k[X]$, le quotient $K[X]/(P)$ est un corps et le théorème de factorisation donne un isomorphisme :*

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

iii) *$K[\alpha]/K$ est une extension finie de degré $n = \deg(P(X))$ et la famille*

$$\{1, \alpha, \alpha^2, \ldots, \alpha^{n-1}\}$$

*est une base de $K[\alpha]/K$.*

PREUVE. i) On vérifie facilement que pour tous $f, g \in K[X]$

$$\varphi(f+g) = (f+g)(\alpha) = f(\alpha) + g(\alpha) = \varphi(f) + \varphi(g),$$
$$\varphi(fg) = (fg)(\alpha) = f(\alpha)g(\alpha) = \varphi(f)\varphi(g).$$

Donc $\varphi$ est un morphisme d'anneaux.

ii) D'après le théorème 1.3, $\ker(\varphi) = I = (P)$. Donc le théorème de factorisation induit un isomorphisme :

$$K[X]/(P) \xrightarrow{\overline{\varphi}} \mathrm{Im}(\varphi), \tag{11}$$

où $\mathrm{Im}(\varphi)$ désigne l'image de $\varphi$. Comme $P$ est un élément irréductible de l'anneau principal $K[X]$, l'idéal $(P)$ est maximal et le quotient $L = K[X]/(P)$ est un corps. Pour tout $f(X) \in K[X]$ on note $\overline{f(X)}$ l'image de $f(X)$ dans $L$ par la projection naturelle. Alors $\{\overline{1}, \overline{X}, \ldots, \overline{X}^{n-1}\}$ est une base de $L$ sur $K$. En outre :

$$P(\overline{X}) = \overline{P(X)} = \overline{0}.$$

En utilisant l'isomorphisme (11), on en déduit que $\mathrm{Im}(\varphi)$ est une sous-extension de $L$ de degré $n$ sur $K$. Comme $\varphi(\overline{X}) = \alpha$, la famille

$$\{1, \alpha, \alpha^2, \ldots, \alpha^{n-1}\}$$

est une base de $\mathrm{Im}(\varphi)$ sur $K$. Toute extension de $K$ contenant $\alpha$ contient aussi les puissances $1, \alpha, \alpha^2, \ldots, \alpha^{n-1}$. On en déduit que $\mathrm{Im}(\varphi) = K[\alpha]$, donc $K[X]/(P) \simeq K[\alpha]$. ∎

**Corollaire 1.5.** *Si $\alpha$ et $\beta \in L$ sont deux éléments algébriques sur $K$, alors $\alpha \pm \beta$, $\alpha\beta$ et $\alpha\beta^{-1}$ (si $\beta \neq 0$) sont algébriques sur $K$. Les éléments de $L$ qui sont algébriques sur $K$ forment un corps.*

Preuve. On considère les extensions

$$K \subseteq K[\alpha] \subseteq K[\alpha, \beta].$$

Par le théorème 1.4, les extensions $K[\alpha]/K$ et $K[\alpha,\beta]/K[\alpha]$ sont finies. Alors le théorème de la base télescopique implique que $K[\alpha,\beta]/K$ est finie. Comme les éléments $\alpha \pm \beta$, $\alpha\beta$ et $\alpha\beta^{-1}$ appartiennent à $K[\alpha,\beta]$, ils sont algébriques sur $K$. ∎

**Définition.**

1) *On dit qu'une extension $L/K$ est simple (ou monogène) s'il existe un élément $\alpha \in L$ tel que $L = K[\alpha]$. Alors on dit que $\alpha$ est un élément primitif pour $L$.*
2) *Soit $P \in K[X]$ un polynôme irréductible. On dit que $L$ est un corps de rupture de $P(X)$ si $L$ est une extension simple de $K$ engendrée par une racine de $P$ :*

$$L = K[\alpha], \qquad P(\alpha) = 0.$$

**Théorème 1.6.** *Soit $P(X) \in K[X]$ un polynôme irréductible. Alors $P$ possède un corps de rupture qui est unique à isomorphisme près.*

Preuve. a) Soit $L = K[X]/(P)$. Comme $P$ est irréductible, l'idéal principal $(P)$ est maximal et $L$ est un corps. Soit $\overline{X}$ est l'image de $X$ dans $L$. Alors $P(\overline{X}) = 0$ et $L = K[\overline{X}]$. Donc $L$ est un corps de rupture de $P$. D'après le théorème 1.4, tout corps de rupture de $P$ est isomorphe à $L$, d'où l'unicité à isomorphisme près. ∎

**Définition.** *Soit $f(X) \in K[X]$ un polynôme non-nul. On dit que $L/K$ est un corps de décomposition de $f(X)$ si*

*1) $f(X) = a(X-\alpha_1)(X-\alpha_2)\cdots(X-\alpha_n)$ dans $L[X]$.*
*2) $L = K[\alpha_1, \alpha_2, \ldots, \alpha_n]$.*

**Théorème 1.7.** *Tout polynôme non-nul possède un corps de décomposition qui est unique à isomorphisme près.*

**Définition.** *On appelle clôture algébrique de $K$ une extension algébrique $\overline{K}/K$ telle que tout polynôme $f(X) \in \overline{K}[X]$ est scindé:*

$$f(X) = a(X-\alpha_1)\cdot(X-\alpha_2)\cdots(X-\alpha_n).$$

**Théorème 1.8** (Steinitz)**.** *Tout corps admet un clôture algébrique. Deux clôtures algébriques de $K$ sont isomorphes.*

## 2. Prolongement des homomorphismes

**Définition.** *On appelle homomorphisme (ou tout simplement morphisme) de corps tout morphisme d'anneaux entre deux corps. Plus explicitement, si $L$ et $M$ sont deux corps, on dit qu'une application $\sigma : L \to M$ est un homomorphisme si et seulement si elle vérifie les propriétés suivantes :*

1) $\sigma(x+y) = \sigma(x)+\sigma(y), \qquad \forall x, y \in L;$
2) $\sigma(xy) = \sigma(x)\sigma(y), \qquad \forall x, y \in L;$
3) $\sigma(1_L) = 1_M.$

**Remarque 2.1.** Un homomorphisme de corps est toujours injectif. En effet, le noyau $\ker(\sigma)$ d'un morphisme $\sigma : L \to M$ est un idéal de $L$. Comme les seuls idéaux d'un corps sont (0) et lui-même et comme $\sigma(1_L) = 1_M$, on trouve que $\ker(\sigma) = (0)$, d'où l'on tire l'injectivité de $\sigma$.

Soit $K$ un corps de caractéristique positive $p$. Alors l'application

$$\varphi : K \to K,$$
$$\varphi(x) = x^p$$

est un morphisme de corps appelé endomorphisme de Frobenius.

**Définition.** *Soit $\sigma : L \to M$ un morphisme de corps et soit $F/L$ une extension. On appelle prolongement de $\sigma$ à $F$ tout homomorphisme $\widehat{\sigma} : F \to E$ à valeurs dans une extension $E/M$ tel que $\hat{\sigma}|_L = \sigma$ :*

$$\begin{array}{ccc} F & \xrightarrow{\widehat{\sigma}} & E \\ \big| & & \big| \\ L & \xrightarrow{\sigma} & M \end{array}$$

Nous étudions le problème de prolongement d'abord pour les extensions finies simples. Soit $F/L$ une extension finie simple et soit $\alpha$ un élément primitif de $F$ sur $L$ ; on a $F = K[\alpha]$. Soit $P(X) = \sum_{k=1}^{n} a_k X^k$ le polynôme minimal de $\alpha$. On note

$$P^{\sigma}(X) = \sum_{k=1}^{n} \sigma(a_k) X^k \in M[X]$$

le polynôme obtenu en appliquant $\sigma$ aux coefficients de $P[X]$.

**Théorème 2.2.** *Soit $E/M$ une extension. Alors :*

i) *Le nombre de prolongements*

$$\widehat{\sigma} : F \to E$$

*de $\sigma$ à $F$ à valeurs dans $E$ est égal au nombre de racines distinctes de $P^\sigma(X)$ dans $E$.*

ii) *Il existe une extension finie $E/M$ telle que $\sigma$ admet un prolongement $\widehat{\sigma} : F \to E$.*

Preuve. i) Soit $\widehat{\sigma} : F \to E$ un prolongement de $\sigma$. Comme $\alpha$ est un élément primitif pour $F/L$, tout élément $x \in F$ s'écrit sous la forme $f(\alpha)$ avec $f(X) = \sum c_k X^k \in L[X]$. Donc

$$\widehat{\sigma}(x)) = \sum \sigma(c_k)\widehat{\sigma}(\alpha)^k.$$

Ce calcul montre que $\widehat{\sigma}$ est complètement déterminé par $\widehat{\sigma}(\alpha)$. En outre :

$$0 = \widehat{\sigma}(P(\alpha)) = \sum_{k=1}^{n} \sigma(a_k)\widehat{\sigma}(\alpha)^k = P^\sigma(\widehat{\sigma}(\alpha))$$

ce qui montre que $\widehat{\sigma}(\alpha)$ est une racine de $P^\sigma(X)$. Donc on a une application injective :

$$\begin{aligned} \{\text{prolongements de } \sigma\} &\to \{\text{racines de } P^\sigma(X) \text{ dans } E\}, \\ \widehat{\sigma} &\mapsto \widehat{\sigma}(\alpha). \end{aligned} \tag{12}$$

Montrons que cette application est surjective. Soit $\beta \in E$ une racine de $P^\sigma(X)$. Pour tout $x = f(\alpha) \in F$ posons

$$\widehat{\sigma}(x) = f^\sigma(\beta).$$

On peut facilement vérifier que $\widehat{\sigma}(x)$ ne dépend pas du choix de $f(X)$. Si $\tilde{f}(X) \in L[X]$ est un autre polynôme vérifiant $x = \tilde{f}(\alpha)$, alors $\tilde{f}(X)$ s'écrit sous la forme $\tilde{f}(X) = f(X) + P(X)h(X)$, d'où

$$\tilde{f}^\sigma(\beta) = f^\sigma(\beta) + P^\sigma(\beta)\, h^\sigma(\beta) = f^\sigma(\beta).$$

Un calcul élémentaire montre que $\widehat{\sigma}$ ainsi défini est un morphisme de corps. Donc l'application (12) est une bijection. On en déduit le i).

ii) Il suffit d'appliquer le i) à un corps de rupture $E$ de $P^\sigma(X)$. ∎

Nous étudions maintenant le cas général.

**Théorème 2.3** (prolongement des homomorphismes)**.** *$\sigma : L \to M$ un homomorphisme de corps et soit $F/L$ une extension finie. Alors :*

i) *Il existe une extension finie $E/M$ et un prolongement $\widehat{\sigma} : F \to E$ de $\sigma$ à $F$ à valeurs dans $E$.*

ii) *Pour tout $E$, le nombre de prolongements*

$$\widehat{\sigma} : F \to E$$

*de $\sigma$ est $\leqslant [F : L]$.*

Preuve. On montre le théorème par récurrence sur le degré $n = [L : K]$. Le cas $n = 1$ est trivial. Supposons que les propriétés i) et ii) sont vraies pour les extensions de degré $< n$. On choisit un élément $\alpha \in F$ tel que $\alpha \notin L$.

i) D'après le théorème 2.2, il existe une extension $E'/M$ telle que $\sigma$ possède un prolongement $\sigma' : L[\alpha] \to E'$. On remarque que $[L : K[\alpha]] < n$. Par l'hypothèse de récurrence, il existe donc une extension $E/E'$ avec un prolongement $\widehat{\sigma} : F \to E$ de $\sigma'$.

ii) On note $P(X)$ le polynôme minimal de $\alpha$ et l'on pose $m = \deg(P) = [L[\alpha] : L]$. Soit $E/M$ une extension finie et soient

$$\widehat{\sigma}_i : L[\alpha] \to E, \qquad 1 \leqslant i \leqslant m'$$

les prolongements de $\sigma$ à $L[\alpha]$. D'après le théorème 2.2, on a :

$$m' \leqslant m.$$

Pour chaque $i$, on note

$$\widehat{\sigma}_{ij} : F \to E, \qquad 1 \leqslant j \leqslant k'_i$$

les prolongements de $\widehat{\sigma}_i$ à $F$ :

$$\begin{array}{ccc} F & \xrightarrow{\widehat{\sigma}_{ij}} & E \\ | & & | \\ L[\alpha] & \xrightarrow{\widehat{\sigma}_i} & E \\ | & & | \\ L & \xrightarrow{\sigma} & M \end{array}$$

Par l'hypothèse de récurrence, on a :

$$k'_i \leqslant [F : L[\alpha]], \qquad 1 \leqslant i \leqslant m'.$$

Soit $n'$ le nombre de prolongements de $\sigma$ à $F$ à valeurs dans $E$. Alors :

$$n' = \sum_{i=1}^{m'} k'_i \leqslant [F : L[\alpha]] \cdot m' = [F : L[\alpha]] \cdot [L[\alpha] : L] = [F : L].$$

Le théorème est démontré. ∎

## 3. Extensions séparables

Rappelons que si $K$ est un corps de caractéristique positive $p$, alors il est muni de l'endomorphisme de Frobenius :

$$\varphi : K \to K$$
$$\varphi(x) = x^p.$$

**Définition.** *Un corps $K$ est parfait s'il est de caractéristique* 0 *ou, lorsqu'il est de caractéristique positive $p$, si l'application de Frobenius est surjective.*

**Exemples.** 1) Tout corps fini $K$ est parfait. En effet, comme l'endomorphisme de Frobenius est injectif, la surjectivité découle de la finitude de $K$.

2) Soit $\mathbf{F}_p = \mathbf{Z}/p\mathbf{Z}$ et soit $\mathbf{F}(t)$ le corps des fractions de l'anneau des polynômes $\mathbf{F}_p[t]$ à coefficients dans $\mathbf{F}_p$. Comme $\varphi(t) = t^p$, il est facile de voir que $K$ n'est pas parfait.

**Définition.** *Soit $K$ un corps.*

*1) On dit qu'un polynôme $f(X) \in K[X]$ est séparable si toutes ses racines dans son corps de décomposition sont simples.*

*2) Un élément algébrique est séparable sur $K$ si son polynôme minimal sur $K$ est séparable.*

On remarque que si $\alpha \in L$ est séparable sur $K$, alors il est séparable sur tout corps intermédiaire $K \subseteq F \subseteq L$. En effet, soient $P(X) \in K[X]$ et $Q(X) \in F[X]$ les polynômes minimaux de $\alpha$ sur $K$ et $F$ respectivement. Alors $Q(X) \mid P(X)$ dans $F[X]$ et donc toutes ses racines sont simples.

**Théorème 3.1.** *1) Un polynôme $f(X) \in K[X]$ est séparable si et seulement si $(f(X), f'(X)) = 1$.*

*2) Tout polynôme irréductible sur un corps parfait est séparable.*

Preuve. 1) Soit $\alpha$ une racine de $f(X)$. En écrivant $f(X)$ sous la forme $f(X) = (X-\alpha)g(X)$ on trouve que

$$f'(X) = (X-\alpha)g'(X) + g(X).$$

Donc

$$(X-\alpha) \mid f'(X) \Leftrightarrow (X-\alpha) \mid g(X) \Leftrightarrow (X-\alpha)^2 \mid f(X).$$

On en déduit que $\alpha$ est une racine multiple de $f(X)$ si et seulement si $(X-\alpha)$ divise $\operatorname{pgcd}(f(X), f'(X))$. Cette équivalence implique que $f(X)$ n'a pas de racines multiples si et seulement si $\operatorname{pgcd}(f(X), f'(X)) = 1$.

2) Nous prouvons le 2) du théorème par l'absurde. Soit $P(X) \in K[X]$ un polynôme irréductible à coefficients dans un corps parfait $K$. Supposons que $P(X)$ n'est pas séparable. Alors $\operatorname{pgcd}(P(X), P'(X)) \neq 1$, d'où $P(X) \mid P'(X)$. Comme $\deg(P') < \deg(P)$, ce n'est possible que si $P'(X) = 0$. On remarque que dans un corps de caractéristique $p$ la dérivée $kX^{k-1}$ de $X^k$ est nulle si et seulement si $p \mid k$. Donc $P'(X)$ est nul si et seulement si $P(X)$ s'écrit sous la forme

$$P(X) = \sum a_i X^{pi}$$

Comme $K$ est parfait, il existent des éléments $b_i \in K$ tels que $b_i^p = a_i$. Alors

$$P(X) = \Big(\sum b_i X^i\Big)^p,$$

ce qui contredit l'irréductibilité de $P(X)$. ∎

**Corollaire 3.2.** *Tout élément algébrique sur un corps parfait est séparable.*

Preuve. C'est clair. ∎

**Exemple.** Soit $K = \mathbf{F}_p(t)$. Alors $X^p - t$ est un polynôme irréductible qui n'est pas séparable.

**Définition.** *Soient $L/K$ et $M/K$ deux extensions d'un corps $K$. On appelle $K$-morphisme (ou morphisme sur $K$) de $L$ dans $M$ tout morphisme de corps $\sigma : L \to M$ tel que $\sigma|_K = \mathrm{id}_K$. On le notera $\sigma : L/K \to M/K$.*

Nous pouvons appliquer le théorème de prolongement des homomorphismes au diagramme

$$\begin{array}{ccc} L & \dashrightarrow & M \\ | & & | \\ K & \xrightarrow{\mathrm{id}_K} & K \end{array}$$

On en déduit que le nombre de morphismes $L/K \to M/K$ est $\leqslant [L : K]$.

**Définition.** *On dit qu'une extension finie $L/K$ de degré $n$ est séparable s'il existe une extension $M/K$ telle que $L/K$ possède $n$ morphismes distincts $L/K \to M/K$.*

**Remarque 3.3.** Il existe une extension $E/K$ telle que $L/K$ possède $n$ morphismes distincts $L/K \to E/K$.

**Proposition 3.4.** *Soit $L/K$ une extension séparable de degré $n$ et soit $\tau : K \to F$ un morphisme de corps. Alors il existe une extension finie $E/F$ telle que $\tau$ admette $n$ prolongements à $L$ à valeurs dans $E$:*

$$\begin{array}{ccc} L & \xrightarrow{\widehat{\tau_i}} & E \\ | & & | \\ K & \xrightarrow{\tau} & F \end{array}$$

*($1 \leqslant i \leqslant n$).*

Preuve. Comme $L/K$ est séparable, il existent $n$ morphismes $\sigma_i : L/K \to M/K$ ($1 \leqslant i \leqslant n$) à valeurs dans une extension finie $M$ de $K$. Par le théorème de prolongement des homomorphismes, le morphisme $\tau : K \to F$ se prolonge en un morphisme $\psi : M \to E$ à valeurs dans une extension finie $E$ de $F$ :

$$\begin{array}{ccccc} L & \xrightarrow{\sigma_i} & M & \xrightarrow{\psi} & E \\ | & \nearrow & & \nearrow & \\ K & \xrightarrow{\tau} & F & & \end{array}$$

En posant $\widehat{\tau_i} = \psi \circ \sigma_i$, on obtient $n$ prolongements de $\tau$ à $L$ à valeurs dans $E$. ∎

**Théorème 3.5.** *Une extension finie simple $L = K[\alpha]$ de $K$ est séparable si et seulement si $\alpha$ est séparable.*

Preuve. Soit $P(X) \in K[X]$ le polynôme minimal de $\alpha$ et soit $n = \deg(P) = [L : K]$. Soit $M$ une extension de $K$. D'après le théorème 2.2, le nombre de morphismes $L/K \to M/K$ est égal au nombre des racines de $P(X)$ dans $M$. Si $L/K$ est séparable, alors il existe $M$ tel que $P(X)$ possède $n$ racines distinctes ; on en déduit que $P(X)$ est séparable. Réciproquement, si $P(X)$ est séparable, on peut prendre comme $M$ un corps de décomposition de $P(X)$. ∎

**Théorème 3.6.** *Soient $K \subset L \subset F$. Alors $F/K$ est séparable si et seulement si $F/L$ et $L/K$ sont séparables.*

PREUVE. Il faut comparer la preuve de ce théorème à celle du théorème 2.3.

Soit $M$ une extension de $K$ et soient

$$\sigma_i : L/K \to M/K, \quad 1 \leqslant i \leqslant m'$$

les $K$-morphismes de $L$ dans $M$. Pour chaque $i$, on note

$$\sigma_{ij} : F/K \to M/K, \quad 1 \leqslant j \leqslant k'_i$$

les prolongements de $\sigma_i$ à $F$. Ces données sont représentées dans le diagramme :

$$\begin{array}{ccc} F & \xrightarrow{\sigma_{ij}} & M \\ | & & | \\ L & \xrightarrow{\sigma_i} & M \\ | & \nearrow & \\ K & & \end{array}$$

Soit $n'$ le nombre de morphismes $F/K \to M/K$. Comme tout $K$-morphisme de $F$ dans $M$ est un prolongement de sa restriction sur $L$, on a

$$n' = \sum_{i=1}^{m'} k'_i.$$

Soient $m = [L : K]$, $k = [F : L]$ et $n = [F : K]$. D'après le théorème de prolongement des homomorphismes, on a :

$$n' \leqslant n, \quad m' \leqslant m, \quad k'_i \leqslant k.$$

Supposons que $F/K$ est séparable. Alors il existe $M$ tel que $n' = n$. Par le théorème de la base télescopique, $n = mk$. Donc

$$\sum_{i=1}^{m'} k'_i = mk.$$

On en déduit que $m' = m$ et $k'_i = k$ pour tout $i$. Donc $L/K$ et $F/L$ sont séparables.

Réciproquement, si $L/K$ et $F/L$ sont séparables, il existe une extension $M$ telle que $m' = m$ et $k'_i = k$ pour tout $1 \leqslant i \leqslant m$. On en déduit que $n' = n$. Donc $F/K$ est séparable. ∎

**Théorème 3.7.** *Une extension finie $L/K$ est séparable si et seulement si tout élément de $L$ est séparable sur $K$.*

PREUVE. $\boxed{\Rightarrow}$ Supposons que $L/K$ est séparable. Soit $\alpha \in L$. Alors $K \subseteq K[\alpha] \subseteq L$ et $K[\alpha]/K$ est séparable par le théorème 3.6. D'après le théorème 3.5, $\alpha$ est séparable.

$\boxed{\Leftarrow}$ Nous démontrons la réciproque par récurrence sur le degré $n = [L : K]$. Le cas $n = 1$ est trivial. Supposons que la propriété est prouvée pour toutes les extensions de degré $< n$. On choisit un élément $\alpha \in L$ tel que $\alpha \notin K$. Comme $\alpha$ est séparable, $K[\alpha]/K$ est une extension séparable non-triviale de $K$. Comme $[L : K[\alpha]] < n$, et comme tout élément de $L$ est séparable sur $K[\alpha]$, l'extension $L/K[\alpha]$

est séparable par l'hypothèse de récurrence. D'après le théorème 3.6, $L/K$ est séparable. ∎

**Corollaire 3.8.** *Toute extension finie d'un corps parfait est séparable.*

## 4. Le théorème de l'élément primitif

Rappelons qu'une extension $L/K$ est simple (ou monogène) s'il existe un élément $\theta \in L$ tel que $L = K[\theta]$. Si c'est le cas, on dit que $\theta$ est un élément primitif pour $L/K$.

**Théorème 4.1** (théorème de l'élément primitif)**.** *Toute extension séparable de degré finie $L/K$ est simple, i.e. il existe $\theta \in L$ tel que $L = K[\theta]$.*

Preuve. a) Supposons d'abord que $K$ est un corps fini. Comme $[L : K] < +\infty$, $L$ est aussi fini. Comme le groupe multiplicatif d'un corps fini est cyclique, il existe $\theta \in L$ tel que $L^* = \langle\theta\rangle$. On en déduit facilement que $L = K[\theta]$.

b) Supposons maintenant que $K$ est infini. On prouve le théorème par récurrence sur $n = [L : K]$.

1) Si $n = 1$, alors $L = K$ et l'assertion est claire.

2) Supposons que toutes les extensions séparables de degré $< n$ sont simples. Soit $L/K$ une extension séparable de degré $n$. Choisissons un élément $\alpha \in L$ tel que $\alpha \notin K$ et posons $F = K[\alpha]$. Alors

$$K \subset F \subset L,$$

où $[L : F] < n$. L'extension $L/F$ est séparable, et par l'hypothèse de récurrence, il existe $\beta \in L$ tel que

$$L = F[\beta] = K[\alpha,\beta].$$

On cherche un élément primitif pour $L/K$ sous la forme

$$\theta = \alpha + c\beta, \qquad c \in K.$$

Comme $L/K$ est séparable, il existe une extension $M/K$ telle que $L/K$ admette $n$ homomorphismes $\sigma_i : L/K \to M/K$ sur $K$ $(1 \leqslant i \leqslant n)$. On pose $\alpha_i = \sigma_i(\alpha)$ et $\beta_i = \sigma_i(\beta)$. Alors :

$$\sigma_i(\theta) = \alpha_i + c\beta_i, \qquad 1 \leqslant i \leqslant n.$$

Supposons que les éléments $\sigma_i(\theta)$ sont deux à deux distincts. Alors l'extension $K[\theta]/K$ admet $n$ homomorphismes $K[\theta] \to M/K$ qui sont induits par les homomorphismes $\sigma_i$. On en déduit que $K[\theta]/K$ est une sous-extension de $L/K$ de degré $n = [L : K]$, d'où $L = K[\theta]$. Donc, il suffit de montrer qu'il existe $c \in K$ tel que

$$\sigma_i(\theta) \neq \sigma_j(\theta), \quad \text{si } i \neq j.$$

La dernière condition s'écrit :

$$c(\beta_j - \beta_i) \neq \alpha_i - \alpha_j \quad \text{si } i \neq j.$$

Comme $L = K[\alpha,\beta]$, chaque $\sigma_i$ est complètement déterminé par le couple $(\alpha_i,\beta_i)$, dce qui signifie que $(\alpha_i,\beta_i) \neq (\alpha_j,\beta_j)$ si $i \neq j$. Donc, il suffit de choisir $c \in K$ tel que

$$c \neq \frac{\alpha_i - \alpha_j}{\beta_j - \beta_i} \qquad \text{pour tous } (i, j) \text{ tels que } \beta_i \neq \beta_j.$$

C'est possible parce que $K$ est infini. ∎

## 5. Extensions normales, galoisiennes. Groupe de Galois

**Définition.** *Une extension finie $L/K$ est normale si et seulement si elle vérifie la propriété suivante :*

*Pour toute extension $M/L$ et tout homomorphisme $\sigma : L/K \to M/K$ on a $\sigma(L) \subseteq L$.*

Comme $[\sigma(L) : K] = [L : K]$, l'inclusion $\sigma(L) \subseteq L$ implique que $\sigma(L) = L$.

**Théorème 5.1.** *Soit $L/K$ une extension finie. Alors les propriétés suivantes sont équivalentes :*

a) *$L/K$ est normale ;*
b) *Tout polynôme irréductible $P(X) \in K[X]$ ayant une racine dans $L$, est scindé sur $L$ (i.e. a toutes ses racines dans $L$) ;*
c) *$L/K$ est un corps de décomposition d'un polynôme $f(X) \in K[X]$.*

Preuve. a) $\Rightarrow$ b).

Supposons que $L/K$ est normale. Soit $P(X) \in K[X]$ un polynôme irréductible ayant une racine $\alpha \in L$. On considère $P(X)$ comme un polynôme à coefficients dans $L$ et l'on note $M$ un corps de décomposition de $P(X)$ sur $L$ ; donc $L \subseteq M$. Soit $\beta \in M$ une racine de $P(X)$. Soit $\tau : K[\alpha]/K \to M/K$ l'unique homomorphisme sur $K$ vérifiant $\tau(\alpha) = \beta$. Par le théorème de prolongement des homomorphismes, il existe une extension $E/M$ et un prolongement $\sigma : L/K \to E/K$ de $\tau$:

$$\begin{array}{ccc} L & \xrightarrow{\sigma} & E \\ | & & | \\ K[\alpha] & \xrightarrow{\tau} & M \end{array}$$

Comme $L/K$ est normale, on a

$$\beta = \tau(\alpha) = \sigma(\alpha) \in \sigma(L) = L.$$

On en déduit que toute racine $\beta \in M$ de $P(X)$ appartient à $L$. Donc $P(X)$ est scindé sur $L$.

b) $\Rightarrow$ c).

Supposons que l'extension $L/K$ vérifie la propriété b). Comme l'extension $L/K$ est finie, elle est engendrée par une famille finie d'éléments :

$$L = K[\alpha_1, \ldots, \alpha_m], \qquad \alpha_1, \ldots, \alpha_m \in L.$$

Pour chaque $i$, on note $P_i(X) \in K[X]$ le polynôme minimal de $\alpha_i$. Soit $f(X) = P_1(X) \cdot P_2(X) \cdots P_m(X)$ et soit $M$ le corps de décomposition de $f(X)$. Il est alors clair que $L \subseteq M$. D'autre part, chaque polynôme $P_i(X)$ a une racine dans $L$ et par la propriété b), est scindé sur $L$. On en déduit que $M \subseteq L$, d'où $L = M$.

c) $\Rightarrow$ a).

Soit $L$ un corps de décomposition d'un polynôme

$$f(X) = X^n + a_{n-1}X^{n-1} + \cdots a_1 X + a_0 \in K[X].$$

Alors

$$L = K[\alpha_1, \ldots, \alpha_n],$$

où $\alpha_1, \ldots, \alpha_n$ sont les racines de $f(X)$ dans $L$. Soit $\sigma : L/K \to E/K$ un homomorphisme sur $K$ à valeurs dans une extension $E$ de $L$. Comme $\sigma|_K = \mathrm{id}$, on a

$$0 = \sigma(f(\alpha_i)) = \sum_{k=0}^{n} \sigma(a_k) \cdot \sigma(\alpha_i)^k = \sum_{k=0}^{n} a_k \sigma(\alpha_i)^k = f(\sigma(\alpha_i)), \quad 1 \leqslant i \leqslant n.$$

Donc $\sigma(\alpha_i)$ est une racine de $f(X)$, d'où

$$\sigma(\alpha_i) \in L, \qquad 1 \leqslant i \leqslant n.$$

On en déduit que $\sigma(L) \subset L$. Donc l'extension $L/K$ est normale. ∎

Nous introduisons les notations suivantes. Si $L$ est un corps, on note $\mathrm{Aut}(L)$ le groupe des automorphismes du corps $L$ ; la loi de composition est donnée par la composition des applications. Si $L/K$ est une extension de corps, on note $\mathrm{Aut}(L/K)$ le groupe des automorphismes de $L$ laissant $K$ invariant :

$$\mathrm{Aut}(L/K) = \{\sigma \in \mathrm{Aut}(L) \mid \sigma|_K = \mathrm{id}_K\}.$$

Par le théorème de prolongement des homomorphismes, $|\mathrm{Aut}(L/K)| \leqslant [L/K]$.

**Définition.** *Une extension finie $L/K$ est galoisienne (où une extension de Galois) si elle est normale et séparable.*

On remarque que si le corps $K$ est parfait, alors toute extension finie de $K$ est séparable et une extension $L/K$ est galoisienne si et seulement si elle est normale.

**Théorème 5.2.** *Une extension finie $L/K$ est galoisienne si et seulement si* $|\mathrm{Aut}(L/K)| = [L : K]$.

Preuve. a) Soit $n = [L : K]$. Supposons que $L/K$ est galoisienne. Alors $L/K$ est séparable et il existe une extension $E/K$ telle que $L$ possède $n$ homomorphismes $\sigma_i : L/K \to E/K$ sur $K$. Comme $L/K$ est normale, pour tout $i$ on a $\sigma_i(L) = L$. Donc les homomorphismes $\sigma_i$ sont les automorphismes de $L$ et $|\mathrm{Aut}(L/K)| = n$.

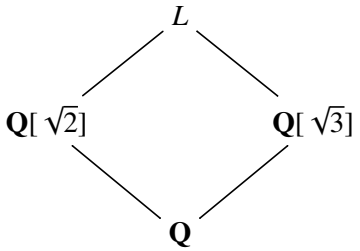
b) Réciproquement, supposons que $|\mathrm{Aut}(L/K)| = n$. Donc il existe $n$ homomorphismes $L/K \to L/K$ ; on en déduit que $L/K$ est séparable. Soit $E$ une extension de $L$. Alors les éléments de $\mathrm{Aut}(L/K)$ nous donnent $n$ homomorphismes $L/K \to E/K$. Comme $L/K$ possède au plus $n$ homomorphismes dans $E/K$, on obtient que tout homomorphisme $L/K \to E/K$ est un automorphisme de $L/K$. Donc $L/K$ est normale. ∎

**Définition.** *Si $L/K$ est une extension galoisienne, on pose* $\mathrm{Gal}(L/K) = \mathrm{Aut}(L/K)$ *et on l'appelle le groupe de Galois de $L$ sur $K$.*

**Exemples.** 1) Le corps $\mathbf{Q}[\sqrt{2}]$ est le corps de décomposition du polynôme $X^2 - 2 \in \mathbf{Q}[X]$. Tout automorphisme de $\mathbf{Q}[\sqrt{2}]$ permute les racines de $X^2 - 2$ et il est complètement déterminé par son action sur $\sqrt{2}$. Donc $\mathrm{Gal}(\mathbf{Q}[\sqrt{2}]/\mathbf{Q}) = \{\mathrm{id}, \sigma\}$, où $\sigma$ est l'unique automorphisme vérifiant $\sigma(\sqrt{2}) = -\sqrt{2}$.

2) Soit $L = \mathbf{Q}[\sqrt{2}, \sqrt{3}]$. Il est clair que $L$ est le corps de décomposition du polynôme $(X^2 - 2)(X^2 - 3)$, donc $L/\mathbf{Q}$ est une extension galoisienne. On veut

d'abord montrer que $[L:\mathbf{Q}]=4$. Les corps $\mathbf{Q}[\sqrt{2}]$ et $\mathbf{Q}[\sqrt{3}]$ sont des sous-extensions de $L/\mathbf{Q}$ ; cette information est récapitulée dans le diagramme suivant :




On a $[\mathbf{Q}[\sqrt{2}]:\mathbf{Q}]=[\mathbf{Q}[\sqrt{3}]:\mathbf{Q}]=2$. Il est facile de voir que $\sqrt{3}\notin\mathbf{Q}[\sqrt{2}]$ : en supposant que $\sqrt{3}$ s'écrit sous la forme $\sqrt{3}=a+b\sqrt{2}$ avec $a,b\in\mathbf{Q}$ on obtient que $3=a^2+2b^2+2ab\sqrt{2}$, d'où une contradiction. Donc $[L:\mathbf{Q}[\sqrt{2}]]=2$ et par le théorème de la base télescopique on trouve :

$$[L:\mathbf{Q}]=[L:\mathbf{Q}[\sqrt{2}]]\cdot[\mathbf{Q}[\sqrt{2}]:\mathbf{Q}]=4.$$

Le groupe $\mathrm{Gal}(L/\mathbf{Q})$ est d'ordre 4. Tout automorphisme $\sigma$ de $L$ est complètement déterminé par $\sigma(\sqrt{2})$ et $\sigma(\sqrt{3})$. En plus, $\sigma(\sqrt{2})=\pm\sqrt{2}$ et $\sigma(\sqrt{3})=\pm\sqrt{3}$. On en déduit que $\mathrm{Gal}(L/\mathbf{Q})=\{\mathrm{id},\sigma_1,\sigma_2,\sigma_3\}$, où

$$\begin{aligned}
\sigma_1(\sqrt{2})&=-\sqrt{2}, \quad \sigma_1(\sqrt{3})=\sqrt{3},\\
\sigma_2(\sqrt{2})&=\sqrt{2}, \quad \sigma_1(\sqrt{3})=-\sqrt{3},\\
\sigma_3(\sqrt{2})&=-\sqrt{2}, \quad \sigma_1(\sqrt{3})=-\sqrt{3}.
\end{aligned}$$

On vérifie facilement que $\sigma_3=\sigma_1\sigma_2$ et $\sigma_1^2=\sigma_2^2=\mathrm{id}$, d'où

$$\mathrm{Gal}(L/\mathbf{Q})\simeq\mathbf{Z}/2\mathbf{Z}\times\mathbf{Z}/2\mathbf{Z}.$$

Soit $\theta=\sqrt{2}+\sqrt{3}$. On voit facilement que les éléments $\theta$, $\sigma_1(\theta)$, $\sigma_2(\theta)$, $\sigma_3(\theta)$ sont 2 à 2 distincts. Donc $\theta$ est un élément primitif pour $L$ :

$$L=\mathbf{Q}[\theta].$$

## 6. Théorème d'indépendance des caractères

Soit $G$ un groupe et soit $L$ un corps quelconque. On appelle caractère de $G$ à valeurs dans $L^*$ tout morphisme de groupes

$$\chi : G\to L^*$$

à valeurs dans le groupe multiplicatif $L^*$ de $L$. L'objectif de cette section est de prouver le théorème suivant :

**Théorème 6.1** (Dedekind)**.** *Toute famille $\{\chi_1,\ldots,\chi_n\}$ de caractères distincts de $G$ est linéairement indépendante sur $L$ :*

$$\sum_{i=1}^{n}\lambda_i\chi_i=0 \quad\Rightarrow\quad \lambda_1=\lambda_2=\ldots=\lambda_n=0.$$

PREUVE. Nous allons montrer ce théorème par l'absurde. Supposons qu'une famille de caractères $\{\chi_1,\ldots,\chi_n\}$ est liée sur $L$. Parmi les relations linéaires entre $\chi_1,\ldots,\chi_n$ on choisit une relation de plus courte longueur. Quitte à renuméroter les caractères, on peut l'écrire sous la forme :

$$\sum_{i=1}^{r}\lambda_i\chi_i = 0, \qquad \lambda_1,\ldots,\lambda_r \neq 0.$$

Donc pour tout $g \in G$, on a :

$$\sum_{i=1}^{r}\lambda_i\chi_i(g) = 0. \tag{13}$$

Soit $h \in G$. En multipliant la relation précédente par $\chi_1(h)$, on obtient :

$$\sum_{i=1}^{r}\lambda_i\chi_1(h)\chi_i(g) = 0. \tag{14}$$

D'autre part, en remplaçant $g$ par $gh$ dans la formule (13) et en utilisant la formule $\chi_i(gh) = \chi_i(g)\chi_i(h)$, on trouve :

$$\sum_{i=1}^{r}\lambda_i\chi_i(h)\chi_i(g) = 0. \tag{15}$$

En soustrayant (14) de (15), on obtient la relation

$$\sum_{i=2}^{r}\lambda_i(\chi_i(h)-\chi_1(h))\chi_i(g) = 0, \qquad g \in G \tag{16}$$

qui est de longueur $< r$. Donc tous les coefficients $\lambda_i(\chi_i(h)-\chi_1(h))$ sont nuls. Comme $\lambda_i \neq 0$, on en déduit que pour tout $i$

$$\chi_i(h) = \chi_1(h), \qquad \forall h \in G.$$

Donc $\chi_1 = \chi_2 = \ldots = \chi_r$, ce qui contredit les hypothèses. ∎

**Corollaire 6.2.** *Soient $K$ et $L$ deux corps. Alors toute famille $\{\sigma_i\}_{i=1}^n$ d'homomorphismes distincts $\sigma_i : K \to L$ est linéairement indépendante sur $L$.*

PREUVE. La restriction $\chi_i = \sigma_i|_{K^*}$ de $\sigma_i$ sur $K^*$ est un caractère de $K^*$ à valeurs dans $L^*$. On pose $G = K^*$ et on applique le théorème de Dedekind à la famille $\{\chi_i,\ldots,\chi_n\}$. ∎

## 7. Théorème d'Artin

Soit $L$ un corps et soit $G$ un sous-groupe fini du groupe $\mathrm{Aut}(L)$. On note

$$L^G = \{x \in L \mid g(x) = x, \quad \forall g \in G\}$$

l'ensemble des éléments de $L$ fixés (ou invariants) par $G$. On voit facilement que $L^G$ est un sous-corps de $L$.

**Théorème 7.1** (Artin)**.** *L'extension $L/L^G$ est une extension galoisienne de degré $|G|$ et $\mathrm{Gal}(L/K) = G$.*

Preuve. Nous donnons une preuve qui met en valeur le théorème de l'indépendance des caractères. Soit $n = |G|$ et $m = [L : K]$. Nous allons prouver que $m$ est fini et $m = n$.

a) On montre par l'absurde que $m \geqslant n$. Supposons que $m < n$ et choisissons une base $\{x_1, \ldots, x_m\}$ de $L/L^G$. On note $\{\sigma_i\}_{i=1}^n$ les éléments de $G$. Soient

$$v_1 = \begin{pmatrix} \sigma_1(x_1) \\ \sigma_1(x_2) \\ \vdots \\ \sigma_1(x_m) \end{pmatrix}, \quad v_2 = \begin{pmatrix} \sigma_2(x_1) \\ \sigma_2(x_2) \\ \vdots \\ \sigma_2(x_m) \end{pmatrix} \cdots, v_n = \begin{pmatrix} \sigma_n(x_1) \\ \sigma_n(x_2) \\ \vdots \\ \sigma_n(x_m) \end{pmatrix}.$$

Chaque automorphisme $\sigma_i$ est $L^G$-linéaire ; il est, donc, complètement déterminé par le vecteur $v_i$.

Les vecteurs $\{v_i\}_{i=1}^n$ forment une famille à $n$ éléments dans $L^m$. Comme $m < n$, cette famille est lié, d'où on trouve qu'il existent $\lambda_1, \lambda_2, \ldots, \lambda_n$ non tous nuls et tels que

$$\sum_{i=1}^{n} \lambda_i v_i = 0.$$

On en déduit que

$$\sum_{i=1}^{n} \lambda_i \sigma_i = 0,$$

ce qui contredit le corollaire 6.2

b) On montre par l'absurde que $m \leqslant n$. Supposons que $m > n$. Soient

$$w_1 = \begin{pmatrix} \sigma_1(x_1) \\ \sigma_2(x_1) \\ \vdots \\ \sigma_n(x_1) \end{pmatrix}, \quad w_2 = \begin{pmatrix} \sigma_1(x_2) \\ \sigma_2(x_2) \\ \vdots \\ \sigma_n(x_2) \end{pmatrix} \cdots, w_m = \begin{pmatrix} \sigma_1(x_m) \\ \sigma_2(x_m) \\ \vdots \\ \sigma_n(x_m) \end{pmatrix}.$$

Les vecteurs $\{w_i\}_{i=1}^m$ forment une famille à $m$ éléments dans $L^n$. Comme $m > n$, cette famille est liée. Choisissons une relation linéaire de plus courte longueur entre ces vecteurs. Quitte à renuméroter les vecteurs, on peut l'écrire sous la forme

$$w_1 + \lambda_2 w_2 + \cdots \lambda_r w_r = 0, \qquad \lambda_2, \ldots, \lambda_r \neq 0 \tag{17}$$

(en divisant par un scalaire, on peut toujours supposer que $\lambda_1 = 1$). Plus explicitement, on a

$$\begin{pmatrix} \sigma_1(x_1) \\ \sigma_2(x_1) \\ \vdots \\ \sigma_n(x_1) \end{pmatrix} + \lambda_2 \begin{pmatrix} \sigma_1(x_2) \\ \sigma_2(x_2) \\ \vdots \\ \sigma_n(x_2) \end{pmatrix} + \cdots + \lambda_r \begin{pmatrix} \sigma_1(x_r) \\ \sigma_2(x_r) \\ \vdots \\ \sigma_n(x_r) \end{pmatrix} = 0, \qquad \lambda_2, \ldots, \lambda_r \neq 0. \tag{18}$$

Appliquons un élément quelconque $\tau \in G$ à cette relation. Comme

$$\tau \begin{pmatrix} \sigma_1(x_i) \\ \sigma_2(x_i) \\ \vdots \\ \sigma_n(x_i) \end{pmatrix} = \begin{pmatrix} \tau\sigma_1(x_i) \\ \tau\sigma_2(x_i) \\ \vdots \\ \tau\sigma_n(x_i) \end{pmatrix},$$

on voit que $\tau$ permute de la même manière les coordonnées des vecteurs $w_1, w_2, \ldots, w_r$. Donc

$$w_1 + \tau(\lambda_2)w_2 + \cdots \tau(\lambda_r)w_r = 0, \quad \forall \tau \in G. \tag{19}$$

En soustrayant (17) de (19), on obtient une relation de longueur $r-1$ :

$$\sum_{i=2}^{r} (\tau(\lambda_i) - \lambda_i)w_i = 0.$$

Donc $\tau(\lambda_i) = \lambda_i$ pour tous $\tau \in G$, d'où l'on tire que $\lambda_2, \ldots, \lambda_r \in L^G$. L'équation (18) donne :

$$\sigma_1(x_1 + \lambda_2 x_2 + \cdots \lambda_r x_r) = \sigma_1(x_1) + \lambda_2\sigma_1(x_2) + \cdots \lambda_r\sigma(x_r) = 0.$$

On en déduit que $x_1 + \lambda_2 x_2 + \cdots \lambda_r x_r = 0$ ce qui contredit à l'indépendance linéaire des éléments $\{x_i\}_{i=1}^m$ sur $L^G$. Donc $m \leqslant n$.

c) Les parties a) et b) montrent que $L/L^G$ est une extension finie de degré $[L : L^G] = n = |G|$. En plus, on a une inclusion naturelle $G \subseteq \mathrm{Aut}(L/L^G)$. Comme

$$\left|\mathrm{Aut}(L/L^G)\right| \leqslant [L : L^G]$$

on obtient que $G = \mathrm{Aut}(L/L^G)$. Maintenant, il découle du théorème 5.2 que $L/L^G$ est galoisienne et $G = \mathrm{Gal}(L/L^G)$. ∎

## 8. Correspondance de Galois

Soient $L/K$ une extension finie galoisienne et $G = \mathrm{Gal}(L/K)$. Soit $K \subset F \subset L$ une sous-extension de $L/K$. Le groupe de Galois $\mathrm{Gal}(L/F)$ est évidemment un sous-groupe de $G$. Réciproquement, à tout sous-groupe $H \leqslant G$ on peut associer le corps $L^H$ des éléments de $L$ fixés par $H$. Il est clair que $K \subset L^H$, donc $L^H$ est une sous-extension de $L/K$. Cela nous donne deux applications entre l'ensemble des sous-extensions $F$ de $L/K$ et l'ensemble des sous-groupes de $G$:

$$\{\text{sous-extensions de } L/K\} \underset{\mathscr{F}}{\overset{\mathscr{G}}{\rightleftarrows}} \{\text{sous-groupes de } G\}$$

$$F \xrightarrow{\quad\mathscr{G}\quad} \mathrm{Gal}(L/F)$$

$$L^H \xleftarrow{\quad\mathscr{F}\quad} H.$$

**Théorème 8.1** (Correspondance de Galois)**.**

i) *Les applications $\mathscr{G}$ et $\mathscr{F}$ sont des bijections réciproques. Pour toute sous-extension $F$ de $L/K$ on a :*

$$L^{\mathrm{Gal}(L/F)} = F.$$

ii) *Soit $F$ une sous-extension de $L/K$ et soit $H = \mathrm{Gal}(L/K)$. Alors $F/K$ est galoisienne si et seulement si $H$ est un sous-groupe distingué dans $G$. Alors*

$$\mathrm{Gal}(F/K) \simeq G/H.$$

Preuve. i) Soit $H \leqslant G$. Alors

$$\mathscr{G} \circ \mathscr{F}(H) = \mathrm{Gal}(L/L^H) = H$$

par le théorème d'Artin. Donc $\mathscr{F} \circ \mathscr{G} = \mathrm{id}$.

Soit maintenant $F$ une sous-extension de $L/K$. Alors

$$\mathscr{F} \circ \mathscr{G}(F) = L^{\mathrm{Gal}(L/F)}.$$

Nous allons montrer que $L^{\mathrm{Gal}(L/F)} = F$. L'inclusion $F \subseteq L^{\mathrm{Gal}(L/F)}$ est claire. En utilisant le théorème d'Artin, on en déduit que

$$|\mathrm{Gal}(L/F)| = [L : L^{\mathrm{Gal}(L/F)}] \leqslant [L : F] = |\mathrm{Gal}(L/F)|.$$

Donc $[L : L^{\mathrm{Gal}(L/F)}] = [L : F]$ et $F = L^{\mathrm{Gal}(L/F)}$.

ii) a) $\boxed{\Rightarrow}$ Soient $F/K$ une sous-extension de $L/K$ et $H = \mathrm{Gal}(L/F)$. Si $F/K$ est galoisienne, alors elle est normale et pour tout $g \in G$ on a $g(F) = F$. Soient $h \in H$ et $x \in F$. Alors $hg(x) = g(x)$ et

$$g^{-1}hg(x) = g^{-1}(hg(x)) = g^{-1}g(x) = x.$$

On en déduit que l'automorphisme $g^{-1}hg$ agit trivialement sur $F$. Donc $g^{-1}hg \in H$ pour tous $g \in G$ et $h \in H$, ce qui signifie que $H \trianglelefteq G$.

b) $\boxed{\Leftarrow}$ Soient $H \trianglelefteq G$ et $F = L^H$. Par le théorème 3.6, $F/K$ est séparable. On va montrer que $F/K$ est normale. Soit $M$ un corps contenant $L$ et soit $\sigma : F/K \to M/K$ un homomorphisme sur $K$. Par le théorème de prolongement des homomorphismes il existent une extension $E/M$ et un homomorphisme $g : L/K \to E/K$ tel que $g|_F = \sigma$. Comme $L/K$ est normale, $g(L) = L$, donc $g \in G$. Soit $h \in H$. Comme $Hg = gH$, il existe $h' \in H$ tel que $hg = gh'$. Alors

$$h(g(x)) = g(h'(x)) = g(x).$$

On en déduit que $\sigma(x) = g(x) \in L^H = F$ pour tout $x \in F$. Donc $F/K$ est normale.

c) Soit $g \in G$ et soit $\pi(g)$ la restriction de $g$ sur $F$. Par la normalité de $F/K$ on a $g(F) = F$, donc $\pi(g) \in \mathrm{Gal}(F/K)$. On voit facilement que l'application

$$\pi : G \to \mathrm{Gal}(F/K)$$

ainsi définie est un morphisme de groupes. En outre

$$\ker(\pi) = \{g \in G \mid g|_F = \mathrm{id}\} = H.$$

Donc $\mathrm{Gal}(F/K) \simeq G/H$. ∎

**Remarque 8.2.** *La correspondance de Galois établit une bijection entre les sous-groupes de $G$ et les sous-extensions de $L/K$. Si $H_1 \leqslant H_2$, alors $L^{H_2} \subseteq L^{H_1}$ et*

$$[L^{H_1} : L^{H_2}] = [H_2 : H_1].$$

**Définition.** *Soient $L$ et $F$ deux corps contenus dans $E$. On appelle compositum de $L$ et $F$ et on note $LF$ le plus petit sous-corps de $E$ contenant $L$ et $F$.*

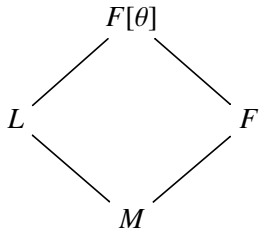
**Exemple.** Soit $L/K$ une extension simple. Alors $L = K[\theta]$, où $\theta$ est un élément primitif pour $L$. Alors pour toute extension $F$ de $K$ le compositum $LF$ est la plus petite extension de $F$ contenant $\theta$, d'où

$$LF = F[\theta].$$

**Lemme 8.3.** *Soient $L/M$ et $F/M$ deux extensions finies d'un corps $M$ telles que $L \cap F = M$. Si $L/M$ est galoisienne, alors $LF/F$ l'est aussi et*

$$[LF : F] = [L : M].$$

Preuve. a) Comme l'extension $L/M$ est galoisienne, elle est séparable, et d'après le théorème de l'élément primitif il existe un élément $\theta \in L$ tel que $L = M[\theta]$. Alors $LF = F[\theta]$ et on a un diagramme




où $LF = F[\theta]$. Nous voulons prouver que $[F[\theta] : F] = [L : M]$. Soit $P \in M[X]$ le polynôme minimal de $\theta$ sur $M$ et soit $Q \in F[X]$ le polynôme minimal de $\theta$ sur $F$. Comme $M \subseteq F$, on a :

$$Q \text{ divise } P \text{ dans } F[X].$$

D'autre part, comme $L/M$ est normale, par le théorème 5.1 $P$ se décompose dans $L[X]$ en produit de facteurs linéaires :

$$P(X) = \prod_{i=1}^{n} (X - \theta_i), \qquad \theta_i \in L, \quad n = [L : K].$$

Donc $Q(X) = \prod_{i \in I} (X - \theta_i)$, avec $I \subseteq \{1, 2, \ldots, n\}$, d'où $Q \in L[X]$. On en déduit que $Q \in F[X] \cap L[X] = M[X]$. Donc $Q(X) = P(X)$ et

$$[F[\theta] : F] = \deg(Q) = \deg(P) = [L : M].$$

b) Comme $Q = P$ et $P$ est séparable, l'extension $F[\theta]/F$ est séparable. En outre, tout $F$-morphisme $\sigma : F[\theta]/F \to E/F$ est complètement déterminé par $\sigma(\theta)$. Comme $\sigma(\theta) \in L$, on en déduit que $\sigma(F[\theta]) \subseteq F[\theta]$. Donc $F[\theta]/F$ est normale. Le lemme est démontré. ∎

**Théorème 8.4.** *Soit $L/K$ une extension galoisienne. Alors pour toute extension finie $F/K$ l'extension $LF/F$ est galoisienne et les groupes de Galois* $\mathrm{Gal}(LF/F)$ *et* $\mathrm{Gal}(L/F \cap L)$ *sont isomorphes. En particulier,* $\mathrm{Gal}(LF/F)$ *est isomorphe à un sous-groupe de* $\mathrm{Gal}(L/K)$.

PREUVE. En appliquant le lemme 8.3 à $M = F \cap L$, on obtient que $LF/F$ est galoisienne.

Soit $g \in \mathrm{Gal}(LF/F)$. On note $r(g) = g|_L$ la restriction de $g$ sur $L$. Il est clair que $g$ agit trivialement sur $F \cap L$. Donc $r(g)$ est un $F \cap L$-morphisme à valeurs dans $LF$ :

$$r(g) : L/(F \cap L) \to LF/(F \cap L).$$

Comme $K \subset F \cap L$ et $L/K$ est galoisienne, l'extension $L/(F \cap L)$ est galoisienne. En particulier, elle est normale, d'où on tire que $r(g) \in \mathrm{Gal}(L/F \cap L)$. Donc nous avons construit une application :

$$r : \mathrm{Gal}(LF/F) \to \mathrm{Gal}(L/F \cap L).$$

Il est clair que $r$ est un morphisme de groupes. Si $g \in \ker(r)$, alors $g|_L = \mathrm{id}_L$, d'où $g(\theta) = \theta$ et $g|_{F[\theta]} = \mathrm{id}_{F[\theta]}$. On en déduit que $\ker(r) = \mathrm{id}$. Donc $r$ est un monomorphisme. D'autre part, d'après le lemme 8.3 on a :

$$|\mathrm{Gal}(LF/F)| = [LF : F] = [L : (L \cap F)] = |\mathrm{Gal}(L/F)|.$$

■

## 9. Exemple du polynôme $X^5 - 10X + 5$

Soit $f(X) \in K[X]$ un polynôme séparable. On fixe un corps de décomposition $L/K$ de $f(X)$ et l'on note $\alpha_1, \ldots, \alpha_n$ ses racines dans $L$ :

$$L = K[\alpha_1, \alpha_2, \ldots, \alpha_n].$$

Le groupe symétrique de l'ensemble des racines est isomorphe à$S_n$.

Les automorphismes $g \in \mathrm{Gal}(L/K)$ permutent les racines de $f(X)$. Chaque automorphisme est complètement déterminé par sont action sur les racines, donc par la permutation

$$\begin{pmatrix} \alpha_1 & \alpha_2 & \ldots & \alpha_n \\ g(\alpha_1) & g(\alpha_2) & \ldots & g(\alpha_n) \end{pmatrix}.$$

On obtient un monomorphisme de groupes :

$$\mathrm{Gal}(L/K) \to S_n.$$

**Théorème 9.1.** *Soit $L$ un corps de décomposition du polynôme $P(X) = X^5 - 10X + 5$ sur $\mathbf{Q}$. Alors*

$$\mathrm{Gal}(L/\mathbf{Q}) \simeq S_5.$$

PREUVE. a) Soit $G = \mathrm{Gal}(L/\mathbf{Q})$. On considère $L$ comme un sous-corps du corps $\mathbf{C}$ des nombres complexes. Le polynôme $P(X)$ est irréductible sur $\mathbf{Q}$ par le critère d'Eisenstein (on pose $p = 5$). Le corps de rupture de $P(X)$ est de degré 5 sur $\mathbf{Q}$, d'où on trouve que 5 divise $|G| = [L : \mathbf{Q}]$. Comme $|S_5| = 5! = 2^3 \cdot 3 \cdot 5$ et $\mathrm{Gal}(L/\mathbf{Q}) \hookrightarrow S_5$, les 5-Sylow de $G$ sont d'ordre 5. Ils sont donc cycliques. On en déduit que $G$ (ou plutôt son image dans $S_5$) contient un 5-cycle.

b) Étudions la variation de la fonction réelle $P : \mathbf{R} \to \mathbf{R}$. Comme $P'(X) = 5X^4 - 10$, elle admet des extrema en $-\sqrt[4]{2}$ et en $\sqrt[4]{2}$ avec $P(-\sqrt[4]{2}) > 0$ et $P(\sqrt[4]{2}) < 0$. Donc, $P(X)$ possède exactement 3 racines réelles qu'on note $\alpha_3, \alpha_4$ et $\alpha_5$. Soient $\alpha_1$ et $\alpha_2$

les racines complexes de $P$. La conjugaison complexe fournit un automorphisme de $L/\mathbf{Q}$ qui permute $\alpha_1$ et $\alpha_2$.

Le théorème découle maintenant du lemme suivant :

**Lemme 9.2.** *Le groupe $S_n$ est engendré par $\sigma = (12)$ et $\tau = (12\cdots n)$.*

Preuve du lemme. Un petit calcul montre que

$$\tau^k \sigma \tau^{-k} = (k+1, k+2).$$

Comme les permutations $(1,2),(2,3),\ldots,(n-1,n)$ engendrent $S_n$, le lemme est démontré. ∎

∎

## 10. Extensions cyclotomiques

Dans cette section, on suppose que $\mathrm{char}(K) = 0$. Pour tout $n \geqslant 1$ on appelle corps cyclotomique et l'on note $K_n$ un corps de décomposition du polynôme $X^n - 1$. Il est clair que $K_1 = K_2 = K$.

Les racines de $X^n - 1$ sont les racines $n$-ièmes de l'unité :

$$\mu_n = \{\zeta \mid \zeta^n = 1\}.$$

On sait que $\mu_n$ est un groupe cyclique d'ordre $n$ et un appelle racine primitive d'ordre $n$ tout générateur de $\mu_n$. On fixe une racine primitive $\zeta_n \in \mu_n$. Une racine $n$-ième de l'unité $\zeta = \zeta_n^a$ est primitive si et seulement si $\mathrm{pgcd}(a,n) = 1$. On note $\mu_n^*$ l'ensemble des racines primitives d'ordre $n$. Alors $|\mu_n^*| = \varphi(n)$, où $\varphi$ est l'indicatrice d'Euler. On a :

$$K_n = K[\zeta_n].$$

L'extension $K_n/K$ est galoisienne et tout automorphisme de $K_n/K$ est complètement déterminé par son action sur $\zeta_n$. Si $g \in \mathrm{Gal}(K_n/K)$, alors $g(\zeta)$ est une racine primitive d'ordre $n$ de l'unité et l'on a :

$$g(\zeta_n) = \zeta_n^a, \qquad \mathrm{pgcd}(a,n) = 1. \tag{20}$$

L'entier $a$ ainsi défini est unique modulo $n$ et l'on note $\chi_n(g)$ sa classe de congruence modulo $n$ :

$$\chi_n(g) = a \mod n \in (\mathbf{Z}/n\mathbf{Z})^*.$$

Donc, on a défini une application

$$\chi_n : \mathrm{Gal}(K_n/K) \to (\mathbf{Z}/n\mathbf{Z})^*.$$

On écrit (20) sous la forme :

$$g(\zeta_n) = \zeta_n^{\chi_n(g)}.$$

**Théorème 10.1.** *L'application*

$$\chi_n : \mathrm{Gal}(K_n/K) \to (\mathbf{Z}/n\mathbf{Z})^*$$

*est un monomorphisme qui ne dépend pas du choix de $\zeta_n$.*

Proof. a) Comme tout automorphisme de $K_n/K$ est complètement déterminé par son action sur $\zeta_n$, l'application $\chi_n$ est injective.

b) Pour tous $g_1, g_2 \in \mathrm{Gal}(K_n/K)$ on a :

$$(g_1g_2)(\zeta_n) = g_1(g_2(\zeta)) = g_1(\zeta_n^{\chi_n(g_2)}) = g_1(\zeta_n)^{\chi_n(g_2)} = \zeta_n^{\chi_n(g_1)\chi_n(g_2)}.$$

Comme, d'autre part, $(g_1g_2)(\zeta_n) = \zeta_n^{\chi_n(g_1g_2)}$, on en déduit que

$$\chi_n(g_1g_2) = \chi_n(g_1)\chi_n(g_2).$$

Donc, $\chi_n$ est un morphisme de groupes.

c) Soit $\zeta = \zeta_n^c$ une autre racine $n$-ième primitive, pgcd (c,n)=1. Alors :

$$g(\zeta) = g(\zeta_n^c) = g(\zeta_n)^c = \zeta_n^{\chi_n(g)\cdot c} = \zeta^{\chi_n(g)}.$$

On en déduit que la $\chi_n$ ne dépend pas du choix de la racine primitive. ∎

**Exercice 12.** Montrer que $\mathrm{Gal}(\mathbf{Q}(\mu_n)/\mathbf{Q}) \simeq (\mathbf{Z}/n\mathbf{Z})^*$. Remarque : le produit

$$\Phi_n(X) = \prod_{\zeta \in \mu_n^*} (X - \zeta)$$

est un polynôme de degré $\varphi(n)$ à coefficients dans $\mathbf{Z}$. En outre, il est irréductible sur $\mathbf{Q}$.

## 11. Extensions de Kummer

Dans cette section, on suppose que $\mathrm{char}(K) = 0$.

**Définition.** *On dit qu'une extension galoisienne $L/K$ est cyclique si* $\mathrm{Gal}(L/K)$ *est cyclique.*

Supposons que $K$ contient une racine primitive d'ordre $n$ de l'unité (et donc contient le groupe $\mu_n$ de toutes les racines $n$-ièmes de l'unité). Sous cette condition, nous pouvons explicitement décrire les extensions cycliques d'ordre $n$ de $K$.

**Théorème 11.1.** *Soit $K$ un corps de caractéristique* 0 *contenant une racine primitive de l'unité d'ordre $n$.*

*i) Soit $a \in K$ et soit $\alpha$ une racine de $X^n - a$. Alors $K[\alpha]/K$ est une extension cyclique de degré $d \mid n$.*

*ii) Si $L/K$ est cyclique d'ordre $n$, alors il existe un élément $a \in K$ tel que $L = K[\alpha]$ avec $\alpha^n - a = 0$.*

On appelle extension de Kummer une extension $L/K$ engendrée sur $K$ par une racine d'un polynôme de la forme $X^n - a \in K[X]$. Le ii) de notre théorème dit que si $K$ contient le groupe $\mu_n$, alors toute extension cyclique d'ordre $n$ est de Kummer.

Preuve. i) On fixe une racine primitive $n$-ième de l'unité $\zeta_n \in K$. Soit $a \in K$ et soit $K[\alpha]/K$ l'extension engendrée par une racine $\alpha$ du polynôme $X^n - a$. Alors :

$$X^n - a = \prod_{i=0}^{n-1} (X - \zeta_n\alpha).$$

Donc $K[\alpha]$ est un corps de décomposition de $X^n - a$. En particulier, l'extension $K[\alpha]/K$ est galoisienne.

Tout automorphisme $g \in \mathrm{Gal}(K[\alpha]/K)$ est complètement déterminé par son action sur $\alpha$. Comme l'action de $g$ permute les racines de $X^n - a$, il existe $\psi(g) \in \mu_n$ tel que

$$g(\alpha) = \psi(g)\alpha.$$

On a donc une application injective bien définie :

$$\psi : \mathrm{Gal}(L/K) \to \mu_n,$$
$$\psi(g) = g(\alpha)/\alpha.$$

Pour tous $g_1, g_2 \in \mathrm{Gal}(K[\alpha]/K)$ on a :

$$g_1 g_2(\alpha) = g_1(g_2(\alpha)) = g_1(\psi(g_2)\alpha) = \psi(g_2)g_1(\alpha) = \psi(g_2)\psi(g_1)\alpha.$$

Comme, d'autre part, $g_1 g_2(\alpha) = \psi(g_1 g_2)\alpha$, on en déduit que

$$\psi(g_1 g_2) = \psi(g_2)\psi(g_1).$$

Donc, $\psi$ est un monomorphisme.

Soit $d = [K[\alpha] : K]$. Comme le groupe de Galois $\mathrm{Gal}(K[\alpha]/K)$ s'injecte dans le groupe cyclique $\mu_n$, on en déduit que

$$d = |\mathrm{Gal}(K[\alpha]/K)| \text{ divise } n = |\mu_n|.$$

Le i) du théorème est démontré.

ii) Supposons que $L/K$ est cyclique de degré $n$. On applique le théorème d'indépendance linéaire des caractères (ou plutôt le corollaire 6.2) aux automorphismes $\{\sigma^i\}_{i=0}^{n-1}$. D'après ce théorème, l'application

$$\sum_{i=0}^{n-1} \zeta_n^{-i}\sigma^i$$

n'est pas nulle. Donc, il existe un élément $\theta \in L$ tel que

$$\alpha = \sum_{i=0}^{n-1} \zeta_n^{-i}\sigma^i(\theta) \neq 0.$$

Alors :

$$\sigma(\alpha) = \sum_{i=0}^{n-1} \zeta_n^{-i}\sigma^{i+1}(\theta) = \sum_{i=0}^{n-1} \zeta_n^{-i-1}\sigma^{i+1}(\theta) = \zeta_n\alpha.$$

Par récurrence, on en déduit que

$$\sigma^k(\alpha) = \zeta_n^k\alpha, \qquad 0 \leqslant k \leqslant n-1.$$

Donc $\alpha, \zeta_n\alpha, \cdots, \zeta_n^{n-1}\alpha$ sont les racines du polynôme minimal $P(X)$ de $\alpha$ sur $K$, d'où

$$P(X) = \prod (X - \sigma^i(\alpha)) = X^n - \alpha^n, \qquad a = \alpha^n \in K.$$

En outre, $[K[\alpha] : K] = n$, d'où $L = K[\alpha]$. Le théorème est démontré. ∎

**Remarque 11.2.** On peut préciser la partie i) du théorème : si $K$ ne contient aucune racine de $a$ d'ordre $m > 1$ divisant $n$, alors $[K[\alpha] : K] = n$.

## 12. Equations résolubles par radicaux

Dans cette section, on suppose que tous les corps sont de caractéristique nulle.

**Définition.** *On dit qu'une extension $M/F$ est radicale élémentaire si $M = F[\alpha]$ où $\alpha$ est une racine d'un polynôme de la forme $X^n - a \in F[X]$. On dit que $M/F$ est radicale, s'il existe une tour*

$$F = M_0 \subset M_1 \subset M_2 \subset \cdots \subset M_k = M,$$

*où les extensions $M_i/M_{i-1}$ sont radicales élémentaires.*

Soit $f(X) \in K[X]$ un polynôme de degré $\geqslant 2$. On note $L$ un corps de décomposition de $f$.

**Définition.** *On dit que l'équation $f(X) = 0$ est résoluble par radicaux s'il existe une extension radicale $M/K$ contenant $L$.*

Donc, dire qu'une équation est résoluble par radicaux revient à dire que toutes ces racines s'expriment à l'aide des fonctions rationnelles et d'extractions successives des racines à partir d'éléments de $K$.

Les équations de degré $\leqslant 4$ sont résolubles par radicaux. Il existent même des formules générales pour la résolution des équations de degré $\leqslant 4$ (Tartaglia, Cardano, Ferrari).

**Théorème 12.1** (Galois)**.** *Soit $K$ un corps et soit $f(X) \in K[X]$. L'équation $f(X) = 0$ est résoluble par radicaux si et seulement si $Gal(L/K)$ est résoluble.*

**Exemple.** *L'équation $X^5 - 10X + 5 = 0$ n'est pas résoluble par radicaux sur* $\mathbf{Q}$.

**Corollaire 12.2** (théorème d'Abel)**.** *Il n'existe pas de formule générale pour la résolution des équations de degré $\geqslant 5$ par radicaux.*

Preuve du théorème de Galois. i) On note $G = \mathrm{Gal}(L/K)$ et $n = |G|$. Supposons que $G$ est résoluble et montrons que $L/K$ est contenue dans une extension radicale.

Soient $F = K(\zeta_n)$ et $E = FL$. Alors $E$ est le corps de décomposition de $f$ sur $F$ et par le théorème 8.4 le groupe de Galois $H = \mathrm{Gal}(E/F)$ est isomorphe à un sous-groupe de $G$. En particulier, $H$ est résoluble et d'après le théorème 3.8, il existe une chaîne normale

$$H = H_0 \trianglelefteq H_1 \trianglelefteq H_2 \trianglelefteq \cdots \trianglelefteq H_k = \{e\}$$

telle que tous les groupes quotients $H_i/H_{i+1}$ sont cycliques. On pose :

$$E_i = E^{H_i}.$$

Alors $\mathrm{Gal}(E_{i+1}/E_i) \simeq H_i/H_{i+1}$ est un groupe cyclique d'ordre divisant $m$. Comme $\zeta_n \in F$, le théorème 11.1 s'applique, d'où l'on déduit que l'extension $E_{i+1}/E_i$ est élémentaire radicale. Donc $E/F$ est radicale. Comme $F/K$ est clairement radicale, on conclut que $E/K$ est radicale.

ii) Supposons que le corps de décomposition $L$ de $f$ est contenu dans une extension radicale $M/K$. Nous utiliserons le lemme suivant.

**Lemme 12.3.** *Il existe une extension galoisienne radicale $\widetilde{M}/K$ contenant $M$.*

Preuve du lemme. On montre le lemme par récurrence sur le nombre $k$ des étages dans la tour

$$K = M_0 \subset M_1 \subset M_2 \subset \cdots \subset M_k = M.$$

Le cas $k = 0$ est évident. Supposons que la propriété est vraie pour les tours radicales de longueur $k-1$. Alors il existe une extension radicale galoisienne $\widetilde{M}_{k-1}/K$ telle que $M_{k-1} \subset \widetilde{M}_{k-1}$. Soit $M = M_{k-1}[\alpha]$, où $\alpha$ est une racine d'une équation de la forme $X^d - a = 0$ avec $a \in M_{k-1}$. On note $P(X) \in K[X]$ le polynôme minimal de $a$ sur $K$ et l'on pose $f(X) = P(X^d)$. Soit $\widetilde{M}$ le corps de décomposition de $f(X)$ sur $\widetilde{M}_{k-1}$. Il est facile de voir que $\widetilde{M}/K$ est galoisienne. D'autre part, $\widetilde{M}$ est engendré sur $\widetilde{M}_{k-1}$ par les racines des polynômes

$$X^d - a_i, \qquad 1 \leqslant i \leqslant \deg(P),$$

où $a_i$ sont les conjugués de $a_i$. On en déduit que $\widetilde{M}/\widetilde{M}_{k-1}$ est radicale. ∎

Revenons à la preuve du théorème. Soit $\widetilde{M}/K$ une extension galoisienne radicale contenant $M$. On pose $m = [\widetilde{M} : K]$. Soient $F = K[\zeta_m]$ et $E = \widetilde{M}[\zeta_m]$. Les extensions $E/K$ et $F/K$ sont galoisiennes.

Comme $\widetilde{M}/K$ est radicale, il existe une tour d'extensions radicales élémentaires :

$$K = \widetilde{M}_0 \subset \widetilde{M}_1 \subset \widetilde{M}_2 \subset \cdots \subset \widetilde{M}_k = \widetilde{M}.$$

Pour tout $i$, on pose $E_i = \widetilde{M}_i[\zeta_m]$. Alors dans la tour

$$F = E_0 \subset E_1 \subset E_2 \subset \cdots \subset E_k = E$$

les extensions $E_{i+1}/E_i$ sont radicales élémentaires d'ordre divisant $m$. Soit $H = \mathrm{Gal}(E/F)$ et soit $H_i = \mathrm{Gal}(E/E_i)$ pour tout $i$. Comme $\zeta_m \in F$, les extensions $E_{i+1}/E_i$ sont galoisiennes cycliques. On en déduit que $H_{i+1} \trianglelefteq H_i$ et par le théorème 11.1, le groupe

$$H_i/H_{i+1} \simeq \mathrm{Gal}(E_{i+1}/E_i)$$

est cyclique. Donc, d'après le théorème 3.8, $\mathrm{Gal}(E/F)$ est résoluble. Comme le quotient

$$\mathrm{Gal}(E/K)/\mathrm{Gal}(E/F) \simeq \mathrm{Gal}(F/K)$$

est résoluble (et même abélien), le groupe $\mathrm{Gal}(E/K)$ est résoluble par la proposition 3.2. Comme le corps de décomposition $L$ de $f$ est une sous-extension de $E/K$, le groupe de Galois $G = \mathrm{Gal}(L/K)$ est un quotient de $\mathrm{Gal}(E/K)$. Donc, il est résoluble et le théorème est démontré. ∎