Théorie de Galois et représentations des groupes finis

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

Théorie de Galois

1. Lemme de Zorn

Le but de cette section est de rappeler l'énoncé du lemme de Zorn et d'en donner quelques applications. Soit X un ensemble.

Définition. *On appelle ordre sur X une relation $\leqslant$ sur X vérifiant les propriétés suivantes :*

- *(Réflexivité). Pour tout $x \in X$, $x \leqslant x$.*
- *(Transitivité). Pour tous $x, y, z \in X$, si $x \leqslant y$ et $y \leqslant z$, alors $x \leqslant z$.*
- *(Antisymétrie) Si $x \leqslant y$ et $y \leqslant x$, alors $x = y$.*

Un ordre sur X est dit total si deux éléments de X sont toujours comparables :

$$\forall x, y \in X, \quad x \leqslant y \text{ ou } y \leqslant x.$$

Un ensemble ordonné est un ensemble muni d'une relation d'ordre.

Exemples. *1) L'ensemble $\mathbf{R}$ muni de l'ordre usuel $\leqslant$ est totalement ordonné.*
2) Soit $\mathbf{P}(E)$ l'ensemble des parties d'un ensemble E. La relation d'inclusion $A \subseteq B$ est un relation d'ordre sur $\mathbf{P}(E)$. Cependant cet ordre n'est pas total si X contient au moins deux éléments.

Soit X un ensemble ordonné. On dit que $a \in X$ est un *élément maximal* de X s'il n'existe aucun autre élément de X qui soit supérieur à a :

$$\forall x \in X, \quad \text{si } a \leqslant x, \text{ alors } a = x.$$

Soit A une partie non vide de X. On dit que $m \in X$ est un *majorant* de A si

$$\forall x \in A, \quad x \leqslant m.$$

Définition. *i) On dit qu'une partie C d'un ensemble ordonné $(X, \leqslant)$ est une chaine, si $\leqslant$ définit un ordre total sur C.*
ii) On dit que X est inductif si toute chaine dans X admet un majorant.

Exemples. *1) Soit X un ensemble ordonné fini. Alors X admet un élément maximal.*
2) Soit $\mathbf{N}_{\geqslant 2}$ l'ensemble des entiers $\geqslant 2$. On définit une relation d'ordre sur $\mathbf{N}_{\geqslant 2}$ en posant :

$$x \leqslant y, \quad si\ y \mid x.$$

Les éléments maximaux dans $\mathbf{N}_{\geqslant 2}$ sont les nombres premiers. Il est facile de voir que $(\mathbf{N}_{\geqslant 2}, \leqslant)$ est inductif.

Lemme 1.1 (Lemme de Zorn)**.** *Tout ensemble inductif admet au moins un élément maximal.*

La preuve du lemme de Zorn utilise l'axiome du choix :

Axiome du choix. *Soit $(X_i)_{i\in I}$ une famille d'ensembles indexée par un ensemble I. Alors il existe une application $f : I \to \bigcup_{i\in I} X_i$ telle que*

$$\forall i \in I, \quad f(i) \in X_i.$$

On dit que f est une fonction de choix.

De façon équivalente, l'axiome du choix affirme que le produit cartésien $\prod_{i\in I} X_i$ d'une famille d'ensembles non vides est non vide.

Rappelons le théorème suivant qui se démontre à l'aide du lemme de Zorn :

Théorème 1.2. *Soit A un anneau commutatif. Alors tout idéal propre de A est inclus dans un idéal maximal de A.*

Preuve. Soit I un idéal propre de A. On note X l'ensemble des idéaux propres J de A tels que $I \subseteq J$. La relation d'inclusion définit un ordre sur X. Les éléments maximaux de X, s'ils existent, sont les idéaux maximaux de A contenant I.

Soit $C \subseteq X$ une chaine. On va montrer que l'union $\mathfrak{a} = \bigcup_{J\in C} J$ est un idéal propre de A.

Soient $x_1, x_2 \in \mathfrak{a}$. Alors il existe des idéaux $J_1, J_2 \in C$ tels que $x_1 \in J_1$ et $x_2 \in J_2$. Comme C est une chaine, $J_1 \subseteq J_2$ ou $J_2 \subseteq J_1$. Pour fixer les idées, supposons que $J_1 \subseteq J_2$. Alors $x_1, x_2 \in J_2$, d'où $x_1 \pm x_2 \in J_2 \subseteq \mathfrak{a}$. En outre, pour tout $a \in A$ on a $ax_1 \in J_1 \subseteq \mathfrak{a}$. Donc $\mathfrak{a}$ est un idéal de A.

Pour montrer que $\mathfrak{a}$ est propre, on remarque que tout $J \in C$ est un idéal propre de A, d'où $1 \notin J$. Donc $1 \notin \mathfrak{a} = \bigcup_{J\in C} J$.

Il est clair que l'idéal $\mathfrak{a}$ est un majorant de C, d'où on déduit que l'ensemble X est inductif. En appliquant le lemme de Zorn on trouve que X contient un élément maximal $\mathfrak{m}$ qui est, par définition, un idéal maximal de A. ∎

Exercice 1. *Montrer que si X et Y sont deux ensembles, alors il y en a au moins un qui peut s'injecter dans l'autre.*

Exercice 2. *Montrer que tout espace vectoriel sur un corps admet une base.*

2. 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 ψ 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 ψ 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 2.1 (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. Dans 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 2.2. *Toute extension finie est algébrique.*

Preuve. Soit L/K une extension finie et soit $n = [L : K]$. Soit α 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 2.3. *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 α 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 α. On note $K[\alpha]$ la plus petite sous-extension de L/K contenant α. 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 2.4. *Soit $\alpha \in L$ un élément algébrique et soit P le polynôme minimal de α. 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 φ est un morphisme d'anneaux.

ii) D'après le théorème 2.3, $\ker(\varphi) = I = (P)$. Donc le théorème de factorisation induit un isomorphisme :

$$K[X]/(P) \xrightarrow{\overline{\varphi}} \mathrm{Im}(\varphi), \tag{1}$$

où $\mathrm{Im}(\varphi)$ désigne l'image de φ. 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 (1), 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 α 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 2.5. *Si α 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 2.4, 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 algébrique L/K est simple (ou monogène) s'il existe un élément $\alpha \in L$ tel que $L = K[\alpha]$. Alors on dit que α 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 2.6. *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 2.4, tout corps de rupture de P est isomorphe à L, d'où l'unicité à isomorphisme près. ∎

3. Corps algébriquement clos

Soit K un corps.

Définition. *On dit que K est algébriquement clos si tout polynôme $f(X) \in K[X]$ est scindé sur K :*

$$f(X) = a(X-\alpha_1)\cdot(X-\alpha_2)\cdots(X-\alpha_n), \qquad \alpha_i \in K, \quad 1 \leqslant i \leqslant n.$$

Proposition 3.1. *Les assertions suivantes sont équivalentes :*

i) K est algébriquement clos ;

ii) Tout polynôme non constant à coefficients dans K admet une racine dans K ;

iii) K n'a pas d'extension algébrique non triviale.

PREUVE. *i*) $\Rightarrow$ *ii*). C'est clair.

ii) $\Rightarrow$ *iii*). Soit L/K une extension algébrique. Soit α un élément quelconque de L et soit $P(X) \in K[X]$ son polynôme minimal. Alors $P(X)$ est irréductible. Comme il admet une racine dans K, il est de degré un. Donc $\alpha \in K$.

iii) $\Rightarrow$ *i*). Supposons qu'il existe un polynôme non scindé $f \in K[X]$. En décomposant f en produit de polynômes irréductibles, on trouve qu'il existe un polynôme irréductible $P(X) \in K[X]$ de degré $n \geqslant 2$. Le corps de rupture de $P(X)$ est une extension algébrique de degré n sur K. Or K n'a pas d'extension algébrique non triviale, d'où une contradiction. ∎

Le théorème de d'Alembert–Gauss affirme que le corps des nombres complexes $\mathbf{C}$ est algébriquement clos.

4. 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. 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 σ.

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 σ 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 α 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 α. On note

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

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

Théorème 4.1. *Soit E/M une extension finie simple. Alors :*

i) *Le nombre de prolongements*

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

de σ 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 σ admet un prolongement $\widehat{\sigma} : F \to E$.*

PREUVE. i) Soit $\widehat{\sigma} : F \to E$ un prolongement de σ. Comme α 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 :

$$\begin{gathered} \{\text{prolongements de } \sigma\} \to \{\text{racines de } P^\sigma(X) \text{ dans } E\}, \\ \widehat{\sigma} \mapsto \widehat{\sigma}(\alpha). \end{gathered} \tag{2}$$

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 (2) 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 4.2 (prolongement des homomorphismes)**.** *Soit $\sigma : L \to M$ 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 σ à F à valeurs dans E.*

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

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

de σ 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 4.1, il existe une extension E'/M telle que σ possède un prolongement $\sigma' : L[\alpha] \to E'$. On remarque que $[F : L[\alpha]] < n$. Par l'hypothèse de récurrence, il existe donc une extension E/E' avec un prolongement $\widehat{\sigma} : F \to E$ de σ'.

ii) On note $P(X)$ le polynôme minimal de α 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 σ à $L[\alpha]$. D'après le théorème 4.1, 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 σ 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. ∎

Nous allons maintenant étendre la théorie précédente aux extensions infinies.

Théorème 4.3. *Soit $\sigma : L \to M$ un morphisme de L dans un corps algébriquement clos M. Alors pour toute extension algébrique F/L il existe un prolongement $\widehat{\sigma} : F \to M$ de σ à F.*

Preuve. Soit X l'ensemble des couples (E, τ), où E est une sous-extension de F/L (i.e. $L \subseteq E \subseteq F$) et $\tau : E \to M$ une extension de σ. On définit un ordre $\leqslant$ sur X en posant :

$$(E, \tau) \leqslant (E', \tau') \quad \text{si } E \subseteq E' \text{ et } \tau'\big|_E = \tau.$$

Soit $C \subseteq X$ une chaine. Alors $E^\circ := \bigcup_{E \in C} E$ est un corps. Pour tout $x \in E^\circ$, il existe $(E, \tau) \in X$ tel que $x \in E$, et l'on pose $\tau^\circ(x) := \tau(x)$. On voit facilement que $\tau^\circ(x)$ ne dépend pas du choix de (E, τ) et nous fournit un morphisme $\tau^\circ : E^\circ \to M$. Donc $(E^\circ, \tau^\circ) \in X$ est un majorant de C. On en déduit que X est inductif.

Par le lemme de Zorn, l'ensemble X admet un élément maximal (H, ψ). Nous allons montrer par l'absurde que $H = F$. Supposons que $H \neq F$. Choisissons un élément $\alpha \in F$ tel que $\alpha \notin H$ et posons $H' := H[\alpha]$. Alors H' est une extension non triviale de H. Soit $P \in H[X]$ le polynôme minimal de α. Comme M est algébriquement clos, il contient les racines du polynôme $P^\sigma \in M[X]$, et par le théorème 4.1, ψ admet un prolongement $\psi' : H' \to M$, ce qui contredit à la maximalité de H. Donc $H = F$ et le morphisme $\widehat{\sigma} := \psi$ définit un prolongement de σ à F. ∎

5. Clôture algébrique

Définition. *On appelle clôture algébrique de K toute extension algébrique $\overline{K}/K$ qui est aussi algébriquement close.*

Théorème 5.1 (Steinitz)**.** *Tout corps admet un clôture algébrique. Deux clôtures algébriques de K sont isomorphes sur K.*

Preuve de l'existence. Soit $\mathscr{P}$ l'ensemble des polynômes *non constants* à coefficients dans K :

$$\mathscr{P} = \{f \in K[X] \mid f \notin K\}.$$

A tout polynôme $f \in \mathscr{P}$ on associe une indéterminée qu'on notera Y_f. Pour toute partie *finie* $S = \{f_1, f_2, \dots, f_m\}$ de $\mathscr{P}$ on pose

$$K[Y_S] := K[Y_{f_1}, Y_{f_2}, \dots, Y_{f_m}].$$

Soit $A := \bigcup_{S \subset \mathscr{P}} K[Y_S]$. Donc A est l'anneau des polynômes en les indéterminées X_f indexées par $\mathscr{P}$. Soit I l'idéal de A engendré par l'ensemble

$$\{f(Y_f) \mid f \in \mathscr{P}\}.$$

Tout élément de I s'écrit sous la forme

$$g_1 \cdot f_1(Y_{f_1}) + g_2 \cdot f_2(Y_{f_2}) + \cdots + g_r \cdot f_r(Y_{f_r}),$$

où $g_1, g_2, \dots, g_r \in A$.

Lemme 5.2. *$I \neq A$.*

Preuve du lemme. Supposons que $I = A$. Alors it existe une relation de la forme

$$g_1 \cdot f_1(Y_{f_1}) + g_2 \cdot f_2(Y_{f_2}) + \cdots + g_r \cdot f_r(Y_{f_r}) = 1, \tag{3}$$

où $g_1, \dots, g_r \in A$. Il existe une partie finie $E \subseteq \mathscr{P}$ telle que les polynômes $g_1, \dots, g_r$, $f_1, \dots, f_r \in K[Y_E]$. Donc la relation (3) ne fait intervenir qu'un nombre fini d'indéterminées que l'on notera $Y_1, \dots, Y_n$ de telle façon que $Y_i = Y_{f_i}$ pour $1 \leqslant i \leqslant r$. On a :

$$g_1(Y_1, \dots, Y_n) \cdot f_1(Y_1) + g_2(Y_1, \dots, Y_n) \cdot f_2(Y_2) + \cdots + g_r(Y_1, \dots, Y_n) \cdot f_r(Y_r) = 1.$$

Soit L/K une extension dans laquelle chaque $f_i(Y_i)$ $(1 \leqslant i \leqslant r)$ a une racine, notée α_i. En posant $Y_i = \alpha_i$ pour $1 \leqslant i \leqslant n$ et $Y_i = 0$ pour $r + 1 \leqslant i \leqslant n$ dans la relation ci-dessus, on obtient $0 = 1$ ce qui est manifestement faux. Donc $I \neq A$. ∎

Revenons à la preuve du théorème. Comme $I \neq A$, il existe un idéal maximal $\mathfrak{m}$ de A tel que $I \subseteq \mathfrak{m}$. Le quotient $E_1 := A/\mathfrak{m}$ est un corps et l'inclusion $K \hookrightarrow A$ induit une inclusion de K dans E_1. En outre, tout polynôme non constant $f \in K[X]$ admet un racine dans E_1.

En répétant les arguments précédents, on construit, par récurrence, une suite $(E_m)_{m \geqslant 1}$ de corps telle que tout polynôme non constant $f \in E_m[X]$ admet une racine dans E_{m+1}. Soit $E := \bigcup_{m \geqslant 1} E_m$ et soit $\overline{K}$ l'ensemble des éléments de E qui sont algébriques sur K. Par le corollaire 2.5, $\overline{K}$ est un corps.

On va montrer que $\overline{K}$ est une clôture algébrique de K. Soit $f(X) \in \overline{K}[X]$. Alors il existe $m \geqslant 1$ tel que $f(X) \in E_m[X]$. Par construction, $f(X)$ admet une racine $\alpha \in E_{m+1}$. De plus, les coefficients de $f(X)$ sont algébriques sur K ce qui implique que α l'est aussi. Donc $\alpha \in \overline{K}$. Ceci prouve que $\overline{K}$ est algébriquement clos (cf. proposition 3.1). ∎

Preuve de l'unicité à isomorphisme près. Soit $\widetilde{K}$ une autre clôture algébrique de K. Par le théorème 4.3, il existe un morphisme $\psi : \overline{K} \to \widetilde{K}$ tel que $\psi|_K = \mathrm{id}_K$. L'image $\psi(\overline{K})$ de $\overline{K}$ dans $\widetilde{K}$ est un corps algébriquement clos. Donc $\widetilde{K}$ est une extension algébrique du corps algébriquement clos $\psi(\overline{K})$, d'où on déduit que $\widetilde{K} = \psi(\overline{K})$ (cf. proposition 3.1). Donc le morphisme ψ est bijectif et établit un isomorphisme entre $\overline{K}$ et $\widetilde{K}$. ∎

6. Corps de décomposition d'un polynôme

Soit K un corps.

Définition. *Soit $f(X) \in K[X]$ un polynôme non constant. On dit que L/K est un corps de décomposition de $f(X)$ si*
1) $f(X) = a(X-\beta_1)(X-\beta_2)\cdots(X-\beta_n)$ dans $L[X]$.
2) $L = K[\beta_1, \beta_2, \ldots, \beta_n]$.

Soit $\overline{K}/K$ une clôture algébrique fixée de K. Alors $f(X)$ se décompose en produit de facteurs linéaires sur $\overline{K}[X]$:

$$f(X) = a(X-\alpha_1)(X-\alpha_2)\cdots(X-\alpha_n), \qquad \alpha_i \in \overline{K}. \tag{4}$$

Le corps $K_f := K[\alpha_1, \alpha_2, \cdots, \alpha_n]$ est le corps de décomposition de $f(X)$ dans $\overline{K}$.

Théorème 6.1. *i) Soit L un corps de décomposition de f. Alors L est isomorphe à K_f sur K.*

ii) Tout polynôme non-nul possède un corps de décomposition qui est unique à isomorphisme près.

Preuve. i) Par le théorème 4.3, il existe un morphisme $\sigma : L \to \overline{K}$ sur K. Alors :

$$f(X) = f^\sigma(X) = a(X-\sigma(\beta_1))(X-\sigma(\beta_2))\cdots(X-\sigma(\beta_n)) \qquad \text{dans } \overline{K}[X].$$

En comparant cette factorisation avec (4), on trouve que

$$\sigma(L) = L[\sigma(\beta_1), \ldots, \sigma(\beta_n)] = K[\alpha_1, \alpha_2, \cdots, \alpha_n] = K_f.$$

Donc σ établit un isomorphisme entre L et K_f.

ii) L'existence est déjà prouvée. Soient L_1 et L_2 deux corps de décomposition de f. Alors $L_1 \simeq K_f \simeq L_2$ sur K, d'où le théorème.

∎

7. 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 α sur K et F respectivement. Alors $Q(X) \mid P(X)$ dans $F[X]$ et donc toutes ses racines sont simples.

Théorème 7.1. *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 α 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 α 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

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

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

Corollaire 7.2. *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 $\sigma : L/K \to M/K$.*

On note $\mathrm{Hom}_K(L, M)$ l'ensemble des K-morphismes $L/K \to M/K$.

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 $\leqslant [L : K]$. En particulier, si $\overline{K}$ est une clôture algébrique de K, alors

$$\left|\mathrm{Hom}_K(L, \overline{K})\right| \leqslant [L : K].$$

Définition. *Soit $\overline{K}$ une clôture algébrique de K. On dit qu'une extension finie L/K de degré n est séparable s'il possède n morphismes distincts $L/K \to \overline{K}/K$.*

Remarque. Si L/K est séparable, alors il existe une extension E/K *finie* telle que L/K possède n morphismes distincts $L/K \to E/K$.

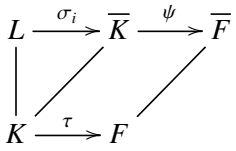
Proposition 7.3. *Soit L/K une extension séparable de degré n et soit $\tau : K \to F$ un morphisme de corps. Soit $\overline{F}$ une clôture algébrique de F. Alors τ admet n prolongements à L à valeurs dans $\overline{F}$:*

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

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

Preuve. Soit $\overline{K}$ une clôture algébrique de K. Comme L/K est séparable, il existent n morphismes $\sigma_i : L/K \to \overline{K}/K$ $(1 \leqslant i \leqslant n)$. Par le théorème de prolongement des homomorphismes, le morphisme $\tau : K \to F$ se prolonge en un morphisme

$\psi : \overline{K} \to \overline{F}$ à valeurs dans une clôture algébrique de F :



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

Théorème 7.4. *Une extension finie simple $L = K[\alpha]$ de K est séparable si et seulement si α est séparable.*

Preuve. Soit $P(X) \in K[X]$ le polynôme minimal de α et soit $n = \deg(P) = [L : K]$. D'après le théorème 4.1, le nombre de morphismes $L/K \to \overline{K}/K$ est égal au nombre des racines de $P(X)$ dans $\overline{K}$. D'autre part, $P(X)$ admet n racines distinctes dans $\overline{K}$ si et seulement si $P(X)$ est séparable. On en déduit le théorème. ∎

Théorème 7.5. *Soient $K \subset L \subset F$. Alors F/K est séparable si et seulement si F/L et L/K sont séparables.*

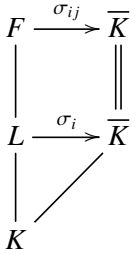
Preuve. Il faut comparer la preuve de ce théorème à celle du théorème 4.2.
Soient

$$\sigma_i : L/K \to \overline{K}/K, \quad 1 \leqslant i \leqslant m'$$

les K-morphismes de L dans $\overline{K}$. Pour chaque i, on note

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

les prolongements de σ_i à F. Ces données sont représentées dans le diagramme :



Soit n' le nombre de morphismes $F/K \to \overline{K}/K$. Comme tout K-morphisme de F dans $\overline{K}$ 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 $n' = n$. 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, alors $m' = m$ et $k'_i = k$ pour tout $1 \leqslant i \leqslant m$. On en déduit que $n' = n$. Donc F/K est séparable. ∎

Théorème 7.6. *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 7.5. D'après le théorème 7.4, α 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 α 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 7.5, L/K est séparable. ∎

Corollaire 7.7. *Toute extension finie d'un corps parfait est séparable.*

8. 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 θ est un élément primitif pour L/K.

Théorème 8.1 (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'extension L/K est séparable, elle admet n homomorphismes $\sigma_i : L/K \to \overline{K}/K$ 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 $K[\theta]/K \to \overline{K}/K$ qui sont induits par les homomorphismes σ_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 σ_i est complètement déterminé par le couple (α_i,β_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. ∎

9. Extensions normales, galoisiennes. Groupe de Galois

On fixe une clôture algébrique $\overline{K}$ de K. Soit L/K une extension finie de K. On suppose que $L \subset \overline{K}$.

Définition. *On dit que L/K est normale si et seulement si*

$$\sigma(L) \subseteq L, \qquad \forall \sigma \in \mathrm{Hom}_K(L, \overline{K}).$$

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

Théorème 9.1. *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. $\boxed{a) \Rightarrow b)}$ Supposons que L/K est normale. Soit $P(X) \in K[X]$ un polynôme irréductible ayant une racine $\alpha \in L$. Soit $\beta \in \overline{K}$ une autre racine de $P(X)$. Soit $\sigma : K[\alpha]/K \to \overline{K}/K$ l'unique morphisme sur K vérifiant $\sigma(\alpha) = \beta$. Par le théorème de prolongement des homomorphismes, il existe un prolongement $\tau : L/K \to \overline{K}/K$ de σ :

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

Comme L/K est normale, on a

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

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

$\boxed{b) \Rightarrow c)}$ 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 α_i. Soit $f(X) = P_1(X) \cdot P_2(X) \cdots P_m(X)$ et soit K_f le corps de décomposition de $f(X)$. Il est alors clair que $L \subseteq K_f$. 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 $K_f \subseteq L$, d'où $L = K_f$.

$\boxed{c) \Rightarrow a).}$ Soit $K_f \subseteq \overline{K}$ 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

$$K_f = K[\alpha_1, \ldots, \alpha_n],$$

où $\alpha_1, \ldots, \alpha_n$ sont les racines de $f(X)$ dans $\overline{K}$. Soit $\sigma \in \mathrm{Hom}_K(K_f, \overline{K})$. Comme $\sigma|_K = \mathrm{id}_K$, 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

$$\sigma(\alpha_i) \in K_f, \qquad 1 \leqslant i \leqslant n.$$

On en déduit que $\sigma(K_f) \subset K_f$. Donc l'extension K_f/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 9.2. *Une extension finie L/K est galoisienne si et seulement si $|\mathrm{Aut}(L/K)| = [L : K]$.*

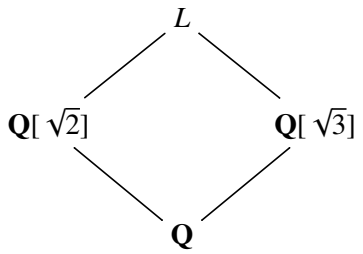
PREUVE. a) Soit $n = [L : K]$. Supposons que L/K est galoisienne. Alors L/K est séparable et il existe une extension E/K telle que L possède n morphismes $\sigma_i : L/K \to \overline{K}/K$ sur K. Comme L/K est normale, pour tout i on a $\sigma_i(L) = L$. Donc les homomorphismes σ_i sont les automorphismes de L et $|\mathrm{Aut}(L/K)| = n$.

b) Réciproquement, supposons que $|\mathrm{Aut}(L/K)| = n$. Donc il existe n morphismes $L/K \to L/K$; on en déduit que L/K est séparable. Comme L/K possède au plus n morphismes dans $\overline{K}/K$, on obtient que tout morphisme $L/K \to \overline{K}/K$ 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 σ 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 σ 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 θ, $\sigma_1(\theta)$, $\sigma_2(\theta)$, $\sigma_3(\theta)$ sont 2 à 2 distincts. Donc θ est un élément primitif pour L :

$$L = \mathbf{Q}[\theta].$$

10. 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 10.1 (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 :

$$\sum_{i=1}^{r} \lambda_i \chi_i(g) = 0. \tag{5}$$

Soit $h \in G$. En multipliant la relation précédente par $\chi_1(h)$, on obtient :

$$\sum_{i=1}^{r} \lambda_i \chi_1(h) \chi_i(g) = 0. \tag{6}$$

D'autre part, en remplaçant g par gh dans la formule (5) et en utilisant la formule $\chi_i(gh) = \chi_i(g)\chi_i(h)$, on trouve :

$$\sum_{i=1}^{r} \lambda_i \chi_i(h) \chi_i(g) = 0. \tag{7}$$

En soustrayant (6) de (7), on obtient la relation

$$\sum_{i=2}^{r} \lambda_i (\chi_i(h) - \chi_1(h)) \chi_i(g) = 0, \qquad g \in G \tag{8}$$

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 10.2. *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 σ_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 $\{\chi_i, \ldots, \chi_n\}$. ∎

11. 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 11.1 (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 σ_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 $\lambda_1, \lambda_2, \ldots, \lambda_n \in L$ 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 10.2

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

$$w_1 + \lambda_2 w_2 + \cdots \lambda_r w_r = 0, \qquad \lambda_2, \ldots, \lambda_r \neq 0 \tag{9}$$

(en divisant par un scalaire, on peut toujours supposer que $\lambda_1 = 1$). Plus explicitement, on a

$$\begin{pmatrix} \sigma_1(x_1) \\ \sigma_2(x_1) \\ \vdots \\ \sigma_n(x_1) \end{pmatrix} + \lambda_2 \begin{pmatrix} \sigma_1(x_2) \\ \sigma_2(x_2) \\ \vdots \\ \sigma_n(x_2) \end{pmatrix} + \cdots + \lambda_r \begin{pmatrix} \sigma_1(x_r) \\ \sigma_2(x_r) \\ \vdots \\ \sigma_n(x_r) \end{pmatrix} = 0, \qquad \lambda_2, \ldots, \lambda_r \neq 0. \tag{10}$$

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 τ permute de la même manière les coordonnées des vecteurs $w_1, w_2, \ldots, w_r$. Donc

$$w_1 + \tau(\lambda_2) w_2 + \cdots \tau(\lambda_r) w_r = 0, \quad \forall \tau \in G. \tag{11}$$

En soustrayant (9) de (11), 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 (10) 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

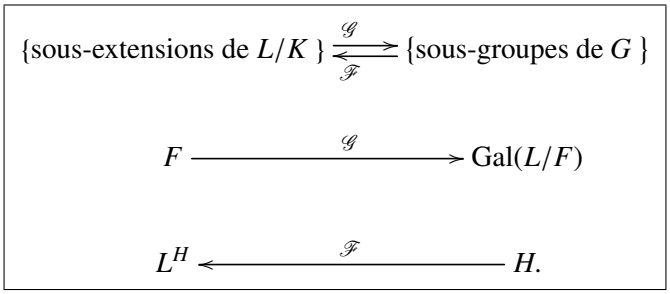
$$\left|\mathrm{Aut}(L/L^G)\right| \leqslant [L : L^G]$$

on obtient que $G = \mathrm{Aut}(L/L^G)$. Maintenant, il découle du théorème 9.2 que L/L^G est galoisienne et $G = \mathrm{Gal}(L/L^G)$. ∎

12. 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:



Théorème 12.1 (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 7.5, F/K est séparable. On va montrer que F/K est normale. Soit $\sigma : F/K \to \overline{K}/K$ un morphisme sur K. Par le théorème de prolongement des homomorphismes il existent une extension E/M et un morphisme $g : L/K \to \overline{K}/K$ 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. *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.*

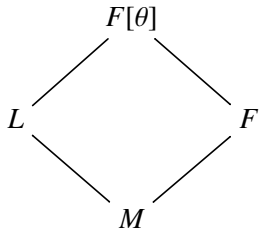
Exemple. Soit L/K une extension simple. Alors $L = K[\theta]$, où θ est un élément primitif pour L. Alors pour toute extension F de K le compositum LF est la plus petite extension de F contenant θ, d'où

$$LF = F[\theta].$$

Lemme 12.2. *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 θ sur M et soit $Q \in F[X]$ le polynôme minimal de θ 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 9.1 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 $I \subseteq \{1,2,\dots,n\}$, 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 12.3. *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 12.2 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 12.2 on a :

$$|\mathrm{Gal}(LF/F)| = [LF : F] = [L : (L\cap F)] = |\mathrm{Gal}(L/F)|.$$

∎

13. Exemple du polynôme $X^5 - 10X + 5$

Soit $f(X) \in K[X]$ un polynôme séparable et soit $K_f \subseteq \overline{K}$ son corps de décomposition. On note $\alpha_1,\dots,\alpha_n$ les racines de f dans K_f :

$$K_f = K[\alpha_1,\alpha_2,\dots,\alpha_n].$$

Le groupe symétrique de l'ensemble des racines est isomorphe à S_n.

Les automorphismes $g \in \mathrm{Gal}(K_f/K)$ permutent les racines de $f(X)$. Chaque automorphisme est complètement déterminé par sont action sur les racines, donc par la permutation

$$\begin{pmatrix} \alpha_1 & \alpha_2 & \dots & \alpha_n \\ g(\alpha_1) & g(\alpha_2) & \dots & g(\alpha_n) \end{pmatrix}.$$

On obtient un monomorphisme de groupes :

$$\mathrm{Gal}(K_f/K) \to S_n.$$

Théorème 13.1. *Soit $\mathbf{Q}_f$ le corps de décomposition du polynôme $f(X) = X^5 - 10X + 5$ sur $\mathbf{Q}$. Alors*

$$\mathrm{Gal}(\mathbf{Q}_f/\mathbf{Q}) \simeq S_5.$$

Preuve. a) Soit $G = \mathrm{Gal}(\mathbf{Q}_f/\mathbf{Q})$. On considère $\mathbf{Q}_f$ comme un sous-corps du corps $\mathbf{C}$ des nombres complexes. Le polynôme $f(X)$ est irréductible sur $\mathbf{Q}$ par le critère d'Eisenstein (on pose $p = 5$). Le corps de rupture de $f(X)$ est de degré 5 sur $\mathbf{Q}$, d'où on trouve que 5 divise $|G| = [\mathbf{Q}_f : \mathbf{Q}]$. 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 $f : \mathbf{R} \to \mathbf{R}$. Comme $f'(X) = 5X^4 - 10$, elle admet des extrema en $-\sqrt[4]{2}$ et en $\sqrt[4]{2}$ avec $P(-\sqrt[4]{2}) > 0$ et $f(\sqrt[4]{2}) < 0$. Donc, $f(X)$ possède exactement 3 racines réelles qu'on note α_3, α_4 et α_5. Soient α_1 et α_2 les racines complexes de f. La conjugaison complexe fournit un automorphisme de $\mathbf{Q}_f/\mathbf{Q}$ qui permute α_1 et α_2.

Le théorème découle maintenant du lemme suivant :

Lemme 13.2. *Le groupe S_n ($n \geqslant 2$) 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. ∎

∎

14. Extensions cyclotomiques

Dans cette section, on suppose que $\mathrm{char}(K) = 0$. On fixe une clôture algébrique $\overline{K}$ de K. Pour tout $n \geqslant 1$ on appelle corps cyclotomique et l'on note K_n le corps de décomposition du polynôme $X^n - 1$ dans $\overline{K}$. 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 μ_n est un groupe cyclique d'ordre n et on appelle racine primitive d'ordre n tout générateur de μ_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 μ_n^* l'ensemble des racines primitives d'ordre n. Alors $|\mu_n^*| = \varphi(n)$, où φ 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 ζ_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 :

$$g(\zeta_n) = \zeta_n^a, \qquad \mathrm{pgcd}(a,n) = 1. \tag{12}$$

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 réécrit (12) sous la forme :

$$g(\zeta_n) = \zeta_n^{\chi_n(g)}.$$

Théorème 14.1. *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 ζ_n.

Proof. a) Comme tout automorphisme de K_n/K est complètement déterminé par son action sur ζ_n, l'application χ_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, χ_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 χ_n ne dépend pas du choix de la racine primitive. ∎

Exercice 3. Montrer que $\mathrm{Gal}(\mathbf{Q}[\zeta_n]/\mathbf{Q}) \simeq (\mathbf{Z}/n\mathbf{Z})^*$. 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 $\mathbf{Q}$.

15. Extensions de Kummer

Dans cette section, on suppose que $\mathrm{char}(K) = 0$.

Définition. *On dit qu'une extension finie L/K est cyclique si elle est cyclique et son groupe de Galois* $\mathrm{Gal}(L/K)$ *est cyclique.*

Supposons que K contient une racine primitive d'ordre n de l'unité (et donc contient le groupe μ_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 15.1. *Soit K un corps de caractéristique 0 contenant une racine primitive de l'unité d'ordre n.*

i) Soit $a \in K$ et soit α 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 μ_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 α 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 α. 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, ψ est un monomorphisme.

Soit $d = [K[\alpha] : K]$. Comme le groupe de Galois $\mathrm{Gal}(K[\alpha]/K)$ s'injecte dans le groupe cyclique μ_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 10.2) 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 α 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. On peut préciser la partie i) du théorème : si K ne contient aucune racine de a d'ordre $m > 1$ divisant n, alors $[K[\alpha] : K] = n$.

16. 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 α 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 K_f le 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 K_f.*

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 16.1 (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 $Gal(K_f/K)$ est résoluble.*

Exemple. *L'équation $X^5 - 10X + 5 = 0$ n'est pas résoluble par radicaux sur* $\mathbf{Q}$.

Corollaire 16.2 (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 $G = \mathrm{Gal}(K_f/K)$ et $n = |G|$. Supposons que G est résoluble et montrons que K_f est contenue dans une extension radicale de K.

Soient $F = K(\zeta_n)$ et $E = FK_f$. Alors E est le corps de décomposition de f sur F et par le théorème 12.3 le groupe de Galois $H = \mathrm{Gal}(E/F)$ est isomorphe à un sous-groupe de G. En particulier, H est résoluble et 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 15.1 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 K_f de f est contenu dans une extension radicale M/K. Nous utiliserons le lemme suivant.

Lemme 16.3. *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 α 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 15.1, le groupe

$$H_i/H_{i+1} \simeq \mathrm{Gal}(E_{i+1}/E_i)$$

est cyclique. Donc, le groupe $\mathrm{Gal}(E/F)$ 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. Comme le corps K_f est une sous-extension de E/K, le groupe de Galois $G = \mathrm{Gal}(K_f/K)$ est un quotient de $\mathrm{Gal}(E/K)$. Donc, il est résoluble et le théorème est démontré. ■

CHAPITRE 2

Représentations des groupes finis

1. Représentations de groupes

1.1. Soit K un corps et soit V un espace vectoriel sur K. On note $\mathrm{GL}(V)$ l'ensemble des automorphismes de V :

$$\mathrm{GL}(V) := \{\varphi : V \to V \mid \varphi \text{ est linéaire et bijective}\}.$$

La composition d'applications donne à $\mathrm{GL}(V)$ une structure de groupe : l'élément neutre est l'application identité et l'inverse φ^{-1} de φ est son application réciproque. Si V est de dimension finie n sur K, alors pour toute base $B = \{v_1, \ldots, v_n\}$ de V l'application

$$\begin{cases} \mathrm{GL}(V) \to \mathrm{GL}_n(K), \\ \varphi \mapsto \text{matrice de } \varphi \text{ dans } B \end{cases}$$

établit un isomorphisme entre $\mathrm{GL}(V)$ et $\mathrm{GL}_n(K)$ qui dépend du choix de B.

Soit G un groupe.

Définition. *Une représentation du groupe G est un espace vectoriel V muni d'un morphisme de groupes $\rho : G \to \mathrm{GL}(V)$.*

Une représentation $\rho : G \to \mathrm{GL}(V)$ définit une action linéaire de G sur V, à savoir :

$$g \cdot v := \rho(g)(v), \qquad \forall g \in G, \quad v \in V.$$

Pour simplifier la notation, on va souvent écrire ρ_g au lieu de $\rho(g)$.

Définition. *Soient $\rho : G \to \mathrm{GL}(V)$ et $\mu : G \to \mathrm{GL}(W)$ deux représentations du même groupe G. On dit qu'une application linéaire $f : V \to W$ est un morphisme de représentations, si*

$$\mu_g(f(v)) = f(\rho_g(v)), \qquad \forall g \in G, \quad v \in V.$$

On peut réécrire la condition ci-dessus sous la forme :

$$\mu_g \circ f = f \circ \rho_g, \qquad \forall g \in G.$$

Exemple. *Soit $G = \{e, \sigma\}$ un groupe d'ordre 2. Soit $A \in \mathrm{GL}_2(K)$ une matrice vérifiant la condition $A^2 = I_2$. Alors l'application $\rho : G \to \mathrm{GL}_2(K)$ définie par*

$$\rho(e) = I_2, \qquad \rho(\sigma) = A$$

est une représentation de G de dimension 2. En particulier, on peut prendre

$$A = \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix}, \quad \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}.$$

1.2. Représentation triviale. Pour tout espace vectoriel V, le morphisme trivial

$$G \to \mathrm{GL}(V), \qquad s \mapsto \mathrm{id}_V, \qquad \forall s \in G$$

définit une représentation appelée la représentation triviale de G sur V.

1.3. Représentations de dimension 1. Soit $\rho : G \to \mathrm{GL}(V)$ une représentation de G. Supposons que $\dim_K(V) = 1$. Alors tout automorphisme de V est de la forme $v \mapsto \lambda v$, où $\lambda \in K^*$ ce qui définit un isomorphisme canonique $\mathrm{GL}(V) \simeq K^*$. En composant ρ avec cet isomorphisme canonique, on obtient un morphisme de groupes

$$\chi : G \xrightarrow{\rho} \mathrm{GL}(V) \xrightarrow{\sim} K^*.$$

Donc χ est un caractère du groupe G à valeurs dans K^*. L'action de G sur V est explicitement donnée par la formule

$$\rho_g(v) = \chi(g)v, \quad \forall g \in G, \quad \forall v \in V.$$

Il est facile de voir que deux représentations de dimension 1 sont isomorphes si et seulement si leurs caractères coïncident.

On note $X(G, K^*)$ l'ensemble des caractères de G à valeurs dans K. Si χ_1 et $\chi_2 \in X(G, K)$ on définit leur produit $\chi_1\chi_2$ par la formule

$$(\chi_1\chi_2)(g) := \chi_1(g)\chi_2(g), \qquad g \in G.$$

On vérifie facilement que $\chi_1\chi_2 \in X(G, K)$ et que le produit ainsi défini munit $X(G, K)$ d'une structure de groupe abélien.

Exercice 4. *Soient G_1 et G_2 deux groupes. Montrer que*

$$X(G_1 \times G_2, K) \simeq X(G_1, K) \times X(G_2, K).$$

Soit $\mathbf{C}$ le corps des nombres complexes. Pour simplifier la notation, on pose $\widehat{G} := X(G, \mathbf{C})$ et on appelle $\widehat{G}$ le groupe dual de G.

Théorème 1.4. *Soit G un groupe abélien fini. Alors :*
i) Le groupe $\widehat{G}$ est isomorphe (non canoniquement) à G.
ii) L'application

$$\begin{cases} \widehat{G} \times G \to \mathbf{C}^*, \\ (\chi, g) \mapsto \chi(g) \end{cases}$$

induit un isomorphisme canonique $\widehat{\widehat{G}} \simeq G$.

Preuve. Supposons d'abord que G est cyclique d'ordre n. Soit σ un générateur de G. On note μ_n le groupe des racines complexes d'ordre n de l'unité. Rappelons que μ_n est cyclique d'ordre n. Un générateur ζ_n de μ_n est appelé une racine primitive d'ordre n de l'unité.

1) Pour tout $\chi \in \widehat{G}$ on a

$$\chi(\sigma)^n = \chi(\sigma^n) = \chi(e) = 1,$$

d'où $\chi(\sigma) \in \mu_n$. On montre que l'application f ainsi définie

$$f : \widehat{G} \to \mu_n, \qquad \chi \mapsto \chi(\sigma)$$

est un isomorphisme de groupes. En effet :

a) On a $f(\chi_1\chi_2) = (\chi_1\chi_2)(\sigma) = \chi_1(\sigma)\chi_2(\sigma) = f(\chi_1)f(\chi_2)$. Donc f est un morphisme de groupes.

b) Si $f(\chi) = 1$, alors $\chi(\sigma) = 1$, d'où $\chi(g) = 1$ pour tout $g \in G$. On en déduit que $\ker(f)$ est trivial, d'où l'injectivité de f.

c) Pour tout $\zeta \in \mu_n$, l'application

$$\chi : G \to \mu_n, \qquad \chi(\sigma^k) = \zeta^k$$

est un caractère de G. Comme $f(\chi) = \zeta$, f est injectif.

Donc f est un isomorphisme de groupes cycliques. On en déduit que

$$\widehat{G} \simeq \mu_n \simeq G.$$

2) On continue de supposer que G est cyclique d'ordre n. On considère l'application

$$\begin{cases} \psi : G \to \widehat{\widehat{G}} = \mathrm{Hom}(\widehat{G}, \mu_n), \\ \psi(g)(\chi) := \chi(g). \end{cases}$$

a) Comme

$$\psi(g_1g_2)(\chi) = \chi(g_1g_2) = \chi(g_1)\chi(g_2) = \psi(g_1)(\chi)\cdot\psi(g_2)(\chi), \qquad \forall g_1, g_2 \in G, \quad \chi \in \widehat{G},$$

on obtient que $\psi(g_1g_2) = \psi(g_1)\psi(g_2)$. Donc ψ est un morphisme de groupes.

b) Supposons que $g \in \ker(\psi)$. Alors $\chi(g) = 1$ pour tout $\chi \in \widehat{G}$. Soit $\zeta_n \in \mu_n$ une racine primitive d'ordre n et soit χ le caractère de G défini par $\chi(\sigma) = \zeta_n$. On écrit g sous la forme $g = \sigma^k$, $k \in \mathbf{N}$. Alors $1 = \chi(g) = \zeta_n^k$, d'où $n \mid k$ et $g = e$. Donc ψ est injectif. Comme $|\widehat{\widehat{G}}| = |\widehat{G}| = |G|$, on en déduit que ψ est un isomorphisme.

Le théorème est donc démontré pour les groupes cycliques.

3) Soit G un groupe abélien fini. Alors G se décompose en produit direct de groupes cycliques :

$$G \simeq G_1 \times G_2 \times \cdots \times G_k.$$

En appliquant l'exercice 4, on obtient que

$$\widehat{G} \simeq \widehat{G}_1 \times \widehat{G}_2 \times \cdots \times \widehat{G}_k.$$

Comme $|\widehat{G}_i| = |G_i|$ par la partie 1) de la preuve, on en déduit que $|\widehat{G}| = |G|$. De même, l'application

$$\begin{cases} \psi : G \to \widehat{\widehat{G}} = \mathrm{Hom}(\widehat{G}, \mu_n), \\ \psi(g)(\chi) := \chi(g). \end{cases}$$

s'écrit comme la composition

$$G \simeq G_1 \times G_2 \times \cdots \times G_k \xrightarrow{(\psi_1,\ldots,\psi_k)} \widehat{\widehat{G}}_1 \times \widehat{\widehat{G}}_2 \times \cdots \times \widehat{\widehat{G}}_k \simeq \widehat{\widehat{G}},$$

où $\psi_i : G_i \to \widehat{\widehat{G}}_i$ est l'application ψ pour le groupe G_i. Par la partie 2) de la preuve, chaque ψ_i est un isomorphisme, d'où on déduit que ψ l'est aussi. Le théorème est démontré. ∎

Remarque. *Soit G un groupe et soit $D(G) := [G,G]$ le groupe dérivé de G. Soit $\chi : G \to K^*$ un caractère. Alors $G/\ker(\chi)$ est un groupe abélien, d'où on déduit que $D(G) \subseteq \ker(\chi)$.*

1.5. Représentation régulière. Soit K^G l'espace vectoriel des sommes finies

$$\sum_{\sigma\in G} a_\sigma \sigma,$$

où $a_\sigma = 0$ pour tous sauf un nombre fini de σ. L'addition et la multiplication par les scalaires sont définies comme suit :

$$\sum_{\sigma\in G} a_\sigma\sigma + \sum_{\sigma\in G} b_\sigma\sigma := \sum_{\sigma\in G}(a_\sigma + b_\sigma)\sigma,$$
$$\lambda\left(\sum_{\sigma\in G} a_\sigma\sigma\right) = \sum_{\sigma\in G}\lambda a_\sigma\sigma.$$

Pour tout $s \in G$, on note $r_s : K^G \to K^G$ l'application linéaire définie par la formule :

$$r_s\left(\sum_{\sigma\in G} a_\sigma\sigma\right) := \sum_{\sigma\in G} a_\sigma(s\sigma), \qquad s \in G.$$

On vérifie facilement que $r_{st} = r_s r_t$. Donc $r_s \in \mathrm{GL}(K^G)$ pour tout $s \in G$ et l'application

$$r : G \to \mathrm{GL}(K^G), \qquad s \mapsto r_s$$

définit une représentation de G sur l'espace K^G appelée la représentations régulière de G.. On note que si G est fini d'ordre g, alors $\dim_K(K^G) = g$.

1.6. Sous-représentations. Soit $\rho : G \to \mathrm{GL}(V)$ une représentation de G et soit W un sous-espace de V stable sous l'action de G :

$$\rho_s(w) \in W, \qquad \forall s \in G, \quad \forall w \in W.$$

Alors la restriction de l'action de G sur W définit un morphisme

$$\rho|_W : G \to \mathrm{GL}(W).$$

On dit que $\rho|_W$ est une sous-représentation de ρ.

Exemple. Soit G un groupe fini et soit $x := \sum_{\sigma\in G} \sigma \in K^G$. Alors

$$r_\tau(x) = \sum_{\sigma\in G} \tau\sigma = \sum_{\sigma\in G} \sigma = x.$$

Le vecteur x engendre l'espace $Kx \subseteq K^G$ de dimension 1 sur lequel G agit trivialement. On en déduit que K^G contient une sous-représentation triviale de dimension 1.

Définition. *Une représentation $\rho : G \to \mathrm{GL}(V)$ est irréductible (ou simple) si $V \neq \{0\}$ et ρ n'admet aucune sous-représentation autre que $\{0\}$ et V.*

1.7. Sommes directes. Soient $\rho : G \to \mathrm{GL}(V)$ et $\mu : G \to \mathrm{GL}(W)$ deux représentations de G. On note $V \oplus W$ la somme directe de V et W. On appelle somme directe des représentations ρ et μ et l'on note $\rho \oplus \mu$ la représentation

$$\rho \oplus \mu : G \to \mathrm{GL}(V \oplus W)$$

définie par

$$(\rho \oplus \mu)_s(v,w) = (\rho_s(v), \rho_s(w)), \qquad s \in G, \quad v \in V, \quad w \in W.$$

En particulier, soit $\rho : G \to \mathrm{GL}(V)$ une représentation et soit $V = \overset{m}{\underset{i=1}{\oplus}} V_i$ une décomposition de V en somme directe de sous-espaces vectoriels stables par ρ. Alors la représentation ρ se décompose en somme directe des sous-représentations $\rho_i : G \to \mathrm{GL}(V_i)$ et l'on note

$$\rho = \overset{m}{\underset{i=1}{\oplus}} \rho_i.$$

Exercice 5. 1) Soit $\mathbf{R}$ le groupe additif des nombres réels. Montrer que l'application

$$\rho : \mathbf{R} \to \mathrm{GL}_2(\mathbf{R}), \qquad \rho_\alpha := \begin{pmatrix} \cos(\alpha) & -\sin(\alpha) \\ \sin(\alpha) & \cos(\alpha) \end{pmatrix}$$

est une représentation de $\mathbf{R}$. On note que $\ker(\rho) = 2\pi\mathbf{Z}$.

2) On note $\rho^{\mathbf{C}}$ la représentation obtenue à partir de ρ par extension des scalaires de $\mathbf{R}$ à $\mathbf{C}$:

$$\rho^{\mathbf{C}} : \mathbf{R} \to \mathrm{GL}_2(\mathbf{C}), \qquad \rho^{\mathbf{C}}_\alpha := \begin{pmatrix} \cos(\alpha) & -\sin(\alpha) \\ \sin(\alpha) & \cos(\alpha) \end{pmatrix}.$$

Montrer que

$$\rho^{\mathbf{C}} = \chi \oplus \chi^{-1},$$

où $\chi : G \to \mathbf{C}^*$ est le caractère $\chi(\alpha) = e^{i\alpha}$.

2. Algèbres sur un corps

Soit K un corps.

Définition. *On appelle algèbre sur K (ou K-algèbre) un ensemble A muni de deux lois de composition internes $+$ et $\cdot$ et d'une loi de composition externe*

$$K \times A \to A, \qquad (\lambda, x) \mapsto \lambda x$$

vérifiant les propriétés suivantes :

1) A est un K-espace vectoriel. On note $+$ l'addition dans A;

2) $(A, +, \cdot)$ est un anneau associatif et unitaire ;

3) Pour tous $\lambda \in K$ et $x, y \in A$,

$$(\lambda x)y = x(\lambda y) = \lambda(xy).$$

Exemples. 1) L'ensemble $M_n(K)$ des matrices carrées de taille n est une K-algèbre pour les lois de composition usuelles.

2) L'ensemble $F[a,b]$ des fonctions réelles $f : [a,b] \to \mathbf{R}$ est une $\mathbf{R}$-algèbre pour l'addition et la multiplication usuelles.

Soient G un groupe et K un corps. On munit l'espace vectoriel K^G du produit défini par :

$$\left(\sum_{\sigma\in G} a_\sigma \sigma\right)\cdot\left(\sum_{\tau\in G} b_\tau \tau\right) = \sum_{\sigma,\tau\in G} (a_\sigma b_\tau)\sigma\tau = \sum_{s\in G} c_s s,$$

où

$$c_s = \sum_{\sigma\tau=s} a_\sigma b_\tau.$$

Le produit ainsi défini munit K^G d'une structure de K-algèbre, notée $K[G]$.

Proposition 2.1. *i) Soit $\rho : G \to \mathrm{GL}(V)$ une représentation de G. Alors l'application*

$$K[G]\times V \to V,$$
$$\left(\sum_{\sigma\in G} a_\sigma\sigma\right) v = \sum_{\sigma\in G} a_\sigma \rho_\sigma(v)$$

définit une structure de $K[G]$-module sur V.

ii) Réciproquement, soit V un $K[G]$-module. Alors V est muni d'une structure naturelle de K-espace vectoriel et pour tout $\sigma \in G$ l'application

$$\rho_\sigma : V \to V, \qquad \rho_\sigma(v) = \sigma v$$

est K-linéaire. En outre, $\rho_{\sigma\tau} = \rho_\sigma\rho_\tau$ pour tous $\sigma,\tau \in G$. Ainsi, l'application

$$\rho : G \to \mathrm{GL}(V), \qquad \sigma \mapsto \rho_\sigma$$

est une représentation de G sur V.

Preuve. La preuve est laissée en exercice (facile). ∎

3. Théorème de Maschke

Soit G un groupe fini d'ordre g et soit K un corps. *Dans cette section, on suppose que la caractéristique de K ne divise pas g*. Cette condition est automatiquement remplie si K est de caractéristique nulle.

Théorème 3.1. *Soit V un $K[G]$-module et soit W un sous module de V. Alors il existe un sous-module W' de V tel que $V = W \oplus W'$.*

Proof. Par le théorème de la base incomplète (qui est valable pour les espaces vectoriels de dimension infinie grâce au lemme de Zorn), il existe un sous-espace vectoriel $F \subseteq V$ tel que

$$M = W \oplus F \qquad \text{en tant qu'espace vectoriel.}$$

Tout élément $x \in V$ s'écrit de façon unique sous la forme $x = w + f$ avec $w \in W$ et $f \in F$ et on définit l'application de projection

$$\pi : M \to W, \qquad \pi(x) := w.$$

Soit

$$p : V \to W,$$
$$p(x) := \frac{1}{n}\sum_{\sigma\in G} \sigma(\pi(\sigma^{-1}(x))), \qquad x \in V.$$

En termes de la représentation $\rho : G \to \mathrm{GL}(V)$ associée au module V, l'application p s'écrit

$$p = \frac{1}{g}\sum_{\sigma\in G}\rho_\sigma \circ \pi \circ \rho_\sigma^{-1}.$$

L'application p est clairement K-linéaire. Pour tout $g \in G$ on a :

$$\begin{aligned} p\circ\rho_\tau &= \frac{1}{g}\sum_{\sigma\in G}\rho_\sigma\circ\pi\circ\rho_\sigma^{-1}\circ\rho_\tau = \frac{1}{g}\sum_{\sigma\in G}\rho_\sigma\circ\pi\circ\rho_{\sigma^{-1}\tau} \\ &= \frac{1}{g}\sum_{\sigma\in G}\rho_\tau\circ\rho_{\tau^{-1}\sigma}\circ\pi\circ\rho_{\sigma^{-1}\tau} = \rho_\tau\circ\left(\frac{1}{g}\sum_{\sigma\in G}\rho_{\tau^{-1}\sigma}\circ\pi\circ\rho_{(\tau^{-1}\sigma)^{-1}}\right) = \rho_\tau\circ p, \end{aligned}$$

ce qui montre que p est un morphisme de $K[G]$-modules. En outre,

$$p(x) = x, \qquad \forall x \in W,$$

d'où on obtient que $p^2 = p$. Alors (cf. lemme ci-dessous), en tant qu'espace vectoriel, V se décompose en somme directe $V = W \oplus W'$, avec $W' = \ker(p)$. Comme p est un morphisme de $K[G]$-modules, W' est un sous-module de V. Le théorème est démontré. ∎

Le lemme suivant est bien connu :

Lemme 3.2. *Soit V un espace vectoriel et soit $p : V \to V$ une application linéaire vérifiant $p^2 = p$. Alors*

$$V = W \oplus W', \qquad W := \mathrm{Im}(p), \quad W' := \ker(p).$$

Preuve. Tout $x \in V$ s'écrit sous la forme $x = w + w'$, où $w = p(x) \in W$ et $w' = x - p(x)$. Le calcul

$$p(w') = p(x) - p^2(x) = p(x) - p(x) = 0$$

montre que $w' \in W'$. Donc, $W + W' = V$. D'autre part, si $x \in W \cap W'$, alors $x = p(y)$, $y \in V$ et on a :

$$x = p(y) = p^2(y) = p(x) = 0.$$

Donc, $W \cap W' = \{0\}$. On en déduit que $V = W \oplus W'$. ∎

Théorème 3.3 (Maschke)**.** *Soit $\rho : G \to \mathrm{GL}(V)$ une représentation de dimension finie (i.e. V est de dimension finie). Alors ρ se décompose en somme directe de représentations irréductibles.*

Preuve. On montre le théorème par récurrence sur la dimension de V en utilisant le théorème 3.1. ∎

4. Lemme de Schur

Soit A un anneau. Rappelons qu'un A-module M est irréductible (ou simple) si $M \neq \{0\}$ et n'admet aucun sous-module autre que $\{0\}$ et M.

Lemme 4.1. *Soit $f : M \to N$ un morphisme non-nul de A-modules simples. Alors f est un isomorphisme.*

PREUVE. Soit $\ker(f)$ le noyau de f. Comme $f \neq 0$, on a $\ker(f) \neq M$, d'où $\ker(f) = 0$ par l'irréductibilité de f. De même, l'image $\mathrm{Im}(f)$ de f est non-nulle, d'où $\mathrm{Im}(f) = N$ par l'irréductibilité de N. ∎

Soient G un groupe et K un corps. Alors une représentation $\rho : G \to \mathrm{GL}(V)$ est irréductible si et seulement si V est irréductible en tant que $K[G]$-module.

Lemme 4.2 (Schur)**.** *i) Soit $f : V \to W$ un morphisme non-nul entre deux représentations irréductibles d'un groupe G. Alors f est un isomorphisme.*

ii) Supposons que G est fini et K est algébriquement clos. Alors :

a) Toute représentation irréductible de G est de dimension finie.

b) Soit $\rho : G \to \mathrm{GL}(V)$ une représentation irréductible et soit $f : V \to V$ un endomorphisme de V. Alors f est une homothétie, i.e. il existe $\lambda \in K$ tel que $f = \lambda \cdot \mathrm{id}_V$.

PREUVE. i) La première assertion est un cas particulier du lemme précédent.

iia) Soit V une représentation irréductible. Soit $v \in V$ un vecteur non-nul et soit $V_0 = \langle \rho_\sigma(v) \mid \sigma \in G \rangle$ le sous espace de V engendré par la famille $S := \{\rho_\sigma(v) \mid \sigma \in G\}$. On voit facilement que l'action de G permute les éléments de S, d'où on déduit que V_0 est une sous-représentation non-triviale de V. L'irréductibilité de V implique que $V = V_0$. D'autre part, comme G est fini, l'ensemble S l'est aussi et V_0 est de dimension finie.

iib) Soit $f : V \to V$ un endomorphisme d'une représentation irréductible V. Comme K est algébriquement clos, f admet une valeur propre $\lambda \in K$. L'application linéaire $\varphi := f - \lambda \mathrm{id}_V$ vérifie

$$\rho_\sigma \circ \varphi = \varphi \circ \rho_\sigma, \qquad \sigma \in G.$$

Donc, φ est un endomorphisme de V. D'autre part, $\ker(\varphi) \neq \{0\}$, et la partie i) du lemme implique que $\varphi = 0$, d'où $f = \lambda \cdot \mathrm{id}_V$. ∎

Corollaire 4.3. *Soit G un groupe abélien fini. Alors toute représentation irréductible de G sur un corps algébriquement clos est de dimension* 1.

PROOF. Soit $\rho : G \to \mathrm{GL}(V)$ une représentation irréductible d'un groupe abélien fini G. Soit $\tau \in G$. Alors :

$$\rho_\sigma \circ \rho_\tau = \rho_{\sigma\tau} = \rho_{\tau\sigma} = \rho_\tau \circ \rho_\sigma, \qquad \forall \sigma \in G.$$

Donc, ρ_τ est un endomorphisme de la représentation V, d'où $\rho_\tau = \lambda \cdot \mathrm{id}_V$, $\lambda \in K$ par le lemme de Schur. On en conclut que pour tout $\tau \in G$, ρ_τ est une homothétie. Ceci implique que tout sous-espace de V est stable sous l'action de G. Comme V est irréductible, on en déduit que $\dim_K V = 1$. ∎

Soit $A = (a_{ij})_{1 \leqslant i,j \leqslant n} \in M_d(K)$ une matrice. On appelle trace de A et l'on note $\mathrm{Tr}(A)$ la somme des éléments diagonaux de A :

$$\mathrm{Tr}(A) = \sum_{i=1}^{d} a_{ii}.$$

Soit $B \in M_d(K)$ une autre matrice. Alors :

$$\mathrm{Tr}(A+B) = \mathrm{Tr}(A) + \mathrm{Tr}(B), \qquad \mathrm{Tr}(AB) = \mathrm{Tr}(BA).$$

En particulier, en posant $A = C^{-1}A$ et $B = C$, on obtient :

$$\mathrm{Tr}(C^{-1}AC) = \mathrm{Tr}(A), \qquad \forall C \in \mathrm{GL}_n(K). \tag{13}$$

Soit $\varphi : V \to V$ une application linéaire. Soit $\mathbf{v} = \{v_i\}_{i=1}^n$ une base de V et soit $A = (a_{ij})_{1 \leqslant i,j \leqslant n}$ la matrice de φ dans cette base. On définit la trace $\mathrm{Tr}(\varphi)$ de φ en posant :

$$\mathrm{Tr}(\varphi) = \sum_{i=1}^{n} a_{ii}.$$

Si $\mathbf{v}' = \{v_i'\}_{i=1}^n$ est une autre base de V et si A' est la matrice de φ dans la base $\mathbf{v}'$, alors

$$A' = C^{-1}AC,$$

où C est la matrice de passage de $\mathbf{v}$ à $\mathbf{v}'$. Donc, la définition de $\mathrm{Tr}(\varphi)$ ne dépend pas du choix de la base.

Proposition 4.4. *Soient $\rho : G \to \mathrm{GL}(V)$ et $\mu : G \to \mathrm{GL}(W)$ deux représentations irréductibles de G sur un corps algégriquement clos K. Soit $\varphi : V \to V$ une application linéaire et soit*

$$\widetilde{\varphi} = \frac{1}{g} \sum_{\sigma \in G} \mu_{\sigma^{-1}} \circ \varphi \circ \rho_\sigma, \qquad g = |G|.$$

Alors :

i) $\widetilde{\varphi}$ est un morphisme de représentations.

ii) $\widetilde{\varphi} = 0$ si ρ et μ ne sont pas isomorphes.

iii) Si $V = W$ et $\rho = \mu$, alors

$$\widetilde{\varphi} = \frac{1}{n}\mathrm{Tr}(\varphi)\,\mathrm{id}_V.$$

Preuve. i) La première assertion découle d'un calcul direct (à comparer avec la preuve du théorème 3.1) :

$$\begin{aligned}\widetilde{\varphi} \circ \rho_\tau &= \frac{1}{g} \sum_{\sigma \in G} \mu_{\sigma^{-1}} \circ \varphi \circ \rho_\sigma \circ \rho_\tau = \frac{1}{g} \sum_{\sigma \in G} \mu_{\sigma^{-1}} \circ \varphi \circ \rho_{\sigma\tau} \\ &= \frac{1}{g} \sum_{\sigma \in G} \mu_\tau \circ \mu_{\tau^{-1}\sigma^{-1}} \circ \varphi \circ \rho_{\sigma\tau} = \mu_\tau \circ \left(\frac{1}{g} \sum_{\sigma \in G} \rho_{(\sigma\tau)^{-1}} \circ \varphi \circ \rho_{\sigma\tau} \right) = \mu_\tau \circ \widetilde{\varphi}.\end{aligned}$$

Donc, $\widetilde{\varphi}$ est un morphisme de représentations.

ii) Du lemme de Schur il découle que $\widetilde{\varphi} = 0$ si ρ et μ ne sont pas isomorphes.

iii) Si $V = W$ et $\rho = \mu$, le lemme de Schur nous dit que

$$\frac{1}{g} \sum_{\sigma \in G} \rho_{\sigma^{-1}} \circ \varphi \circ \rho_\sigma = \widetilde{\varphi} = \lambda\,\mathrm{id}_V, \qquad \lambda \in K.$$

En notant que $\mathrm{Tr}(\rho_{\sigma^{-1}} \circ \varphi \circ \rho_\sigma) = \mathrm{Tr}(\varphi)$, on en déduit que

$$n\lambda = \mathrm{Tr}(\lambda \,\mathrm{id}_V) = \frac{1}{g}\sum_{\sigma\in G} \mathrm{Tr}\left(\rho_{\sigma^{-1}} \circ \varphi \circ \rho_\sigma\right) = \frac{1}{g}\sum_{\sigma\in G} \mathrm{Tr}(\varphi) = \mathrm{Tr}(\varphi).$$

Donc, $\lambda = \frac{1}{n}\mathrm{Tr}(\varphi)$, et la proposition est démontrée. ∎

On fixe des bases $\mathbf{v}$ et $\mathbf{w}$ des espaces V et W et l'on note

$$A(\sigma) = (a_{ij}(\sigma))_{1\leqslant i,j\leqslant n}, \qquad B(\sigma) = (b_{ij}(\sigma))_{1\leqslant i,j\leqslant m}$$

les matrices de ρ_σ et μ_σ dans ces bases.

Corollaire 4.5. *Soient $\rho : G \to \mathrm{GL}(V)$ et $\mu : G \to \mathrm{GL}(W)$ deux représentations irréductibles de G.*

i) Si les représentations ρ et μ ne sont pas isomorphes, alors :

$$\frac{1}{g}\sum_{\sigma\in G} a_{i_1 j_1}(\sigma) b_{i_2,j_2}(\sigma^{-1}) = 0, \qquad \textit{pour tous } 1 \leqslant i_1, j_1 \leqslant n,\ 1 \leqslant i_2, j_2 \leqslant m.$$

ii) Si $(V,\rho) = (W,\mu)$ et $\mathbf{v} = \mathbf{w}$, alors

$$\frac{1}{g}\sum_{\sigma\in G} a_{i_1 j_1}(\sigma) b_{i_2,j_2}(\sigma^{-1}) = \begin{cases} \dfrac{1}{n}, & \textit{si } i_1 = j_2 \textit{ et } j_1 = i_2; \\ 0, & \textit{sinon.} \end{cases}$$

Preuve. Pour une application linéaire $\varphi : V \to V$, on note $X = (x_{ij})_{1\leqslant i\leqslant m, 1\leqslant j\leqslant n}$ (respectivement $\widetilde{X} = (\widetilde{x_{ij}})_{1\leqslant i\leqslant m,1\leqslant j\leqslant n}$) la matrice de φ (respectivement $\widetilde{\varphi}$) dans les bases $\mathbf{v}, \mathbf{w}$. On note $\varphi_{st} : V \to V$ $(1 \leqslant s \leqslant m,\ 1 \leqslant t \leqslant n)$ l'application linéaire dont la matrice dans les bases fixées est définie par

$$x_{ij} = \begin{cases} 1, & \text{si } i = s,\ j = t, \\ 0, & \text{sinon.} \end{cases}$$

Alors, pour toute application φ, on a :

$$\widetilde{x}_{i_2,j_1} = \frac{1}{g}\sum_{\sigma\in G}\sum_{j_2=1}^{m}\sum_{i_1=1}^{n} b_{i_2 j_2}(\sigma^{-1}) x_{j_2 i_1} a_{i_1,j_1}(\sigma), \qquad \forall 1 \leqslant i_2 \leqslant m, \quad 1 \leqslant j_1 \leqslant n. \tag{14}$$

i) Supposons que ρ et μ ne sont pas isomorphes. Par le point ii) de la proposition 4.4, $\widetilde{\varphi} = 0$ et donc $\widetilde{x}_{i_2,j_1} = 0$ pour tous i_2, j_1. En posant $\varphi = \varphi_{j_2 i_1}$ pour j_2 et i_1 fixés, on en déduit que

$$\frac{1}{g}\sum_{\sigma\in G} a_{i_1 j_1}(\sigma) b_{i_2,j_2}(\sigma^{-1}) = 0.$$

ii) Supposons maintenant que $(V,\rho) = (W,\mu)$ et $\mathbf{v} = \mathbf{w}$. Posons $\varphi = \varphi_{j_2 i_1}$. Alors :

$$\mathrm{Tr}(\varphi_{j_2 i_1}) = \begin{cases} 1, & \text{si } j_2 = i_1, \\ 0, & \text{sinon.} \end{cases}$$

Par le point iii) de la proposition 4.4, $\widetilde{\varphi}_{j_2 i_1} = n\mathrm{id}_V$ si $j_2 = i_1$ et $\widetilde{\varphi}_{j_2 i_1} = 0$ sinon. Donc, l'équation (14) s'écrit :

$$\frac{1}{g}\sum_{\sigma\in G} b_{i_2 j_2}(\sigma^{-1}) a_{i_1, j_1}(\sigma) = \begin{cases} \dfrac{1}{n}, & \text{si } j_2 = i_1 \text{ et } i_2 = j_1, \\ 0, & \text{sinon.} \end{cases}$$

■

5. Caractères d'un groupe fini

Soient G un groupe fini d'ordre g. On note $F(G, \mathbf{C})$ l'ensemble des applications $f : G \to \mathbf{C}$. Si $f_1, f_2 \in F(G, \mathbf{C})$, on définit leur somme $f_1 + f_2$ par la formule usuelle :

$$(f_1 + f_2)(\sigma) = f_1(\sigma) + f_2(\sigma), \qquad \sigma \in G.$$

De même, si $f \in F(G, \mathbf{C})$ et $\lambda \in \mathbf{C}$, on définit le produit $\lambda f \in F(G, \mathbf{C})$ par :

$$(\lambda f)(\sigma) = \lambda f(\sigma), \qquad \sigma \in G.$$

Soit

$$\delta_\sigma(\tau) = \begin{cases} 1, & \text{si } \sigma = \tau \\ 0, & \text{sinon.} \end{cases}$$

Toute fonction $f \in F(G, \mathbf{C})$ s'écrit sous la forme

$$f = \sum_{\sigma\in G} f(\sigma)\delta_\sigma.$$

On en déduit facilement que $F(G, \mathbf{C})$ est un $\mathbf{C}$-espace vectoriel de dimension g et que la famille $\{\delta_\sigma\}_{\sigma\in G}$ est une base canonique de $F(G, \mathbf{C})$.

On munit l'espace $F(G, \mathbf{C})$ de l'application

$$\langle\,,\,\rangle : F(G, \mathbf{C}) \times F(G, \mathbf{C}) \to \mathbf{C},$$
$$\langle f_1, f_2\rangle := \frac{1}{g}\sum_{\sigma\in G} f_1(\sigma)\overline{f_2(\sigma)},$$

où $\overline{f_2(\sigma)}$ désigne le conjugué complexe de $f_2(\sigma)$. On vérifie facilement les propriétés suivantes :

- $\langle f_1 + \lambda f_2, h\rangle = \langle f_1, h\rangle + \lambda\langle f_2, h\rangle$, $\quad \forall \lambda \in \mathbf{C}, \quad f_1, f_2, h \in F(G, \mathbf{C})$,
- $\langle f, h\rangle = \overline{\langle h, f\rangle}$, $\quad \forall f, h \in F(G, \mathbf{C})$,
- $\langle f, f\rangle \geqslant 0$ $\quad \forall f \in F(G, \mathbf{C})$,
- $\langle f, f\rangle = 0$ $\quad$ si et seulement si $f = 0$.

Donc, $\langle\,,\,\rangle$ est une forme hermitienne définie positive (produit scalaire) sur $F(G, \mathbf{C})$.

On appelle fonction centrale sur G une application $f : G \to \mathbf{C}$ vérifiant la condition

$$f(\sigma^{-1}\tau\sigma) = f(\tau), \qquad \forall \sigma, \tau \in G.$$

Rappelons que le groupe G agit sur lui-même par conjugaison et que cette action fournit une décomposition de G en union disjointe des classes de conjugaison :

$$G = \bigcup_{i=1}^{m} C_i, \qquad C_i = \{s^{-1}\sigma_i s \mid s \in G\},$$

où, pour chaque i, σ_i désigne un représentant de la classe C_i. On voit facilement que l'ensemble $C(G,K)$ des fonctions centrales sur G est un sous-espace vectoriel de $F(G,\mathbf{C})$ de dimension m.

Définition. *Soit $\rho : G \to \mathrm{GL}(V)$ une représentation de G sur un $\mathbf{C}$-espace vectoriel V de dimension finie n. On appelle caractère de ρ l'application*

$$\chi_\rho : G \to \mathbf{C}, \qquad \chi_\rho(\sigma) = \mathrm{Tr}(\rho(\sigma)), \quad \forall \sigma \in G.$$

Explicitement, soit $\mathbf{v}$ une base de V et soit $A(\sigma) = (a_{ij}(\sigma))_{1\leqslant i,j\leqslant n}$ la matrice de $\rho(\sigma)$ dans cette base. Alors :

$$\chi_\rho(\sigma) = \mathrm{Tr}(A(\sigma)) = \sum_{i=1}^{n} a_{ii}(\sigma).$$

Remarque. Si $\dim_K(V) = 1$, le caractère de ρ coïncide avec le caractère du groupe G associé à ρ dans la section 1.3.

On note que si deux représentations ρ et μ sont isomorphes, alors $\chi_\rho = \chi_\mu$.

Proposition 5.1. *i) Soit $\rho : G \to \mathrm{GL}(V)$ une représentation de G sur un $\mathbf{C}$-espace vectoriel V de dimension n. Alors :*

i) $\chi_\rho(e) = n$;
ii) χ_ρ *est une fonction centrale ;*
iii) $\chi_\rho(\sigma^{-1}) = \overline{\chi_\rho(\sigma)}, \quad \forall \sigma \in G.$

Preuve. ia) On a $\chi_\rho(e) = \mathrm{Tr}(I_n) = n$.

ib) On a $\chi_\rho(\tau^{-1}\sigma\tau) = \mathrm{Tr}(\rho_\tau^{-1} \circ \rho_\sigma \circ \rho_\tau) = \mathrm{Tr}(\rho_\sigma) = \chi_\rho$.

ic) On a $\rho(\sigma)^g = \rho(\sigma)^g = \rho(e) = \mathrm{id}_V$. Donc le polynôme $X^g - 1$ est un polynôme annulateur de $\rho(\sigma)$. Le polynôme minimal $P(X)$ de $\rho(\sigma)$ divise $X^g - 1$, d'où on déduit que les valeurs propres $\{\lambda_i\}_{i=1}^n$ de $\rho(\sigma)$ (comptées avec multiplicité) sont des racines g-ièmes de l'unité. En particulier, on a $\lambda_i^{-1} = \overline{\lambda}_i$. Donc

$$\chi_\rho(\sigma^{-1}) = \mathrm{Tr}(\rho(\sigma)^{-1}) = \sum_{i=1}^{n} \lambda_i^{-1} = \sum_{i=1}^{n} \overline{\lambda}_i = \overline{\chi_\rho(\sigma)}.$$

■

Proposition 5.2. *Soient $\rho : G \to \mathrm{GL}(V)$ et $\mu : G \to \mathrm{GL}(W)$ deux représentations complexes et soit $\rho \oplus \mu$ leur somme directe. Alors :*

$$\chi_{\rho\oplus\mu} = \chi_\rho + \chi_\mu.$$

Preuve. On identifie V et W avec les sous-espaces $V \oplus \{0\}$ et $\{0\} \oplus W$ de la somme directe $V \oplus W$. On fixe des bases $\mathbf{v} = \{v_i\}_{i=1}^n$ et $\mathbf{w} = \{w_i\}_{i=1}^m$ de V et W respectivement ; alors $\mathbf{v} \cup \mathbf{w}$ est une base de $V \oplus W$. Soient $A(\sigma) = (a_{ij}(\sigma))_{1\leqslant i,j\leqslant n}$ les

matrices de $\rho(\sigma)$ et $\mu(\sigma)$ dans les bases $\mathbf{v}$ et $\mathbf{w}$. Alors la matrice de $(\rho\oplus\mu)(\sigma)$ dans la base $\mathbf{v}\cup\mathbf{w}$ est la matrice bloc-diagonale $C(\sigma)$ composée des blocs $A(\sigma)$ et $B(\sigma)$:

$$C(\sigma)=\begin{pmatrix}A(\sigma) & 0\\ 0 & B(\sigma)\end{pmatrix}.$$

Donc, on a :

$$\chi_{\rho\oplus\mu}(\sigma)=\operatorname{Tr}(C(\sigma))=\operatorname{Tr}(A(\sigma))+\operatorname{Tr}(B(\sigma))=\chi_\rho(\sigma)+\chi_\mu(\sigma).$$

■

Théorème 5.3 (Relations d'orthogonalité pour les caractères)**.** *Soient $\rho : G\to \mathrm{GL}(V)$ et $\mu : G\to \mathrm{GL}(W)$ deux représentations complexes irréductibles de G. Alors :*

$$\left\langle\chi_\rho,\chi_\mu\right\rangle=\begin{cases}0, & \text{si } \rho\not\simeq\mu,\\ 1, & \text{si } \rho\simeq\mu.\end{cases}$$

Preuve. Soient $A(\sigma)$ et $B(\sigma)$ les matrices des applications ρ_σ et μ_σ dans des bases fixées de V et W. Alors :

$$\begin{aligned}\left\langle\chi_\rho,\chi_\mu\right\rangle&=\frac{1}{g}\sum_{\sigma\in G}\chi_\rho(\sigma)\overline{\chi_\mu(\sigma)}=\frac{1}{g}\sum_{\sigma\in G}\chi_\rho(\sigma)\overline{\chi_\mu(\sigma)}=\frac{1}{g}\sum_{\sigma\in G}\left(\sum_{i=1}^{n}a_{ii}(\sigma)\right)\cdot\left(\sum_{j=1}^{m}\overline{b_{jj}(\sigma)}\right)\\&=\frac{1}{g}\sum_{i=1}^{n}\sum_{j=1}^{m}\left(\sum_{\sigma\in G}a_{ii}(\sigma)\overline{b_{jj}(\sigma)}\right)=\frac{1}{g}\sum_{i=1}^{n}\sum_{j=1}^{m}\left(\sum_{\sigma\in G}a_{ii}(\sigma)b_{jj}(\sigma^{-1})\right).\end{aligned}$$

Maintenant, le théorème découle du corollaire 4.5. Si $\rho\not\simeq\mu$, on a :

$$\frac{1}{g}\sum_{\sigma\in G}a_{ii}(\sigma)b_{jj}(\sigma^{-1})=0,\quad\text{for all}\quad 1\leqslant i\leqslant n,\quad 1\leqslant j\leqslant m,$$

d'où $\left\langle\chi_\rho,\chi_\mu\right\rangle=0$. Si $\rho\simeq\mu$, alors :

$$\frac{1}{g}\sum_{\sigma\in G}a_{ii}(\sigma)b_{jj}(\sigma^{-1})=\begin{cases}\dfrac{1}{n}, & \text{si } i=j,\\ 0, & \text{sinon,}\end{cases}$$

d'où $\left\langle\chi_\rho,\chi_\mu\right\rangle=1$. Le théorème est démontré. ■

Théorème 5.4. *Soit $\rho : G\to \mathrm{GL}(V)$ une représentation complexe et soit*

$$V\simeq\bigoplus_{i=1}^{s}V_i \tag{15}$$

une décomposition de (ρ,V) en somme directe de représentations irréductibles (ρ_i,V_i). Pour toute représentation irréductible $\pi : G\to\mathrm{GL}(U)$, on note m_π le nombre de sous-représentations V_i isomorphes à (π,U). Alors :

$$m_\pi:=\left\langle\chi_\rho,\chi_\pi\right\rangle.$$

PREUVE. Par la proposition 5.2,

$$\chi_\rho = \sum_{i=1}^{s} \chi_{\rho_i},$$

d'où :

$$\left\langle \chi_\rho, \chi_\pi \right\rangle = \sum_{i=1}^{s} \left\langle \chi_{\rho_i}, \chi_\pi \right\rangle,$$

et le théorème découle du théorème 5.3. ∎

Définition. *Avec les notations et hypothèses du théorème 5.4, on appelle m_π la multiplicité de π dans ρ. Le théorème 5.4 implique que m_π ne dépend pas du choix de la décomposition de ρ en somme directe de représentations irréductibles.*

Corollaire 5.5. *Soient ρ et ρ' deux représentations. Alors $\rho \simeq \rho'$ si et seulement si $\chi_\rho = \chi_{\rho'}$.*

PREUVE. On sait déjà que

$$\rho \simeq \rho' \Rightarrow \chi_\rho = \chi_{\rho'}.$$

Réciproquement, supposons que $\chi_\rho = \chi_{\rho'}$. Pour toute représentation irréductible $\pi : G \to \mathrm{GL}(U)$, on note m_π (respectivement m'_π) la multiplicité de π dans ρ (respectivement ρ'). Alors

$$m_\pi = \left\langle \chi_\rho, \chi_\pi \right\rangle = \left\langle \chi_{\rho'}, \chi_\pi \right\rangle = m'_\pi.$$

ce qui montre que les décompositions de ρ et ρ' en sommes directes de représentations irréductibles sont isomorphes. ∎

Pour chaque caractère χ de G on note V_χ une représentation associée à χ. Par le corollaire 5.5, V_χ est unique à isomorphisme près. Soit

$$\mathrm{Irr}(G) := \{\chi \mid V_\chi \text{ irréductible}\}.$$

Pour toute représentation U de G, on note $U^{\oplus k}$ la somme directe de k copies de U. Alors on peut réécrire la décomposition (15) sous la forme :

$$V \simeq \bigoplus_{\chi \in \mathrm{Irr}(G)} V_\chi^{\oplus m_\chi}, \qquad m_\chi = \left\langle \chi_\rho, \chi \right\rangle. \tag{16}$$

Corollaire 5.6. *On a :*

$$\left\langle \chi_\rho, \chi_\rho \right\rangle = \sum_{\chi \in \mathrm{Irr}(G)} m_\chi^2.$$

En particulier, ρ est irréductible si et seulement si $\left\langle \chi_\rho, \chi_\rho \right\rangle = 1$.

PREUVE. Par la proposition 5.2, on a $\chi_\rho = \sum_{\chi \in \mathrm{Irr}(G)} m_\chi \chi$. Donc, par les relations d'orthogonalité pour les caractères :

$$\left\langle \chi_\rho, \chi_\rho \right\rangle = \sum_{\chi, \chi' \in \mathrm{Irr}(G)} m_\chi m_{\chi'} \left\langle \chi, \chi' \right\rangle = \sum_{\chi \in \mathrm{Irr}(G)} m_\chi^2.$$

∎

6. Décomposition de la représentation régulière

Soit $r : G \to \mathrm{GL}(\mathbf{C}^G)$ la représentation régulière de G. On note χ_G le caractère de r. Rappelons que pour tout $s \in G$, l'application linéaire r_s agit sur la base canonique $\{\sigma\}_{\sigma\in G}$ de $\mathbf{C}^G$ par $r_s(\sigma) = s\sigma$. On en déduit facilement que

$$\chi_G(s) = \begin{cases} g, & \text{si } s = e, \\ 0, & \text{sinon.} \end{cases} \tag{17}$$

Pour tout caractère $\chi \in \mathrm{Irr}(G)$, on pose $n_\chi = \dim_{\mathbf{C}} V_\chi$ et l'on note m_χ la multiplicité de la représentation V_χ dans $\mathbf{C}^G$.

Théorème 6.1. *i) Pour tout $\chi \in \mathrm{Irr}(G)$ on a :*

$$\langle \chi_G, \chi \rangle = n_\chi.$$

ii) La représentation régulière se décompose en somme directe :

$$\mathbf{C}^G \simeq \bigoplus_{\chi\in\mathrm{Irr}(G)} V_\chi^{\oplus n_\chi}.$$

En particulier, $m_\chi = n_\chi$ pour tout $\chi \in \mathrm{Irr}(G)$.

Preuve. i) En appliquant la formule (17), on obtient :

$$\langle \chi_G, \chi \rangle = \frac{1}{g} \sum_{\sigma\in G} \chi_G(\sigma) \cdot \overline{\chi(\sigma)} = \frac{1}{g} \chi_G(e) \cdot \overline{\chi(e)} = n_\chi.$$

ii) La deuxième assertion découle du point i) appliqué à la décomposition (16).

■

Corollaire 6.2. *On a :*

$$\sum_{\chi\in\mathrm{Irr}(G)} n_\chi^2 = g.$$

Preuve. En combinant le corollaire 5.6 et le point i) du théorème 6.1, on obtient :

$$\sum_{\chi\in\mathrm{Irr(G)}} n_\chi^2 = \langle \chi_G, \chi_G \rangle = \frac{1}{g} \sum_{\sigma\in G} \chi_G(\sigma) \cdot \overline{\chi_G(\sigma)} = g.$$

■

Théorème 6.3. *La famille $\{\chi \,|\, \chi \in \mathrm{Irr}(G)\}$ est une base orthonormée de $C(G, \mathbf{C})$.*

On déduit immédiatement de ce théorème le corollaire important suivant :

Corollaire 6.4. *Le nombre de représentations irréductibles de G à isomorphisme près est égal au nombre de classes de conjugaison dans G.*

Pour démontrer le théorème, on a besoin d'un lemme auxiliaire.

Lemme 6.5. *i) Soit $f \in C(G, \mathbf{C})$ et soit $\rho : G \to \mathrm{GL}(V)$ une représentation de dimension n. Alors l'application*

$$\varphi : V \to V,$$
$$\varphi(v) := \sum_{\sigma\in G} f(\sigma)\rho_\sigma(v), \qquad v \in V$$

est un morphisme de représentations.

ii) Supposons que ρ est irréductible. Alors :

$$\sum_{\sigma\in G} f(\sigma)\rho_\sigma = \frac{g}{n}\left\langle \chi_\rho, \overline{f}\right\rangle \cdot \mathrm{id}_V, \qquad n := \dim_{\mathbf{C}}(V).$$

Preuve du lemme. i) Pour tout $\tau \in G$, on a :

$$\rho_\tau^{-1}\circ\varphi\circ\rho_\tau = \rho_\tau^{-1}\circ\left(\sum_{\sigma\in G} f(\sigma)\rho_\sigma\right)\circ\rho_\tau = \sum_{\sigma\in G} f(\sigma)\rho_\tau^{-1}\circ\rho_\sigma\circ\rho_\tau = \sum_{\sigma\in G} f(\sigma)\rho_{\tau^{-1}\sigma\tau}$$

En posant $s := \tau^{-1}\sigma\tau$ et en utilisant le fait que $f(\tau s\tau^{-1}) = f(s)$, on réécrit la dernière expression sous la forme

$$\sum_{\sigma\in G} f(\sigma)\rho_{\tau^{-1}\sigma\tau} = \sum_{s\in G} f(\tau s\tau^{-1})\rho_s = \sum_{s\in G} f(s)\rho_s = \varphi.$$

Donc $\rho_\tau^{-1}\circ\varphi\circ\rho_\tau = \varphi$, d'où $\varphi\circ\rho_\tau = \rho_\tau\circ\varphi$, ce qui montre que φ est un morphisme de représentations.

ii) Si ρ est irréductible, l'application φ est une homothétie par le lemme de Schur. Donc :

$$\sum_{\sigma\in G} f(\sigma)\rho_\sigma = \lambda\cdot\mathrm{id}_V, \qquad \lambda\in\mathbf{C}.$$

Pour déterminer λ, on calcule les traces :

$$\lambda\cdot n = \mathrm{Tr}(\lambda\cdot\mathrm{id}_V) = \sum_{\sigma\in G} f(\sigma)\mathrm{Tr}(\rho_\sigma) = \sum_{\sigma\in G} f(\sigma)\chi_\rho(\sigma) = g\left\langle \chi_\rho, \overline{f}\right\rangle.$$

Donc :

$$\lambda = \frac{g}{n}\left\langle \chi_\rho, \overline{f}\right\rangle.$$

Le lemme est démontré. ∎

Passons à la preuve du théorème.

Preuve du théorème. Rappelons que le caractère d'une représentation est une fonction centrale. Les relations d'orthogonalité pour les caractères montrent que $\{\chi \mid \chi \in \mathrm{Irr}(G)\}$ est une famille orthonormée. En particulier, elle est libre. Comme toute famille orthonormée peut être complétée en une base orthonormée, pour montrer que $\{\chi \mid \chi \in \mathrm{Irr}(G)\}$ est une base, il suffit de vérifier que le seul vecteur orthogonal à cette famille est le vecteur nul :

$$\langle \chi, f\rangle = 0, \quad \forall \chi\in\mathrm{Irr}(G) \qquad \Rightarrow \qquad f = 0.$$

Supposons que $\langle \chi, f\rangle = 0$ pour tout $\chi \in \mathrm{Irr}(G)$. Alors, par le lemme précédent, pour toute représentation irréductible π de G, on a :

$$\sum_{\sigma\in G} \overline{f(\sigma)}\pi_\sigma = \frac{g}{n}\langle \chi_\pi, f\rangle\cdot\mathrm{id} = 0.$$

Comme la représentation régulière $r : G \to \mathrm{GL}(\mathbf{C}^G)$ se décompose en somme directe de représentations irréductibles, on en déduit que

$$\sum_{\sigma\in G} \overline{f(\sigma)} r_\sigma = 0.$$

Donc :

$$\sum_{\sigma\in G}\overline{f(\sigma)}\sigma=\sum_{\sigma\in G}\overline{f(\sigma)}r_\sigma(e)=\left(\sum_{\sigma\in G}\overline{f(\sigma)}r_\sigma\right)(e)=0.$$

On en déduit que $f(\sigma)=0$ pour tout $\sigma\in G$, d'où le théorème. ∎

7. Représentations des groupes diédraux

7.1. Pour tout entier $n\geqslant 3$ on note D_{2n} le groupe diédral d'ordre $2n$. Rappelons que D_{2n} est défini comme le groupe des isométries du plan conservant un polygône régulier à n côté. Le groupe D_{2n} est engendré par deux éléments s et r vérifiant les relations suivantes :

$$r^n=e,\qquad s^2=e,\qquad srs=r^{-1}.$$

On note que $s^{-1}=s$ et $sr^i=r^{-i}s$ pour tout $i\in\mathbf{Z}$. On en déduit que tout élément de D_{2n} s'écrit de façon unique sous la forme

$$s^ar^b,\qquad s\in\{0,1\},\quad b\in\{0,n-1\}.$$

En outre,

$$\left(s^{a_1}r^{b_1}\right)\cdot\left(s^{a_2}r^{b_2}\right)=s^{a_1+a_2}r^{b_2+(-1)^{a_2}b_1}.$$

Le groupe cyclique $C_n:=\langle r\rangle$ est un sous-groupe distingué de D_{2n} d'indice 2.

Dans cette section, nous classifions les représentations irréductibles de D_{2n}.

7.2. Le cas de n pair. On note $Z(D_{2n})$ et $[D_{2n},D_{2n}]$ le centre le groupe dérivé de D_{2n}.

Proposition 7.3. *Soit $n\geqslant 3$ un entier pair. Alors :*

i) $Z(D_{2n})=\{e,r^{n/2}\}$.

ii) $[D_{2n},D_{2n}]$ *est le sous-groupe cyclique d'ordre $n/2$ engendré par r^2.*

iii) *L'abélianisé $D_{2n}/[D_{2n},D_{2n}]$ de D_{2n} est engendré par les classes $\overline{r}$ et $\overline{s}$ vérifiant $\overline{r}^2=\overline{s}^2=\overline{e}$. En particulier, il est isomorphe à $\mathbf{Z}/2\mathbf{Z}\oplus\mathbf{Z}/2\mathbf{Z}$.*

iv) D_{2n} *admet $\dfrac{n}{2}+3$ classes de conjugaison, à savoir :*

$$\begin{aligned}
&\mathrm{Conj}(e)=\{e\},\\
&\mathrm{Conj}(r^{n/2})=\{r^{n/2}\},\\
&\mathrm{Conj}(r^i)=\{r^i,r^{-i}\},\qquad 1\leqslant i\leqslant\frac{n}{2}-1,\\
&\mathrm{Conj}(s)=\left\{sr^{2j}\mid 0\leqslant j\leqslant\frac{n}{2}-1\right\},\\
&\mathrm{Conj}(sr)=\left\{sr^{2j+1}\mid 0\leqslant j\leqslant\frac{n}{2}-1\right\}.
\end{aligned}$$

Preuve. i) Soit $x\in G$. Alors $x\in Z(G)$ si et seulement si $xs=sx$ et $xr=rx$. En écrivant x sous la forme $x=s^ar^b$, on trouve que $xs=s^{a+1}r^{-b}$ et $rx=s^ar^{(-1)^a+b}$, d'où $r^b=r^{-b}$ et $(-1)^a=1$. Donc $a=0$ et $r^{2b}=e$, ce qui montre que $x=r^b$ avec $b\in\{0,n/2\}$.

ii) Le groupe dérivé est engendré par les commutateurs $[x,y]=x^{-1}y^{-1}xy$. On vérifie facilement les formules suivantes :

- Si $x, y \in C_n$, alors $[x,y] = e$.
- Si $x \in C_n$ et $y \in sC_n$, alors $[x,y] = x^{-1}(y^{-1}xy) = x^{-2}$.
- Si $x \in sC_n$ et $y \in C_n$, alors $[x,y] = (x^{-1}(y^{-1}x)y = y^2$.
- Si $x \in sC_n$ et $y \in sC_n$, alors, en posant $z := yx \in C_n$:

$$[x,y] = x^{-1}y^{-1}xy = z^{-1}xzx^{-1} = [z, x^{-1}] = z^{-2}.$$

On en déduit que $[x,y] \in \left\langle r^2 \right\rangle$ pour tous $x, y \in D_{2n}$. En outre, $[s,r] = r^2$, d'où $[D_{2n}, D_{2n}] = \left\langle r^2 \right\rangle$. Comme $2 \mid n$, l'élément r^2 engendre un sous-groupe d'ordre $n/2$ de C_n.

iii) Le groupe $D_{2n}/[D_{2n}, D_{2n}]$ est le groupe abélien engendré par les classes $\overline{s}$ et $\overline{r}$, qui sont d'ordre 2 par le point ii). Donc $D_{2n}/[D_{2n}, D_{2n}] \simeq \langle \overline{s} \rangle \oplus \langle \overline{r} \rangle$.

iv) On note $\mathrm{Conj}(x)$ la classe de conjugaison de x. Comme $e, r^{n/2} \in Z(D_{2n})$, on a $\mathrm{Conj}(e) = \{e\}$ et $\mathrm{Conj}(r^{n/2}) = \{r^{n/2}\}$. Si $x \in C_n$, alors pour tout $y \in sC_n$, on a $y^{-1}xy = x^{-1}$, d'où $\mathrm{Conj}(r^i) = \{r^i, r^{-i}\}$ pour tous $0 \leqslant i \leqslant n-1$. On note que $\mathrm{Conj}(r^i) = \mathrm{Conj}(r^{n-i})$ et que $r^i \neq r^{-i}$ si et seulement si $i \notin \{0, n/2\}$. En outre, $(sr^j)^{-1}s(sr^j) = sr^{2j}$ et $(sr^j)^{-1}(sr)(sr^j) = sr^{2j-1}$. Donc

$$\mathrm{Conj}(s) = \left\{ sr^{2j} \mid 0 \leqslant j \leqslant \frac{n}{2} - 1 \right\}, \quad \mathrm{Conj}(sr) = \left\{ sr^{2j+1} \mid 0 \leqslant j \leqslant \frac{n}{2} - 1 \right\}.$$

L'union de ces classes coïncide avec D_{2n}. ∎

On construit maintenant les représentations irréductibles de D_{2n}. Les représentations de degré 1 sont données par les morphismes $\psi : D_{2n} \to \mathbf{C}^*$. Comme $\mathbf{C}^*$ est abélien, chaque ψ se factorise à travers $D_{2n}/[D_{2n}, D_{2n}]$. Par le point iii) de la proposition 7.3, $D_{2n}/[D_{2n}, D_{2n}]$ est la somme directe des groupes d'ordre 2 engendrés par $\overline{s}$ et $\overline{r}$. Comme chaque morphisme $\overline{\psi} : \langle \overline{s} \rangle \oplus \langle \overline{r} \rangle \to \mathbf{C}^*$ est complètement défini par ses valeurs $\overline{\psi}(\overline{s})$ et $\overline{\psi}(\overline{r})$, nous avons exactement quatre morphismes suivants :

$$\begin{aligned}
&\overline{\psi}_1(\overline{s}) = 1, && \psi_1(\overline{r}) = 1,\\
&\overline{\psi}_2(\overline{s}) = 1, && \psi_2(\overline{r}) = -1,\\
&\overline{\psi}_3(\overline{s}) = -1, && \psi_3(\overline{r}) = 1,\\
&\overline{\psi}_4(\overline{s}) = -1, && \psi_4(\overline{r}) = -1.
\end{aligned}$$

Les caractères associés $\psi_i : D_{2n} \to \mathbf{C}^*$ du groupe D_{2n} s'écrivent explicitement :

$$\begin{aligned}
&\psi_1(r^i) = 1, && \psi_1(sr^i) = 1,\\
&\psi_2(r^i) = (-1)^i, && \psi_2(sr^i) = (-1)^i,\\
&\psi_3(r^i) = 1, && \psi_3(sr^i) = -1,\\
&\psi_4(r^i) = (-1)^i, && \psi_4(sr^i) = (-1)^{i+1}.
\end{aligned}$$

On note que ψ_1 est le caractère trivial.

Nous allons maintenant construire des représentations explicites de degré 2 de D_{2n}. Posons $\zeta_n = e^{2\pi i/n}$. Alors ζ_n est une racine primitive de l'unité d'ordre n. Soient :

$$R_k = \begin{pmatrix} \zeta_n^k & 0 \\ 0 & \zeta_n^{-k} \end{pmatrix}, \qquad S = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}.$$

On note que $S^2 = I_n$, $R_k^n = I_n$ et $SR_kS = R_k^{-1}$. Donc l'application

$$\rho_k : D_{2n} \to \mathrm{GL}_2(\mathbf{C}), \qquad \rho_k(s^a r^b) := S^a R_k^b$$

est un morphisme de groupe bien défini que nous allons considéré comme une représentation de D_{2n} sur l'espace vectoriel $\mathbf{C}^2$. Les propriétés suivantes se démontrent facilement :

- $\rho_{n+k} = \rho_k$. C'est clair puisque $R_{k+n} = R_k$.
- Pour tout k, les représentations ρ_k et ρ_{n-k} sont isomorphes. En effet, l'application linéaire

  $$f : \mathbf{C}^2 \to \mathbf{C}^2, \qquad f\begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} y \\ x \end{pmatrix},$$

  vérifie la propriété $\rho_{n-k} \circ f = f \circ \rho_k$ et établit donc un isomorphisme $\rho_k \simeq \rho_{n-k}$.
- Les représentations ρ_0 et $\rho_{n/2}$ sont réductibles. En effet, le sous-espace vectoriel engendré par le vecteur $\begin{pmatrix} 1 \\ 1 \end{pmatrix}$ est invariant sous l'action de D_{2n}.
- Les représentations ρ_k sont irréductibles pour $1 \leqslant k \leqslant \frac{n}{2} - 1$. En effet, si $W \subset \mathbf{C}^2$ est une sous-représentation de ρ_k de degré 1 et si $v = \begin{pmatrix} x \\ y \end{pmatrix}$ est un générateur de W, alors $\rho_s(v), \rho_r(v) \in W$, d'où

  $$S\begin{pmatrix} x \\ y \end{pmatrix} = \lambda\begin{pmatrix} x \\ y \end{pmatrix}, \quad R_k\begin{pmatrix} x \\ y \end{pmatrix} = \mu\begin{pmatrix} x \\ y \end{pmatrix}, \qquad \lambda, \mu \in \mathbf{C}.$$

  On en déduit les relations :

  $$x = \pm y, \qquad \zeta_n^k x = \mu x, \qquad \zeta_n^{-k} y = \mu y,$$

  d'où on tire que $x = y = 0$.
- Les représentations ρ_k où $1 \leqslant k \leqslant n/2 - 1$ sont deux à deux non isomorphes car les matrices $\rho_k(r)$ n'ont pas les mêmes valeurs propres.

En résumé, nous avons construit $n/2 - 1$ représentations irréductibles

$$\rho_k : D_{2n} \to \mathrm{GL}_2(\mathbf{C}), \qquad 1 \leqslant k \leqslant \frac{n}{2} - 1,$$

ce qui, avec les représentations ψ_i $(1 \leqslant i \leqslant 4)$ nous donne $n/2 + 3$ représentations irréductibles deux à deux non isomorphes de D_{2n}. Comme le nombre de classes de conjugaison de D_{2n} est égal à $n/2 + 3$, on en déduit qu'on a trouvé toutes les représentations irréductibles de D_{2n} à isomorphisme près.

7.4. Le cas de n impair. On commence par déterminer le groupe dérivé et les classes de conjugaison du groupe D_{2n} pour n impair.

Proposition 7.5. *Soit $n \geqslant 3$ un entier impair. Alors :*

i) $Z(D_{2n}) = \{e\}$.

ii) $[D_{2n}, D_{2n}] = C_n$.

iii) *L'abélianisé $D_{2n}/[D_{2n}, D_{2n}]$ de D_{2n} est engendré par la classe $\overline{s}$. En particulier, il est isomorphe à $\mathbf{Z}/2\mathbf{Z}$.*

iv) *D_{2n} admet $\dfrac{n+3}{2}$ classes de conjugaison, à savoir :*

$$\begin{aligned}
&\mathrm{Conj}(e) = \{e\},\\
&\mathrm{Conj}(r^i) = \{r^i, r^{-i}\}, \quad 1 \leqslant i \leqslant \frac{n-1}{2},\\
&\mathrm{Conj}(s) = sC_n.
\end{aligned}$$

Preuve. i) La preuve de la proposition 7.3 montre que $x = s^a r^b \in Z(D_{2n})$ si et seulement si $a = 0$ et $r^{2b} = e$. Or, comme $\mathrm{pgcd}(2, n) = 1$, on en déduit que $r^b = e$, d'où $x = e$.

ii) Dans la preuve du point ii) de la proposition 7.3 on a déjà vu que $[D_{2n}, D_{2n}] = \left\langle r^2 \right\rangle$. Comme $\mathrm{pgcd}(2, n) = 1$, l'élément r^2 est un générateur de C_n. Donc $[D_{2n}, D_{2n}] = C_n$.

iii) On déduit de l'assertion précédente que $D_{2n}/[D_{2n}, D_{2n}] = D_{2n}/C_n = \langle \overline{s} \rangle$.

iv) On a $\mathrm{Conj}(e) = \{e\}$. Comme $2 \nmid n$, chaque classe $\mathrm{Conj}(r^i) = \{r^i, r^{-i}\}$ pour $1 \leqslant i \leqslant \frac{n-1}{2}$ contient exactement 2 éléments et ces classes sont 2 à 2 distinctes. En outre,

$$\mathrm{Conj}(s) = \left\{ sr^{2j} \mid 0 \leqslant j \leqslant n-1 \right\}.$$

Comme r^2 engendre C_n, on en déduit que $\mathrm{Conj}(s) = sC_n$. L'union de ces classes coïncide avec D_{2n}. ∎

Il existent exactement deux morphismes $\langle \overline{s} \rangle \to \mathbf{C}^*$: le morphisme trivial $\overline{\psi}_1$ et le morphisme $\overline{\psi}_2$ défini par $\overline{\psi}_2(\overline{s}) = -1$. Comme $D_{2n}/[D_{2n}, D_{2n}] = \langle \overline{s} \rangle$, les représentations de D_{2n} de degré 1 sont données par les caractères

$$\begin{aligned}
&\psi_1(r^i) = 1, && \psi_2(sr^i) = 1,\\
&\psi_2(r^i) = 1, && \psi_2(sr^i) = -1.
\end{aligned}$$

On note que ψ_1 est le caractère trivial.

Les représentations ρ_k ($1 \leqslant k \leqslant \frac{n-1}{2}$) sont irréductibles et deux à deux distinctes. Avec les représentations de degré 1, ça nous donne $\frac{n+3}{2}$ représentations irréductibles de D_{2n}. Comme le nombre de classes de conjugaison de D_{2n} est égal à $\frac{n+3}{2}$, on a trouvé toutes les représentations irréductibles de D_{2n} à isomorphisme près.

.