7 Théorie des groupes, polynômes symétriques, résolution des équations

Version du 13 décembre 2005

27 Théorie des groupes

Nous rassemblons dans cette section un certain nombre de résultats de théorie des groupes qui seront utilisés au fur et à mesure, dans la suite du cours. D'autre part, chacun de ces résultats est important en soi (pour l'Agrégation, par exemple).

27.1 Ordre d'un élément, théorème de Lagrange

Lemme 27.1.1 (Théorème de Lagrange) [1] *Soient G un groupe fini et H un sous-groupe. L'ordre de H divise celui de G ; plus précisément, on a*

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

Démonstration. C'est clair, car G est réunion disjointe des classes à gauche gH, et chacune est de cardinal $|H|$. □

Définition 27.1.2 (Indice d'un sous-groupe) *Le cardinal de G/H s'appelle l'***indice** *de H dans G.*

Définition et proposition 27.1.3 (Ordre d'un élément) *Soient G un groupe arbitraire et $g \in G$. On note $\langle g \rangle$ le sous-groupe engendré par g ; c'est l'ensemble des g^n, pour $n \in \mathbb{Z}$.*

[1] 1736-1813, *cf.* [ChL, §4.2]

*Si $\langle g \rangle$ est fini, son cardinal s'appelle l'***ordre** *de g ; c'est le plus petit entier $d > 0$ tel que $g^d = 1$, on a $\langle g \rangle \cong \mathbb{Z}/d\mathbb{Z}$ et tout $n \in \mathbb{Z}$ tel que $g^n = 1$ est un multiple de d.*

Si $\langle g \rangle$ est infini, il est isomorphe à $\mathbb{Z}$, et dans ce cas on dit que g est d'ordre infini.

Démonstration. L'application $\mathbb{Z} \to \langle g \rangle$, $n \mapsto g^n$ est un morphisme de groupes surjectif. S'il est injectif, c'est un isomorphisme de $\mathbb{Z}$ sur $\langle g \rangle$.

Sinon, son noyau K est un sous-groupe non nul de $\mathbb{Z}$, donc de la forme $d\mathbb{Z}$, où d est le plus petit élément > 0 de K, et le reste de la proposition en découle. □

Corollaire 27.1.4 *Soient G un groupe fini et $g \in G$. Alors g est d'ordre fini, divisant $|G|$. En particulier, si $n = |G|$, alors $g^n = 1$ pour tout $g \in G$.*

Définition 27.1.5 *Soit G un groupe fini, de cardinal n. Le PPCM des ordres des éléments de G s'appelle l'***exposant** *de G. D'après ce qui précède, c'est un diviseur de $|G|$.*

27.2 Groupes en action

Définition 27.2.1 *Soit E un ensemble. L'ensemble* $\mathrm{Bij}(E)$ *des bijections de E sur E forme un groupe, pour la composition des applications.*

Définition 27.2.2 (Action d'un groupe sur un ensemble) *Soient G un groupe et E un ensemble. On dit que G* **agit sur** *E si l'on s'est donné un morphisme de groupes, pas nécessairement injectif, $\phi : G \to \mathrm{Bij}(E)$. Pour tout $g \in G$, $x \in E$, on écrit $g \cdot x$, ou simplement gx, au lieu de $\phi(g)(x)$.*

*L'application $G \times E \to E$, $(g, x) \mapsto gx$ s'appelle l'***action** *de G sur E. On voit facilement que la condition que $\phi : G \to \mathrm{Bij}(E)$ soit un morphisme de groupes équivaut aux deux conditions suivantes : pour tout $x \in E$ et $g, g' \in G$,*

$$(A) \qquad 1 \cdot x = x \qquad \text{et} \qquad g \cdot (g'x) = (gg') \cdot x.$$

Donc, se donner une **action de G sur** *E équivaut à se donner une application $G \times E \to E$ vérifiant les deux conditions ci-dessus.*

Définition 27.2.3 (Points fixes) *Soit G un groupe opérant sur un ensemble X. L'ensemble des points fixes est*

$$X^G = \{x \in X \mid gx = x,\ \forall g \in G\}.$$

Lemme 27.2.4 *Soit G un groupe fini opérant sur un ensemble X et soit $x \in X$. Notons $\mathcal{O}(x)$ l'orbite de x et G_x son stabilisateur. L'application $\phi_x : G \to \mathcal{O}(x)$ induit une bijection $G/G_x \xrightarrow{\sim} \mathcal{O}(x)$ et donc l'on a*

$$|G| = |G_x| \cdot |\mathcal{O}(x)|.$$

Démonstration. Posons $H = G_x$. Pour tout $g \in G$, $h \in H$, on a $\phi_x(gh) = gx = \phi_x(g)$. Par conséquent, ϕ_x induit une application $\psi_x : G/H \to \mathcal{O}(x)$, définie par $\psi_x(gH) = gx$. Cette application est clairement surjective. Reste à voir qu'elle est injective. Pour cela, il faut voir que si $\psi_x(gH) = \psi_x(g'H)$ alors $gH = g'H$. Mais ceci est clair, car si $gx = g'x$ alors $x = g^{-1}g'x$ et donc $g^{-1}g' \in H$, d'où $g' \in gH$ et $g'H = gH$. Ceci prouve la première assertion, et la seconde découle alors du lemme 27.1.1. □

Définition 27.2.5 *Soit G un groupe opérant sur un ensemble X. On dit que l'action est* **transitive** *si les éléments de X forment une seule orbite pour l'action de G.*

Définition 27.2.6 (Action d'un groupe sur une k-algèbre) *Soit k un anneau et soit A une k-algèbre.*

1) Un k-automorphisme de A est un automorphisme d'anneau $\phi : A \xrightarrow{\sim} A$ tel que $\phi(\lambda) = \lambda$ pour tout $\lambda \in k$. L'ensemble des k-automorphismes de A forme un groupe, noté $\mathrm{Aut}_k(A)$.

2) Soit G un groupe arbitraire. On dit que G agit sur la k-algèbre A (sous entendu : par automorphismes d'algèbre) si l'on s'est donné un morphisme de groupes $\phi : G \to \mathrm{Aut}_k(A)$. Ceci équivaut à se donner, pour tout $g \in G$, un automorphisme de k-algèbre $\phi(g)$, de telle sorte que $\phi(gh) = \phi(g)\phi(h)$. Pour $a \in A$ et $g \in G$, on notera simplement $g(a)$ au lieu de $\phi(g)(a)$.

3) On note $A^G = \{a \in A \mid g(a) = a, \forall g \in G\}$. C'est une sous-$k$-algèbre de A, appelée la sous-algèbre des **invariants** *de G.*

Exemple 27.2.7 Le groupe $\mu_n(\mathbb{C})$ des racines n-èmes de l'unité dans $\mathbb{C}$ agit sur $\mathbb{C}[X]$ par $\xi \cdot P(X) = P(\xi X)$, c.-à-d., si $P = a_0 + a_1X + \cdots + a_dX^d$, alors

$$\xi \cdot P = a_0 + a_1\xi X + a_2\xi^2X^2 + \cdots + a_d\xi^dX^d,$$

pour tout $\xi \in \mu_n(\mathbb{C})$. On voit que P est invariant si et seulement si $a_i = 0$ pour $i \notin n\mathbb{Z}$. Par conséquent, la sous-algèbre des invariants est $\mathbb{C}[X^n]$.

27.3 Groupes symétriques et théorème de Cayley

Définition 27.3.1 *On note S_n le groupe des permutations de $\{1,\dots,n\}$, c.-à-d., des bijections de $\{1,\dots,n\}$ sur lui-même. C'est un groupe de cardinal $n!$, car une permutation σ est déterminée par la donnée de $\sigma(1)$, pour lequel il y a n choix, puis de $\sigma(2)$, pour lequel il reste $n-1$ choix, etc.*

Notation 27.3.2 On représente en général un élément τ de S_n par son écriture « à deux lignes » : sur la première ligne, on écrit $1,2,3,\dots,n$, dans cet ordre, et sur la seconde on écrit les nombres $\tau(1),\tau(2),\tau(3),\dots,\tau(n)$. Ainsi, par exemple,

$$\tau = \begin{pmatrix} 123456 \\ 356124 \end{pmatrix}$$

est un élément de S_6. Pour certaines permutations, on utilise une écriture plus condensée, introduite ci-dessous.

Définition 27.3.3 (Transpositions et cycles) *Pour $i \neq j$, on note (ij) la permutation qui échange i et j et laisse les autres éléments inchangés.*

*Plus généralement, pour $r \geq 2$, on dit que τ est un r-**cycle** s'il existe $i_1,\dots,i_r$, deux à deux distincts, tels que $\tau(j) = j$ pour $j \notin \{i_1,\dots,i_r\}$ et*

$$\tau(i_1) = i_2,\ \tau(i_2) = i_3, \cdots, \tau(i_{r-1}) = i_r,\ \tau(i_r) = i_1.$$

Dans ce cas, on note $\tau = (i_1 i_2 \cdots i_r)$, et l'on dit que l'ensemble $\{i_1,\dots,i_r\}$ est le **support** *du cycle τ. Par exemple, dans S_6, (253) et (1635) désignent, respectivement, les permutations suivantes :*

$$\begin{pmatrix} 123456 \\ 152436 \end{pmatrix} \quad et \quad \begin{pmatrix} 123456 \\ 625413 \end{pmatrix}.$$

Si τ est une transposition, il est clair que $\tau^2 = \mathrm{id}$. Plus généralement, si c est un r-cycle, on voit que les éléments $\mathrm{id}, c, \dots, c^{r-1}$ sont deux à deux distincts, et $c^r = \mathrm{id}$. Par conséquent, c est d'ordre r.

Lemme 27.3.4 *Soient $c = (i_1 \cdots i_r)$ un r-cycle et $\tau \in S_n$. Alors $c' = \tau c \tau^{-1}$ est le r-cycle $(\tau(i_1) \cdots \tau(i_r))$.*

Démonstration. C'est clair car si $j \notin \{\tau(i_1),\dots,\tau(i_r)\}$ alors $c\tau^{-1}(j) = \tau^{-1}(j)$ et donc $c'(j) = j$; d'autre part, pour tout $k = 1,\dots,r$ on a $c'(\tau(i_k)) = \tau(i_{k+1})$ (avec la convention $i_{r+1} = i_1$). □

Remarque 27.3.5 Si E est un ensemble quelconque à n éléments, alors le groupe $\mathrm{Bij}(E)$ est isomorphe à S_n. En effet, on peut identifier E à $\{1,\dots,n\}$ en choisissant une numérotation $x_1,\dots,x_n$ des éléments de E.

Proposition 27.3.6 (Théorème de Cayley) *Soit G un groupe fini, de cardinal n. Alors G est isomorphe à un sous-groupe de S_n.*

Démonstration. On fait opérer G sur lui même par translation à gauche ; c.-à-d., pour $g \in G$, soit τ_g l'application $G \to G$, $h \mapsto gh$. C'est une bijection de G sur lui-même (d'inverse $\tau_{g^{-1}}$), et l'application $G \to \mathrm{Bij}(G)$, $g \mapsto \tau_g$, est injective (car $g = \tau_g(1)$), et est un morphisme de groupes puisque

$$\forall g, g', h \in G, \qquad (\tau_g \circ \tau_{g'})(h) = \tau_g(g'h) = gg'h = \tau_{gg'}(h).$$

Ceci prouve la proposition. □

27.4 Décomposition en cycles, engendrement par les transpositions

Remarque 27.4.1 On voit facilement que des cycles de supports disjoints commutent. Par exemple, si $\sigma = (25)$ et $\tau = (1364)$ alors

$$\sigma\tau = \begin{pmatrix} 123456 \\ 356124 \end{pmatrix} = \tau\sigma.$$

Théorème 27.4.2 (Décomposition en cycles de supports disjoints) *Tout élément de S_n s'écrit de façon unique comme produit de cycles de supports disjoints.*

Démonstration. Par récurrence sur n. C'est clair si $n = 2$, car $S_2 = \{\mathrm{id}, (12)\}$. Supposons le théorème démontré pour S_{n-1} et soit $\sigma \in S_n$. Considérons l'orbite sous $\langle\sigma\rangle$ de 1 :

$$E = \{\sigma^i(1) \mid i \geq 1\},$$

et soit r son cardinal. Notons σ_1 la restriction de σ à E ; c'est un r-cycle. Si $r = n$, alors $\sigma = \sigma_1$ est un n-cycle. Sinon, soit σ_2 la restriction de σ à $\{1,\dots,n\} \setminus E$. Par hypothèse de récurrence, σ_2 s'écrit comme un produit de cycles de supports disjoints, et donc il en est de même de $\sigma = \sigma_1\sigma_2$. Ceci prouve l'existence. De plus, si

$$\sigma = c_1 \cdots c_s = c'_1 \cdots c'_t$$

sont deux décompositions de σ en produit de cycles de supports disjoints, alors, quitte à renuméroter les c_i et c'_j, on peut supposer que 1 appartient au support de c_1 et c'_1. Alors c_1 et c'_1 sont tous deux égaux au cycle

$$c = (1\sigma(1)\sigma^2(1)\cdots\sigma^{r-1}(1)),$$

où r est le cardinal de l'orbite sous $\langle\sigma\rangle$ de 1. Notons F le complémentaire de cette orbite dans $\{1,\ldots,n\}$. Alors

$$c_2\cdots c_s = c'_2\cdots c'_t$$

sont deux décompositions en produit de cycles de supports disjoints de $c^{-1}\sigma$, considéré comme élément de $\mathrm{Bij}(F)$. Par hypothèse de récurrence, on obtient que $t = s$ et que $c_i = c'_i$ pour $i = 2,\ldots,s$ (quitte à renuméroter les c'_j). Ceci prouve l'unicité. Le théorème est démontré. □

Théorème 27.4.3 (S_n est engendré par les transpositions) *S_n est engendré par les transpositions $s_i = (i, i+1)$, pour $i = 1,\ldots,n-1$.*

Démonstration. On procède par récurrence sur n. Le résultat est clair pour $n = 2$. Supposons $n \geq 3$ et le résultat établi pour $n-1$. On identifie S_{n-1} au sous-groupe de S_n formé des permutations τ telles que $\tau(n) = n$. Posons $s_i = (i, i+1)$, pour $i = 1,\ldots,n-1$, et notons H le sous-groupe de S_n engendré par les s_i.

Soit $\sigma \in S_n$. Si $\sigma(n) = n$, alors $\sigma \in S_{n-1}$ et donc, par hypothèse de récurrence, σ appartient au sous-groupe engendré par les s_i, pour $i \leq n-2$, donc a fortiori $\sigma \in H$. On peut donc supposer que $\sigma(n) = i < n$. Mais alors, $s_i\sigma(n) = i+1$, et si $i+1 < n$ alors $s_{i+1}s_i\sigma(n) = i+2$, etc. On obtient ainsi que

$$s_{n-1}\cdots s_i\sigma(n) = n.$$

Alors, d'après ce qui précède, $\tau := s_{n-1}\cdots s_i\sigma$ appartient à H et donc $\sigma = s_i\cdots s_{n-1}\tau$ appartient aussi à H. Ceci prouve le théorème. □

Le théorème ci-dessous sera utile plus loin (29.4).

Théorème 27.4.4 *S_n est engendré par chacun des sous-ensembles suivants :*

1) *les transpositions $(1, i)$, pour $i = 2,\ldots,n$;*
2) *pour j fixé, les transpositions (ij), avec $i \neq j$;*
3) *une transposition et un n-cycle arbitraires.*

Démonstration. Pour trois éléments distincts $i, j, k \in \{1, \ldots, n\}$, on a

$$(*) \qquad (jk)(ij)(jk) = (ik).$$

En particulier, on a $(1, i) = (1, i-1)(i-1, i)(1, i-1)$. On en déduit que le sous-groupe engendré par les $(1, i)$ contient $s_1, s_2, \ldots, s_{n-1}$ donc égale S_n. Ceci prouve 1).

Fixons j arbitraire, et soit H_j le sous-groupe engendré par les (ij), pour $i \neq j$. On a vu que $H_1 = S_n$. Pour $j \neq 1$, on a $(ij) = (1j)(1i)(1j)$ pour tout $i \neq j$; par conséquent H_j est conjugué à H_1 donc égale S_n. Ceci prouve 2).

Prouvons 3). Notons H le sous-groupe engendré par τ et c. Traitons d'abord le cas où $\tau = (12)$ et $c = (12 \cdots n)$. Dans ce cas, on a, pour $k = 1, \ldots, n-2$,

$$c^k = \begin{pmatrix} 1 & 2 & 3 & \cdots & n \\ k+1 & k+2 & k+3 & \cdots & k \end{pmatrix}.$$

Par conséquent, d'après le lemme 27.3.4, $c^k(12)c^{-k}$ est la transposition $(k+1, k+2)$. Donc, H contient les transpositions $(i, i+1)$, pour $i = 1, \ldots, n-1$, qui engendrent S_n d'après le théorème 27.4.3. On obtient donc $H = S_n$ dans ce cas.

Maintenant, soient $\tau = (ij)$ et c arbitraires. D'abord, en conjugant si nécessaire τ et c par la transposition $(j, c(i))$, on se ramène au cas où $j = c(i)$.

On se ramène ensuite au cas déjà traité comme suit. Lorsque k décrit $0, 1, \ldots, n-1$, les éléments $c^k(i)$ décrivent $\{1, \ldots, n\}$; on peut donc considérer la permutation $\phi \in S_n$ définie par

$$\phi(r) = c^{r-1}(i), \qquad \text{pour } r = 0, 1, \ldots, n-1.$$

(En particulier, $\phi(1) = i$ et $\phi(2) = c(i) = j$). Alors, la conjugaison par ϕ^{-1} envoie H sur le sous-groupe de S_n engendré par $\phi^{-1}(ij)\phi = (12)$ et

$$\phi^{-1}(ic(i)c^2(i) \cdots c^{n-1}(i))\phi = (12 \cdots n).$$

Celui-ci égale S_n, et donc $H = S_n$. Le théorème est démontré. □

27.5 Action sur $k[X_1, \ldots, X_n]$ et signature

Lemme 27.5.1 *Soit k un anneau commutatif. Tout élément $\sigma \in S_n$ induit un k-automorphisme ϕ_σ de la k-algèbre $k[X_1, \ldots, X_n]$, défini par*

$$(*) \qquad \phi_\sigma(X_i) = X_{\sigma(i)}, \quad \forall i = 1, \ldots, n.$$

L'application $\sigma \mapsto \phi_\sigma$ est un **morphisme de groupes injectif** *; par conséquent, S_n s'identifie à un sous-groupe du groupe des k-automorphismes de $k[X_1, \ldots, X_n]$.*

Démonstration. D'après la propriété universelle de $A := k[X_1, \ldots, X_n]$, il existe, pour tout $\sigma \in S_n$, un unique morphisme de k-algèbres $\phi_\sigma : A \to A$ vérifiant $(*)$. De plus, il résulte de $(*)$ que $\phi_{\mathrm{id}} = \mathrm{id}_A$ et que $\phi_\sigma \circ \phi_\tau = \phi_{\sigma\tau}$. Ceci entraîne, d'une part, que chaque ϕ_σ est un automorphisme de A, d'inverse $\phi_{\sigma^{-1}}$, et, d'autre part, que l'application $\sigma \mapsto \phi_\sigma$ est un morphisme de groupes de S_n dans $\mathrm{Aut}_k(A)$. Enfin, $(*)$ montre aussi que $\phi_\sigma = \mathrm{id}_A$ ssi $\sigma = \mathrm{id}$, et donc $\sigma \mapsto \phi_\sigma$ est un isomorphisme de S_n sur le sous-groupe $\{\phi_\sigma\}_{\sigma \in S_n}$ de $\mathrm{Aut}_k(A)$. □

Notation 1) Pour tout $P \in k[X_1, \ldots, X_n]$, on écrira simplement $\sigma(P)$ au lieu de $\phi_\sigma(P)$.

2) Le groupe à deux éléments est noté $\{\pm 1\}$ en notation multiplicative.

Théorème 27.5.2 (Signature d'une permutation) *Il existe un unique morphisme de groupes surjectif $\varepsilon : S_n \to \{\pm 1\}$ tel que $\varepsilon(\tau) = -1$ pour toute transposition $\tau = (ij)$. On l'appelle la* **signature**.

Démonstration. Soit k un corps de caractérisque $\neq 2$, par exemple $k = \mathbb{Q}$. Alors $1 \neq -1$ dans k et donc $\{1, -1\}$ est un sous-groupe de $k^\times$. On a vu que S_n opère par automorphismes d'algèbre sur $A = k[X_1, \ldots, X_n]$. Considérons le polynôme

$$V_n = \prod_{1 \leq i < j \leq n} (X_i - X_j).$$

Soit $\sigma \in S_n$. Alors $\sigma(V_n) = \prod_{1 \leq i < j \leq n} (X_{\sigma(i)} - X_{\sigma(j)})$ et, pour tout $i < j$,

$$\sigma(X_i - X_j) = \begin{cases} X_{\sigma(i)} - X_{\sigma(j)}, & \text{si } \sigma(i) < \sigma(j); \\ -(X_{\sigma(j)} - X_{\sigma(i)}), & \text{si } \sigma(j) < \sigma(i). \end{cases}$$

On en déduit que

$$(*) \qquad \sigma(V_n) = (-1)^{\ell(\sigma)} V_n,$$

où

$$\ell(\sigma) = |\{i < j \mid \sigma(i) > \sigma(j)\}|$$

est le **nombre d'inversions** de σ. On définit alors la signature de σ par :

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

C'est un morphisme de groupes $S_n \to \{\pm 1\}$. En effet, pour $\sigma, \tau \in S_n$ on a

$$\varepsilon(\sigma\tau) V_n = (\sigma\tau)(V_n) = \sigma(\varepsilon(\tau) V_n) = \varepsilon(\tau)\varepsilon(\sigma) V_n,$$

d'où $\varepsilon(\sigma\tau) = \varepsilon(\sigma)\varepsilon(\tau)$.

D'autre part, pour $i < j$ soit τ_{ij} la transposition qui échange i et j. On vérifie facilement que les inversions de τ_{ij} sont les couples (i,j) et (i,k), (k,j) pour $i < k < j$; leur nombre est $1 + 2(j-i-1)$, d'où $\varepsilon(\tau_{ij}) = -1$.

Enfin, puisque les transpositions engendrent S_n, d'après le théorème 27.4.3, ε est uniquement déterminé. Le théorème est démontré. □

Définition 27.5.3 *1) On dit qu'une permutation $\sigma \in S_n$ est* **paire**, *resp.* **impaire**, *si $\varepsilon(\sigma) = 1$, resp. -1. Ceci équivaut à dire que σ s'écrit comme produit d'un nombre pair (resp. impair) de transpositions.*

2) $\operatorname{Ker}\varepsilon$ *est appelé* **groupe alterné** *d'ordre n, et noté A_n. Il est formé des permutations paires, et est de cardinal $n!/2$.*

Exemple 27.5.4 Pour $n = 2$, $S_2 \cong \{\pm 1\}$ et $A_2 = \{1\}$. Pour $n = 3$, S_3 est un groupe non-commutatif d'ordre 6, et A_3 est isomorphe à $\mathbb{Z}/3\mathbb{Z}$ et formé des permutations $1 = \mathrm{id}$ et c, $c^2 = c^{-1}$, où

$$c = \begin{pmatrix} 123 \\ 231 \end{pmatrix}, \qquad c^2 = c^{-1} = \begin{pmatrix} 123 \\ 312 \end{pmatrix}.$$

27.6 Conjugaison des cycles, générateurs de A_n

Théorème 27.6.1 *Soit $r \leq n$. Tous les r-cycles de S_n sont conjugués, et sont de signature $(-1)^{r-1}$.*

Démonstration. Soit $c = (i_1 i_2 \cdots i_r)$ un r-cycle arbitraire et soit c_0 le r-cycle $(12\cdots r)$. Choisissons une bijection de $\{r+1, \ldots, n\}$ sur $\{1, \ldots, n\} \setminus \{i_1, \ldots, i_r\}$ et soit τ la permutation définie par $\tau(k) = i_k$ pour $k \leq r$ et $\tau(k) = \phi(k)$ pour $k > r$. Alors, on vérifie facilement que $\tau c_0 \tau^{-1} = c$. Ceci prouve la première assertion. En particulier, on a $\varepsilon(c) = \varepsilon(c_0)$. Par conséquent, il suffit de calculer $\varepsilon(c_0)$. Or, on voit facilement que

$$s_1 s_2 \cdots s_{r-1} = c_0,$$

d'où $\varepsilon(c_0) = (-1)^{r-1}$. □

Théorème 27.6.2 (Générateurs de A_n) *On a $A_2 = \{1\}$ et, pour $n \geq 3$, A_n est engendré par les produits de deux transpositions et aussi par les 3-cycles.*

Démonstration. Il est clair que $A_2 = \{1\}$. Supposons $n \geq 3$ et soit $\sigma \in A_n$. D'après le théorème 27.4.3, on peut écrire σ comme un produit

$$s_{i_1} s_{i_2} \cdots s_{i_N} \qquad (\text{où } s_i = (i, i+1)).$$

Comme $\varepsilon(s_i) = -1$ pour tout i, l'entier N ci-dessus est pair, disons $N = 2m$. Par conséquent,

$$\sigma = (s_{i_1} s_{i_2}) \cdots (s_{i_{2m-1}} s_{i_{2m}})$$

appartient au sous-groupe engendré par les produits de deux transpositions. Ceci prouve la première assertion.

D'après le théorème 27.6.1, tout 3-cycle appartient à A_n. Donc, pour établir la deuxième assertion, il suffit de montrer que tout produit $(ij)(pq)$ de deux transpositions appartient au sous-groupe de A_n engendré par les 3-cycles. Trois cas peuvent se produire. Si $\{i, j\} = \{p, q\}$, alors $(ij) = (pq)$ et le produit est l'identité. Si les ensembles $\{i, j\}$ et $\{p, q\}$ ont un élément en commun, on peut supposer que $q = j$. Dans ce cas, on voit facilement que le produit $(ij)(jp)$ envoie p sur i, i sur j, et j sur p, et laisse inchangés les autres nombres ; c'est donc le 3-cycle (ijp).

Enfin, supposons $\{i, j\}$ et $\{p, q\}$ disjoints. Dans ce cas, considérons le produit de 3-cycles $\sigma := (ijp)(jpq)$. On vérifie que σ envoie i sur j, j sur i, p sur q et q sur p, et laisse inchangés les autres nombres. Donc $(ijp)(jpq) = (ij)(pq)$, et ceci achève la preuve de la deuxième assertion. Le théorème est démontré. □

27.7 Groupes résolubles

Soit G un groupe fini. Si H est un sous-groupe de G, on écrira $H \lhd G$ ou bien $G \rhd H$ pour signifier que H est un sous-groupe normal de G.

Définition 27.7.1 *G est* **résoluble** *s'il existe une suite finie de sous-groupes*

$$G = G_0 \rhd G_1 \rhd \cdots \rhd G_r \rhd G_{r+1} = \{1\}$$

telle que le groupe quotient G_i/G_{i+1} soit abélien, pour $i = 0, \ldots, r$.

Définition 27.7.2 *1) Pour $x, y \in G$, on définit leur* **commutateur** *$[x, y] := xyx^{-1}y^{-1}$. On a $[x, y] = 1$ ssi $xy = yx$, c.-à-d., ssi x et y commutent.*

2) On appelle **groupe dérivé** *de G, et on note $D(G)$, le sous-groupe de G engendré par les commutateurs $[x, y]$, pour $x, y \in G$. On a $D(G) = \{1\}$ ssi G est abélien.*

Pour tout morphisme $\phi : G \to G'$, il est clair que $\phi([x,y]) = [\phi(x), \phi(y)]$.

Lemme 27.7.3 1) *On a $D(G) = \phi(D(G))$ pour tout automorphisme de G. En particulier, $D(G)$ est un sous-groupe normal de G.*

2) *Si H est un sous-groupe de G, on a $D(H) \subseteq D(G)$*

3) *Si $\pi : G \to G'$ est un morphisme surjectif, alors $D(G') = \pi(D(G))$.*

4) *Soit $H \lhd G$. Alors G/H abélien $\Leftrightarrow H \supseteq D(G)$.*

Démonstration. 1) Soit ϕ un automorphisme de G. Alors $\phi(D(G))$ est le sous-groupe engendré par les $\phi([x,y]) = [\phi(x), \phi(y)]$, donc égale $D(G)$.

2) H est le sous-groupe engendré par les $[x,y]$, pour $x, y \in H$, donc est contenu dans $D(G)$. Il est clair que $\pi(D(G)) \subseteq D(G')$. Réciproquement, $D(G')$ est engendré par les commutateurs $[\pi(x), \pi(y)] = \pi([x,y])$, donc est contenu dans $\pi(D(G))$. Ceci prouve 3). Enfin, posons $G' = G/H$ et notons π la projection $G \to G'$. Alors

$$G' \text{ abélien } \Leftrightarrow \{1\} = D(G') = \pi(D(G)) \Leftrightarrow D(G) \subseteq H.$$

Ceci prouve 4). □

Définition 27.7.4 *On pose $D^0(G) = G$, $D^1(G) = D(G)$ et pour $i \geq 1$ on définit $D^{i+1}(G) = D(D^i(G))$. D'après ce qui précède, chaque $D^{i+1}(G)$ est normal dans $D^i(G)$ et le quotient $D^i(G)/D^{i+1}(G)$ est abélien. La suite*

$$G \rhd D^1(G) \rhd D^2(G) \rhd \cdots$$

s'appelle la **série dérivée** *de G, et $D^i(G)$ s'appelle le i-ème groupe dérivé de G.*

Proposition 27.7.5 *G est résoluble ssi il existe $r \geq 0$ tel que $D^r(G) = \{1\}$.*

Démonstration. Si $D^r(G) = \{1\}$ alors, comme chaque $D^i(G)/D^{i+1}(G)$ est abélien, il résulte de la définition que G est résoluble. Réciproquement, supposons G résoluble. Alors il existe une suite finie

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

telle que chaque G_i/G_{i+1} soit abélien. Alors, on déduit du lemme précédent (points 4. et 2.) que $D(G) \subseteq G_1$, puis que $D(D(G)) \subseteq D(G_1) \subseteq G_2$, etc. On obtient ainsi, par récurrence, que $D^i(G) \subseteq G_i$ pour tout i. Par conséquent, $D^r(G) = \{1\}$. La proposition est démontrée. □

Corollaire 27.7.6 *Soient G un groupe, H un sous-groupe arbitraire, N un sous-groupe normal, et $G' = G/N$.*

1) *Si G est résoluble, H et G' le sont aussi.*

2) *Réciproquement, si N et G' sont résolubles, G l'est aussi.*

Démonstration. Notons π la projection $G \to G'$. En procédant par récurrence, on déduit du lemme 27.7.3 (points 2. et 3.) que $D^i(H) \subseteq D^i(G)$ et $\pi(D^i(G)) = D^i(G')$ pour tout $i \geq 0$. Par conséquent, si G est résoluble, H et G' le sont aussi.

Réciproquement, supposons N et G' résolubles. Alors, il existe $r, s \geq 1$ tels que $D^s(N) = \{1\}$ et $\{1\} = D^r(G') = \pi(D^r(G))$, d'où $D^r(G) \subseteq N$. Alors $D^{r+s}(G) \subseteq D^s(N) = \{1\}$, et ceci montre que G est résoluble. □

Exemples 27.7.7 1) Le groupe symétrique S_3 est résoluble car $A_3 \cong \mathbb{Z}/3$ et $S_3/A_3 \cong \{\pm 1\}$.

2) **Exercice : S_4 est résoluble**. On note (ij) la permutation qui échange i et j. Montrer que les éléments de A_4 d'ordre ≤ 2 sont l'identité et les trois permutations suivantes : $(12)(34)$, $(13)(24)$ et $(14)(23)$. Montrer que ces 4 éléments forment un groupe isomorphe à $(\mathbb{Z}/2) \times (\mathbb{Z}/2)$, noté V_4, et normal dans A_4. En utilisant le fait que $|A_4| = 12$, en déduire que $A_4/V_4 \cong \mathbb{Z}/3$, puis en conclure que S_4 est résoluble.

27.8 A_n n'est pas résoluble, pour $n \geq 5$

Proposition 27.8.1 *Si $n \geq 5$, tout 3-cycle appartient à $D(A_n)$. Par conséquent, on a $A_n = D(A_n) = D^i(A_n)$, pour tout $i \geq 1$.*

Démonstration. Soit (abc) un 3-cycle arbitraire. Choisissons deux éléments d, e dans $\{1, \ldots, n\} \setminus \{a, b, c\}$; ceci est possible puisque $n \geq 5$. Considérons la permutation

$$\sigma := (adc)(bec)(acd)(bce).$$

Comme (acd), resp. (bce), est l'inverse de (adc), resp. (bec), alors σ est le commutateur de (acd) et (bec), donc appartient à $D(A_n)$. Calculons les images par σ de a, b, c, d, e. On a :

$$\begin{cases} a \to c \to b \\ b \to c \to d \to c \\ c \to e \to c \to a \\ d \to a \to d \\ e \to b \to e \end{cases}$$

et, bien sûr, σ laisse inchangés les autres nombres. Donc, $\sigma = (abc)$!

Comme les 3-cycles engendrent A_n, d'après le théorème 27.6.2, ceci montre que $A_n = D(A_n)$, et donc $A_n = D^i(A_n)$ pour tout $i \geq 1$. La proposition est démontrée. □

Corollaire 27.8.2 *Pour $n \geq 5$, A_n et S_n ne sont pas résolubles.*

Démonstration. Soit $n \geq 5$. A_n n'est pas résoluble, puisque $A_n = D^i(A_n)$ pour tout $i \geq 1$. Par conséquent, S_n ne l'est pas non plus, d'après le corollaire 27.7.6. Plus précisément, comme tout commutateur est de signature 1, on a $D(S_n) \subseteq A_n$ pour tout n, et l'égalité $A_n = D(A_n)$ entraîne a fortiori $A_n = D(S_n)$. □

Remarque 27.8.3 En fait, on a $D(S_n) = A_n$ pour tout n. C'est clair pour $n = 2$, et pour $n \geq 3$ il suffit de montrer que tout 3-cycle (ijk) est un commutateur dans S_n. C'est bien le cas, car $(ijk) = (jk)(ij)(jk)(ij)$.

Définition 27.8.4 *On dit qu'un groupe G est* **simple** *s'il est non abélien et si ses seuls sous-groupes distingués sont $\{1\}$ et G. Dans ce cas, on a nécessairement $D(G) = G$. En particulier, un groupe simple n'est pas résoluble.*

Remarque 27.8.5 On peut montrer, en fait, que A_n est simple pour $n \geq 5$. Voir, par exemple, [Pe1, §I.8] ou [Ja1, Thm. 4.11].

27.9 Groupes abéliens finis

Le théorème fondamental de structure pour les modules de type fini sur un anneau principal vu au chapitre 5 (21.2.2) donne, en particulier, le théorème ci-dessous, puisqu'un groupe abélien fini est un module de type fini et de torsion sur l'anneau principal $\mathbb{Z}$!

Théorème 27.9.1 (Structure des groupes abéliens finis)

1) *Soit A un A-groupe abélien fini. Alors*

$$A \cong \mathbb{Z}/(a_1) \oplus \mathbb{Z}/(a_2) \oplus \cdots \oplus \mathbb{Z}/(a_r),$$

pour des entiers $a_1, \ldots, a_r > 0$ vérifiant $a_i \mid a_{i+1}$ pour $i = 1, \ldots, r-1$, et uniquement déterminés.

2) *Cette décomposition se raffine comme suit. Soit $a_r = p_1^{m_1} \cdots p_n^{m_n}$ la décomposition de a_r en facteurs irréductibles. On a la décomposition primaire*

$$A = \bigoplus_{i=1}^{n} A(p_i),$$

et chaque $A(p_i)$ se décompose en une somme directe

$$A(p_i) = \bigoplus_{s=1}^{t_i} \mathbb{Z}/(p_i)^{n_s(p_i)},$$

où la suite $1 \leq n_1(p_i) \leq \cdots \leq n_{t_i}(p_i)$ est uniquement déterminée. En particulier, $n_{t_i}(p_i) = m_i$ et $\operatorname{Ann} A(p_i) = (p_i^{m_i})$.

D'autre part, on a le lemme suivant.

Lemme 27.9.2 *Pour tout diviseur d de n, le groupe cyclique $\mathbb{Z}/n\mathbb{Z}$ contient un élément x d'ordre d.*

Démonstration. Écrivons $n = dr$; alors l'image $\overline{r}$ de r dans $\mathbb{Z}/n\mathbb{Z}$ est d'ordre $n/r = d$. Plus généralement, pour $m \in \mathbb{Z}^\times$ arbitraire, son image $\overline{m}$ dans $\mathbb{Z}/n\mathbb{Z}$ est d'ordre n/s, où s est le PGCD de m et n.

En effet, écrivons $m = m's$ et $n = n's$; alors m' et n' sont premiers entre eux. Si ℓm est un multiple de n, disons kn, alors

$$\ell m's = \ell m = kn = kn's,$$

d'où $kn' = \ell m'$ et donc n' divise ℓ, d'après le lemme de Gauss. Ceci montre que l'ordre de $\overline{m}$ est $m' = n/s$. □

Corollaire 27.9.3 *Soit A un groupe abélien fini de cardinal n et soit m son* **exposant**, *c.-à-d., le* PPCM *des ordres des éléments de A. Alors, il existe un élément de A d'ordre m. De plus, pour tout diviseur premier p de n, il existe un élément de A d'ordre p.*

Démonstration. D'après le théorème de structure des groupes abéliens finis, on a

$$A \cong \mathbb{Z}/(a_1) \oplus \mathbb{Z}/(a_2) \oplus \cdots \oplus \mathbb{Z}/(a_r),$$

pour des entiers $a_1, \ldots, a_r > 0$ vérifiant $a_i \mid a_{i+1}$ pour $i = 1, \ldots, r-1$. Comme tout élément de $\mathbb{Z}/(a_i)$ a pour ordre un diviseur de a_i, donc de a_r, on voit que l'exposant de A est a_r, d'où la première assertion.

D'autre part, $n = |A|$ égale $a_1 \cdots a_r$ donc les diviseurs premiers de n sont les diviseurs premiers de m. La deuxième assertion découle alors du lemme précédent. □

Remarque 27.9.4 On peut ainsi démontrer le corollaire de façon élémentaire, sans invoquer le théorème de structure, *cf.* un exercice des TD.

27.10 Centre d'un groupe et équation des classes

Définition 27.10.1 (Centre d'un groupe) *Soit G un groupe. On appelle* **centre de** *G, et l'on note $Z(G)$, le sous-ensemble*

$$Z(G) = \{h \in G \mid \forall g \in G,\, hg = gh\}.$$

Lemme 27.10.2 *$Z := Z(G)$ est un sous-groupe de G, tel que $\phi(Z) = Z$ pour tout automorphisme de G. En particulier, $Z(G)$ est un sous-groupe distingué.*

Démonstration. D'abord, $Z(G)$ contient l'élément 1. Soient $z, z' \in Z(G)$ et $g \in G$. D'une part, l'égalité $gz = zg$ entraîne $z^{-1}g = gz^{-1}$. D'autre part, on a $gzz' = zgz' = zz'g$. Ceci montre que $Z(G)$ est un sous-groupe de G. Observons aussi que

$$(\dagger) \qquad Z(G) = \{z \in G \mid \forall g \in G, \quad gzg^{-1} = z\}.$$

Soit ϕ un automorphisme de G. Pour tout $g \in G$, on a

$$\phi(z) = \phi(g)\phi(z)\phi(g)^{-1},$$

et comme $\phi(g)$ parcourt G, ceci montre que $\phi(z) \in Z$, c.-à-d., $\phi(Z) \subseteq Z$. De même, $\phi^{-1}(Z) \subseteq Z$ et donc $\phi(Z) = Z$. Ceci prouve le lemme. □

Remarque 27.10.3 1) G est abélien ssi $G = Z(G)$.

2) Pour un groupe $G \neq \{1\}$ arbitraire, on peut avoir $Z(G) = \{1\}$. C'est le cas, par exemple pour $G = S_3$ (exercice !).

Proposition 27.10.4 (Équation des classes) *Soit G un groupe fini ; on le fait opérer sur lui même par conjugaison, c.-à-d., $g \cdot h = ghg^{-1}$ pour $g, h \in G$. Les orbites sont appelées* **classes de conjugaison**. *Les points fixes sont exactement les éléments de $Z(G)$ et, si l'on désigne par $\mathcal{O}(x_1), \ldots, \mathcal{O}(x_r)$ les orbites dans $G \setminus Z(G)$, on a l'équation des classes :*

$$(**) \qquad |G| = |Z(G)| + \sum_{i=1}^{r} \frac{|G|}{|C_G(x_i)|},$$

où $C_G(x_i) = \{g \in G \mid gx_ig^{-1} = x_i\}$ désigne le **centralisateur** *dans G de x_i.*

Démonstration. Que les points fixes soient exactement les éléments de $Z(G)$ est clair. La seconde assertion résulte du fait que G est la réunion disjointe de $Z(G)$ et des orbites $\mathcal{O}(x_i)$, chacune étant de cardinal $|G|/|C_G(x_i)|$ d'après le lemme 27.2.4. □

27.11 p-groupes et théorèmes de Sylow

Définition 27.11.1 (p-groupes finis) *Soit p un nombre premier. Un groupe fini G est un p-**groupe** si $|G|$ est une puissance de p.*

Lemme 27.11.2 (Points fixes d'un p-groupe) *Soit G un p-groupe fini agissant sur un ensemble fini X. Alors*

$$|X^G| \equiv |X| \mod p.$$

En particulier, si $|X| \notin p\mathbb{Z}$, alors $X^G \neq \emptyset$.

Démonstration. Soit $x \in X \setminus X^G$. Alors, le cardinal de l'orbite Gx est > 1, et divise $|G| = p^n$, donc est divisible par p. Le lemme en découle, puisque X est la réunion disjointe de X^G et des orbites dans $X \setminus X^G$. □

Théorème 27.11.3 (Centre d'un p-groupe fini) *Soit G un p-groupe fini $\neq \{1\}$.*

1) *$Z(G)$ est $\neq \{1\}$, donc contient un élément d'ordre p.*

2) *G possède au moins un sous-groupe distingué d'indice p.*

Démonstration. $Z(G)$ est un groupe abélien, de cardinal divisant $|G| = p^n$. De plus, d'après l'équation des classes (27.10.4) et le lemme précédent, $Z(G)$ est $\neq \{1\}$, donc son cardinal est divisible par p. Il contient donc au moins un élément d'ordre p, d'après le corollaire 27.9.3. Ceci prouve 1).

On démontre 2) par récurrence sur $|G|$. Si G est abélien, il est somme directe de sous-groupes cycliques

$$G = \mathbb{Z}x_1 \oplus \cdots \oplus \mathbb{Z}x_r.$$

Alors le sous-groupe $H = \mathbb{Z}px_1 \oplus \bigoplus_{i>1} \mathbb{Z}x_i$ est d'indice p. On peut donc supposer G non abélien. Alors $G/Z(G)$ est un p-groupe non trivial, de cardinal $< |G|$ d'après 1). Donc, par hypothèse de récurrence, $G/Z(G)$ possède un sous-groupe normal H d'indice p, et l'image réciproque de H dans G est un sous-groupe normal d'indice p. Le théorème est démontré. □

Définition 27.11.4 *Soient G un groupe fini, p un nombre premier divisant $|G|$, et p^n la plus grande puissance de p divisant $|G|$. On appelle p-**sous-groupe de Sylow de** G tout sous-groupe de G de cardinal p^n.*

Que de tels sous-groupes existent n'est pas immédiat ; ceci a été établi en 1872 par Sylow, qui a démontré les points 1), 2) et 3) du théorème ci-dessous. Dans la littérature, ces trois assertions sont parfois appelées les théorèmes I, II et III de Sylow.

Théorème 27.11.5 (Théorèmes de Sylow) *Soient G un groupe fini, p un nombre premier divisant $|G|$, et p^n la plus grande puissance de p divisant $|G|$. Notons $\mathcal{S}_p(G)$ l'ensemble des sous-groupes de G de cardinal p^n. Alors :*

1) *$\mathcal{S}_p(G)$ est non-vide, c.-à-d., il existe au moins un sous-groupe de G de cardinal p^n.*

2) *Tout p-sous-groupe de G est contenu dans un p-sous-groupe de Sylow. De plus, ces derniers sont tous conjugués, c.-à-d., pour tout $H, H' \in \mathcal{S}_p(G)$, il existe $g \in G$ tel que $H' = gHg^{-1}$.*

3) *$|\mathcal{S}_p(G)|$ divise $|G|$ et est congru à 1 modulo p.*

Démonstration. On démontre 1) par récurrence sur $|G|$. Considérons l'équation des classes :

$$(**) \qquad |G| = |Z(G)| + \sum_{i=1}^{r} \frac{|G|}{|C_G(x_i)|},$$

où $\mathcal{O}(x_1), \ldots, \mathcal{O}(x_r)$ sont les classes de conjugaison dans $G \setminus Z(G)$. Comme p divise $|G|$, de deux choses l'une.

i) Si p ne divise pas $|Z(G)|$, alors il existe $i \in \{1, \ldots, r\}$ tel que p ne divise pas $|G|/|C_G(p_i)|$; alors p^n divise le cardinal de $C_G(x_i)$, qui est un sous-groupe propre de G, puisque $x_i \notin Z(G)$. Donc, par hypothèse de récurrence, $C_G(x_i)$ contient un sous-groupe de cardinal p^n.

ii) Si p divise $Z(G)$, alors $Z(G)$ contient un élément x d'ordre p, d'après le corollaire 27.9.3. Comme $gxg^{-1} = x$ pour tout $g \in G$, le sous-groupe $\langle x \rangle$ est normal dans G, et $\overline{G} := G/\langle x \rangle$ est de cardinal $p^{n-1}s < |G|$. Par hypothèse de récurrence, $\overline{G}$ contient un sous-groupe H de cardinal p^{n-1}, et l'image réciproque de H dans G est de cardinal p^n. Ceci prouve 1).

Soit maintenant P un p-sous-groupe de Sylow de G et soit Q un p-sous-groupe arbitraire de G. Alors Q agit par translations à gauche sur $X = G/P$, de cardinal premier à p. Donc, d'après le lemme 27.11.2, X^Q est non vide, c.-à-d., il existe $g \in G$ tel que $QgP = gP$. Alors $g^{-1}Qg \subseteq P$. Ceci prouve la première assertion de 2). Si de plus Q est un p-sous-groupe de Sylow, alors $g^{-1}Qg$ est, comme P, de cardinal p^n et donc $g^{-1}Qg = P$. Ceci prouve 2). En particulier, $\mathcal{S}_p(G)$ est une orbite sous G, donc son cardinal divise celui de G.

Reste à voir que $|\mathcal{S}_p(G)| \equiv 1$ modulo p. Soit $P \in \mathcal{S}_p(G)$. Faisons agir P sur $\mathcal{S}_p(G)$ par conjugaison ; alors P est un point fixe, et toute orbite non-triviale est de cardinal divisible par p (puisque P est un p-groupe). Donc

il suffit de montrer que P est l'unique point fixe de P dans $\mathcal{S}_p(G)$. Soit $Q \in \mathcal{S}_p(G)$ un tel point fixe, alors $xQx^{-1} = Q$ pour tout $x \in P$, c.-à-d., P normalise Q.

Soit N le sous-groupe de G engendré par P et Q ; son ordre divise celui de G et, par conséquent, P et Q sont des p-sous-groupes de Sylow de N. D'une part, Q est normalisé par Q et P, donc est normal dans N. D'autre part, d'après le point 2) appliqué à N, il existe $n \in N$ tel que $nQn^{-1} = P$, d'où $P = Q$. Ceci achève la preuve du point 3) et du théorème. □

On a utilisé dans la preuve de 3) le corollaire ci-dessous de 2).

Corollaire 27.11.6 *Soient G un groupe fini et P un p-sous-groupe de Sylow de G. Si P est normal, c'est l'unique p-sous-groupe de Sylow de G.*

Corollaire 27.11.7 (Théorème de Cauchy) [2] *Soient G un groupe fini et p un diviseur premier de $|G|$. Alors G contient un élément d'ordre p.*

Démonstration. Ceci résulte du premier théorème de Sylow et du théorème 27.11.3. □

Exercice 27.11.8 (Une application des théorèmes de Sylow) Soit G un groupe fini de cardinal 42 ou 84. Montrer que G n'est pas simple (étudier les 7-sous-groupes de Sylow).

Remarque 27.11.9 La démonstration des points 1) et 2) est tirée de [Se, §8.4] ; celle du point 3) de [Pe1, §I.5].

28 Polynômes symétriques et groupes de Galois

On va donner dans le paragraphe suivant une démonstration du « théorème fondamental de l'algèbre » (3.1.1) basée sur la théorie de Galois, le premier théorème de Sylow, et la structure des p-groupes finis 27.11.3. Pour une autre démonstration, voir [Sa], Appendice au Chap. II.

28.1 Une application de Galois plus Sylow : $\mathbb{C}$ est algébriquement clos

Lemme 28.1.1 1) *Tout nombre complexe $z \neq 0$ admet n racines n-ièmes dans $\mathbb{C}$.*

2) *Tout $P \in \mathbb{C}[X]$ de degré 2 est scindé.*

[2] 1789-1857, *cf.* [ChL, §4.2]

3) *Tout $P \in \mathbb{R}[X]$ de degré* **impair** *admet au moins une racine dans $\mathbb{R}$.*

Démonstration. 1) (Ce fait a déjà été utilisé, de façon cruciale, dans la démonstration d'Argand, *cf.* 3.2). Posons $z = re^{i\theta}$, avec $r > 0$ et $\theta \in [0, 2\pi[$, et soit $\sqrt[n]{r}$ la racine n-ième de r dans $\mathbb{R}_+$. Alors, les racines n-èmes de z sont les nombres complexes

$$\sqrt[n]{r}\; e^{i\frac{\theta+2k\pi}{n}}, \qquad k = 0, \ldots, n-1.$$

2) On peut supposer P unitaire. Écrivant

$$P = X^2 - 2aX + b = (X-a)^2 + b - a^2,$$

on voit que les deux racines de P sont $a \pm \sqrt{a^2 - b}$.

3) La fonction $\mathbb{R} \to \mathbb{R}$, $x \mapsto P(x)$ est continue. De plus, comme P est de degré impair, on a $\lim_{x\to\pm\infty} P(x) = \pm\infty$. Donc, d'après le théorème des valeurs intermédiaires, il existe $x_0 \in \mathbb{R}$ tel que $P(x_0) = 0$. □

Démontrons maintenant que $\mathbb{C}$ est algébriquement clos. On rappelle qu'en caractéristique 0, tout polynôme est séparable, (Corollaire 25.2.4).

D'abord, l'extension $\mathbb{R} \subset \mathbb{C}$ est de degré 2 et galoisienne, car $\mathbb{C}$ est le corps de décomposition du polynôme X^2+1. Le groupe de Galois $\mathrm{Gal}(\mathbb{C}/\mathbb{R})$ est d'ordre 2, donc isomorphe à $\mathbb{Z}/2\mathbb{Z}$; il est engendré par la conjugaison complexe $\tau : z \mapsto \overline{z}$, où $\overline{z} = x - iy$ si $z = x + iy$, $x, y \in \mathbb{R}$.

Soit $P \in \mathbb{C}[X]$ un polynôme irréductible et soit K un corps de décomposition de P sur $\mathbb{C}$. D'après le théorème 26.1.5, l'extension $\mathbb{C} \subseteq K$ est galoisienne. Posons $G_1 = \mathrm{Gal}(K/\mathbb{C})$ et $n = [K : \mathbb{C}] = |G_1|$, et écrivons $n = 2^d r$, avec r impair. Alors,

$$[K : \mathbb{R}] = [K : \mathbb{C}]\,[\mathbb{C} : \mathbb{R}] = 2^{d+1} r.$$

D'après le théorème 24.2.5, l'automorphisme τ de $\mathbb{C}$ se prolonge en un automorphisme $\widetilde{\tau}$ de K. Posons $G_2 = \mathrm{Aut}_{\mathbb{R}}(K)$.

Lemme 28.1.2 *L'extension $\mathbb{R} \subset K$ est galoisienne, de groupe G_2.*

Démonstration. En effet, $K^{G_2} \subseteq K^{G_1} \cap K^{\widetilde{\tau}} = \mathbb{C}^{\tau} = \mathbb{R}$. □

Maintenant, d'après le théorème de Sylow, G possède au moins un sous-groupe H de cardinal 2^{d+1}. Alors, $L := K^H$ est de degré r sur $\mathbb{R}$. Soient $x \in L$ et $Q = \mathrm{Irr}_{\mathbb{R}}(x)$ son polynôme minimal sur $\mathbb{R}$. Alors $\deg Q = [\mathbb{R}(x) : \mathbb{R}]$ divise $[L : \mathbb{R}] = r$ donc est impair.

Or, on a vu que tout polynôme réel de degré impair a une racine dans $\mathbb{R}$. Donc, Q étant irréductible, il est de degré 1, d'où $x \in \mathbb{R}$. Ceci prouve que $L = \mathbb{R}$ et donc $r = 1$. Par conséquent,

$$[K : \mathbb{C}] = 2^d.$$

Montrons que $d = 0$. Supposons, au contraire, $d \geq 1$. Dans ce cas, $G_1 = \mathrm{Gal}(K/\mathbb{C})$ est un 2-groupe non trivial donc contient un sous-groupe (distingué) H d'indice 2, d'après le théorème 27.11.3. Alors, $K' = K^H$ est de degré 2 sur $\mathbb{C}$. Soit $x \in K' \setminus \mathbb{C}$; son polynôme minimal $\mathrm{Irr}_{\mathbb{C}}(x)$ est de degré 2 et irréductible dans $\mathbb{C}[X]$. Mais ceci est une contradiction, puisque dans $\mathbb{C}[X]$, tout polynôme de degré 2 est scindé ! Cette contradiction montre que $d = 0$, d'où $[K : \mathbb{C}] = 1$. Ceci montre que $\mathbb{C}$ est algébriquement clos.

28.2 Groupe de Galois d'un polynôme

Théorème 28.2.1 ($\mathrm{Gal}(P/k)$ **est un sous-groupe de** S_n**)**
Soit k un corps et soit $P \in k[X]$ un polynôme, resp. K/k une extension, séparable de degré n. Soit L un corps de décomposition sur k de P, resp. $\widetilde{K}$ une clôture galoisienne de K/k. Alors :

1) $\mathrm{Gal}(P/k) = \mathrm{Gal}(L/k)$ *est isomorphe à un sous-groupe de S_n, donc son ordre divise $n!$.*

1′) $\mathrm{Gal}(\widetilde{K}/k)$ *est isomorphe à un sous-groupe de S_n, donc d'ordre divisant $n!$.*

2) *Si P est irréductible,* $\mathrm{Gal}(P/k)$ *agit transitivement sur les n racines de P et donc son ordre est divisible par n.*

3) *Plus généralement, écrivons $P = P_1^{m_1} \cdots P_r^{m_r}$, où les P_i sont irréductibles et deux à deux distincts. Posons $d_i = \deg P_i$ et $Q = P_1 \cdots P_r$. Alors* $\mathrm{Gal}(P/k) = \mathrm{Gal}(Q/k)$ *est un sous-groupe de*

$$S_{d_1} \times \cdots \times S_{d_r}.$$

Démonstration. Soit K/k une extension séparable de degré n. D'après le théorème de l'élément primitif (26.7.3 ou 25.4.2), $K = k[\xi]$ pour un certain $\xi \in K$, et $Q = \mathrm{Irr}_k(\xi)$ est séparable sur k, de degré n. Soit M un corps de décomposition sur k de P. D'après la preuve du théorème 26.7.1, M est une clôture galoisienne de K/k. Par conséquent, l'assertion 1′) est un cas particulier de l'assertion 1), que nous allons établir.

Soient donc $P \in k[X]$ un polynôme séparable de degré n, et L un corps de décomposition de P sur k. L'extension $k \subseteq L$ est galoisienne, d'après

le deuxième théorème fondamental 26.1.5, et son groupe de Galois est noté $\mathrm{Gal}(P/k)$. Soient $x_1, \ldots, x_n$ les racines de P dans K, et soit $g \in \mathrm{Gal}(P/k)$. Comme $g(P) = P$, alors $g(x_1), \ldots, g(x_n)$ sont les racines de P dans K ; par conséquent, g induit une permutation $\sigma_g \in S_n$ telle que $g(x_i) = x_{\sigma_g(i)}$ pour tout $i = 1, \ldots, n$. On voit facilement que l'application $g \mapsto \sigma_g$ est un morphisme de groupes. De plus, ce morphisme est injectif puisque les x_i engendrent K sur k. Ceci prouve 1) et 1′).

2) Si P est irréductible, ses racines $x_1, \ldots, x_n$ sont deux à deux distinctes et forment l'orbite $\mathcal{O}(x_1)$ de x_1 sous $G := \mathrm{Gal}(P/k)$, d'après le corollaire 26.1.7. D'après le lemme 27.2.4, posant

$$H = \mathrm{Stab}_G(x_1) = \{g \in G \mid g(x_1) = x_1\},$$

l'on a $|G| = |H| \cdot |\mathcal{O}(x_1)| = n|H|$. Ceci prouve 2).

3) Plus généralement, écrivons $P = P_1^{m_1} \cdots P_r^{m_r}$ et, pour $i = 1, \ldots, r$, soient $d_i = \deg P_i$ et $\alpha_{i1}, \ldots, \alpha_{id_i}$ les racines de P_i dans K. Soit $g \in G$. Comme $g(P_i) = P_i$, pour tout i, alors g permute les racines de chaque P_i et donc induit une permutation

$$\sigma_g = (\sigma_{g,1}, \ldots, \sigma_{g,r}) \in S_{d_1} \times \cdots \times S_{d_r}$$

telle que $g(\alpha_{ij}) = \alpha_{i\sigma_{g,i}(j)}$ pour tout i, j. Comme précédemment, l'application $g \mapsto \sigma_g$ est un morphisme de groupes, et est injective puisque les α_{ij} engendrent K sur k. Ceci prouve le point 3). □

Remarque 28.2.2 1) Observons aussi que, pour i fixé, les racines α_{ij} sont deux à deux distinctes, puisque P_i est séparable par hypothèse. Par conséquent, $|\mathrm{Gal}(P/k)|$ est divisible par chaque d_i et donc par leur ppcm.

2) De plus, le polynôme minimal de α_{ij} est P_i. Comme $P_i \neq P_{i'}$ pour $i \neq i'$, ceci entraîne que les α_{ij} sont deux à deux distincts.

28.3 Polynômes symétriques

Dans cette section, sauf mention contraire, k désigne un anneau commutatif arbitraire. On a vu (27.5.1) que S_n s'identifie à un sous-groupe du groupe des k-automorphismes de la k-algèbre $k[X_1, \ldots, X_n]$.

Définition 28.3.1 *Soit $P \in k[X_1, \ldots, X_n]$. On dit que P est un* **polynôme symétrique** *si l'on a $\sigma(P) = P$ pour tout $\sigma \in S_n$, c.-à-d., si P est invariant par toute permutation des variables $X_1, \ldots, X_n$. On note*

$$k[X_1, \ldots, X_n]^{S_n}$$

la sous-algèbre des polynômes symétriques. (On voit facilement que c'est une sous-algèbre.)

Exemple 28.3.2 Soit $n = 2$. Les polynômes $X_1 + X_2$, X_1X_2, et $X_1^2X_2 + X_2^2X_1$ sont symétriques. Le polynôme $X_1 + X_2^2$ ne l'est pas.

Définition 28.3.3 (Polynômes symétriques élémentaires) *On pose :*

$$\begin{aligned} e_1 &= X_1 + \cdots + X_n, \\ e_2 &= \textstyle\sum_{1\le i<j\le n} X_iX_j, \\ &\vdots \\ e_k &= \textstyle\sum_{1\le i_1<\cdots<i_k\le n} X_{i_1}\cdots X_{i_k}, \\ &\vdots \\ e_n &= X_1\cdots X_n. \end{aligned}$$

Ce sont des polynômes symétriques, appelés les **polynômes symétriques élémentaires**.

28.4 Relations entre coefficients et racines d'un polynôme

Soient k un corps et $P = X^n + a_1X^{n-1} + \cdots + a_n$ un polynôme unitaire, de degré $n \ge 1$, à coefficients dans k. Soit K une extension de k dans laquelle P est scindé. Alors, dans $K[X]$, on a l'égalité

$$P = (X - x_1)(X - x_2)\cdots(X - x_n), \tag{1}$$

où $x_1, \ldots, x_n$ sont les racines de P dans K, non nécessairement distinctes, c.-à-d., comptées avec leur multiplicité.

Développons le terme de droite de (1). Le coefficient de X^n est, bien sûr, 1. Celui de X^{n-1} est $-(x_1 + \cdots + x_n)$, c.-à-d., $-e_1(x_1, \ldots, x_n)$, et celui de X^{n-2} est $\sum_{i<j} x_ix_j = e_2(x_1, \ldots, x_n)$. Plus généralement, le coefficient de X^{n-r} est

$$(-1)^r \sum_{1\le i_1<\cdots<i_r\le n} X_{i_1}\cdots X_{i_r} = (-1)^r e_r(x_1, \ldots, x_n).$$

En particulier, le coefficient constant est $(-1)^n e(x_1, \ldots, x_n)$. On a donc obtenu la proposition suivante.

Proposition 28.4.1 (Relation entre coefficients et racines d'un polynôme)

Soient k un corps, $P = X^n + a_1X^{n-1} + \cdots + a_n$ un polynôme unitaire de degré $n \geq 1$, à coefficients dans k, et $x_1, \ldots, x_n$ les racines de P dans une extension K de k. Pour $i = 1, \ldots, n$, on a

$$a_i = (-1)^i \, e_i(x_1, \ldots, x_n).$$

28.5 Le théorème fondamental des polynômes symétriques

Définition 28.5.1 (Éléments algébriquements indépendants) *Soit A une k-algèbre. Des éléments $e_1, \ldots, e_n \in A$ sont dits* **algébriquement indépendants** *sur s'ils vérifient la propriété suivante.*

> *Soient $T_1, \ldots, T_n$ des indéterminées et $P \in k[T_1, \ldots, T_n]$.*
> *Si $P(e_1, \ldots, e_n) = 0$, alors $P = 0$.*

Ceci équivaut à dire que le morphisme de k-algèbres $k[T_1, \ldots, T_n] \to A$ défini par $\phi(T_i) = e_i$ est un isomorphisme ; ceci entraîne, en particulier, que la sous-algèbre de A engendrée par $e_1, \ldots, e_n$ est isomorphe à $k[T_1, \ldots, T_n]$.

Théorème 28.5.2 (Théorème fondamental des polynômes symétriques)
La sous-algèbre $k[X_1, \ldots, X_n]^{S_n}$ des polynômes symétriques est engendrée sur k par les polynômes symétriques élémentaires $e_1, \ldots, e_n$. De plus, ces éléments sont algébriquement indépendants sur k. Donc, tout polynôme symétrique S s'écrit de façon unique comme un polynôme $P(e_1, \ldots, e_n)$. En résumé, on a un isomorphisme

$$k[X_1, \ldots, X_n]^{S_n} \cong k[e_1, \ldots, e_n],$$

et le terme de droite est un anneau de polynômes.

Exemple 28.5.3 Pour $r \geq 1$, posons $S_r = X_1^r + \cdots + X_n^r$. (Les S_r s'appellent les sommes de Newton). On a $S_1 = e_1$, et

$$e_1^2 = \sum_{i=1}^{n} X_i^2 + 2 \sum_{i<j} X_i X_j, \quad \text{d'où } S_2 = e_1^2 - 2e_2. \tag{1}$$

De même,

$$e_1^3 = \sum_{i=1}^{n} X_i^3 + 3 \sum_{i \neq j} X_i^2 X_j + 3! \sum_{i<j<k} X_i X_j X_k.$$

D'autre part,

$$e_1e_2 = \left(\sum_k X_k\right)\left(\sum_{i<j} X_iX_j\right) = \sum_{i<j}(X_i^2X_j + X_iX_j^2) + 3\sum_{i<j<k} X_iX_jX_k.$$

Posant $m_{21} = \sum_{i\neq j} X_i^2X_j$ (voir 28.5.4 plus loin), on en déduit que

$$m_{21} = e_1e_2 - 3e_3 \quad \text{et} \quad S_3 = e_1^3 - 3e_1e_2 + 3e_3. \tag{2}$$

Démonstration. $k[X_1, \ldots, X_n]$ est un k-module libre, de base les monômes $X^\nu := X_1^{\nu_1}\cdots X_n^{\nu_n}$, pour $\nu \in \mathbb{N}^n$. (On rappelle que, dans ce paragraphe, k désigne un anneau commutatif arbitraire.)

Posons $I = \{1, \ldots, n\}$. On regarde $\mathbb{N}^n$ comme l'ensemble des applications $\nu : I \to \mathbb{N}$, $i \mapsto \nu_i = \nu(i)$. On fait agir S_n sur $\mathbb{N}^n$ par la formule :

$$(\sigma\nu)(i) = \nu(\sigma^{-1}(i)), \quad \forall \sigma \in S_n, \nu \in \mathbb{N}^n, i \in I.$$

On vérifie alors que $\sigma(X^\nu) = X^{\sigma(\nu)}$ pour tout ν.

Soit $P \in k[X_1, \ldots, X_n]$ un polynôme symétrique. Écrivons $P = \sum_\nu c_\nu X^\nu$, où les c_ν sont nuls sauf pour un nombre fini d'entre eux. Comme les X^ν sont linéairement indépendants sur k, l'égalité

$$\sum_\nu c_\nu X^\nu = P = \sigma(P) = \sum_\nu c_\nu X^{\sigma(\nu)}$$

entraîne $c_\nu = c_{\sigma(\nu)}$, pour tout $\nu \in \mathbb{N}^n$ et tout $\sigma \in S_n$. Par conséquent, P est combinaison k-linéaire des polynômes symétriques obtenus en additionnant les monômes dans une même orbite :

$$M(\nu) := \sum_{\mu \in S_n\nu} X^\mu.$$

Il est utile, maintenant, de choisir un représentant dans chaque orbite.

Définition 28.5.4 *On dit que $\nu \in \mathbb{N}^n$ est* **dominant** *s'il vérifie $\nu_1 \geq \nu_2 \geq \cdots \geq \nu_n \geq 0$. On notera Λ l'ensemble des n-uplets dominants. Il est clair que toute orbite de S_n dans $\mathbb{N}^n$ contient exactement un élément de Λ. Pour $\lambda \in \Lambda$, on désignera par m_λ l'élément considéré plus haut, c.-à-d.,*

$$m_\lambda = \sum_{\mu \in S_n\lambda} X^\mu.$$

Pour démontrer le théorème, on a besoin d'introduire sur $\mathbb{N}^n$ l'ordre lexicographique, défini comme suit.

Définition 28.5.5 *Soient $\mu, \nu \in \mathbb{N}^n$. On dit que $\mu \leq \nu$ si $\mu = \nu$ ou bien s'il existe $i \in \{1, \ldots, n\}$ tel que $\mu_j = \nu_j$ pour $j < i$, et $\mu_i < \nu_i$. C'est un ordre* **total**, *c.-à-d., quelques soient $\mu, \nu \in \mathbb{N}^n$, on a $\mu \leq \nu$ ou $\nu \leq \mu$. De plus, $\leq$ est* **compatible avec l'addition sur** $\mathbb{N}^n$, *c.-à-d.,*

$$(\dagger) \qquad \left.\begin{array}{c} \mu \leq \nu \\ \mu' \leq \nu' \end{array}\right\} \Longrightarrow \mu + \mu' \leq \nu + \nu'.$$

D'autre part, soit λ un n-uplet dominant. On voit facilement que λ est l'unique élément maximal, pour l'ordre $\leq$, de l'orbite $S_n\lambda$. C.-à-d., on a :

$$(*) \qquad \forall \lambda \in \Lambda,\ \forall \mu \in S_n\lambda, \qquad \mu \leq \lambda.$$

Le point crucial dans la démonstration du théorème 28.5.2 est le lemme suivant.

Lemme 28.5.6 (Lemme-clé) *Pour tout $\lambda, \lambda' \in \Lambda$, on a*

$$m_\lambda m_{\lambda'} = m_{\lambda+\lambda'} + \sum_{\substack{\theta \in \Lambda \\ \theta < \lambda+\lambda'}} c_\theta m_\theta.$$

Démonstration. D'une part, il résulte de $(*)$ et $(\dagger)$ que

$$(1) \qquad m_\lambda m_{\lambda'} = X^{\lambda+\lambda'} + \sum_{\substack{\mu \in \mathbb{N}^n \\ \mu < \lambda+\lambda'}} c_\mu X^\mu.$$

D'autre part, écrivons

$$(2) \qquad m_\lambda m_{\lambda'} = \sum_{\theta \in \Lambda} a_\theta m_\theta,$$

où $a_\theta = 0$ sauf pour un nombre fini d'indices. Posons $E := \{\theta \in \Lambda \mid a_\theta \neq 0\}$; c'est un ensemble fini non-vide. Comme l'ordre lexicographique $\leq$ est un ordre total, E admet un unique élément maximal θ_0. On peut donc écrire :

$$(3) \qquad m_\lambda m_{\lambda'} = a_{\theta_0} m_{\theta_0} + \sum_{\substack{\theta \in \Lambda \\ \theta < \theta_0}} a_\theta m_\theta.$$

Alors, d'après $(*)$, le monôme X^{θ_0} n'apparaît que dans m_{θ_0}, et θ_0 est un élément maximal de l'ensemble des $\mu \in \mathbb{N}^n$ tels que X^μ intervienne avec un

coefficient non nul dans l'écriture de $m_\lambda m_{\lambda'}$. Comparant avec (1), on obtient que $\theta_0 = \lambda + \lambda'$ et $a_{\theta_0} = 1$. On obtient donc que

$$m_\lambda m_{\lambda'} = m_{\lambda+\lambda'} + \sum_{\substack{\theta\in\Lambda \\ \theta<\lambda+\lambda'}} a_\theta m_\theta.$$

Ceci prouve le lemme. □

On peut maintenant terminer la démonstration du théorème 28.5.2. Comme $e_1, \ldots, e_n$ sont invariants par S_n, la sous-algèbre qu'ils engendrent, notée $k[e]$, est contenue dans la sous-algèbre des invariants. Pour montrer l'inclusion réciproque

$$k[X_1, \ldots, X_n]^{S_n} \subseteq k[e] := k[e_1, \ldots, e_n],$$

il suffit de montrer que m_λ est un polynôme en $e_1, \ldots, e_n$, pour tout $\lambda \in \Lambda$. On va montrer ceci par récurrence sur

$$N(\lambda) := \lambda_1 + \cdots + \lambda_n.$$

Si $N(\lambda) = 0$, alors $\lambda = 0$ et $m_\lambda = 1$. Pour $i = 1, \ldots, n$, posons

$$\varepsilon_i = (1, \ldots, 1, 0, \ldots, 0),$$

où 1 apparaît i fois, et observons que $m_{\varepsilon_i} = e_i$.

Soit maintenant $N \geq 2$ et supposons le résultat établi pour tout $\theta \in \Lambda$ tel que $N(\theta) < N$. Soit $\lambda \in \Lambda$ tel que $N(\lambda) = N$. Si $\lambda = (d, \ldots, d) = d\varepsilon_n$, alors $m_\lambda = e_n^d$. Sinon, soit i l'unique entier ≥ 1 tel que

$$\lambda_1 = \cdots = \lambda_i > \lambda_{i+1} \geq \cdots \lambda_n.$$

Posons $\lambda' = \lambda - \varepsilon_i$. Alors λ' est dominant, et est $< \lambda$. De plus, d'après le lemme précédent, l'on a

$$m_\lambda = e_i m_{\lambda'} - \sum_{\substack{\theta\in\Lambda \\ \theta<\varepsilon_i+\lambda'=\lambda}} a_\theta m_\theta.$$

Par hypothèse de récurrence, $m_\theta \in k[e]$, pour tout $\theta < \lambda$, y compris $\theta = \lambda'$. L'égalité ci-dessus montre alors que $m_\lambda \in k[e]$ Ceci prouve la première assertion du théorème.

Il reste à voir que $e_1, \ldots, e_n$ sont algébriquement indépendants sur k. Soit $P \in k[T_1, \ldots, T_n]$ non nul. Écrivons

$$P = \sum_{\nu\in\mathbb{N}^n} c_\nu T^\nu,$$

et soit $E = \{\nu \mid c_\nu \neq 0\}$. C'est un ensemble fini non vide. Comme, pour $i = 1, \ldots, n$,

$$e_i = X_1 X_2 \cdots X_i + \text{ monômes plus petits},$$

on déduit de (†) que, pour tout $\nu \in \mathbb{N}^n$,

$$e_1^{\nu_1} \cdots e_n^{\nu_n} = X_1^{\nu_1+\cdots+\nu_n} X_2^{\nu_2+\cdots+\nu_n} \cdots X_n^{\nu_n} + \text{ monômes plus petits.}$$

Ceci conduit à considérer sur $\mathbb{N}^n$ l'ordre $\preceq$ suivant. Observons que l'application $\phi : \mathbb{N}^n \to \mathbb{N}^n$,

$$(\nu_1, \ldots, \nu_n) \mapsto (\sum_{i=1}^n \nu_i, \sum_{i=2}^n \nu_i, \ldots, \nu_n)$$

est injective, car la donnée de $\phi(\nu)$ permet de retrouver ν_n, puis ν_{n-1}, etc. On pose alors

$$\nu \preceq \nu' \Longleftrightarrow \phi(\nu) \leq \phi(\nu');$$

c'est une relation d'ordre sur $\mathbb{N}^n$. Soit ν_0 un élément maximal de E pour $\preceq$. Alors $c_{\nu_0} \neq 0$, et $P(e_1, \ldots, e_n)$ égale $c_{\nu_0} X^{\nu_0}$ plus une combinaison linéaire finie de monômes X^μ, avec $\mu < \nu_0$ pour l'ordre lexicographique. Par conséquent, $P(e_1, \ldots, e_n) \neq 0$. Ceci montre que $e_1, \ldots, e_n$ sont algébriquement indépendants sur k. Le théorème est démontré. □

28.6 Invariants dans le corps des fractions

Lemme 28.6.1 *Soient A un anneau intègre et K son corps des fractions. Tout automorphisme τ de A se prolonge de façon unique en un automorphisme $\widetilde{\tau}$ de K. De plus, l'application $\tau \mapsto \widetilde{\tau}$ est un morphisme injectif de groupes.*

Démonstration. Soit $\tau \in \mathrm{Aut}(A)$ et soient $a, b \in$, avec $b \neq 0$. L'égalité $a = (ab^{-1})b$ dans K montre que toute extension $\widetilde{\tau}$ de τ doit vérifier

$$(*) \qquad \widetilde{\tau}(ab^{-1}) = \tau(a)\tau(b)^{-1}.$$

Réciproquement, on peut définir une application $\widetilde{\tau} : K \to K$ par la formule ci-dessus. Elle est bien définie, car si $ab^{-1} = cd^{-1}$ alors $ad = bc$, d'où $\tau(a)\tau(d) = \tau(b)\tau(c)$.

On vérifie alors sans peine que $\widetilde{\tau}$ est un automorphisme de K. De plus, $(*)$ montre que $\widetilde{\mathrm{id}_A} = \mathrm{id}_K$ et que $\widetilde{\sigma\tau} = \widetilde{\sigma}\widetilde{\tau}$. Donc $\tau \mapsto \widetilde{\tau}$ est un morphisme de groupes, de $\mathrm{Aut}(A)$ vers $\mathrm{Aut}(K)$. Il est de plus injectif, puisque $\widetilde{\tau}(a) = \tau(a)$, pour tout $a \in A$. □

Proposition 28.6.2 *Soient A un anneau intègre, K son corps des fractions, et G un groupe* **fini** *agissant par automorphismes sur A.*

1) *Tout élément de K s'écrit sous la forme a/b, où $b \in A^G$.*

2) *Par conséquent, $K^G = \mathrm{Frac}(A^G)$.*

Démonstration. 1) Soit $x = c/d$ dans K. Comme G est fini, on peut écrire

$$x = \frac{c}{d} = \frac{c \prod_{g \neq 1} g(d)}{\prod_{g \in G} g(d)},$$

et ceci prouve 1). D'autre part, il est clair que $\mathrm{Frac}(A^G) = \{ab^{-1} \mid a, b \in A^G,\ b \neq 0\}$ est un sous-corps de K^G. Réciproquement, si $x \in K^G$, on peut écrire, d'après 1), $x = a/b$, avec $b \in A^G$. Alors, pour tout $g \in G$, l'égalité $g(x) = x$ entraîne $g(a) = a$. Donc $a \in A^G$ et $x \in \mathrm{Frac}(A^G)$. Ceci prouve la proposition. □

28.7 Fractions rationnelles symétriques

Soit k un corps et soient $X_1, \ldots, X_n$ des indéterminées. Le groupe symétrique S_n opère par automorphismes dans $k[X_1, \ldots, X_n]$ et donc dans son corps des fractions $k(X_1, \ldots, X_n)$. On rappelle que $e_1, \ldots, e_n$ désignent les polynômes symétriques élémentaires.

Théorème 28.7.1 (Théorème des fractions rationnelles symétriques)

1) *On a $k(X_1, \ldots, X_n)^{S_n} = k(e_1, \ldots, e_n)$.*

2) *Par conséquent, l'extension $k(e_1, \ldots, e_n) \subset k(X_1, \ldots, X_n)$ est galoisienne, de groupe S_n.*

Démonstration. 1) résulte de la proposition précédente et du théorème fondamental des polynômes symétriques. Le point 2) découle alors du théorème d'Artin. □

Remarque 28.7.2 Soit X une **autre** indéterminée ; considérons le polynôme suivant, à coefficients dans le corps $k(e_1, \ldots, e_n)$,

$$(*) \qquad Q = X^n - e_1 X^{n-1} + \cdots + (-1)^n e_n.$$

Dans l'extension $k(e_1, \ldots, e_n) \subset k(X_1, \ldots, X_n)$, ce polynôme a pour racines $X_1, \ldots, X_n$, qui sont deux à deux distinctes. Par conséquent, Q est séparable sur le corps $k(e) := k(e_1, \ldots, e_n)$.

28.8 L'équation générale de degré n

Soient k un corps, $a_1, \ldots, a_n$ des indéterminées, $K = k(a_1, \ldots, a_n)$ le corps des fractions rationnelles en ces indéterminées. Soit X une autre indéterminée. Considérons le polynôme

$$(**) \qquad P = X^n - a_1 X^{n-1} + \cdots + (-1)^n a_n.$$

L'équation $P(x) = 0$ s'appelle l'équation générale sur k de degré n.

Lorsque $\mathrm{car}(k) = 0$, on voudrait savoir s'il existe une formule « universelle » exprimant les racines de P (dans une extension de K) comme une fonction des a_i obtenue par itération de fonctions polynômiales et de fonctions « extraction de racines d-èmes » (pour tout entier $d \geq 2$). Par exemple, pour $n = 2$, on sait que les racines de

$$X^2 - aX + b = 0$$

sont $(a \pm \sqrt{\Delta})/2$, où Δ désigne le discriminant $a^2 - 4b$. On rappelle que cette formule s'obtient en écrivant

$$X^2 - aX + b = (X - \frac{a}{2})^2 + b - \frac{a^2}{4}.$$

On verra plus loin qu'il existe des formules analogues, mais plus compliquées, pour les équations de degré 3 ou 4, mais qu'il n'existe pas de telles formules pour l'équation générale de degré $n \geq 5$. Commençons par établir le théorème suivant.

Théorème 28.8.1 (S_n est le groupe de Galois de l'équation générale de degré n)
Soit $L = K(x_1, \ldots, x_n)$ un corps de décomposition sur $K = k(a_1, \ldots, a_n)$ du polynôme P ci-dessus. Alors l'extension $K \subset L$ est galoisienne, de groupe S_n. En particulier, les x_i sont deux à deux distincts et P est séparable sur K.

Plus précisément, soient $X_1, \ldots, X_n$ des indéterminées et $e_1, \ldots, e_n$ les polynômes symétriques élémentaires en $X_1, \ldots, X_n$. Alors l'isomorphisme $\phi : k[e_1, \ldots, e_n] \xrightarrow{\sim} k[a_1, \ldots, a_n]$ défini par $\phi(e_i) = a_i$ pour $i = 1, \ldots, n$ se prolonge en des isomorphismes

$$(\dagger) \qquad \begin{array}{ccc} k(e_1, \ldots, e_n) & \subset & k(X_1, \ldots, X_n) \\ \cong\downarrow & & \cong\downarrow \\ k(a_1, \ldots, a_n) & \subset & k(x_1, \ldots, x_n) \end{array}$$

Démonstration. On a vu que les e_i sont algébriquement indépendants donc engendrent un anneau de polynômes. Par la propriété universelle, il existe un unique ϕ comme indiqué, et c'est un isomorphisme puisque les a_i sont algébriquement indépendants. Par conséquent, ϕ induit un isomorphisme des corps de fractions, qu'on désignera encore par ϕ.

Posons $Q = X^n - e_1X^{n-1} + \cdots + (-1)e_n$. Alors, $k(X_i)$ est un corps de décomposition sur $k(e_i)$ de Q. De plus, $\phi(Q) = P$ et, par hypothèse, $L = K(x_i)$ est un corps de décomposition de P sur K. Donc, par le premier théorème fondamental 24.2.5, ϕ se prolonge en un isomorphisme $\psi : k(X_i) \xrightarrow{\sim} L$.

De plus, ψ induit une bijection entre l'ensemble des racines de Q et de P. Par conséquent, les x_i sont deux à deux distincts et P est séparable sur K. Donc, d'après le deuxième théorème fondamental 26.1.5, l'extension $K \subset L$ est galoisienne. Déterminons son groupe de Galois $\mathrm{Gal}(L/K) = \mathrm{Aut}_K(L)$.

On voit facilement que l'application $\tau \mapsto \psi \circ \tau \circ \psi^{-1}$ est un isomorphisme de $G = \mathrm{Aut}_{k(e_i)}(k(X_i))$, dont l'isomorphisme inverse est par $\sigma \mapsto \psi^{-1} \circ \sigma \circ \psi$. On obtient donc, en utilisant le théorème 28.7.1, les isomorphismes

$$\mathrm{Gal}(L/K) \cong \mathrm{Gal}(k(X_1, \ldots, X_n)/k(e_1, \ldots, e_n)) \cong S_n.$$

Ceci prouve le théorème. □

28.9 Discriminant d'un polynôme

Soit A un anneau commutatif. On rappelle que l'opérateur de dérivation $D : A[X] \to A[X]$ est l'application A-linéaire définie par $D(1) = 0$ et $D(X^n) = nX^{n-1}$, pour tout $n \geq 1$.

Lemme 28.9.1 *Soient $P_1, \ldots, P_r \in A[X]$. On a*

$$D(P_1 \cdots P_r) = \sum_{i=1}^{r} P_1 \cdots D(P_i) \cdots P_r.$$

Démonstration. Par récurrence sur r. On a déjà vu le cas $r = 2$ (Lemme 25.2.2). Supposons $r \geq 3$ et le résultat établi pour $r-1$. D'après le cas $r = 2$, l'on a

$$D(P_1 \cdots P_r) = D(P_1)P_2 \cdots P_r + P_1 D(P_2 \cdots P_r),$$

et le résultat découle alors de l'hypothèse de récurrence. □

Théorème 28.9.2 (Discriminant du polynôme général de degré n) *Soient $X_1, \dots, X_n$ des indéterminées, et $e_1, \dots, e_n$ les polynômes symétriques élémentaires en $X_1, \dots, X_n$. Posons $a_i = (-1)^i e_i$. Soient $T_1, \dots, T_n$ d'autres indéterminées. Il existe un unique polynôme $\Delta_n \in \mathbb{Z}[T_1, \dots, T_n]$ tel que*

$$\Delta_n(a_1, \dots, a_n) = \prod_{1 \leq i < j \leq n} (X_i - X_j)^2. \tag{1}$$

Ce polynôme Δ_n est appelé le discriminant du polynôme

$$P = X^n + a_1 X^{n-1} + \cdots + a_n,$$

et est aussi noté disc_P. *De plus, on a*

$$\prod_{i=1}^{n} P'(X_i) = (-1)^{\frac{n(n-1)}{2}} \Delta_n(a_1, \dots, a_n). \tag{2}$$

Démonstration. Posons $\Pi = \prod_{1 \leq i < j \leq n} (X_i - X_j)^2$; c'est un élément de $\mathbb{Z}[X_1, \dots, X_n]^{S_n}$. Donc, d'après le théorème fondamental des polynômes symétriques 28.5.2, il existe un unique polynôme $\Delta_n^- \in \mathbb{Z}[T_1, \dots, T_n]$, tel que

$$\Delta_n^-(e_1, \dots, e_n) = \Pi.$$

Soit ϕ l'automorphisme de $\mathbb{Z}[T_1, \dots, T_n]$ défini par $\phi(T_i) = (-1)^i T_i$ pour tout i, et soit $\Delta_n = \phi(\Delta_n^-)$. Alors, Δ_n est l'unique élément de $\mathbb{Z}[T_1, \dots, T_n]$ vérifiant

$$\Delta_n(a_1, \dots, a_n) = \Delta_n^-(e_1, \dots, e_n) = \Pi.$$

Ceci prouve la première assertion. De plus, comme

$$P = X^n + \sum_{i=1}^{n} (-1)^i e_i X^{n-i} = \prod_{i=1}^{n} (X - X_i),$$

il résulte du lemme précédent que

$$P' = \sum_{i=1}^{n} \prod_{j \neq i} (X - X_j).$$

Donc, pour $i = 1, \dots, n$, on a $P'(X_i) = \prod_{j \neq i} (X_i - X_j)$. Par conséquent,

$$\prod_{i=1}^{n} P'(X_i) = \prod_{i \neq j} (X_i - X_j) = (-1)^{\frac{n(n-1)}{2}} \Pi.$$

Ceci prouve le théorème. □

Corollaire 28.9.3 (Discriminant d'un polynome $P \in k[X]$)
Soient k un corps et $P = X^n + \sum_{i=1}^{n} a_i X^{n-i}$ un polynôme unitaire de degré n à coefficients dans k. Soit L une extension de k dans laquelle P est scindé et soient $x_1, \ldots, x_n$ les racines de P dans L. Alors

$$\prod_{1 \leq i < j \leq n} (x_i - x_j)^2 = \Delta_n(a_1, \ldots, a_n).$$

En particulier, P a une racine multiple ssi $\Delta_n(a_1, \ldots, a_n) = 0$.

Démonstration. Plaçons-nous dans l'anneau $R = \mathbb{Z}[X_1, \ldots, X_n]$ et posons $V_n = \prod_{1 \leq i < j \leq n}(X_i - X_j)$ et $A_i = (-1)^i e_i$ pour $i = 1, \ldots, n$. D'après le théorème précédent, on a dans R l'égalité

$$(*) \qquad V_n^2 = \Delta_n(A_1, \ldots, A_n).$$

Soit ϕ l'unique morphisme d'anneaux de R dans L, défini par $\phi(X_i) = x_i$. Pour $r = 1, \ldots, n$, on a

$$\phi(A_r) = (-1)^r \sum_{i_1 < \cdots < i_r} \phi(X_{i_1} \cdots X_{i_r}) = (-1)^r e_r(x_1, \ldots, x_n) = a_r.$$

Par conséquent, appliquant ϕ à l'égalité $(*)$, on obtient

$$\prod_{1 \leq i < j \leq n} (x_i - x_j)^2 = \Delta_n(a_1, \ldots, a_n).$$

La dernière assertion est alors claire. Le corollaire est démontré. □

Proposition 28.9.4 (Discriminant d'un trinôme $X^n + pX + q$)
Soient k un corps et $p, q \in k$. Le discriminant du trinôme $P = X^n + pX + q$, noté disc_P, égale

$$(-1)^{n(n-1)/2} \left((1-n)^{n-1} p^n + n^n q^{n-1} \right).$$

En particulier, pour

$$\begin{aligned} P &= X^2 + aX + b, \qquad \mathrm{disc}_P = a^2 - 4b; \\ P &= X^3 + pX + q, \qquad \mathrm{disc}_P = -4p^3 - 27q^2. \end{aligned}$$

Démonstration. Soit L une extension de k dans laquelle P est scindé et soient $x_1, \ldots, x_n$ les racines de P dans L. D'après l'égalité (2) du théorème 28.9.2, l'égalité à démontrer est équivalente à la suivante :

$$\prod_{i=1}^{n} P'(x_i) = (1-n)^{n-1} p^n + n^n q^{n-1}.$$

Or, $P'(X) = nX^{n-1} + p$. Supposons d'abord $q \neq 0$. Alors, pour $i = 1, \ldots, n$, l'on a $x_i \neq 0$ et

$$x_i^{n-1} = -p - \frac{q}{x_i}. \tag{1}$$

On en déduit que $\prod_{i=1}^n P'(x_i)$ égale

$$(*) \quad (1-n)^n p^n + \frac{(-n)^n q^n}{x_1 \cdots x_n} + \sum_{r=1}^{n-1} (1-n)^r p^r (-nq)^{n-r} e_{n-r}(x_1^{-1}, \ldots, x_n^{-1}).$$

Or, $x_1 \cdots x_n = (-1)^n q$ et, d'autre part, on voit facilement que

$$e_{n-r}(x_1^{-1}, \ldots, x_n^{-1}) = \frac{e_r(x_1, \ldots, x_n)}{x_1 \cdots x_n} = \begin{cases} 0 & \text{si } 1 \leq r \leq n-2; \\ \dfrac{-p}{q} & \text{si } r = n-1. \end{cases}$$

Par conséquent, on déduit de $(*)$ que $\prod_{i=1}^n P'(x_i)$ égale

$$(**) \qquad n^n q^{n-1} + (1-n)^{n-1} p^n (1 - n + n) = n^n q^{n-1} + (1-n)^{n-1} p^n.$$

Ceci prouve le résultat voulu, lorsque $q \neq 0$. Lorsque $q = 0$, l'argument est analogue : $x_n = 0$ est racine simple, $P'(0) = p$, et pour les autres racines $x_1, \ldots, x_{n-1}$, l'on a $P'(x_i) = (1-n)p$. On obtient ainsi que $\prod_{i=1}^n P'(x_i) = (1-n)^{n-1} p^n$ lorsque $q = 0$. Ceci démontre la proposition. □

28.10 L'extension intermédiaire associée au discriminant

Soient k un corps de caractéristique $\neq 2$, $P \in k[X]$ un polynôme séparable de degré n, K un corps de décomposition de P sur k, et $G = \mathrm{Gal}(K/k)$. Choisissons une numérotation $x_1, \ldots, x_n$ des racines de P dans K et soit ϕ le plongement de G dans S_n défini dans le théorème 28.2.1. Posons

$$d = \prod_{1 \leq i < j \leq n} (x_i - x_j).$$

On a vu que

$$(*) \qquad g(d) = \varepsilon(\phi(g))d, \qquad \forall g \in G.$$

On notera $\varepsilon(g)$ au lieu de $\varepsilon(\phi(g))$. (On peut montrer que $\varepsilon(g)$ ne dépend que de g, et pas de la numérotation $x_1, \ldots, x_n$.)

Théorème 28.10.1 (L'extension intermédiaire $k \subseteq k[d] \subseteq K$)
On suppose $\mathrm{car}(k) \neq 2$. *Soient* P, K, ϕ *et* d *comme plus haut. On a :* $d \in k \Leftrightarrow \phi(G) \subseteq A_n$. *Lorsque* $d \notin k$, *l'extension* $k \subset k[d]$, *resp.* $k[d] \subseteq K$, *est galoisienne, de groupe* $\{\pm 1\}$, *resp.* $\phi(G) \cap A_n$. *De plus,* $\phi(G) \cap A_n$ *est de cardinal* $|G|/2$.

Démonstration. Supposons $\phi(G) \subseteq A_n$. Alors $(*)$ montre que d est invariant par G, donc appartient à k. (Cet argument s'applique également si $\mathrm{car}(k) = 2$.)

Réciproquement, supposons $\phi(G) \not\subseteq A_n = \ker \varepsilon$, et soit $g \in G$ tel que $\phi(g) \notin A_n$. Alors $g(d) = -d$ est différent de d donc $d \notin k$. Posons $\Delta = d^2$. D'après $(*)$, Δ est invariant par G donc appartient à k. (Plus précisément, d'après le corollaire 28.9.3, Δ est le discriminant de P). Le polynôme $X^2 - \Delta$ est séparable sur k, car il a deux racines distinctes d et $-d$. Comme $k[d]$ est le corps de décomposition sur k de $X^2 - \Delta$, on obtient que l'extension $k \subset k[d]$ est galoisienne, de degré 2, et donc de groupe $\{\pm 1\}$.

D'autre part, soit H le fixateur de $k[d]$ dans G. D'après le théorème principal de la théorie de Galois 26.6.1, l'extension $k[d] \subseteq K$ est galoisienne, de groupe H. Or, comme $k[d]$ est engendré sur k par d, l'on a

$$H = \{g \in G \mid g(d) = d\}.$$

Alors, comme $\mathrm{car}(k) \neq 2$, on déduit de $(*)$ que $H = \{g \in G \mid \phi(G) \in A_n\}$, et donc ϕ induit un isomorphisme de H sur $\phi(G) \cap A_n$. Enfin, on obtient que $|H| = |G|/2$, par exemple car $\varepsilon \circ \phi$ induit un isomorphisme $G/H \cong \{\pm 1\}$. Ou bien, en utilisant le théorème d'Artin et la multiplicativité des degrés, on peut dire que

$$|H| = [K : k(d)] = \frac{[K : k]}{2} = \frac{|G|}{2}.$$

Ceci prouve le théorème. □

Remarque 28.10.2 Dans le théorème précédent, l'hypothèse $\mathrm{car}(k) \neq 2$ est nécessaire. En effet, soit $k = \mathbb{F}_2$. Le polynôme $P = X^2 + X + 1$ a deux racines distinctes dans $\mathbb{F}_4$, car son dérivé est $P' = 1$. Par conséquent,

$$\mathrm{Gal}(P/k) = \mathrm{Gal}(\mathbb{F}_4/\mathbb{F}_2) = \{\pm 1\} = S_2.$$

Pourtant, l'on a $\Delta = 1$ et donc d égale 1 et appartient à k.

28.11 L'équation de degré 3

Soit $Y^3 + aY^2 + bY + c$ un polynôme unitaire de degré 3, à coefficients dans un sous-corps de $\mathbb{C}$. En faisant le changement de variable $X = Y + a/3$, on se ramène à l'équation

$$0 = X^3 + pX + q, \tag{1}$$

où $p = b - a^2/3$ et $q = 2a^3/27 - ba/3 + c$. Si $p = 0$, les racines de (1) sont les racines cubiques de $-q$; on supposera donc dans la suite $p \neq 0$.

L'équation (1) a été résolue au XVIe siècle, voir par exemple [Ti] pour une discussion historique. En language moderne, on peut présenter cette solution comme suit. Cherchons X sous la forme $X = y + z$, où y, z sont deux indéterminées auxiliaires. Alors, (1) équivaut à

$$y^3 + z^3 + (3yz + p)(y + z) + q = 0. \tag{2}$$

Par conséquent, si l'on pose $z = -p/3y$, on obtient l'équation

$$y^3 - \frac{p^3}{27y^3} + q = 0,$$

d'où, en multipliant par y^3, l'équation

$$y^6 + qy^3 - \left(\frac{p}{3}\right)^3 = 0. \tag{3}$$

Par conséquent, y^3 est racine de l'équation du second degré

$$T^2 + qT - \left(\frac{p}{3}\right)^3 = 0. \tag{4}$$

De façon plus symétrique, on peut dire que si l'on impose $yz = -p/3$, alors y^3 et z^3 sont solutions de

$$y^3 z^3 = -(p/3)^3 \quad \text{et} \quad y^3 + z^3 = -q,$$

donc sont les racines de l'équation du second degré (4). Quitte à permuter y et z, on peut donc écrire

$$\left\{ \begin{array}{rcl} y^3 & = & -\frac{q}{2} + \frac{1}{2}\sqrt{q^2 + 4\left(\frac{p}{3}\right)^3} = -\frac{q}{2} + \sqrt{\left(\frac{q}{2}\right)^2 + \left(\frac{p}{3}\right)^3} = A, \\ z^3 & = & -\frac{q}{2} \pm \frac{1}{2}\sqrt{q^2 + 4\left(\frac{p}{3}\right)^3} = -\frac{q}{2} - \sqrt{\left(\frac{q}{2}\right)^2 + \left(\frac{p}{3}\right)^3} = B. \end{array} \right.$$

Observons que $AB \neq 0$, puisqu'on a supposé $p \neq 0$. Soit α l'une des racines cubiques dans $\mathbb{C}$ de A ; les deux autres sont $j\alpha$ et $j^2\alpha$, où $j = \exp(2i\pi/3)$. Soit β la racine cubique de B déterminée par la condition $\alpha\beta = -p/3$, c.-à-d., $\beta = -p/3\alpha$. Alors, les racines de l'équation (1) sont

$$(5) \qquad \begin{cases} x_1 &= \alpha + \beta, \\ x_2 &= j\alpha + j^2\beta, \\ x_3 &= j^2\alpha + j\beta. \end{cases}$$

Remarque 28.11.1 Posons $P = X^3 + pX + q$. Soit $K = \mathbb{Q}(p, q)$ le sous-corps de $\mathbb{C}$ engendré par les coefficients de P et soit L le sous-corps de $\mathbb{C}$ engendré par les racines x_1, x_2, x_3 de P dans $\mathbb{C}$ (il contient K puisque $p = x_1x_2 + x_1x_3 + x_2x_3$ et $q = -x_1x_2x_3$). Posons

$$\Delta = -27q^2 - 4p^3 = -3(3 \cdot 2)^2\Delta';$$

c'est le **discriminant** de P. On a vu précédemment que $\Delta = [(x_1 - x_2)(x_1 - x_3)(x_2 - x_3)]^2$; par conséquent l'élément

$$(x_1 - x_2)(x_1 - x_3)(x_2 - x_3) \in L$$

est une racine carrée de Δ.

1) Les formules (5) montrent que les racines de P s'écrivent comme somme de racines cubiques de $-q/2 \pm \sqrt{\Delta'}$. Mais attention, en général ces racines cubiques n'appartiennent pas à L. Toutefois, on verra plus loin que ces racines cubiques sont dans L si le sous-corps $K[\sqrt{\Delta}]$ contient $i\sqrt{3}$ ou, de façon équivalente, $j = (-1 + i\sqrt{3})/2$.

2) Supposons P **irréductible** sur K. Alors $G := \mathrm{Gal}(L/K)$ est un sous-groupe de S_3 d'ordre divisible par 3. Si $d = \sqrt{\Delta}$ appartient à K alors, d'après le théorème 28.10.1, G est contenu dans $A_3 \cong \mathbb{Z}/3\mathbb{Z}$, et donc $G = A_3$. D'autre part, si $d \notin K$, alors $|G| = [L : K]$ est divisible par $[K[d] : K] = 2$, d'où $|G| = 6$ et $G = S_3$. Par conséquent, on a, pour P irréductible de degré 3,

$$\begin{cases} \mathrm{Gal}(P/K) \cong A_3 \cong \mathbb{Z}/3\mathbb{Z} & \text{si } \sqrt{\Delta} \in K; \\ \mathrm{Gal}(P/K) \cong S_3 & \text{si } \sqrt{\Delta} \notin K. \end{cases}$$

29 Équations résolubles par radicaux

Dans cette section, k est un sous-corps de $\mathbb{C}$. En particulier, k est de caractéristique 0 et donc toute extension algébrique de k est séparable.

29.1 Extensions radicales

Définition 29.1.1 *Une suite finie d'extensions de corps $k = K_0 \subseteq K_1 \subseteq \cdots \subseteq K_r$ s'appelle une tour d'extensions (ou une tour de corps).*

Définition 29.1.2 *Soit L une extension algébrique de k contenue dans $\mathbb{C}$. Nous dirons que l'extension $k \subseteq L$ est :*

1) **radicale élémentaire** *s'il existe $a \in L$ et $n \geq 1$ tels que $L = K[a]$ et $a^n \in K$.*

2) **radicale** *s'il existe une tour*

$$k = L_0 \subseteq L_1 \subseteq \cdots \subseteq L_r = L$$

telle que chaque extension $L_{i-1} \subseteq L_i$ soit radicale élémentaire. Donc, ceci équivaut à dire qu'il existe $a_1, \ldots, a_r \in L$ et des entiers $n_1, \ldots, n_r \geq 1$ tels que $L_i = L_{i-1}[a_i]$ et $a_i^{n_i} \in L_{i-1}$.

Définition 29.1.3 *Soit $P \in k[X]$ de degré ≥ 1 et soit K le sous-corps de $\mathbb{C}$ engendré par k et les racines de P dans $\mathbb{C}$. On dit que P (ou l'équation $P(x) = 0$) est* **résoluble par radicaux** *sur k s'il existe une extension radicale $k \subseteq L$ contenant K c.-à-d., telle que $k \subseteq K \subseteq L$.*

Remarque 29.1.4 Comme $\mathbb{C}$ est algébriquement clos, P y est scindé, et donc K est un corps de décomposition de P sur k. De plus, comme P est séparable, puisque $\mathrm{car}(k) = 0$, l'extension $k \subseteq K$ est galoisienne. On rappelle que son groupe de Galois est désigné par $\mathrm{Gal}(P/k)$.

Le but de ce chapitre est de démontrer le théorème suivant.

Théorème 29.1.5 *Si P est résoluble par radicaux, alors le groupe* $\mathrm{Gal}(P/k)$ *est résoluble.*

Remarque 29.1.6 1) Grâce à ce théorème, on pourra donner des exemples d'équations non résolubles par radicaux, en montrant que le groupe de Galois correspondant n'est pas résoluble.

2) En fait, on peut aussi montrer que la réciproque est vraie : si $\mathrm{Gal}(P/k)$ est résoluble, alors P est résoluble par radicaux ; mais ceci est un peu plus difficile. On renvoie pour cela le lecteur intéressé à [Art, §III.C], [ChL, §5.6] ou [Ti, §14.4].

3) L'idée de la démonstration du théorème est très simple, et peut s'expliquer comme suit. Avec les notations précédentes, on suppose K contenu

dans une extension radicale L. **Supposons de plus que** chaque extension $L_i \subseteq L_{i+1}$ soit galoisienne, pour $i = 0, \ldots, r-1$, et que $k \subseteq L_r = L$ le soit aussi. Soit $G = \mathrm{Gal}(L/k)$ et notons G_i le fixateur dans G de L_i. Alors, on peut montrer (voir plus bas) que les hypothèses entraînent que

$$G = G_0 \rhd G_1 \rhd \cdots \rhd G_r = \{1\}$$

et que chaque G_i/G_{i+1} est abélien. Donc, G est résoluble. Enfin, $k \subseteq K \subseteq L$ et l'extension $k \subseteq K$ est galoisienne. Par conséquent, d'après le théorème 26.6.1, $\mathrm{Gal}(P/k)$ est un groupe quotient de G, donc est aussi résoluble.

La difficulté technique est que l'extension radicale $k \subset L$ donnée par l'hypothèse du théorème n'est pas nécessairement galoisienne. Ainsi, pour faire marcher la démonstration, il faut montrer que, partant d'une extension radicale L contenant K, on peut modifier L pour obtenir une extension radicale vérifiant les hypothèses faites plus haut. Ceci est l'objet des paragraphes suivants.

29.2 Adjonction de racines de l'unité

Une extension radicale, même élémentaire, n'est pas nécessairement galoisienne. Par exemple, on a vu dans le chapitre 7 que l'extension $\mathbb{Q} \subset \mathbb{Q}[\sqrt[3]{2}]$ n'est pas galoisienne. Mais on n'a pas ce problème si le corps de base contient suffisamment de racines de l'unité.

On rappelle que, pour tout $n \geq 2$, le groupe des racines n-èmes de l'unité dans $\mathbb{C}$, qu'on note $\mu_n(\mathbb{C})$, est un groupe cyclique d'ordre n. Il est formé des éléments $e^{i\frac{2k\pi}{n}}$, pour $k = 0, \ldots, n-1$. Ses éléments d'ordre exactement n s'appellent les **racines primitives d'ordre** n de l'unité ; ce sont les $e^{i\frac{2k\pi}{n}}$ avec k premier à n. Chaque racine primitive d'ordre n engendre $\mu_n(\mathbb{C})$; par conséquent un sous-groupe de $\mathbb{C}^\times$, resp. un sous-corps de $\mathbb{C}$, contient $\mu_n(\mathbb{C})$ ssi il contient une racine primitive de l'unité d'ordre n.

Définition 29.2.1 *Soit L une extension algébrique de K contenue dans $\mathbb{C}$. Nous dirons que l'extension $K \subseteq L$ est radicale élémentaire* **d'exposant divisant** *n s'il existe $a \in L^\times$ et $n \geq 1$ tels que $L = K[a]$ et $a^n \in K$.*

Cette définition est justifiée par l'observation suivante. L'ensemble des $m \in \mathbb{Z}$ tels que $a^m \in K$ forme un sous-groupe de $\mathbb{Z}$; il est donc de la forme $d\mathbb{Z}$, pour un certain $d \geq 1$, qui divise n puisque $a^n \in K$. On appellera d l'exposant de l'extension ; c'est aussi l'ordre de l'image de a dans le groupe quotient $L^\times/K^\times$.

Proposition 29.2.2 *Soient K un sous-corps de $\mathbb{C}$ et $K \subseteq L$ une extension radicale élémentaire d'exposant divisant n, c.-à-d., $L = K[a]$, avec $a^n \in K$. On suppose que K contient une racine primitive d'ordre n de l'unité ξ. Alors :*

1) *L'extension $K \subseteq K[a]$ est galoisienne, et son groupe de Galois est isomorphe à $\mathbb{Z}/d\mathbb{Z}$, pour un certain d divisant n.*

2*) d est le plus petit entier ≥ 1 tel que $a^d \in K$, et le polynôme minimal de a sur K est $X^d - a^d$.*

Démonstration. L'hypothèse entraîne que $\mu_n(\mathbb{C})$ est contenu dans K donc est égal au groupe $\mu_n(K)$ des racines n-èmes de l'unité dans K. Soit $P = \mathrm{Irr}_K(a)$ le polynôme minimal de a sur K ; par hypothèse, il divise $X^n - a^n$. Ce dernier a toutes ses racines dans $K[a]$: ce sont les $\xi^j a$, pour $j = 0, \ldots, n-1$. Par conséquent, $K[a]$ est un corps de décomposition de P sur K, donc est galoisien sur K. Notons G son groupe de Galois.

Pour tout $g \in G$, $g(a)$ est une racine de $X^n - a^n$ donc égale $\lambda(g)a$, pour un certain $\lambda(g) \in \mu_n(K)$. Pour tout $g, g' \in G$, on a

$$\lambda(gg')a = (g'g)(a) = g'(\lambda(g)a) = \lambda(g)g'(a) = \lambda(g')\lambda(g)a.$$

Par conséquent, l'application $\lambda : G \to \mu_n(K)$ est un morphisme de groupes. Elle est de plus injective, car si $g(a) = g'(a)$ alors $g = g'$, puisque $K[a]$ est engendré sur K par a. Donc G s'identifie au sous-groupe $\lambda(G)$ de $\mu_n(K)$. Comme ce dernier est cyclique, engendré par ξ, alors $\lambda(G)$ est d'ordre d divisant n, et est engendré par $\xi^{n/d}$. Ceci prouve déjà le point 1).

D'autre part, P est de degré $\deg_K(a) = |G| = d$. De plus, pour tout $g \in G$, on a

$$g(a^d) = (g(a))^d = \lambda(g)^d a^d = a^d,$$

puisque $\lambda(g)$ a pour ordre un diviseur de d. Par conséquent, $a^d \in K$ et P divise $X^d - a^d$. Pour une question de degré, on a l'égalité, et d est le plus petit entier ≥ 1 tel que $a^d \in K$. Ceci prouve la proposition. □

La proposition précédente montre l'intérêt d'adjoindre des racines de l'unité. On est ainsi amené à étudier les extensions $K \subseteq K[\xi]$, où ξ est une racine primitive de l'unité d'ordre n, appelées **extensions cyclotomiques**.

Lemme 29.2.3 *Soit n un entier ≥ 2. Le groupe des éléments inversibles de l'anneau commutatif $\mathbb{Z}/n\mathbb{Z}$ est formé des classes $a + n\mathbb{Z}$ telles que a soit premier à n. On notera ce groupe $(\mathbb{Z}/n\mathbb{Z})^\times$ ou $U(n)$.*

Démonstration. Si $\mathrm{pgcd}(a, n) = 1$ alors, d'après le théorème de Bezout, il existe b, c tels que $ba + cn = 1$. Ceci montre que la classe de b modulo n est l'inverse de celle de a.

Réciproquement, s'il existe b tel que $ba \equiv 1$ modulo n, il existe d tel que $ba - 1 = dn$, soit $ba - dn = 1$, et donc a est premier avec n. Ceci prouve le lemme. □

Proposition 29.2.4 (Extensions cyclotomiques) *Soient $K \subseteq \mathbb{C}$ et ξ une racine primitive de l'unité d'ordre n. L'extension $K \subseteq K[\xi]$ est galoisienne et son groupe de Galois est isomorphe à un sous-groupe de $(\mathbb{Z}/n\mathbb{Z})^\times$.*

Démonstration. Posons $L = K[\xi]$. C'est un corps de décomposition du polynôme $X^n - 1$, qui est séparable, puisque son dérivé est nX^{n-1}. (Cet argument vaut aussi en caractéristique p, si p ne divise pas n). Par conséquent, l'extension $K \subseteq L$ est galoisienne. Notons G son groupe de Galois.

Soit $g \in G$. Comme g est un automorphisme du corps K, alors $g(\xi)$ est une racine de l'unité de même ordre que ξ, donc une racine primitive d'ordre n. Par conséquent, comme $\mu_n(\mathbb{C})$ est cyclique, on a $g(\xi) = \xi^{a(g)}$, pour un certain entier $a(g) \in \{1, \ldots, n-1\}$ premier avec n. En effet, si on avait $\mathrm{pgcd}(a(g), n) = d > 1$, alors $\xi^{a(g)}$ serait d'ordre $n/d < n$. On obtient donc une application

$$a : G \to (\mathbb{Z}/n\mathbb{Z})^\times,$$

qui est injective puisque L est engendré sur K par ξ. De plus, cette application est un morphisme de groupes. En effet, pour $g, g' \in G$, on a

$$\xi^{a(g'g)} = (g'g)(\xi) = g'(\xi^{a(g)}) = (g'(\xi))^{a(g)} = \xi^{a(g)a(g')},$$

d'où $a(g'g) = a(g')a(g)$. La proposition est démontrée. □

Remarque 29.2.5 1) Le groupe $G := \mathrm{Gal}(K[\xi]/K)$ dépend du corps K. Par exemple, si K contient déjà ξ, alors $K = K[\xi]$ et $G = \{1\}$.

2) À l'autre extrême, si $K = \mathbb{Q}$, on peut montrer que $G := \mathrm{Gal}(\mathbb{Q}[\xi]/\mathbb{Q})$ est isomorphe à $(\mathbb{Z}/n\mathbb{Z})^\times$. Ceci équivaut au fait que G opère transitivement sur l'ensemble des racines primitives d'ordre n, et aussi au fait que le polynôme cyclotomique Φ_n est irréductible dans $\mathbb{Q}[X]$. Pour cela, voir [Esc, Chap. 9].

Le dernier ingrédient dans la démonstration du théorème 29.1.5 est le suivant.

Proposition 29.2.6 *Considérons des extensions de degré fini $k \subseteq K \subseteq L$, avec $\mathrm{car}(k) = 0$. On suppose :*

1) *il existe $a \in L$ et $n \geq 1$ tels que $L = K[a]$ et $a^n \in K$ (c.-à-d., $K \subseteq L$ est radicale élémentaire d'exposant divisant n)*

2) *$k \subseteq K$ est galoisienne.*

Soit P le polynôme minimal de a **sur** *k et soit Ω un corps de décomposition de P sur K. Alors :*

a) *l'extension $k \subseteq \Omega$ est galoisienne, et*

b) *il existe une tour*

$$K = K_0 \subseteq K_1 \subseteq \cdots \subseteq K_t = \Omega,$$

où chaque extension K_i/K_{i-1} est radicale élémentaire d'exposant divisant n.

Démonstration. Posons $P = \mathrm{Irr}_k(a)$. Rappelons que, puisque $\mathrm{car}(k) = 0$, tout polynôme est séparable. D'autre part, d'après le lemme 25.1.6, K est un corps de décomposition sur k d'un polynôme (séparable !) Q. Alors, on voit que Ω est un corps de décomposition sur k du polynôme QP. Par conséquent, d'après le second théorème fondamental 26.1.5, l'extension $k \subseteq \Omega$ est galoisienne. Ceci prouve a).

Montrons que l'extension $K \subseteq \Omega$ vérifie b). Soient $a = a_1, \ldots, a_m$ les racines de P dans Ω (c.-à-d., les conjugués sur k de a dans Ω). Posons $K_0 = K$ et $K_i = K_{i-1}[a_i]$, pour $i = 1, \ldots, m$. Montrons que chaque extension K_i/K_{i-1} est radicale élémentaire d'exposant divisant n. Pour $i = 1$, c'est l'hypothèse $a^n \in K$. Fixons $i \geq 2$. Il existe, d'après le théorème 24.1.1, un k-isomorphisme $\tau_i : k[a] \xrightarrow{\sim} k[a_i]$. Comme Ω est un corps de décomposition de QP sur k alors, d'après le premier théorème fondamental 24.2.5, τ_i se prolonge en un élément σ_i de $G := \mathrm{Aut}_k(\Omega)$.

Enfin, comme l'extension $k \subseteq K$ est galoisienne, alors $g(K) = K$, pour tout $g \in G$, d'après le théorème principal de la théorie de Galois 26.6.1 (point 3.). Par conséquent, on obtient que $a_i^n = \sigma_i(a^n)$ appartient à K donc, a fortiori, à K_{i-1}. Ceci prouve que l'extension K_i/K_{i-1} est radicale élémentaire, d'exposant divisant n. La proposition est démontrée. □

Remarque 29.2.7 Attention ! Si les extensions $k \subseteq K$ et $K \subseteq L$ sont galoisiennes, il n'est **pas vrai** en général que l'extension $k \subseteq L$ soit galoisienne. Par exemple,

(1) les extensions $\mathbb{Q} \subset \mathbb{Q}[\sqrt{2}]$ et $\mathbb{Q}[\sqrt{2}] \subset \mathbb{Q}[\sqrt[4]{2}]$ sont galoisiennes,

(2) mais l'extension $\mathbb{Q} \subseteq \mathbb{Q}[\sqrt[4]{2}]$ n'est pas galoisienne !

En effet, si $\mathrm{car}(K) \neq 2$ et $a^2 \in K$, l'extension $K \subseteq K[a]$ est galoisienne, car $K[a]$ est le corps de décomposition du polynôme séparable $X^2 - a^2$, dont les racines sont $\pm a$. Ceci prouve (1).

Posons $\alpha = \sqrt[4]{2}$; par définition, c'est la racine carrée dans $\mathbb{R}_+^*$ de $\sqrt{2}$. Par conséquent, on a $L := \mathbb{Q}[\alpha] \subseteq \mathbb{R}$. D'autre part, le polynôme $P = X^4 - 2$ est irréductible sur $\mathbb{Q}$. En effet, il n'a pas de racines dans $\mathbb{Q}$, donc la seule factorisation possible serait de la forme

$$X^4 - 2 = (X^2 + aX + b)(X^2 - aX + c),$$

avec $a, b, c \in \mathbb{Q}$. Alors $bc = -2$, $a(c-b) = 0$ et $b+c-a^2 = 0$, et ceci entraîne $a = 0$ (sinon $b^2 = -2$, impossible), $c = -b$, d'où $b^2 = 2$, contradiction. Par conséquent, P est le polynôme minimal de α sur $\mathbb{Q}$. Or, les racines de P dans $\mathbb{C}$ sont $\pm\alpha$ et $\pm i\alpha$, et les deux dernières ne sont pas dans L puisque $L \subseteq \mathbb{R}$. Ceci montre que l'extension $\mathbb{Q} \subseteq L$ n'est pas quasi-galoisienne.

29.3 Démonstration du théorème 29.1.5

Armé des trois propositions précédentes, on peut maintenant démontrer le théorème 29.1.5. Soient k un sous-corps de $\mathbb{C}$ et K le sous-corps engendré par les racines dans $\mathbb{C}$ d'un polynôme $P \in k[X]$ de degré ≥ 1. On suppose l'équation $P(x) = 0$ résoluble par radicaux, c.-à-d., que K est contenu dans une extension radicale L de k. Donc, il existe des entiers $n_1, \ldots, n_r \geq 1$ et $a_1, \ldots, a_r \in L$, tels que, posant $L_0 = k$ et $L_i = L_{i-1}[a_i]$, on ait $a_i^{n_i} \in L_{i-1}$ pour $i = 1, \ldots, r$. De façon plus condensée, on dira que K est contenu dans la tour

$$k = L_0 \subseteq \cdots \subseteq L_r.$$

En fait, il est commode de s'autoriser aussi l'indice -1 et de poser $k = L_{-1} = L_0$. Notons n le ppcm des n_i et soit ξ une racine primitive de l'unité d'ordre n.

Posons $L'_{-1} = k$ et $L'_i = L_i[\xi]$ pour $i = 0, \ldots, r$. Alors $L'_i = L'_{i-1}[a_i]$, pour $i = 1, \ldots, r$, et l'on a la tour radicale :

$$k = L'_{-1} \subseteq L'_0 \subseteq L'_1 \subseteq \cdots \subseteq L'_r.$$

De plus, d'après la proposition 29.2.4, l'extension $k \subseteq L'_0 = k[\xi]$ est galoisienne, de groupe de Galois abélien.

Pour tout $i = 1, \ldots, r$, notons A_i l'ensemble des racines de $P_i = \mathrm{Irr}_k(a_i)$ (le polynôme minimal de a_i **sur** k) dans $\mathbb{C}$, et posons $L''_0 = L'_0$ et $L''_i = L''_{i-1}[A_i]$. Alors, on a les tours

$$\begin{array}{ccccccc} k \subseteq L'_0 & \subseteq & L'_1 & \subseteq \cdots \subseteq & L'_r \\ \| & & \cap & & \cap \\ L''_0 & \subseteq & L''_1 & \subseteq \cdots \subseteq & L''_r \end{array}$$

De plus, chaque extension $k \subseteq L_i''$ est galoisienne, car L_i'' est un corps de décomposition sur k du polynôme $(X^n - 1)P_1 \cdots P_i$. Alors, il résulte de la proposition 29.2.6 que chaque extension $L_{i-1}'' \subseteq L_i''$ se raffine en une tour d'extensions radicales élémentaires d'exposant divisant n. En mettant bout à bout ces tours et en renumérotant, de la façon évidente, tous les corps apparaissant dans la grande tour ainsi obtenue, on obtient une tour

$$k = \widetilde{L}_{-1} \subseteq L_0'' = \widetilde{L}_0 \subseteq \widetilde{L}_1 \subseteq \cdots \subseteq \widetilde{L}_N = L_r'',$$

où chaque extension $\widetilde{L}_{i-1} \subseteq \widetilde{L}_i$, pour $i = 1, \ldots, N$ est radicale élémentaire d'exposant divisant n, et donc galoisienne, d'après la proposition 29.2.2, puisque L_0'' contient $\mu_n(\mathbb{C})$. De plus, l'extension $k \subseteq L_0'' = k[\xi]$ est galoisienne, de groupe abélien, d'après la proposition 29.2.4.

Enfin, comme on l'a vu plus haut, l'extension $k \subseteq \widetilde{L}_N = L_r''$ est galoisienne. Notons G son groupe de Galois et, pour $i = -1, 0, \ldots, N$, notons G_i le fixateur de $\widetilde{L}_i$. Alors,

$$G = G_{-1} \supseteq G_0 \supseteq \cdots \supseteq G_N = \{1\}.$$

D'après le théorème d'Artin, chaque G_i est le groupe de Galois de $\widetilde{L}_N$ sur $\widetilde{L}_i$. De plus, comme l'extension $\widetilde{L}_i \subseteq \widetilde{L}_{i+1}$ est galoisienne alors, d'après le point 3. du théorème principal de la théorie de Galois 26.6.1, G_{i+1} est un sous-groupe normal de G_i et G_i/G_{i+1} est isomorphe à $\mathrm{Gal}(\widetilde{L}_{i+1}/\widetilde{L}_i)$, dont on a vu qu'il était abélien pour $i = -1$, et cyclique pour $i = 0, \ldots, N$. Par conséquent, G est résoluble !

Finalement, comme $k \subseteq K \subseteq \widetilde{L}_N$ et l'extension $k \subseteq K$ est galoisienne, alors, d'après le point 3. du théorème 26.6.1, à nouveau, $\mathrm{Gal}(K/k)$ est isomorphe au quotient G/H, où H désigne le fixateur dans G de K. Par conséquent, d'après le corollaire 27.7.6, $\mathrm{Gal}(K/k) = \mathrm{Gal}(P/k)$ est résoluble. Ceci achève la démonstration du théorème 29.1.5.

29.4 Un exemple de polynôme $P \in \mathbb{Q}[X]$ non résoluble par radicaux

Proposition 29.4.1 (Critère d'Eisenstein) *Soit $P \in \mathbb{Z}[X]$ un polynôme unitaire de degré $n \geq 1$. Écrivons $P = X^n + \sum_{i=0}^{n-1} a_i X^i$. S'il existe un nombre premier p divisant chaque a_i mais tel que p^2 ne divise pas a_0, alors P est irréductible dans $\mathbb{Z}[X]$ et aussi dans $\mathbb{Q}[X]$.*

Démonstration. Si P est irréductible dans $\mathbb{Z}[X]$, il résulte du Lemme des contenus de Gauss que P est aussi irréductible dans $\mathbb{Q}[X]$; on a vu cela

dans le chapitre 4, Proposition 16.4.7. Il suffit donc de montrer que P est irréductible dans $\mathbb{Z}[X]$.

Supposons $P = QR$, avec $Q, R \in \mathbb{Z}[X]$ tous deux non inversibles. Comme P est unitaire, Q et R sont tous deux de degré ≥ 1 et donc de degré $< n$. Réduisons l'égalité $P = QR$ modulo p, c.-à-d., passons à l'anneau quotient $A := \mathbb{Z}[X]/(p) \cong \mathbb{F}_p[X]$. Comme p divise chaque a_i, on obtient

$$X^n = \pi(Q)\pi(R),$$

où π désigne la projection. Comme A est factoriel et X irréductible, ceci entraîne que $\pi(Q) = \lambda X^d$ et $\pi(R) = \lambda^{-1} X^{n-d}$, pour un certain $d \in \{1, \ldots, n\}$ et $\lambda \in \mathbb{F}_p^\times$. On en déduit que p divise le terme constant de Q et de R, et alors l'égalité $P = QR$ entraîne que p^2 divise a_0, une contradiction. Cette contradiction montre que P est irréductible dans $\mathbb{Z}[X]$. La proposition est démontrée. □

Remarque 29.4.2 Le critère d'Eisenstein s'étend sans difficulté en remplaçant $\mathbb{Z}$ par un anneau factoriel quelconque.

Théorème 29.4.3 *Le polynôme $P = X^5 - 10X + 5$ n'est pas résoluble par radicaux sur $\mathbb{Q}$.*

Démonstration. Soit K le sous-corps de $\mathbb{C}$ engendré par les racines de P et soit $G = \mathrm{Gal}(K/\mathbb{Q})$. C'est un sous-groupe de S_5, d'après le théorème 28.2.1, et son cardinal égale $[K : \mathbb{Q}]$.

D'une part, il résulte du critère d'Eisenstein que P est irréductible dans $\mathbb{Q}[X]$. Par conséquent, pour toute racine a de P, le sous-corps $\mathbb{Q}[a]$ est de degré 5 sur $\mathbb{Q}$. Donc, d'après la multiplicativité des degrés, $|G| = [K : \mathbb{Q}]$ est divisible par 5. Par conséquent, d'après le théorème de Sylow 27.11.5, G contient un sous-groupe d'ordre 5. Alors, tout élément $\neq \mathrm{id}$ de ce sous-groupe est un 5-cycle, donc G contient un 5-cycle.

D'autre part, étudions les variations sur $\mathbb{R}$ de la fonction $x \mapsto P(x)$, ceci sans calculatrice ! Le polynôme dérivé P' égale $5(X^4 - 2)$, donc s'annule exactement deux fois, en $\alpha := \sqrt[4]{2} > 0$ et en $-\alpha < 0$, et P est croissant sur $]-\infty, -\alpha]$ et sur $[\alpha, +\infty[$, et décroissant sur $[-\alpha, \alpha]$. Comme $P(-\alpha) > P(0) = 5$, alors P s'annule exactement une fois dans l'intervalle $]-\infty, 0]$. Évaluons maintenant $P(\alpha)$. On a $1 < \alpha < 2$, donc $\alpha^5 = 2\alpha < 4$ et $-10\alpha < -10$, d'où $P(\alpha) < -1$. Par conséquent, P s'annule une fois entre 0 et α et une fois entre α et $+\infty$.

Donc P a exactement 3 racines réelles, appelons-les x_1, x_2, x_3, et deux racines complexes (non-réelles) conjuguées, x_4 et $x_5 = \overline{x_4}$. Par conséquent, la

conjugaison complexe $z \mapsto \overline{z}$, induit un $\mathbb{Q}$-automorphisme de K, c.-à-d., un élément de G, dont l'image dans S_5 est la transposition $\tau = (45)$. Comme on a vu plus haut que G contient aussi un 5-cycle, il résulte du théorème 27.4.4 que $G = S_5$. Comme S_5 n'est pas résoluble, d'après le corollaire 27.8.2, le théorème 29.1.5 montre que P n'est pas résoluble par radicaux sur $\mathbb{Q}$. □

29.5 La réciproque du théorème 29.1.5

Pour établir la réciproque du théorème 29.1.5, on utilise les deux théorèmes suivants, qui sont intéressants en eux-mêmes.

Théorème 29.5.1 *Soient k un corps arbitraire, K et L deux extensions de degré fini de k, contenues dans une extension Ω de k. On note KL le sous-corps de Ω engendré par K et L ; on l'appelle* **extension composée** *de K et L. On suppose l'extension $k \subseteq K$ galoisienne, et on pose $G = \mathrm{Gal}(K/k)$. Alors l'extension $L \subseteq KL$ est aussi galoisienne, et son groupe de Galois s'identifie au sous-groupe de G fixant les éléments de $K \cap L$.*

Pour la démonstration, voir [Art, §II.0, Th.29] ou [ChL, §5.3]. Ce théorème est parfois appelé « théorème des irrationalités naturelles » (en anglais, "Theorem on Natural irrationalities"), car il généralise un théorème d'Abel (1826) ainsi appelé. Voir [Ti, §13.3, p.219] pour une discussion historique.

Théorème 29.5.2 (Extensions cycliques) *Soient $n \geq 2$ et $K \subset L$ une extension galoisienne de degré n. On suppose que K contient une racine primitive de l'unité d'ordre exactement n, et que $\mathrm{Gal}(L/K) \cong \mathbb{Z}/n\mathbb{Z}$. Alors il existe $a \in L$ tel que $L = K[a]$ et $a^n \in K$, et le polynôme minimal de a sur K est $X^n - a^n$.*

Pour la démonstration, voir [Esc, §§10.4, 10.5] ou [ChL, Thm. 5.4.1].

En utilisant les deux théorèmes précédents, on peut établir la réciproque du théorème 29.1.5, c.-à-d., on obtient le théorème ci-dessous. Pour une démonstration, on renvoie à [Art, §III.C], [ChL, §5.6] ou [Ti, Thm. 14.22]. La notion de résolubilité par radicaux adoptée dans [Ti] est apparemment plus restrictive, mais en fait équivalente, voir [Ti, §13.2], en particulier, Propositions 13.2 et 13.5, et [Esc, §11.5].

Théorème 29.5.3 *Soient k un corps de caractéristique 0 et K un corps de décomposition sur k d'un polynôme non-constant $P \in k[X]$. On pose $G = \mathrm{Gal}(P/k) = \mathrm{Gal}(K/k)$. Alors l'équation $P(x) = 0$ est résoluble par radicaux ssi G est résoluble.*

Table des matières

Bibliographie

[Art] E. Artin, Galois Theory, nouvelle édition, Dover, 1998.

[AM] M. Atiyah, I. G. Macdonald, Commutative algebra, Addison-Wesley, 1969.

[BAlg] N. Bourbaki, Algèbre, Chapitres 4 à 7, Masson, 1981.

[BM] J. Briançon, Ph. Maisonobe, Éléments d'algèbre commutative (niveau M1), Ellipses, 2004.

[De] R. Dedekind, Sur la théorie des nombres entiers algébriques, Gauthier-Villars, 1877 ; traduit en anglais avec une introduction de J. Stillwell dans : Theory of algebraic integers, Cambridge Univ. Press 1996.

[ChL] A. Chambert-Loir, A field guide to algebra, Springer, 2005 ; version française : Algèbre corporelle (sic !), Presses de l'École polytechnique, 2005.

[Die] J. Dieudonné, Cours de géométrie algébrique, tome 2, P.U.F., 1974.

[Dou] A. Douady, R. Douady, Algèbre et théories galoisiennes (2 tomes), Cedic Fernand Nathan, 1977, 2ème éd., Cassini, 2005.

[Elk] R. Elkik, Cours d'algèbre, Ellipses, 2002.

[Esc] J.-P. Escofier, Théorie de Galois, Dunod, 2000.

[Ja1] N. Jacobson, Basic algebra I, W. H. Freeman & Co., 1974.

[Ja2] N. Jacobson, Basic algebra II, W. H. Freeman & Co., 1980.

[Kru] W. Krull, Idealtheorie, Springer Verlag, 1937 (2e édition 1968).

[La] S. Lang, Algebra, Addison-Wesley, 1965. Traduction française de la 3ème édition : Algèbre, Dunod, 2004.

[Ne04] J. Nekovàř, Théorie de Galois, cours UPMC 2003/4, disponible à l'adresse : www.math.jussieu.fr/~nekovar/co/ln

[Pe1] D. Perrin, Cours d'algèbre, E.N.S.J.F. 1981, et 3ème édition, Ellipses, 1996.

[Pe2] D. Perrin, Géométrie algébrique - Une introduction, Inter Éditions/-CNRS Éditions, 1995.

[Sa] P. Samuel, Théorie algébrique des nombres, Hermann, 1967.

[Se] J.-P. Serre, Représentations linéaires des groupes finis, (3ème édition corrigée), Hermann, 1978.

[St] J. Stillwell, Chapitre d'introduction dans [De].

[Ti] J.-P. Tignol, Galois' Theory of algebraic equations, World Scientific, 2001.

[vdW] B. L. van der Waerden, History of algebra from al-Khwarizmi to Emmy Noether, Springer Verlag, 1985.