IX. GROUPES ET POLYNÔMES SYMÉTRIQUES, RÉSOLUTION D'ÉQUATIONS

SÉANCES DU 19, 20, 26 ET 27 NOVEMBRE

19. Théorie des groupes

[(10)] 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 le Capes ou l'Agrégation, par exemple).

19.1. Ordre d'un élément, théorème de Lagrange. —

***Lemme 19.1* (Théorème de Lagrange).** — [(11)] *Soient* G *un groupe fini et* H *un sous-groupe. L'ordre de* H *divise celui de* G *; plus précisément, on a*

$$|\mathrm{G}| = |\mathrm{H}| \cdot |(\mathrm{G}/\mathrm{H})|.$$

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

***Définition 19.2* (Indice d'un sous-groupe).** — Le cardinal de G/H est appelé l'**indice** de H dans G.

***Définition et proposition 19.3* (Ordre d'un élément).** — *Soient* G *un groupe arbitraire et* $g \in \mathrm{G}$. *On note* $\langle g \rangle$ *le sous-groupe engendré par* g *; c'est l'ensemble des* g^n*, pour* $n \in \mathbb{Z}$.

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.*

[(10)] version corrigée du 20/11/07

[(11)] 1736-1813, cf. [**ChL**, § 4.2]

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

Définition 19.5 **(Exposant d'un groupe fini)**. — 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 $|\mathrm{G}|$ et c'est le plus petit entier $m > 0$ tel que $g^m = 1$ pour tout $g \in \mathrm{G}$.

19.2. Groupes en action. —

Définition 19.6. — Soit E un ensemble. L'ensemble Bij(E) des bijections de E sur E forme un groupe, pour la composition des applications.

Définition 19.7 **(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 $\phi : \mathrm{G} \to \mathrm{Bij(E)}$ (pas nécessairement injectif). Pour tout $g \in \mathrm{G}$, $x \in \mathrm{E}$, on écrit $g \cdot x$, ou simplement gx, au lieu de $\phi(g)(x)$.

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

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

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

Définition 19.8 **(Points fixes)**. — Soit G un groupe opérant sur un ensemble X. L'ensemble des points fixes est

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

Lemme 19.9. — *Soit* G *un groupe opérant sur un ensemble* X *et soit* H *un sous-groupe* **normal** *de* G. *Alors :*

1) X^{H} *est stable par l'action de* G.

2) *L'action* $\mathrm{G} \to \mathrm{Bij}(\mathrm{X}^{\mathrm{H}})$ *se factorise en une action de* G/H *sur* X^{H}, *et l'on a :*

$$(\mathrm{X}^{\mathrm{H}})^{\mathrm{G/H}} = \mathrm{X}^{\mathrm{G}}.$$

Démonstration. — Soient $x \in \mathrm{X}^{\mathrm{H}}$, $g \in \mathrm{G}$ et $h \in \mathrm{H}$. Alors

$$h \cdot (gx) = g\,(g^{-1}hg)x = gx \qquad (\text{car } g^{-1}hg \in \mathrm{H})\ .$$

Ceci montre que $gx \in \mathrm{X}^{\mathrm{H}}$, d'où 1). Le point 2) est laissé au lecteur. □

***Définition 19.10* (Orbites et stabilisateurs).** — Soit G un groupe opérant sur un ensemble X, et soit $x \in \mathrm{X}$. L'**orbite** de x est l'ensemble des transformés de x par G :

$$\mathscr{O}(x) = \mathrm{G}x = \{gx \mid g \in \mathrm{G}\}.$$

Le **stabilisateur** de x est le sous-groupe de G suivant :

$$\mathrm{Stab}_{\mathrm{G}}(x) = \{g \in \mathrm{G} \mid gx = x\};$$

on le note aussi G_x.

Lemme 19.11. — *Soit* G *un groupe fini opérant sur un ensemble* X *et soit* $x \in \mathrm{X}$. *L'application* $\phi_x : \mathrm{G} \to \mathscr{O}(x)$ *induit une bijection* $\mathrm{G}/\mathrm{G}_x \xrightarrow{\sim} \mathscr{O}(x)$ *et donc l'on a*

$$|\mathrm{G}| = |\mathrm{G}_x| \cdot |\mathscr{O}(x)|.$$

Démonstration. — Posons $\mathrm{H} = \mathrm{G}_x$. Pour tout $g \in \mathrm{G}$, $h \in \mathrm{H}$, on a $\phi_x(gh) = gx = \phi_x(g)$. Par conséquent, ϕ_x induit une application $\psi_x : \mathrm{G}/\mathrm{H} \to \mathscr{O}(x)$, définie par $\psi_x(g\mathrm{H}) = gx$. Cette application est clairement surjective. Reste à voir qu'elle est injective. Pour cela, il faut voir que si $\psi_x(g\mathrm{H}) = \psi_x(g'\mathrm{H})$ alors $g\mathrm{H} = g'\mathrm{H}$. Mais ceci est clair, car si $gx = g'x$ alors $x = g^{-1}g'x$ et donc $g^{-1}g' \in \mathrm{H}$, d'où $g' \in g\mathrm{H}$ et $g'\mathrm{H} = g\mathrm{H}$. Ceci prouve la première assertion, et la seconde découle alors du lemme 19.1. □

Définition 19.12. — 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 19.13* (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 $\phi : \mathrm{A} \xrightarrow{\sim} \mathrm{A}$ tel que $\phi(\lambda) = \lambda$ pour tout $\lambda \in k$. L'ensemble des k-automorphismes de A forme un groupe, noté $\mathrm{Aut}_k(\mathrm{A})$.

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 $\phi : \mathrm{G} \to \mathrm{Aut}_k(\mathrm{A})$. Ceci équivaut à se donner, pour tout $g \in \mathrm{G}$, un automorphisme de k-algèbre $\phi(g)$, de telle sorte que $\phi(gh) = \phi(g)\phi(h)$. Pour $a \in \mathrm{A}$ et $g \in \mathrm{G}$, on notera simplement $g(a)$ au lieu de $\phi(g)(a)$.

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

Exemple 19.14. — 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 $P = a_0 + a_1 X + \cdots + a_d X^d$, alors

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

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 $\mathbb{C}[X^n]$.

19.3. Groupes symétriques : premières propriétés. —

Définition 19.15. — On note S_n le groupe des permutations de $\{1, \ldots, n\}$, c.-à-d., des bijections de $\{1, \ldots, n\}$ 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.

Remarque 19.16. — Si E est un ensemble quelconque à n éléments, alors le groupe Bij(E) est isomorphe à S_n. En effet, on peut identifier E à $\{1, \ldots, n\}$ en choisissant une numérotation $x_1, \ldots, x_n$ des éléments de E.

Proposition 19.17 **(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. □

Notation 19.18. — On représente en général un élément τ de S_n par son écriture « à deux lignes » : sur la première ligne, on écrit $1, 2, 3, \ldots, n$, dans cet ordre, et sur la seconde on écrit les nombres $\tau(1), \tau(2), \tau(3), \ldots, \tau(n)$. 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 19.19 **(Cycles et transpositions)**. — Pour $i \neq j$, on note (ij) la permutation qui échange i et j et laisse les autres éléments inchangés ; on dit que (ij) est une **transposition**.

Plus généralement, pour $r \geqslant 2$, on dit que τ est un r**-cycle** s'il existe $i_1, \ldots, i_r$, deux à deux distincts, tels que $\tau(j) = j$ pour $j \notin \{i_1, \ldots, i_r\}$ 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 $\{i_1, \ldots, i_r\}$ est le **support** du cycle τ.

Par exemple, dans S_6, (253) et (1635) désignent, respectivement, les permutations suivantes :

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

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 $\mathrm{id}, c, \ldots, c^{r-1}$ sont deux à deux distincts, et $c^r = \mathrm{id}$. Par conséquent, c est d'ordre r.

Proposition 19.20. — *Tous les r-cycles sont conjugués entre eux. Plus précisément, soient $c = (i_1 \cdots i_r)$ un r-cycle et $\tau \in \mathrm{S}_n$. Alors $c' = \tau c \tau^{-1}$ est le r-cycle $(\tau(i_1) \cdots \tau(i_r))$.*

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

Remarque 19.21. — 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 19.22 **(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 $\mathrm{S}_2 = \{\mathrm{id}, (12)\}$. Supposons le théorème démontré pour S_{n-1} et soit $\sigma \in \mathrm{S}_n$. Considérons l'orbite sous $\langle\sigma\rangle$ de 1 :

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

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 $\{1, \ldots, n\} \setminus \mathrm{E}$. 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 $\{1,\dots,n\}$. 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 Bij(F). Par hypothèse de récurrence, on obtient que $t=s$ et que $c_i=c'_i$ pour $i=2,\dots,s$ (quitte à renuméroter les c'_j). Ceci prouve l'unicité. Le théorème est démontré. □

19.4. Engendrement par les transpositions. —

Théorème 19.23 **(S_n est engendré par les transpositions)**. — *Les transpositions $s_i=(i,i+1)$, pour $i=1,\dots,n-1$, engendrent S_n.*

Démonstration. — On procède par récurrence sur n. Le résultat est clair pour $n=2$. Supposons $n\geqslant 3$ 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 $i=1,\dots,n-1$, et notons H le sous-groupe de S_n engendré par les s_i.

Soit $\sigma\in\mathrm{S}_n$. Si $\sigma(n)=n$, alors $\sigma\in\mathrm{S}_{n-1}$ et donc, par hypothèse de récurrence, σ appartient au sous-groupe engendré par les s_i, pour $i\leqslant n-2$, donc a fortiori $\sigma\in\mathrm{H}$. 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. □

Théorème 19.24. — *S_n est engendré par chacun des sous-ensembles suivants :*

1) *les transpositions $(1,i)$, pour $i=2,\dots,n$;*
2) *pour j fixé, les transpositions (ij), avec $i\neq j$;*
3) *la transposition (12) et le n-cycle $(12\cdots n)$.*

Démonstration. — Pour trois éléments distincts $i,j,k\in\{1,\dots,n\}$, 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 $s_1,s_2,\dots,s_{n-1}$ 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 $\mathrm{H}_1=\mathrm{S}_n$. 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 (12) et $c = (12\cdots n)$. Pour $k = 1, \ldots, n-2$, on a :

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

Par conséquent, d'après la proposition 19.20, $c^k(12)c^{-k}$ 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 19.23. Ceci prouve 3). □

Le corollaire ci-dessous sera utile plus loin (21.4).

Corollaire 19.25. — *Soit $p \geqslant 2$ un nombre premier. Alors S_p est engendré par tout couple formé d'une transposition τ et d'un p-cycle c.*

Démonstration. — Notons H le sous-groupe engendré par τ et c. Pour montrer que $\mathrm{H} = \mathrm{S}_p$, il suffit de montrer qu'un conjugué de H égale S_p. Donc, on peut se ramener au cas où $\tau = (12)$.

D'autre part, le sous-groupe $\langle c \rangle$ est isomorphe à $\mathbb{Z}/p\mathbb{Z}$; comme p est premier, alors chaque c^k est un générateur de $\langle c \rangle$, c.-à-d., chaque c^k est encore un p-cycle.

Lorsque k décrit $1, \ldots, p-1$, les éléments $c^k(i)$ décrivent $\{2, \ldots, p\}$, donc il existe un unique k tel que le p-cycle c^k envoie 1 sur 2. Remplaçant c par c^k, on se ramène donc au cas où $c(1) = 2$.

Considérons alors la permutation $\phi \in \mathrm{S}_p$ définie par

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

(En particulier, $\phi(1) = 1$ et $\phi(2) = c(1) = 2$). Alors $\phi^{-1}(12)\phi = (12)$ et

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

Donc, d'après le théorème précédent, on a $\phi^{-1}\mathrm{H}\phi = \mathrm{S}_p$, et il en résulte que $\mathrm{H} = \mathrm{S}_p$. Le corollaire est démontré. □

Remarque 19.26. — Dans S_4, la transposition (12) et le 4-cycle $c = (1324)$ engendrent un sous-groupe propre (d'ordre 8). Donc, le corollaire précédent ne s'étend pas au cas où p n'est pas premier.

Dans l'exemple, la démonstration échoue car la puissance c^2 de c qui vérifie $c^2(1) = 2$ n'est plus un 4-cycle : on a $c^2 = (12)(34)$ qui est d'ordre 2.

19.5. Signature et groupe alterné A_n. —

Lemme 19.27. — *Soit k un anneau commutatif. Tout élément $\sigma \in \mathrm{S}_n$ induit un k-automorphisme ϕ_σ de la k-algèbre $k[\mathrm{X}_1, \ldots, \mathrm{X}_n]$, défini par*

$$(*) \qquad \phi_\sigma(\mathrm{X}_i) = \mathrm{X}_{\sigma(i)}, \quad \forall\, i = 1, \ldots, n.$$

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 $k[\mathrm{X}_1, \ldots, \mathrm{X}_n]$.*

Démonstration. — D'après la propriété universelle de $\mathrm{A} := k[\mathrm{X}_1, \ldots, \mathrm{X}_n]$, il existe, pour tout $\sigma \in \mathrm{S}_n$, un unique morphisme de k-algèbres $\phi_\sigma : \mathrm{A} \to \mathrm{A}$ vérifiant $(*)$. De plus, il résulte de $(*)$ que $\phi_{\mathrm{id}} = \mathrm{id}_\mathrm{A}$ 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 $\mathrm{Aut}_k(\mathrm{A})$. Enfin, $(*)$ montre aussi que $\phi_\sigma = \mathrm{id}_\mathrm{A}$ ssi $\sigma = \mathrm{id}$, et donc $\sigma \mapsto \phi_\sigma$ est un isomorphisme de S_n sur le sous-groupe $\{\phi_\sigma\}_{\sigma \in \mathrm{S}_n}$ de $\mathrm{Aut}_k(\mathrm{A})$. □

Notation 1) Pour tout $\mathrm{P} \in k[\mathrm{X}_1, \ldots, \mathrm{X}_n]$, on écrira simplement $\sigma(\mathrm{P})$ au lieu de $\phi_\sigma(\mathrm{P})$.

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

Théorème 19.28 **(Signature d'une permutation)**. — *Il existe un unique morphisme de groupes surjectif $\varepsilon : \mathrm{S}_n \to \{\pm 1\}$ 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 $\mathrm{A} = k[\mathrm{X}_1, \ldots, \mathrm{X}_n]$. Considérons le polynôme

$$\mathrm{V}_n = \prod_{1 \leqslant i < j \leqslant n} (\mathrm{X}_i - \mathrm{X}_j).$$

Soit $\sigma \in \mathrm{S}_n$. Alors $\sigma(\mathrm{V}_n) = \prod_{1 \leqslant i < j \leqslant n} (\mathrm{X}_{\sigma(i)} - \mathrm{X}_{\sigma(j)})$ et, pour tout $i < j$,

$$\sigma(\mathrm{X}_i - \mathrm{X}_j) = \begin{cases} \mathrm{X}_{\sigma(i)} - \mathrm{X}_{\sigma(j)}, \text{ si } \sigma(i) < \sigma(j); \\ -(\mathrm{X}_{\sigma(j)} - \mathrm{X}_{\sigma(i)}), \text{ si } \sigma(j) < \sigma(i). \end{cases}$$

On en déduit que

$$(*) \qquad \sigma(\mathrm{V}_n) = (-1)^{\ell(\sigma)} \mathrm{V}_n,$$

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 $\mathrm{S}_n \to \{\pm 1\}$. En effet, pour $\sigma, \tau \in \mathrm{S}_n$ on a

$$\varepsilon(\sigma\tau)\mathrm{V}_n = (\sigma\tau)(\mathrm{V}_n) = \sigma(\varepsilon(\tau)\mathrm{V}_n) = \varepsilon(\tau)\varepsilon(\sigma)\mathrm{V}_n,$$

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 19.23, ε est uniquement déterminé. Le théorème est démontré. □

Définition 19.29. — 1) On dit qu'une permutation $\sigma \in \mathrm{S}_n$ 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 19.30. — Pour $n = 2$, $\mathrm{S}_2 \cong \{\pm 1\}$ et $\mathrm{A}_2 = \{1\}$. 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

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

Proposition 19.31. — *Soit $r \leqslant n$. Tous les r-cycles de S_n sont conjugués, et sont de signature $(-1)^{r-1}$.*

Démonstration. — On a déjà vu (19.20) que tous les r-cycles sont conjugués, donc de même signature. Par conséquent, il suffit de calculer la signature du cycle

$$c_0 = (12\cdots r).$$

Or, on voit facilement que

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

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

Théorème 19.32 **(Générateurs de A_n)**. — *On a $\mathrm{A}_2 = \{1\}$ et, pour $n \geqslant 3$, A_n est engendré par les produits de deux transpositions et aussi par les 3-cycles.*

Démonstration. — Il est clair que $\mathrm{A}_2 = \{1\}$. Supposons $n \geqslant 3$ et soit $\sigma \in \mathrm{A}_n$. D'après le théorème 19.23, on peut écrire σ comme un produit

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

Comme $\varepsilon(s_i) = -1$ pour tout i, l'entier N ci-dessus est pair, disons $\mathrm{N} = 2m$. 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 la proposition 19.31, 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. □

19.6. Série dérivée et groupes résolubles. — Soit G un groupe. Si H est un sous-groupe de G, on écrira $\mathrm{H} \lhd \mathrm{G}$ ou bien $\mathrm{G} \rhd \mathrm{H}$ pour signifier que H est un sous-groupe normal de G.

Définition 19.33. — G est **résoluble** s'il existe une suite finie de sous-groupes

$$\mathrm{G} = \mathrm{G}_0 \rhd \mathrm{G}_1 \rhd \cdots \rhd \mathrm{G}_r \rhd \mathrm{G}_{r+1} = \{1\}$$

telle que le groupe quotient $\mathrm{G}_i/\mathrm{G}_{i+1}$ soit abélien, pour $i = 0, \ldots, r$.

Définition 19.34. — 1) Pour $x, y \in \mathrm{G}$, 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 $\mathrm{D}(\mathrm{G})$, le sous-groupe de G engendré par les commutateurs $[x,y]$, pour $x, y \in \mathrm{G}$. On a $\mathrm{D}(\mathrm{G}) = \{1\}$ ssi G est abélien.

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

Lemme 19.35. — 1) *On a* $\mathrm{D}(\mathrm{G}) = \phi(\mathrm{D}(\mathrm{G}))$ *pour tout automorphisme de* G. *En particulier,* $\mathrm{D}(\mathrm{G})$ *est un sous-groupe normal de* G.

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

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

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

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

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

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

Ceci prouve 4). □

Définition 19.36. — On pose $\mathrm{D}^0(\mathrm{G}) = \mathrm{G}$, $\mathrm{D}^1(\mathrm{G}) = \mathrm{D}(\mathrm{G})$ et pour $i \geqslant 1$ on définit $\mathrm{D}^{i+1}(\mathrm{G}) = \mathrm{D}(\mathrm{D}^i(\mathrm{G}))$. D'après ce qui précède, chaque $\mathrm{D}^{i+1}(\mathrm{G})$ est normal dans $\mathrm{D}^i(\mathrm{G})$ et le quotient $\mathrm{D}^i(\mathrm{G})/\mathrm{D}^{i+1}(\mathrm{G})$ est abélien. La suite

$$\mathrm{G} \rhd \mathrm{D}^1(\mathrm{G}) \rhd \mathrm{D}^2(\mathrm{G}) \rhd \cdots$$

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

Proposition 19.37. — G *est résoluble ssi il existe* $r \geqslant 0$ *tel que* $\mathrm{D}^r(\mathrm{G}) = \{1\}$.

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

$$\mathrm{G} = \mathrm{G}_0 \rhd \mathrm{G}_1 \rhd \cdots \rhd \mathrm{G}_{r-1} \rhd \mathrm{G}_r = \{1\}$$

telle que chaque $\mathrm{G}_i/\mathrm{G}_{i+1}$ soit abélien. Alors, on déduit du lemme précédent (points 4. et 2.) que $\mathrm{D}(\mathrm{G}) \subseteq \mathrm{G}_1$, puis que $\mathrm{D}(\mathrm{D}(\mathrm{G})) \subseteq \mathrm{D}(\mathrm{G}_1) \subseteq \mathrm{G}_2$, etc. On obtient ainsi, par récurrence, que $\mathrm{D}^i(\mathrm{G}) \subseteq \mathrm{G}_i$ pour tout i. Par conséquent, $\mathrm{D}^r(\mathrm{G}) = \{1\}$. La proposition est démontrée. □

Corollaire 19.38. — *Soient* G *un groupe.*

1) *Si* G *est résoluble, tout sous-groupe (resp. tout groupe quotient) est résoluble.*

2) *Réciproquement, si* N *est un sous-groupe normal tel que* N *et* G/N *soient résolubles, alors* G *est résoluble.*

Démonstration. — 1) Soient H un sous-groupe et G' un groupe quotient de G. Notons π la projection $\mathrm{G} \to \mathrm{G}'$. En procédant par récurrence, on déduit du lemme 19.35 (points 2. et 3.) que $\mathrm{D}^i(\mathrm{H}) \subseteq \mathrm{D}^i(\mathrm{G})$ et $\pi(\mathrm{D}^i(\mathrm{G})) = \mathrm{D}^i(\mathrm{G}')$ pour tout $i \geqslant 0$. Par conséquent, si G est résoluble, H et G' le sont aussi.

2) Supposons N et $\mathrm{G}' = \mathrm{G}/\mathrm{N}$ soient résolubles. Alors, il existe $r, s \geqslant 1$ tels que $\mathrm{D}^s(\mathrm{N}) = \{1\}$ et $\{1\} = \mathrm{D}^r(\mathrm{G}') = \pi(\mathrm{D}^r(\mathrm{G}))$, d'où $\mathrm{D}^r(\mathrm{G}) \subseteq \mathrm{N}$. Alors $\mathrm{D}^{r+s}(\mathrm{G}) \subseteq \mathrm{D}^s(\mathrm{N}) = \{1\}$, et ceci montre que G est résoluble. □

Exemples 19.39. — 1) Le groupe symétrique S_3 est résoluble car $\mathrm{A}_3 \cong \mathbb{Z}/3$ et $\mathrm{S}_3/\mathrm{A}_3 \cong \{\pm 1\}$.

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 $\leqslant 2$ 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 $|\mathrm{A}_4| = 12$, en déduire que $\mathrm{A}_4/\mathrm{V}_4 \cong \mathbb{Z}/3$, puis en conclure que S_4 est résoluble.

Proposition 19.40. — *On a* $\mathrm{D}(\mathrm{S}_n) = \mathrm{A}_n$ *pour tout* n.

Démonstration. — On a $\mathrm{D}(\mathrm{S}_n) \subseteq \mathrm{A}_n$ puisque tout commutateur appartient à $\operatorname{Ker}\varepsilon$. Si $n = 2$, on a $\mathrm{S}_2 \cong \{\pm 1\}$ et $\mathrm{D}(\mathrm{S}_2) = \{1\} = \mathrm{A}_2$. Pour montrer que $\mathrm{D}(\mathrm{S}_n) = \mathrm{A}_n$ pour $n \geqslant 3$, il suffit de montrer, d'après le théorème 19.32, que tout 3-cycle (ijk) est un commutateur dans S_n. C'est bien le cas, car

$$(ijk) = (jk)(ij)(jk)(ij).$$

□

19.7. A_n n'est pas résoluble, pour $n \geqslant 5$. —

Théorème 19.41. — *Si $n \geqslant 5$, tout 3-cycle appartient à $\mathrm{D}(\mathrm{A}_n)$. Par conséquent, pour $n \geqslant 5$ on a :*

$$\mathrm{A}_n = \mathrm{D}(\mathrm{A}_n) = \mathrm{D}^i(\mathrm{A}_n) = \mathrm{D}^i(\mathrm{S}_n), \qquad \forall\, i \geqslant 1,$$

et donc A_n et S_n ne sont pas résolubles.

Démonstration. — Soit (abc) un 3-cycle arbitraire. Choisissons deux éléments d, e dans $\{1, \ldots, n\} \setminus \{a, b, c\}$; ceci est possible puisque $n \geqslant 5$. 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 $\mathrm{D}(\mathrm{A}_n)$. 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 19.32, ceci montre que $\mathrm{A}_n = \mathrm{D}(\mathrm{A}_n)$, et donc $\mathrm{A}_n = \mathrm{D}^i(\mathrm{A}_n)$ pour tout $i \geqslant 1$.

Ceci entraîne que A_n n'est pas résoluble, et donc S_n ne l'est pas non plus. De plus, comme $\mathrm{D}(\mathrm{S}_n) = \mathrm{A}_n$ (19.40), on a $\mathrm{D}^i(\mathrm{S}_n) = \mathrm{D}^{i+1}(\mathrm{A}_n) = \mathrm{A}_n$ pour tout $i \geqslant 1$. Le théorème est démontré. □

Définition 19.42. — 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 $\mathrm{D}(\mathrm{G}) = \mathrm{G}$. En particulier, un groupe simple n'est pas résoluble.

Remarque 19.43. — 1) On peut avoir $\mathrm{G} = \mathrm{D}(\mathrm{G})$ sans que G soit simple, c.-à-d., le fait que G soit simple est strictement que fort que l'égalité $\mathrm{G} = \mathrm{D}(\mathrm{G})$.

2) En fait, on peut montrer le résultat plus fort que A_n est simple pour $n \geqslant 5$. Voir, par exemple, [**Pe1**, § I.8] ou [**Ja1**, Thm. 4.11].

19.8. Exposant d'un groupe abélien fini. — Le théorème fondamental de structure pour les modules de type fini sur un anneau principal vu au chapitre VI (14.1) 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 19.44 **(Structure des groupes abéliens finis)**. — *Soit* M *un groupe fini abélien.*

1) *Alors*

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

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*

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

et chaque $\mathrm{M}(p_i)$ *se décompose en une somme directe*

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

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

D'autre part, on a le lemme suivant.

Lemme 19.45. — *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 19.46. — *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.

1) *Il existe un élément de* A *d'ordre* m.

2) *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

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

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, $n = |\mathrm{A}|$ 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. □

19.9. Centre d'un groupe et équation des classes. — [12]

***Définition 19.47* (Centre d'un groupe).** — Soit G un groupe. Le **centre de** G est

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

Lemme 19.48. — $\mathrm{Z} := \mathrm{Z}(\mathrm{G})$ *est un sous-groupe de* G*, tel que* $\phi(\mathrm{Z}) = \mathrm{Z}$ *pour tout automorphisme de* G*. En particulier,* Z(G) *est un sous-groupe distingué.*

Démonstration. — D'abord, Z(G) contient l'élément 1. Soient $z, z' \in \mathrm{Z}(\mathrm{G})$ et $g \in \mathrm{G}$. 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

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

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

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

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

Remarque 19.49. — 1) G est abélien $\Leftrightarrow$ $\mathrm{G} = \mathrm{Z}(\mathrm{G})$.

2) Pour un groupe $\mathrm{G} \neq \{1\}$ arbitraire, on peut avoir $\mathrm{Z}(\mathrm{G}) = \{1\}$. C'est le cas, par exemple pour $\mathrm{G} = \mathrm{S}_3$ (exercice !).

***Proposition 19.50* (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* $g, h \in \mathrm{G}$*. Les orbites sont appelées* **classes de conjugaison**. *Les points fixes sont exactement les éléments de* Z(G) *et, si l'on désigne par* $\mathscr{O}(x_1), \ldots, \mathscr{O}(x_r)$ *les orbites dans* $\mathrm{G} \setminus \mathrm{Z}(\mathrm{G})$*, on a l'équation des classes :*

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

[12] Ce paragraphe et le suivant n'ont pas été traités en cours.

où $\mathrm{C_G}(x_i) = \{g \in \mathrm{G} \mid gx_ig^{-1} = x_i\}$ *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 $\mathscr{O}(x_i)$, chacune étant de cardinal $|\mathrm{G}|/|\mathrm{C_G}(x_i)|$ d'après le lemme 19.11. □

19.10. p-groupes et théorèmes de Sylow. — [13]

***Définition 19.51* (p-groupes finis).** — Soit p un nombre premier. Un groupe fini G est un **p-groupe** si |G| est une puissance de p.

***Lemme 19.52* (Points fixes d'un p-groupe).** — *Soit* G *un p-groupe fini agissant sur un ensemble fini* X. *Alors*

$$|\mathrm{X^G}| \equiv |\mathrm{X}| \mod p.$$

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

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

***Théorème 19.53* (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 $|\mathrm{G}| = p^n$. De plus, d'après l'équation des classes (19.50) 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 19.46. Ceci prouve 1).

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

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

Alors le sous-groupe $\mathrm{H} = \mathbb{Z}px_1 \oplus \bigoplus_{i>1} \mathbb{Z}x_i$ est d'indice p. On peut donc supposer G non abélien. Alors G/Z(G) est un p-groupe non trivial, de cardinal $< |\mathrm{G}|$ 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. □

***Corollaire 19.54*.** — *Soit* G *un p-groupe fini. Alors* G *est* **résoluble**.

[13] Ce paragraphe n'a pas été traité en cours.

Démonstration. — Donnons deux démonstrations. Par application répétée du point 2) du théorème précédent, on obtient une suite décroissante de sous-groupes :

$$\mathrm{G} = \mathrm{G}_0 \rhd \mathrm{G}_1 \rhd \mathrm{G}_2 \rhd \cdots \rhd \mathrm{G}_{n+1} = \{1\}.$$

telle que $\mathrm{G}_i/\mathrm{G}_{i+1} \cong \mathbb{Z}/p\mathbb{Z}$ pour $i = 0, 1, \ldots, n$. Ceci montre que G est résoluble.

2ème démonstration. Par hypothèse, $|\mathrm{G}| = p^r$. On procède par récurrence sur r. Si $r = 0$ alors $\mathrm{G} = \{1\}$ et il n'y a rien à montrer. Supposons $r \geqslant 1$ et le résultat établi pour $r - 1$. D'après le théorème précédent, $\mathrm{Z}(\mathrm{G})$ est non-trivial donc est un groupe abélien d'ordre p^s avec $s > 0$. Alors $\overline{\mathrm{G}} := \mathrm{G}/\mathrm{Z}(\mathrm{G})$ est d'ordre p^{r-s}, donc résoluble par hypothèse de récurrence. Donc G est résoluble, puisque $\mathrm{Z}(\mathrm{G})$ et $\overline{\mathrm{G}}$ le sont. □

Définition 19.55. — Soient G un groupe fini, p un nombre premier divisant $|\mathrm{G}|$, et p^n la plus grande puissance de p divisant $|\mathrm{G}|$. 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 19.56* (Théorèmes de Sylow)**. — *Soient* G *un groupe fini, p un nombre premier divisant $|\mathrm{G}|$, et p^n la plus grande puissance de p divisant $|\mathrm{G}|$. Notons $\mathscr{S}_p(\mathrm{G})$ l'ensemble des sous-groupes de* G *de cardinal p^n. Alors :*

1) *$\mathscr{S}_p(\mathrm{G})$ 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 $\mathrm{H}, \mathrm{H}' \in \mathscr{S}_p(\mathrm{G})$, il existe $g \in \mathrm{G}$ tel que $\mathrm{H}' = g\mathrm{H}g^{-1}$.*

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

Démonstration. — On démontre 1) par récurrence sur $|\mathrm{G}|$. Considérons l'équation des classes :

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

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

i) Si p ne divise pas $|\mathrm{Z}(\mathrm{G})|$, alors il existe $i \in \{1, \ldots, r\}$ tel que p ne divise pas $|\mathrm{G}|/|\mathrm{C}_{\mathrm{G}}(p_i)|$; alors p^n divise le cardinal de $\mathrm{C}_{\mathrm{G}}(x_i)$, qui est un sous-groupe

propre de G, puisque $x_i \notin \mathrm{Z(G)}$. Donc, par hypothèse de récurrence, $\mathrm{C_G}(x_i)$ 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 19.46. Comme $gxg^{-1} = x$ pour tout $g \in \mathrm{G}$, le sous-groupe $\langle x \rangle$ est normal dans G, et $\overline{\mathrm{G}} := \mathrm{G}/\langle x \rangle$ est de cardinal $p^{n-1}s < |\mathrm{G}|$. Par hypothèse de récurrence, $\overline{\mathrm{G}}$ 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 $\mathrm{X} = \mathrm{G}/\mathrm{P}$, de cardinal premier à p. Donc, d'après le lemme 19.52, X^{Q} est non vide, c.-à-d., il existe $g \in \mathrm{G}$ tel que $\mathrm{Q}g\mathrm{P} = g\mathrm{P}$. Alors $g^{-1}\mathrm{Q}g \subseteq \mathrm{P}$. Ceci prouve la première assertion de 2). Si de plus Q est un p-sous-groupe de Sylow, alors $g^{-1}\mathrm{Q}g$ est, comme P, de cardinal p^n et donc $g^{-1}\mathrm{Q}g = \mathrm{P}$. Ceci prouve 2). En particulier, $\mathscr{S}_p(\mathrm{G})$ est une orbite sous G, donc son cardinal divise celui de G.

Reste à voir que $|\mathscr{S}_p(\mathrm{G})| \equiv 1$ modulo p. Soit $\mathrm{P} \in \mathscr{S}_p(\mathrm{G})$. Faisons agir P sur $\mathscr{S}_p(\mathrm{G})$ 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 $\mathscr{S}_p(\mathrm{G})$. Soit $\mathrm{Q} \in \mathscr{S}_p(\mathrm{G})$ un tel point fixe, alors $x\mathrm{Q}x^{-1} = \mathrm{Q}$ pour tout $x \in \mathrm{P}$, 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 $n \in \mathrm{N}$ tel que $n\mathrm{Q}n^{-1} = \mathrm{P}$, d'où $\mathrm{P} = \mathrm{Q}$. 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 19.57. — *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 19.58 **(Théorème de Cauchy)**. — [(14)] *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 19.53. □

Exercice 19.59 **(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 19.60. — La démonstration des points 1) et 2) est tirée de [**Se**, § 8.4] ; celle du point 3) de [**Pe1**, § I.5].

(14) 1789-1857, cf. [**ChL**, § 4.2]

20. Polynômes symétriques et groupes de Galois

20.1. Une caractérisation des extensions galoisiennes. — Commençons par réparer un oubli dans le chapitre VIII : la réciproque du Corollaire 17.12.

Proposition 20.1. — *Soit* K/k *une extension de degré fini et soit* $\mathrm{G} = \mathrm{Aut}_k(\mathrm{K})$. *On suppose que* $\mathrm{K}^{\mathrm{G}} = k$. *Alors* K/k *est galoisienne.*

Démonstration. — D'après le théorème d'Artin 17.10, on a $[\mathrm{K} : \mathrm{K}^{\mathrm{G}}] = |\mathrm{G}|$. Donc, l'hypothèse entraîne que $|\mathrm{G}| = [\mathrm{K} : k]$, donc K/k est galoisienne. □

20.2. Galois plus Sylow $\Rightarrow$ $\mathbb{C}$ est algébriquement clos. — [(15)] On va donner dans ce paragraphe suivant une démonstration du « théorème fondamental de l'algèbre » (10.24) basée sur la théorie de Galois, le premier théorème de Sylow, et la structure des p-groupes finis 19.53. Pour une autre démonstration, voir [**Sa**], Appendice au Chap. II.

Lemme 20.2. — 1) *Tout nombre complexe* $z \neq 0$ *admet* n *racines* n*-ièmes dans* $\mathbb{C}$.

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

3) *Tout* $\mathrm{P} \in \mathbb{R}[\mathrm{X}]$ *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. § 10.6). 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

$$\mathrm{P} = \mathrm{X}^2 - 2a\mathrm{X} + b = (\mathrm{X} - a)^2 + b - a^2,$$

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

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

Démontrons maintenant que $\mathbb{C}$ est algébriquement clos. On rappelle qu'en caractéristique 0, tout polynôme est séparable (Corollaire 16.12).

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 $\mathrm{X}^2 + 1$. Le groupe de Galois $\mathrm{Gal}(\mathbb{C}/\mathbb{R})$ est

[(15)] Ce paragraphe n'a pas été traité en cours.

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 $\mathrm{P} \in \mathbb{C}[\mathrm{X}]$ un polynôme irréductible et soit K un corps de décomposition de $\mathrm{P}\overline{\mathrm{P}}$ sur $\mathbb{C}$. D'après le théorème 17.8, l'extension $\mathbb{C} \subseteq \mathrm{K}$ est galoisienne. Posons $\mathrm{G}_1 = \mathrm{Gal}(\mathrm{K}/\mathbb{C})$ et $n = [\mathrm{K} : \mathbb{C}] = |\mathrm{G}_1|$, et écrivons $n = 2^d r$, avec r impair. Alors,

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

Comme $\tau(\mathrm{P}\overline{\mathrm{P}}) = \mathrm{P}\overline{\mathrm{P}}$ alors, d'après le théorème 15.44, la conjugaison complexe τ se prolonge en un $\mathbb{R}$-automorphisme $\widetilde{\tau}$ de K. Posons $\mathrm{G}_2 = \mathrm{Aut}_{\mathbb{R}}(\mathrm{K})$.

Lemme 20.3. — *L'extension* $\mathbb{R} \subset \mathrm{K}$ *est galoisienne, de groupe* G_2.

Démonstration. — En effet, comme G_2 contient G_1 et $\widetilde{\tau}$, on a

$$\mathrm{K}^{\mathrm{G}_2} \subseteq \mathrm{K}^{\mathrm{G}_1} \cap \mathrm{K}^{\widetilde{\tau}} = \mathbb{C}^{\tau} = \mathbb{R},$$

et donc, d'après la proposition 20.1, $\mathrm{K}/\mathbb{R}$ est galoisienne (et G_2 est engendré par G_1 et $\widetilde{\tau}$). □

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

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

Montrons que $d = 0$. Supposons, au contraire, $d \geqslant 1$. Dans ce cas, $\mathrm{G}_1 = \mathrm{Gal}(\mathrm{K}/\mathbb{C})$ est un 2-groupe non trivial donc contient un sous-groupe (distingué) H d'indice 2, d'après le théorème 19.53. Alors, $\mathrm{K}' = \mathrm{K}^{\mathrm{H}}$ est de degré 2 sur $\mathbb{C}$. Soit $x \in \mathrm{K}' \setminus \mathbb{C}$; son polynôme minimal $\mathrm{Irr}_{\mathbb{C}}(x)$ est de degré 2 et irréductible dans $\mathbb{C}[\mathrm{X}]$. Mais ceci est une contradiction, puisque dans $\mathbb{C}[\mathrm{X}]$, tout polynôme de degré 2 est scindé ! Cette contradiction montre que $d = 0$, d'où $[\mathrm{K} : \mathbb{C}] = 1$. Ceci montre que $\mathbb{C}$ est algébriquement clos.

20.3. Groupe de Galois d'un polynôme. —

Théorème 20.4 **(**$\mathrm{Gal}(\mathrm{P}/k)$ **est un sous-groupe de** S_n**)**. — *Soit* k *un corps et soit* $\mathrm{P} \in k[\mathrm{X}]$ *un polynôme, resp.* K/k *une extension, séparable de degré* n. *Soit* L *un corps de décomposition sur* k *de* P, *resp.* $\widetilde{\mathrm{K}}$ *une clôture galoisienne de* K/k. *Alors :*

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

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

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

3) *Plus généralement, écrivons* $\mathrm{P} = \mathrm{P}_1^{m_1} \cdots \mathrm{P}_r^{m_r}$*, où les* P_i *sont irréductibles et deux à deux distincts. Posons* $d_i = \deg \mathrm{P}_i$ *et* $\mathrm{Q} = \mathrm{P}_1 \cdots \mathrm{P}_r$*. Alors* $\mathrm{Gal}(\mathrm{P}/k) = \mathrm{Gal}(\mathrm{Q}/k)$ *est un sous-groupe de*

$$\mathrm{S}_{d_1} \times \cdots \times \mathrm{S}_{d_r}.$$

Démonstration. — Soit K/k une extension séparable de degré n. D'après le théorème de l'élément primitif (16.20), $\mathrm{K} = k[\xi]$ pour un certain $\xi \in \mathrm{K}$, et $\mathrm{Q} = \mathrm{Irr}_k(\xi)$ est séparable sur k, de degré n. Soit M un corps de décomposition sur k de P. D'après la preuve du théorème 17.22, 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 $\mathrm{P} \in k[\mathrm{X}]$ un polynôme séparable de degré n, et L un corps de décomposition de P sur k. L'extension $k \subseteq \mathrm{L}$ est galoisienne, d'après le théorème 17.8, et son groupe de Galois est noté $\mathrm{Gal}(\mathrm{P}/k)$. Soient $x_1, \ldots, x_n$ les racines de P dans K, et soit $g \in \mathrm{Gal}(\mathrm{P}/k)$. Comme $g(\mathrm{P}) = \mathrm{P}$, alors $g(x_1), \ldots, g(x_n)$ sont les racines de P dans K ; par conséquent, g induit une permutation $\sigma_g \in \mathrm{S}_n$ 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 $\mathscr{O}(x_1)$ de x_1 sous $\mathrm{G} := \mathrm{Gal}(\mathrm{P}/k)$, d'après le théorème 17.8. D'après le lemme 19.11, posant

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

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

3) Plus généralement, écrivons $\mathrm{P} = \mathrm{P}_1^{m_1} \cdots \mathrm{P}_r^{m_r}$ et, pour $i = 1, \ldots, r$, soient $d_i = \deg \mathrm{P}_i$ et $\alpha_{i1}, \ldots, \alpha_{id_i}$ les racines de P_i dans K. Soit $g \in \mathrm{G}$. Comme $g(\mathrm{P}_i) = \mathrm{P}_i$, pour tout i, alors g permute les racines de chaque P_i et donc induit une permutation

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

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 20.5. — 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, $|\mathrm{Gal}(\mathrm{P}/k)|$ est divisible par chaque d_i et donc par leur ppcm.

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

20.4. Polynômes symétriques. — Dans cette section, sauf mention contraire, k désigne un anneau commutatif arbitraire. On a vu (19.27) que S_n s'identifie à un sous-groupe du groupe des k-automorphismes de la k-algèbre $k[\mathrm{X}_1, \ldots, \mathrm{X}_n]$.

Définition 20.6. — Soit $\mathrm{P} \in k[\mathrm{X}_1, \ldots, \mathrm{X}_n]$. On dit que P est un **polynôme symétrique** si l'on a $\sigma(\mathrm{P}) = \mathrm{P}$ pour tout $\sigma \in \mathrm{S}_n$, c.-à-d., si P est invariant par toute permutation des variables $\mathrm{X}_1, \ldots, \mathrm{X}_n$. On note

$$k[\mathrm{X}_1, \ldots, \mathrm{X}_n]^{\mathrm{S}_n}$$

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

Exemple 20.7. — Soit $n = 2$. Les polynômes $\mathrm{X}_1 + \mathrm{X}_2$, $\mathrm{X}_1\mathrm{X}_2$, et $\mathrm{X}_1^2\mathrm{X}_2 + \mathrm{X}_2^2\mathrm{X}_1$ sont symétriques. Le polynôme $\mathrm{X}_1 + \mathrm{X}_2^2$ ne l'est pas.

Définition 20.8 **(Polynômes symétriques élémentaires)**. — On pose :

$$\begin{aligned}
e_1 &= e_1(\mathrm{X}_1, \ldots, \mathrm{X}_n) = \mathrm{X}_1 + \cdots + \mathrm{X}_n,\\
e_2 &= e_2(\mathrm{X}_1, \ldots, \mathrm{X}_n) = \textstyle\sum_{1 \leqslant i < j \leqslant n} \mathrm{X}_i\mathrm{X}_j,\\
&\vdots\\
e_k &= e_k(\mathrm{X}_1, \ldots, \mathrm{X}_n) = \textstyle\sum_{1 \leqslant i_1 < \cdots < i_k \leqslant n} \mathrm{X}_{i_1} \cdots \mathrm{X}_{i_k},\\
&\vdots\\
e_n &= e_n(\mathrm{X}_1, \ldots, \mathrm{X}_n) = \mathrm{X}_1 \cdots \mathrm{X}_n.
\end{aligned}$$

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

20.5. Relations entre coefficients et racines d'un polynôme. — Soient k un anneau commutatif arbitraire, et $\mathrm{X}_1, \ldots, \mathrm{X}_n$ des indéterminées. On pose :

$$\mathrm{A} = k[\mathrm{X}_1, \ldots, \mathrm{X}_n].$$

Soit T une autre indéterminée. Considérons dans A[T] le polynôme suivant :

$$(*) \qquad \mathrm{P}(\mathrm{T}) = (\mathrm{T} - \mathrm{X}_1) \cdots (\mathrm{T} - \mathrm{X}_n).$$

(On l'appelle parfois le « *polynôme universel de degré n* ».)

Développons le terme de droite de $(*)$. Le coefficient de T^n est, bien sûr, 1. Celui de T^{n-1} est $-(\mathrm{X}_1 + \cdots + \mathrm{X}_n)$, c.-à-d., $-e_1(\mathrm{X}_1, \ldots, \mathrm{X}_n)$, et celui de T^{n-2} est $\sum_{i<j} \mathrm{X}_i\mathrm{X}_j = e_2(\mathrm{X}_1, \ldots, \mathrm{X}_n)$. Plus généralement, le coefficient de T^{n-r} est

$$(-1)^r \sum_{1 \leqslant i_1 < \cdots < i_r \leqslant n} \mathrm{X}_{i_1} \cdots \mathrm{X}_{i_r} = (-1)^r e_r(\mathrm{X}_1, \ldots, \mathrm{X}_n).$$

En particulier, le coefficient constant est $(-1)^n e(\mathrm{X}_1, \ldots, \mathrm{X}_n)$. On a donc obtenu le théorème suivant.

***Théorème 20.9* (Relations entre coefficients et racines).** — 1) *On a l'égalité suivante, dans l'anneau* $(\mathbb{Z}[\mathrm{X}_1, \ldots, \mathrm{X}_n])[\mathrm{T}]$ *:*

$$\prod_{i=1}^{n}(\mathrm{T} - \mathrm{X}_i) = \mathrm{T}^n + \sum_{i=1}^{n}(-1)^i\, e_i(\mathrm{X}_1, \ldots, \mathrm{X}_n)\, \mathrm{T}^{n-i}. \tag{1}$$

2) *Soient* k *un corps,* $\mathrm{P} = \mathrm{T}^n + a_1\mathrm{T}^{n-1} + \cdots + a_n \in k[\mathrm{T}]$*, et* $x_1, \ldots, x_n$ *les racines de* P *dans une extension* K *de* k*. Pour* $i = 1, \ldots, n$*, on a*

$$a_i = (-1)^i\, e_i(x_1, \ldots, x_n). \tag{2}$$

Démonstration. — On a vu le point 1) plus haut. Le point 2) en découle, en considérant le morphisme d'anneaux

$$\phi : \mathrm{A} = \mathbb{Z}[\mathrm{X}_1, \ldots, \mathrm{X}_n] \longrightarrow \mathrm{K}, \qquad \mathrm{X}_i \mapsto x_i.$$

Il se prolonge en un morphisme d'anneaux $\mathrm{A}[\mathrm{T}] \to \mathrm{K}[\mathrm{T}]$ qui envoie le « *polynôme universel* »

$$(\mathrm{T} - \mathrm{X}_1)\cdots(\mathrm{T} - \mathrm{X}_n) = \mathrm{T}^n + \sum_{i=1}^{n}(-1)^i\, e_i(\mathrm{X}_1, \ldots, \mathrm{X}_n)\, \mathrm{T}^{n-i}$$

sur le polynôme

$$(\mathrm{T} - x_1)\cdots(\mathrm{T} - x_n) = \mathrm{T}^n + \sum_{i=1}^{n}(-1)^i\, e_i(x_1, \ldots, x_n)\, \mathrm{T}^{n-i} \in \mathrm{K}[\mathrm{T}].$$

Comme $x_1, \ldots, x_n$ sont les racines de P dans K (comptées avec multiplicité), le polynôme ci-dessus égale P. Donc, par comparaison des coefficients, on obtient

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

Le théorème est démontré. □

***Remarque 20.10*.** — Soit k un corps. Bien sûr, si on considère un polynôme de degré n non nécessairement unitaire :

$$\mathrm{P} = a_0\mathrm{T}^n + a_1\mathrm{T}^{n-1} + \cdots + a_n \in k[\mathrm{T}], \qquad a_0 \neq 0,$$

et si $x_1, \ldots, x_n$ sont les racines, dans une extension K de k, de P (et donc aussi du polynôme unitaire P/a_0), alors les relations (2) deviennent :

$$\forall\, i = 1, \ldots, n, \qquad a_0\, e_i(x_1, \ldots, x_n) = (-1)^i\, a_i. \tag{2'}$$

20.6. Le théorème fondamental des polynômes symétriques. —

Définition 20.11 **(Éléments algébriquements indépendants)**

Soient k un anneau commutatif et A une k-algèbre. Des éléments $e_1, \ldots, e_n \in \mathrm{A}$ sont dits **algébriquement indépendants sur** k s'ils vérifient la propriété suivante :

Si $\mathrm{P} \in k[\mathrm{T}_1, \ldots, \mathrm{T}_n]$ (où les T_i sont des indéterminées) et si $\mathrm{P}(e_1, \ldots, e_n) = 0$, alors $\mathrm{P} = 0$.

Ceci équivaut à dire que le morphisme de k-algèbres $k[\mathrm{T}_1, \ldots, \mathrm{T}_n] \to \mathrm{A}$ défini par $\phi(\mathrm{T}_i) = e_i$ est un isomorphisme ; ceci entraîne, en particulier, que la sous-algèbre de A engendrée par $e_1, \ldots, e_n$ est isomorphe à l'anneau de polynômes $k[\mathrm{T}_1, \ldots, \mathrm{T}_n]$.

Théorème 20.12 **(Th. fondamental des polynômes symétriques)**

La sous-algèbre $k[\mathrm{X}_1, \ldots, \mathrm{X}_n]^{\mathrm{S}_n}$ 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 $\mathrm{P}(e_1, \ldots, e_n)$. En résumé, on a un isomorphisme

$$k[\mathrm{X}_1, \ldots, \mathrm{X}_n]^{\mathrm{S}_n} \cong k[e_1, \ldots, e_n],$$

et le terme de droite est un anneau de polynômes.

Exemple 20.13. — Pour $r \geqslant 1$, posons $\mathrm{S}_r = \mathrm{X}_1^r + \cdots + \mathrm{X}_n^r$. (Les S_r s'appellent les sommes de Newton). On a $\mathrm{S}_1 = e_1$, et

$$e_1^2 = \sum_{i=1}^{n} \mathrm{X}_i^2 + 2 \sum_{i<j} \mathrm{X}_i \mathrm{X}_j, \qquad \text{d'où} \qquad \mathrm{S}_2 = e_1^2 - 2e_2. \tag{1}$$

De même,

$$e_1^3 = \sum_{i=1}^{n} \mathrm{X}_i^3 + 3 \sum_{i \neq j} \mathrm{X}_i^2 \mathrm{X}_j + 3! \sum_{i<j<k} \mathrm{X}_i \mathrm{X}_j \mathrm{X}_k.$$

D'autre part,

$$e_1 e_2 = \left(\sum_k \mathrm{X}_k \right) \left(\sum_{i<j} \mathrm{X}_i \mathrm{X}_j \right) = \sum_{i<j} (\mathrm{X}_i^2 \mathrm{X}_j + \mathrm{X}_i \mathrm{X}_j^2) + 3 \sum_{i<j<k} \mathrm{X}_i \mathrm{X}_j \mathrm{X}_k.$$

Posant $m_{21} = \sum_{i \neq j} \mathrm{X}_i^2 \mathrm{X}_j$ (voir 20.14 plus loin), on en déduit que

$$m_{21} = e_1 e_2 - 3e_3 \qquad \text{et} \qquad \mathrm{S}_3 = e_1^3 - 3e_1 e_2 + 3e_3. \tag{2}$$

Démonstration du théorème. — $k[X_1, \dots, X_n]$ 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 $I = \{1, \dots, n\}$. 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 $P \in k[X_1, \dots, X_n]$ 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 20.14. — On dit que $\nu \in \mathbb{N}^n$ est **dominant** s'il vérifie $\nu_1 \geqslant \nu_2 \geqslant \cdots \geqslant \nu_n \geqslant 0$. 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 20.12, on a besoin d'introduire sur $\mathbb{N}^n$ l'ordre « degré-puis-lexicographique », défini comme suit.

Définition 20.15. — 1) Pour tout $\mu = (\mu_1, \dots, \mu_n) \in \mathbb{N}^n$, on pose

$$|\mu| = \mu_1 + \cdots + \mu_n.$$

Alors le monôme X^μ est de degré $|\mu|$.

2) Soient $\mu, \nu \in \mathbb{N}^n$. On dit que $\mu \leqslant \nu$ si : $|\mu| < |\nu|$, ou bien $|\mu| = |\nu|$ et il existe $i \in \{1, \dots, n\}$ tel que $\mu_j = \nu_j$ pour $j < i$, et $\mu_i < \nu_i$, ou bien $\mu = \nu$.

C'est un ordre **total**, c.-à-d., quelques soient $\mu, \nu \in \mathbb{N}^n$, on a $\mu \leqslant \nu$ ou $\nu \leqslant \mu$. De plus, $\leqslant$ est **compatible avec l'addition sur** $\mathbb{N}^n$, c.-à-d.,

$$(\dagger) \qquad \left.\begin{matrix} \mu \leqslant \nu \\ \mu' \leqslant \nu' \end{matrix}\right\} \Rightarrow \mu + \mu' \leqslant \nu + \nu'.$$

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

$$(*) \qquad \forall\, \lambda \in \Lambda,\ \forall\, \mu \in \mathrm{S}_n\lambda, \qquad \mu \leqslant \lambda.$$

Le point crucial dans la démonstration du théorème 20.12 est le lemme suivant.

***Lemme 20.16* (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

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

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 $\mathrm{E} := \{\theta \in \Lambda \mid a_\theta \neq 0\}$; c'est un ensemble fini non-vide. Comme $\leqslant$ 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. □

***Lemme 20.17*.** — *Soit $\lambda \in \Lambda$. L'ensemble des $\mu \in \Lambda$ tels que $\mu \leqslant \lambda$ est fini.*

Démonstration. — Les coordonnées d'un tel μ vérifient $0 \leqslant \mu_i \leqslant \mu_1 \leqslant \lambda_1$, donc cet ensemble est fini. □

On peut maintenant terminer la démonstration du théorème 20.12. Comme $e_1, \dots, e_n$ 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

$$k[\mathrm{X}_1, \dots, \mathrm{X}_n]^{\mathrm{S}_n} \subseteq k[e] := k[e_1, \dots, e_n],$$

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

$$\mathrm{N}(\lambda) := |\{\theta \in \Lambda \mid \theta \leqslant \lambda\}|.$$

Bien sûr, si $\lambda = 0$ on a $m_\lambda = 1$. D'autre part, si $\theta < \lambda$, alors $\mathrm{N}(\theta) < \mathrm{N}(\lambda)$.

Pour $i = 1, \dots, n$, posons $\varepsilon_i = (1, \dots, 1, 0, \dots, 0)$, où 1 apparaît i fois, et observons que

$$m_{\varepsilon_i} = e_i.$$

Soit $\lambda = (\lambda_1, \dots, \lambda_n) \in \Lambda$. Observons d'abord que si $\lambda \neq 0$, alors $\mathrm{N}(\lambda) \geqslant 1$. En effet, si tous les λ_i sont égaux, c.-à-d., si $\lambda = (d, \dots, d) = d\varepsilon_n$, avec $d \geqslant 1$, alors on a $d\varepsilon_n > (d-1)\varepsilon_n$ d'une part, et

$$m_{d\varepsilon_n} = (e_n)^d \tag{1}$$

d'autre part. Sinon, soit i l'unique entier $\geqslant 1$ tel que

$$\lambda_1 = \cdots = \lambda_i > \lambda_{i+1} \geqslant \cdots \geqslant \lambda_n;$$

alors $\lambda' = \lambda - \varepsilon_i$ est dominant, et est $< \lambda$.

Le cas $\mathrm{N}(\lambda) = 0$ (auquel cas $\lambda = 0$ et $m_\lambda = 1$) étant ainsi traité, on peut supposer $\mathrm{N}(\lambda) \geqslant 1$ et le résultat établi pour tout $\theta \in \Lambda$ tel que $\mathrm{N}(\theta) < \mathrm{N}(\lambda)$. De plus, d'après ce qui précède, si $\lambda = d\varepsilon_n$ alors $m_\lambda = (e_n)^d$, et sinon on peut écrire

$$\lambda = \lambda' + \varepsilon_i,$$

avec $\lambda' = \lambda - \varepsilon_i$ dominant et $< \lambda$. Alors, d'après le lemme-clé 20.16, 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 pour $\theta = \lambda'$. L'égalité ci-dessus montre alors que $m_\lambda \in k[e]$ Ceci prouve la première assertion du théorème.

Il reste à voir que $e_1, \dots, e_n$ sont algébriquement indépendants sur k. Soit $\mathrm{P} \in k[\mathrm{T}_1, \dots, \mathrm{T}_n]$ non nul. Écrivons

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

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

$$e_i = \mathrm{X}_1\mathrm{X}_2\cdots\mathrm{X}_i + \text{ monômes plus petits},$$

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

$$e_1^{\nu_1}\cdots e_n^{\nu_n} = \mathrm{X}_1^{\nu_1+\cdots+\nu_n}\mathrm{X}_2^{\nu_2+\cdots+\nu_n}\cdots\mathrm{X}_n^{\nu_n} + \text{ monômes plus petits}.$$

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

$$(\nu_1, \ldots, \nu_n) \mapsto (\nu_1 + \cdots + \nu_n, \nu_2 + \cdots + \nu_n, \ldots, \nu_{n-1} + \nu_n, \nu_n)$$

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

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

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 $\mathrm{P}(e_1, \ldots, e_n)$ égale $c_{\nu_0}\mathrm{X}^{\nu_0}$ plus une combinaison linéaire finie de monômes X^μ, avec $\mu < \nu_0$ pour l'ordre lexicographique. Par conséquent, $\mathrm{P}(e_1, \ldots, e_n) \neq 0$. Ceci montre que $e_1, \ldots, e_n$ sont algébriquement indépendants sur k. Le théorème est démontré. □

20.7. Fractions rationnelles symétriques. —

Lemme 20.18. — *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 $\tau \in \mathrm{Aut}(\mathrm{A})$ 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 $\widetilde{\tau} : \mathrm{K} \to \mathrm{K}$ 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 $\widetilde{\mathrm{id}_\mathrm{A}} = \mathrm{id}_\mathrm{K}$ et que $\widetilde{\sigma\tau} = \widetilde{\sigma}\widetilde{\tau}$. Donc $\tau \mapsto \widetilde{\tau}$ est un morphisme de groupes, de Aut(A) vers Aut(K). Il est de plus injectif, puisque $\widetilde{\tau}(a) = \tau(a)$, pour tout $a \in \mathrm{A}$. □

Proposition 20.19. — *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* $b \in \mathrm{A}^\mathrm{G}$.
2) *Par conséquent,* $\mathrm{K}^\mathrm{G} = \mathrm{Frac}(\mathrm{A}^\mathrm{G})$.

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

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

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

Soit k un corps et soient $\mathrm{X}_1, \ldots, \mathrm{X}_n$ des indéterminées. Le groupe symétrique S_n opère par automorphismes dans $k[\mathrm{X}_1, \ldots, \mathrm{X}_n]$ et donc dans son corps des fractions $k(\mathrm{X}_1, \ldots, \mathrm{X}_n)$. On rappelle que $e_1, \ldots, e_n$ désignent les polynômes symétriques élémentaires.

Théorème 20.20 **(Théorème des fractions rationnelles symétriques)**

1) *On a* $k(\mathrm{X}_1, \ldots, \mathrm{X}_n)^{\mathrm{S}_n} = k(e_1, \ldots, e_n)$.

2) *Par conséquent, l'extension* $k(e_1, \ldots, e_n) \subset k(\mathrm{X}_1, \ldots, \mathrm{X}_n)$ *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 20.21. — Soit X une **autre** indéterminée ; considérons le polynôme suivant, à coefficients dans le corps $k(e_1, \ldots, e_n)$,

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

Dans l'extension $k(e_1, \ldots, e_n) \subset k(\mathrm{X}_1, \ldots, \mathrm{X}_n)$, ce polynôme a pour racines $\mathrm{X}_1, \ldots, \mathrm{X}_n$, qui sont deux à deux distinctes. Par conséquent, Q est séparable sur le corps $k(e) := k(e_1, \ldots, e_n)$.

20.8. L'équation générale de degré n**.** — Soient k un corps, $a_1, \ldots, a_n$ des indéterminées, $\mathrm{K} = k(a_1, \ldots, a_n)$ le corps des fractions rationnelles en ces indéterminées. Soit X une autre indéterminée. Considérons le polynôme

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

L'équation $\mathrm{P}(x) = 0$ 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 $d \geqslant 2$). Par exemple, pour $n = 2$, on sait que les racines de

$$\mathrm{X}^2 - a\mathrm{X} + b = 0$$

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

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

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 $n \geqslant 5$. Commençons par établir le théorème suivant.

***Théorème 20.22* (Groupe de Galois de l'équation générale de degré n)**

Soit $\mathrm{L} = \mathrm{K}(x_1, \ldots, x_n)$ *un corps de décomposition sur* $\mathrm{K} = k(a_1, \ldots, a_n)$ *du polynôme* P *ci-dessus. Alors l'extension* $\mathrm{K} \subset \mathrm{L}$ *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 $\mathrm{X}_1, \ldots, \mathrm{X}_n$ *des indéterminées et* $e_1, \ldots, e_n$ *les polynômes symétriques élémentaires en* $\mathrm{X}_1, \ldots, \mathrm{X}_n$. *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*

$$(\dagger) \qquad \begin{array}{ccc} k(e_1, \ldots, e_n) & \subset & k(\mathrm{X}_1, \ldots, \mathrm{X}_n) \\ \cong\downarrow & & \cong\downarrow \\ k(a_1, \ldots, a_n) & \subset & k(x_1, \ldots, x_n) \end{array}$$

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 $\mathrm{Q} = \mathrm{X}^n - e_1\mathrm{X}^{n-1} + \cdots + (-1)e_n$. Alors, $k(\mathrm{X}_i)$ est un corps de décomposition sur $k(e_i)$ de Q. De plus, $\phi(\mathrm{Q}) = \mathrm{P}$ et, par hypothèse, $\mathrm{L} = \mathrm{K}(x_i)$ est un corps de décomposition de P sur K. Donc, d'après le théorème 15.44, ϕ se prolonge en un isomorphisme $\psi : k(\mathrm{X}_i) \xrightarrow{\sim} \mathrm{L}$.

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 théorème 17.8, l'extension $\mathrm{K} \subset \mathrm{L}$ est galoisienne. Déterminons son groupe de Galois $\mathrm{Gal}(\mathrm{L}/\mathrm{K}) = \mathrm{Aut}_{\mathrm{K}}(\mathrm{L})$.

On voit facilement que l'application $\tau \mapsto \psi \circ \tau \circ \psi^{-1}$ est un isomorphisme de $\mathrm{G} = \mathrm{Aut}_{k(e_i)}(k(\mathrm{X}_i))$, dont l'isomorphisme inverse est par $\sigma \mapsto \psi^{-1} \circ \sigma \circ \psi$. On obtient donc, en utilisant le théorème 20.20, les isomorphismes

$$\mathrm{Gal}(\mathrm{L}/\mathrm{K}) \cong \mathrm{Gal}(k(\mathrm{X}_1, \ldots, \mathrm{X}_n)/k(e_1, \ldots, e_n)) \cong \mathrm{S}_n.$$

Ceci prouve le théorème. □

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

Lemme 20.23. — *Soient* $\mathrm{P}_1, \ldots, \mathrm{P}_r \in \mathrm{A}[\mathrm{X}]$. *On a*

$$\mathrm{D}(\mathrm{P}_1 \cdots \mathrm{P}_r) = \sum_{i=1}^{r} \mathrm{P}_1 \cdots \mathrm{D}(\mathrm{P}_i) \cdots \mathrm{P}_r.$$

Démonstration. — Par récurrence sur r. On a déjà vu le cas $r = 2$ (Lemme 16.10). Supposons $r \geqslant 3$ et le résultat établi pour $r - 1$. D'après le cas $r = 2$, l'on a

$$\mathrm{D}(\mathrm{P}_1 \cdots \mathrm{P}_r) = \mathrm{D}(\mathrm{P}_1)\mathrm{P}_2 \cdots \mathrm{P}_r + \mathrm{P}_1\mathrm{D}(\mathrm{P}_2 \cdots \mathrm{P}_r),$$

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

Théorème 20.24 **(Discriminant du polynôme général de degré** n**)**

Soient $\mathrm{X}_1, \ldots, \mathrm{X}_n$ *des indéterminées, et* $e_1, \ldots, e_n$ *les polynômes symétriques élémentaires en* $\mathrm{X}_1, \ldots, \mathrm{X}_n$. *Posons* $a_i = (-1)^i e_i$. *Soient* $\mathrm{T}_1, \ldots, \mathrm{T}_n$ *d'autres indéterminées. Il existe un unique polynôme* $\Delta_n \in \mathbb{Z}[\mathrm{T}_1, \ldots, \mathrm{T}_n]$ *tel que*

$$\Delta_n(a_1, \ldots, a_n) = \prod_{1 \leqslant i < j \leqslant n} (\mathrm{X}_i - \mathrm{X}_j)^2. \tag{1}$$

Ce polynôme Δ_n *est appelé le discriminant du polynôme*

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

et est aussi noté $\mathrm{disc}_{\mathrm{P}}$. *De plus, on a*

$$\prod_{i=1}^{n} \mathrm{P}'(\mathrm{X}_i) = (-1)^{\frac{n(n-1)}{2}} \Delta_n(a_1, \ldots, a_n). \tag{2}$$

Démonstration. — Posons $\Pi = \prod_{1 \leqslant i < j \leqslant n} (\mathrm{X}_i - \mathrm{X}_j)^2$; c'est un élément de $\mathbb{Z}[\mathrm{X}_1, \ldots, \mathrm{X}_n]^{\mathrm{S}_n}$. Donc, d'après le théorème fondamental des polynômes symétriques 20.12, il existe un unique polynôme $\Delta_n^- \in \mathbb{Z}[\mathrm{T}_1, \ldots, \mathrm{T}_n]$, tel que

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

Soit ϕ l'automorphisme de $\mathbb{Z}[\mathrm{T}_1, \ldots, \mathrm{T}_n]$ défini par $\phi(\mathrm{T}_i) = (-1)^i \mathrm{T}_i$ pour tout i, et soit $\Delta_n = \phi(\Delta_n^-)$. Alors, Δ_n est l'unique élément de $\mathbb{Z}[\mathrm{T}_1, \ldots, \mathrm{T}_n]$ vérifiant

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

Ceci prouve la première assertion. De plus, comme

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

il résulte du lemme précédent que

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

Donc, pour $i = 1, \ldots, n$, on a $\mathrm{P}'(\mathrm{X}_i) = \prod_{j \neq i} (\mathrm{X}_i - \mathrm{X}_j)$. Par conséquent,

$$\prod_{i=1}^{n} \mathrm{P}'(\mathrm{X}_i) = \prod_{i \neq j} (\mathrm{X}_i - \mathrm{X}_j) = (-1)^{\frac{n(n-1)}{2}} \Pi.$$

Ceci prouve le théorème. □

***Corollaire 20.25* (Discriminant d'un polynome $\mathrm{P} \in k[\mathrm{X}]$)**

Soient k un corps et $\mathrm{P} = \mathrm{X}^n + \sum_{i=1}^{n} a_i \mathrm{X}^{n-i}$ 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

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

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

Démonstration. — Plaçons-nous dans l'anneau $\mathrm{R} = \mathbb{Z}[\mathrm{X}_1, \ldots, \mathrm{X}_n]$ et posons $\mathrm{V}_n = \prod_{1 \leqslant i < j \leqslant n} (\mathrm{X}_i - \mathrm{X}_j)$ et $\mathrm{A}_i = (-1)^i e_i$ pour $i = 1, \ldots, n$. D'après le théorème précédent, on a dans R l'égalité

$$(*) \qquad \mathrm{V}_n^2 = \Delta_n(\mathrm{A}_1, \ldots, \mathrm{A}_n).$$

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

$$\phi(\mathrm{A}_r) = (-1)^r \sum_{i_1 < \cdots < i_r} \phi(\mathrm{X}_{i_1} \cdots \mathrm{X}_{i_r}) = (-1)^r e_r(x_1, \ldots, x_n) = a_r.$$

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

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

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

***Proposition 20.26* (Discriminant d'un trinôme $\mathrm{X}^n + p\mathrm{X} + q$)**

Soient k un corps et $p, q \in k$. Le discriminant du trinôme $\mathrm{P} = \mathrm{X}^n + p\mathrm{X} + q$, noté $\mathrm{disc}_{\mathrm{P}}$, égale

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

En particulier, pour

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

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 20.24, l'égalité à démontrer est équivalente à la suivante :

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

Or, $\mathrm{P}'(\mathrm{X}) = n\mathrm{X}^{n-1} + p$. 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 $\prod_{i=1}^{n} \mathrm{P}'(x_i)$ égale

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

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

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

Par conséquent, on déduit de $(*)$ que $\prod_{i=1}^{n} \mathrm{P}'(x_i)$ 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, $\mathrm{P}'(0) = p$, et pour les autres racines $x_1, \ldots, x_{n-1}$, l'on a $\mathrm{P}'(x_i) = (1-n)p$. On obtient ainsi que $\prod_{i=1}^{n} \mathrm{P}'(x_i) = (1-n)^{n-1}p^n$ lorsque $q = 0$. Ceci démontre la proposition. □

20.10. L'extension intermédiaire associée au discriminant. — Soient k un corps de caractéristique $\neq 2$, $\mathrm{P} \in k[\mathrm{X}]$ un polynôme séparable de degré n, K un corps de décomposition de P sur k, et $\mathrm{G} = \mathrm{Gal}(\mathrm{K}/k)$. 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 20.4. Posons

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

On a vu que

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

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

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

Réciproquement, supposons $\phi(\mathrm{G}) \not\subseteq \mathrm{A}_n = \ker \varepsilon$, et soit $g \in \mathrm{G}$ tel que $\phi(g) \notin \mathrm{A}_n$. 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 20.25, Δ est le discriminant de P). Le polynôme $\mathrm{X}^2 - \Delta$ est séparable sur k, car il a deux racines distinctes d et $-d$. Comme $k[d]$ est le corps de décomposition sur k de $\mathrm{X}^2 - \Delta$, 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 17.18, l'extension $k[d] \subseteq \mathrm{K}$ est galoisienne, de groupe H. Or, comme $k[d]$ est engendré sur k par d, l'on a

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

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

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

Ceci prouve le théorème. □

Remarque 20.28. — Dans le théorème précédent, l'hypothèse $\mathrm{car}(k) \neq 2$ est nécessaire. En effet, soit $k = \mathbb{F}_2$. Le polynôme $\mathrm{P} = \mathrm{X}^2 + \mathrm{X} + 1$ a deux racines distinctes dans $\mathbb{F}_4$, car son dérivé est $\mathrm{P}' = 1$. Par conséquent,

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

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

20.11. L'équation de degré 3, selon Tartaglia (1535). — Considérons un polynôme unitaire de degré 3, à coefficients dans un sous-corps de $\mathbb{C}$:

$$\mathrm{Y}^3 + a\mathrm{Y}^2 + b\mathrm{Y} + c.$$

En faisant le changement de variable $\mathrm{X} = \mathrm{Y} + a/3$, on se ramène au polynôme

$$\mathrm{X}^3 + p\mathrm{X} + q, \qquad \text{où} \quad \begin{cases} p = b - a^2/3; \\ q = 2a^3/27 - ba/3 + c. \end{cases} \tag{1}$$

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 [**Esc**, § 2.2] ou [**Ti**, Chap. 2] pour une discussion historique. En language moderne, on peut présenter cette solution comme suit.

Cherchons X sous la forme $\mathrm{X} = y + z$, 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

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

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

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

Observons que $\mathrm{AB} \neq 0$, 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

$$\begin{cases} x_1 = \quad \alpha + \beta, \\ x_2 = j\alpha + j^2\beta, \\ x_3 = j^2\alpha + j\beta. \end{cases} \tag{5}$$

20.12. Équations de degré $2, 3, 4$: approche galoisienne. — Dans ce qui suit, le corps de base k est de caractéristique $\neq 2, 3$; par exemple, $k = \mathbb{Q}$.

20.12.1. Équations de degré 2. — Soient x_1, x_2 les deux racines de l'équation

$$x^2 - bx + c = 0.$$

Alors $x_1 + x_2 = b$ et $x_1 x_2 = c$. Posons $y = x_1 - x_2$. Alors :

$$2x_1 = b + y, \quad 2x_2 = b - y, \qquad y^2 = (x_1 + x_2)^2 - 4x_1x_2 = b^2 - 4c.$$

Donc $y = \pm\sqrt{b^2 - 4c}$ et $x_1,\ x_2 = (b \pm \sqrt{b^2 - 4c})/2$.

20.12.2. Équations de degré 3. — Considérons l'équation

$$x^3 + a_1x^2 + a_2x + a_3 = 0. \tag{1}$$

Il est naturel de généraliser l'introduction de $y = x_1 - x_2$ pour l'équation de degré 2 de la manière suivante. On pose

$$y_1 = x_1 + jx_2 + j^2x_3 \qquad \text{et} \qquad y_2 = x_1 + j^2x_2 + jx_3,$$

où $j = e^{2i\pi/3} = (-1 + i\sqrt{3})/2$, et $j^2 = j^{-1} = e^{-2i\pi/3} = (-1 - i\sqrt{3})/2$ sont les racines cubiques primitives de l'unité.

Le groupe symétrique S_3 est engendré par les transpositions $s_1 = (12)$ et $s_2 = (23)$, et l'on a :

$$s_1(y_1) = x_2 + jx_1 + j^2x_3 = jy_2, \qquad s_1(y_2) = x_2 + j^2x_1 + jx_3 = j^2y_1,$$
$$s_2(y_1) = x_1 + jx_3 + j^2x_2 = y_2, \qquad s_2(y_2) = x_1 + j^2x_3 + jx_2 = y_1.$$

Il en résulte que y_1y_2 et $y_1^3 + y_2^3$ sont invariants par S_3, c.-à-d., sont des polynômes symétriques en x_1, x_2, x_3. Donc, d'après le théorème fondamental des polynômes symétriques, on peut exprimer y_1y_2 et $y_1^3 + y_2^3$ en fonction des polynômes symétriques élémentaires, c.-à-d., des coefficients a_1, a_2, a_3 de l'équation (1). Désignant par S_r la somme de Newton $x_1^r + x_2^r + x_3^r$, pour $r \geqslant 1$, et posant

$$m_{21} = x_1^2x_2 + x_1x_2^2 + x_1^2x_3 + x_1x_3^2 + x_2^2x_3 + x_2x_3^2,$$

on obtient :

$$y_1y_2 = \mathrm{S}_2 - e_2, \qquad y_1^3 + y_2^3 = 2\mathrm{S}_3 + 12e_3 - 3m_{2,1}.$$

D'autre part, on a vu en 20.13 que :

$$\mathrm{S}_2 = e_1^2 - 2e_2, \qquad m_{2,1} = e_1e_2 - 3e_3, \qquad \mathrm{S}_3 = e_1s_2 - m_{2,1} = e_1^3 - 3e_1e_2 + 3e_3.$$

On obtient donc

$$y_1y_2 = e_1^2 - 3e_2, \qquad y_1^3 + y_2^3 = 2e_1^3 - 9e_1e_2 + 27e_3. \tag{2}$$

Par conséquent, les cubes y_1^3, y_2^3 sont les racines de l'équation quadratique

$$(\mathrm{X} - y_1^3)(\mathrm{X} - y_2^3) = \mathrm{X}^2 - (2e_1^3 - 9e_1e_2 + 27e_3)\mathrm{X} + (e_1^2 - 3e_2)^3 = 0 \tag{3}$$

et l'on a de plus la relation

$$y_1 y_2 = e_1^2 - 3e_2. \tag{4}$$

Comme dans le paragraphe 20.11, en faisant le changement de variable $\mathrm{X} = x + a_1/3$, on peut mettre l'équation (1) sous la forme plus simple :

$$\mathrm{X}^3 + p\mathrm{X} + q = 0, \qquad \text{où} \quad \begin{cases} p = a_2 - a^2/3; \\ q = 2a_1^3/27 - a_2 a_1/3 + a_3. \end{cases} \tag{5}$$

On a alors :

$$e_1 = 0, \qquad e_2 = p, \qquad e_3 = -q,$$

donc (2) s'écrit

$$y_1 y_2 = -3p, \qquad y_1^3 + y_2^3 = -27q,$$

et y_1^3, y_2^3 sont les racines de l'équation quadratique

$$(\mathrm{X} - y_1^3)(\mathrm{X} - y_2^3) = \mathrm{X}^2 + 27q\mathrm{X} - 27p^3 = 0. \tag{6}$$

On a donc :

$$y_1^3, y_2^3 = 27\left(-\frac{q}{2} \pm \sqrt{\left(\frac{p}{3}\right)^3 + \left(\frac{q}{2}\right)^2}\right), \tag{7}$$

avec de plus la condition $y_1 y_2 = -3p$. Revenant aux solutions x_1, x_2, x_3 de l'équation (5), on déduit du système

$$\begin{cases} 0 = x_1 + x_2 + x_3 \\ y_1 = x_1 + jx_2 + j^2 x_3 \\ y_2 = x_1 + j^2 x_2 + jx_3 \end{cases}$$

que

$$x_1 = \frac{y_1 + y_2}{3}, \qquad x_2 = \frac{j^2 y_1 + j y_2}{3}, \qquad x_3 = \frac{j y_1 + j^2 y_2}{3}.$$

On obtient donc, finalement, que x_1, x_2, x_3 sont donnés par les « formules de Cardan » :

$$\begin{aligned} x_1 &= \sqrt[3]{-\tfrac{q}{2} + \sqrt{\left(\tfrac{p}{3}\right)^3 + \left(\tfrac{q}{2}\right)^2}} + \sqrt[3]{-\tfrac{q}{2} - \sqrt{\left(\tfrac{p}{3}\right)^3 + \left(\tfrac{q}{2}\right)^2}} \\ x_2 &= j^2\sqrt[3]{-\tfrac{q}{2} + \sqrt{\left(\tfrac{p}{3}\right)^3 + \left(\tfrac{q}{2}\right)^2}} + j\sqrt[3]{-\tfrac{q}{2} - \sqrt{\left(\tfrac{p}{3}\right)^3 + \left(\tfrac{q}{2}\right)^2}} \\ x_3 &= j\sqrt[3]{-\tfrac{q}{2} + \sqrt{\left(\tfrac{p}{3}\right)^3 + \left(\tfrac{q}{2}\right)^2}} + j^2\sqrt[3]{-\tfrac{q}{2} - \sqrt{\left(\tfrac{p}{3}\right)^3 + \left(\tfrac{q}{2}\right)^2}}, \end{aligned}$$

où les racines cubiques choisies sont reliées par la condition $y_1 y_2 = -3p$, c.-à-d.,

$$\sqrt[3]{-\frac{q}{2} + \sqrt{\left(\frac{p}{3}\right)^3 + \left(\frac{q}{2}\right)^2}} \cdot \sqrt[3]{-\frac{q}{2} - \sqrt{\left(\frac{p}{3}\right)^3 + \left(\frac{q}{2}\right)^2}} = -\frac{p}{3}.$$

Exemple. (Emprunté au polycopié de Jan Nekovàř [**Ne04**].) Considérons l'équation

$$x^3 - 8x - 8 = 0,$$

qui a une racine évidente $x_1 = -2$, donc se factorise

$$x^3 - 8x - 8 = (x+2)(x^2 - 2x - 4) = (x+2)(x - (1+\sqrt{5}))(x - (1-\sqrt{5})),$$

c.-à-d., ses racines sont :

$$x_1 = -2, \qquad x_2 = 1+\sqrt{5}, \qquad x_3 = 1-\sqrt{5}. \tag{$*$}$$

D'autre part, les formules de Cardan pour $p = q = -8$ montrent que

$$\begin{aligned} x_1 &= \sqrt[3]{4 + \tfrac{4i}{9}\sqrt{15}} + \sqrt[3]{4 - \tfrac{4i}{9}\sqrt{15}} \\ x_2 &= j^2\sqrt[3]{4 + \tfrac{4i}{9}\sqrt{15}} + j\sqrt[3]{4 - \tfrac{4i}{9}\sqrt{15}} \\ x_3 &= j\sqrt[3]{4 + \tfrac{4i}{9}\sqrt{15}} + \sqrt[3]{4 - \tfrac{4i}{9}\sqrt{15}} \end{aligned}$$

avec la normalisation

$$\sqrt[3]{4 + \frac{4i}{9}\sqrt{15}} \cdot \sqrt[3]{4 - \frac{4i}{9}\sqrt{15}} = \frac{8}{3}.$$

Il n'est pas du tout évident d'après les formules de Cardan que l'on obtienne les formules $(*)$! Bien sûr, les formules de Cardan montrent que

$$y_1, y_2 = -3 \pm i\sqrt{15},$$

d'où

$$\sqrt[3]{4 \pm \frac{4i}{9}\sqrt{15}} = -1 \pm \frac{i\sqrt{15}}{3}, \tag{$**$}$$

mais il n'est pas possible de déduire $(**)$ sans avoir déjà trouvé les racines $(*)$.

Remarque 20.29. — Soit $\mathrm{P} = \mathrm{X}^3 + a_1\mathrm{X}^2 + a_2\mathrm{X}^2 + a_3$ un polynôme unitaire de degré 3 et soit Δ son discriminant. On a vu que par le changement de variable $\mathrm{Y} = \mathrm{X} + a_1/3$, P se met sous la forme

$$\mathrm{Y}^3 + p\mathrm{Y} + q, \qquad \text{où} \quad \begin{cases} p = a_2 - a^2/3; \\ q = 2a_1^3/27 - a_2a_1/3 + a_3. \end{cases}$$

Comme $\Delta = -4p^3 - 27q^2$, on en déduit que

$$\Delta = -4a_2^3 - 27a_3^2 + a_1^2a_2^2 + 18a_1a_2a_3 - 4a_1^3a_3. \tag{$\dagger$}$$

Proposition 20.30. — *Soient* K *un sous-corps de* $\mathbb{C}$ *et* $\mathrm{P} \in \mathrm{K}[\mathrm{X}]$ *un polynôme* **irréductible** *unitaire de degré* 3. *Soit* Δ *le discriminant de* P. *Alors, on a :*

$$\begin{cases} \mathrm{Gal}(\mathrm{P}/\mathrm{K}) \cong \mathrm{A}_3 \cong \mathbb{Z}/3\mathbb{Z}, & \text{si } \sqrt{\Delta} \in \mathrm{K}; \\ \mathrm{Gal}(\mathrm{P}/\mathrm{K}) \cong \mathrm{S}_3, & \text{si } \sqrt{\Delta} \notin \mathrm{K}. \end{cases}$$

Démonstration. — Comme P est irréductible sur K, alors $G := \mathrm{Gal}(L/K)$ est un sous-groupe de S_3 d'ordre divisible par 3, d'après le théorème 20.4.

Si $d = \sqrt{\Delta}$ appartient à K alors, d'après le théorème 20.27, 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 $G = S_3$. □

Remarque 20.31. — 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 $\mathbb{C}$. Alors, le discriminant de P est

$$\Delta = ((x_1 - x_2)(x_1 - x_3)(x_2 - x_3))^2 = -27q^2 - 4p^3.$$

Il est commode de poser

$$\Delta' = \frac{-1}{27 \cdot 4}\,\Delta;$$

alors les formules de Cardan 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, $j = (-1 + i\sqrt{3})/2$.

20.12.3. Équations de degré 4. — À nouveau, par le changement de variable $X = Y + a_1/4$, on peut mettre un polynôme unitaire de degré 4 arbitraire

$$Y^4 + a_1 Y^3 + a_2 Y^2 + a_3 Y + a_4$$

sous la forme

$$P = X^4 + pX^2 + qX + r. \tag{1}$$

Soient $x_1, \ldots, x_4$ les racines de P dans une clôture algébrique de k.

On a vu (en exercice !) que S_4 est résoluble ; plus précisément, on a la chaîne suivante de sous-groupes :

$$S_4 \rhd A_4 \rhd V_4,$$

où $V_4 = \{\mathrm{id}, (12)(34), (13)(24), (14)(23)\}$ est le sous-groupe formé des éléments d'ordre 2 de A_4. On cherche des polynômes en les x_i qui sont invariants par V_4. On rencontre essentiellement les deux choix suivants.

1) Posons

$$\begin{cases} z_1 = x_1x_2 + x_3x_4; \\ z_2 = x_1x_3 + x_2x_4; \\ z_3 = x_1x_4 + x_2x_4. \end{cases}$$

On note S_r les sommes de Newton et on rappelle que m_{211} est la somme des symétrisés du monôme $x_1^2x_2x_3$ (il y a 12 termes), et m_{222} et m_{3111} sont définis

de façon analogue (cf. Déf. 20.14). Alors, on a :

$$\begin{cases} z_1 + z_2 + z_3 = m_{11} = e_2 = p; \\ z_1z_2 + z_1z_3 + z_2z_3 = m_{211} = e_1e_3 - 4e_4 = -4r; \\ z_1z_2z_3 = m_{3111} + m_{222}. \end{cases}$$

De plus, on vérifie que

$$m_{3111} = \mathrm{S}_2e_4 = (e_1^2 - 2e_2)e_4, \qquad m_{222} = e_3^2 - 2m_{2211} = e_3^2 - 2e_2e_4.$$

d'où

$$z_1z_2z_3 = -4pr + (-q)^2 = q^2 - 4pr.$$

Par conséquent, z_1, z_2, z_3 sont les racines du polynômes de degré 3 suivant :

$$\mathrm{Q} = \mathrm{Y}^3 - p\mathrm{Y}^2 - 4r\mathrm{Y} + (4pr - q^2). \tag{2}$$

Ce polynôme est appelé le polynôme (cubique) résolvant de l'équation quartique $\mathrm{P}(x) = 0$. Observons que

$$\begin{cases} z_1 - z_2 = (x_1 - x_4)(x_2 - x_3); \\ z_1 - z_3 = (x_1 - x_3)(x_2 - x_4); \\ z_2 - z_3 = (x_1 - x_2)(x_3 - x_4); \end{cases}$$

Par conséquent, le polynôme résolvant Q a même discriminant que P. D'après la formule 20.29 (†) donnant le discriminant d'un polynôme de degré 3, on obtient que le discriminant de P est

$$\Delta_4 = 16p^4r - 4p^3q^2 - 8 \cdot 16p^2r^2 + 9 \cdot 16prq^2 + 4^4r^3 - 27q^4.$$

2) Un autre choix possible est de prendre

$$\begin{cases} y_1 = (x_1 + x_2)(x_3 + x_4) = z_2 + z_3; \\ y_2 = (x_1 + x_3)(x_2 + x_4) = z_1 + z_3; \\ y_3 = (x_1 + x_4)(x_2 + x_3) = z_1 + z_2. \end{cases}$$

Alors, on vérifie que y_1, y_2, y_3 sont racines du polynôme résolvant

$$\mathrm{R} = \mathrm{Y}^3 - 2p\mathrm{Y}^2 + (p^2 - 4r)\mathrm{Y} + q^2. \tag{3}$$

Comme $y_1 - y_2 = z_2 - z_1$, $y_1 - y_3 = z_3 - z_1$, et $y_2 - y_3 = z_3 - z_2$, alors R a même discriminant que Q et P.

Supposons avoir résolu (2) ou (3), c.-à-d., supposons connus y_1, y_2, y_3. Comme

$$x_1 + x_2 + x_3 + x_4 = 0,$$

on obtient

$$\begin{cases} -y_1 = (x_1 + x_2)^2; \\ -y_2 = (x_1 + x_3)^2; \\ -y_3 = (x_1 + x_4)^2; \end{cases}$$

en fait, on ne peut pas choisir de façon indépendante ces 3 racines carrées, car on a la relation

$$(*) \quad (x_1+x_2)(x_1+x_3)(x_1+x_4) = x_1^3 + x_1^2(x_2+x_3+x_4) + e_3 = e_3 = -q.$$

Ceci permet d'obtenir x_1, x_2, x_3, x_4. En effet, on a

$$x_1+x_2 = \sqrt{-y_1}, \qquad x_1+x_3 = \sqrt{-y_2}, \qquad x_1+x_4 = \sqrt{-y_3},$$

les racines carrés étant choisies de façon à vérifier $(*)$, et donc, puisque $x_1 + x_2 + x_3 + x_4 = 0$, on obtient

$$2x_1 = 3x_1 + x_2 + x_3 + x_4 = \sqrt{-y_1} + \sqrt{-y_2} + \sqrt{-y_3},$$

et l'on a des formules analogues pour x_2, x_3, x_4.

Remarque 20.32. — Supposons P irréductible. Dans ce cas, le groupe de Galois $\mathrm{Gal}(\mathrm{P}/k)$ est un sous-groupe de S_4 qui agit transitivement sur $\{1,2,3,4\}$, d'après le théorème 20.4. Pour la description des différents cas possibles, voir [**ChL**, 5.5, pp.117-8] ou [**Esc**, 16.2.5–9].

21. 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.

21.1. Extensions radicales. —

Définition 21.1. — Une suite finie d'extensions de corps $k = \mathrm{K}_0 \subseteq \mathrm{K}_1 \subseteq \cdots \subseteq \mathrm{K}_r$ s'appelle une tour d'extensions (ou une tour de corps).

Définition 21.2. — Soit L une extension algébrique de k contenue dans $\mathbb{C}$. Nous dirons que l'extension $k \subseteq \mathrm{L}$ est :

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

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

$$k = \mathrm{L}_0 \subseteq \mathrm{L}_1 \subseteq \cdots \subseteq \mathrm{L}_r = \mathrm{L}$$

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

Définition 21.3. — Soit $\mathrm{P} \in k[\mathrm{X}]$ de degré $\geqslant 1$ 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 $\mathrm{P}(x) = 0$) est **résoluble par radicaux** sur k s'il existe une extension radicale $k \subseteq \mathrm{L}$ contenant K, c.-à-d., telle que $k \subseteq \mathrm{K} \subseteq \mathrm{L}$.

Remarque 21.4. — 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 $k \subseteq \mathrm{K}$ est galoisienne. On rappelle que son groupe de Galois est désigné par $\mathrm{Gal}(\mathrm{P}/k)$.

Le but de ce chapitre est de démontrer le théorème suivant, qui donne une condition nécessaire pour que P soit résoluble par radicaux.

Théorème 21.5. — *Si* P *est résoluble par radicaux, alors le groupe* $\mathrm{Gal}(\mathrm{P}/k)$ *est résoluble.*

Corollaire 21.6. — *L'équation générale de degré* $n \geqslant 5$ *n'est pas résoluble par radicaux, puisque son groupe de Galois est* S_n*, qui n'est pas résoluble.*

Remarque 21.7. — 1) On donnera plus loin (Thm. 21.17) un exemple explicite de polynôme $\mathrm{P} \in \mathbb{Q}[\mathrm{X}]$ non résoluble par radicaux, en montrant que le groupe de Galois correspondant n'est pas résoluble.

2) On peut aussi montrer que la réciproque du théorème est vraie : si $\mathrm{Gal}(\mathrm{P}/k)$ 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 $\mathrm{L}_i \subseteq \mathrm{L}_{i+1}$ soit galoisienne, pour $i = 0, \ldots, r-1$, et que $k \subseteq \mathrm{L}_r = \mathrm{L}$ le soit aussi. Soit $\mathrm{G} = \mathrm{Gal}(\mathrm{L}/k)$ et notons G_i le fixateur dans G de L_i. Alors, on peut montrer (voir plus bas) que les hypothèses entraînent que

$$\mathrm{G} = \mathrm{G}_0 \rhd \mathrm{G}_1 \rhd \cdots \rhd \mathrm{G}_r = \{1\}$$

et que chaque $\mathrm{G}_i/\mathrm{G}_{i+1}$ est abélien. Donc, G est résoluble. Enfin, $k \subseteq \mathrm{K} \subseteq \mathrm{L}$ et l'extension $k \subseteq \mathrm{K}$ est galoisienne. Par conséquent, d'après le théorème 17.18, $\mathrm{Gal}(\mathrm{P}/k)$ est un groupe quotient de G, donc est aussi résoluble.

La difficulté technique est que l'extension radicale $k \subset \mathrm{L}$ 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.

21.2. 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 $n \geqslant 2$, 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 21.8. — Soit L une extension algébrique de K contenue dans $\mathbb{C}$. Nous dirons que l'extension $\mathrm{K} \subseteq \mathrm{L}$ est radicale élémentaire **d'exposant divisant** n s'il existe $a \in \mathrm{L}^\times$ et $n \geqslant 1$ tels que $\mathrm{L} = \mathrm{K}[a]$ et $a^n \in \mathrm{K}$.

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

Proposition 21.9. — *Soient* K *un sous-corps de* $\mathbb{C}$ *et* $\mathrm{K} \subseteq \mathrm{L}$ *une extension radicale élémentaire d'exposant divisant* n*, c.-à-d.,* $\mathrm{L} = \mathrm{K}[a]$*, avec* $a^n \in \mathrm{K}$*. On suppose que* K *contient une racine primitive d'ordre* n *de l'unité* ξ*. Alors :*

1) *L'extension* $\mathrm{K} \subseteq \mathrm{K}[a]$ *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* $\geqslant 1$ *tel que* $a^d \in \mathrm{K}$*, et le polynôme minimal de* a *sur* K *est* $\mathrm{X}^d - a^d$*.*

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

Pour tout $g \in \mathrm{G}$, $g(a)$ est une racine de $\mathrm{X}^n - a^n$ donc égale $\lambda(g)a$, pour un certain $\lambda(g) \in \mu_n(\mathrm{K})$. Pour tout $g, g' \in \mathrm{G}$, 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 $\lambda : \mathrm{G} \to \mu_n(\mathrm{K})$ est un morphisme de groupes. Elle est de plus injective, car si $g(a) = g'(a)$ alors $g = g'$, puisque $\mathrm{K}[a]$ est engendré sur K par a. Donc G s'identifie au sous-groupe $\lambda(\mathrm{G})$ de $\mu_n(\mathrm{K})$. Comme ce dernier est cyclique, engendré par ξ, alors $\lambda(\mathrm{G})$ 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 $\deg_\mathrm{K}(a) = |\mathrm{G}| = d$. De plus, pour tout $g \in \mathrm{G}$, 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, $a^d \in \mathrm{K}$ et P divise $\mathrm{X}^d - a^d$. Pour une question de degré, on a l'égalité, et d est le plus petit entier $\geqslant 1$ tel que $a^d \in \mathrm{K}$. 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 $\mathrm{K} \subseteq \mathrm{K}[\xi]$, où ξ est une racine primitive de l'unité d'ordre n, appelées **extensions cyclotomiques**.

Lemme 21.10. — *Soit n un entier $\geqslant 2$. 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 $\mathrm{U}(n)$.*

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

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

Soit $g \in \mathrm{G}$. 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

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

qui est injective puisque L est engendré sur K par ξ. De plus, cette application est un morphisme de groupes. En effet, pour $g, g' \in \mathrm{G}$, 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 21.12. — 1) Le groupe $\mathrm{G} := \mathrm{Gal}(\mathrm{K}[\xi]/\mathrm{K})$ dépend du corps K. Par exemple, si K contient déjà ξ, alors $\mathrm{K} = \mathrm{K}[\xi]$ et $\mathrm{G} = \{1\}$.

2) À l'autre extrême, si $\mathrm{K} = \mathbb{Q}$, on peut montrer que $\mathrm{G} := \mathrm{Gal}(\mathbb{Q}[\xi]/\mathbb{Q})$ 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 21.5 est le suivant.

Proposition 21.13. — *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 $n \geqslant 1$ 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. Puisque K/k est galoisienne alors, d'après le théorème 17.8, K est un corps de décomposition sur k d'un polynôme (séparable !) Q. On voit alors que Ω est un corps de décomposition sur k du polynôme QP. Par conséquent, d'après le théorème 17.8, à nouveau, 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 $i \geqslant 2$. Il existe, d'après le théorème 15.35, 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 théorème 15.44, 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 point 5) du théorème 17.18. 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 21.14. — **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 car(K) $\neq 2$ et $a^2 \in \mathrm{K}$, l'extension $\mathrm{K} \subseteq \mathrm{K}[a]$ est galoisienne, car $\mathrm{K}[a]$ est le corps de décomposition du polynôme séparable $\mathrm{X}^2 - a^2$, 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 $\mathrm{L} := \mathbb{Q}[\alpha] \subseteq \mathbb{R}$. D'autre part, le polynôme $\mathrm{P} = \mathrm{X}^4 - 2$ 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

$$\mathrm{X}^4 - 2 = (\mathrm{X}^2 + a\mathrm{X} + b)(\mathrm{X}^2 - a\mathrm{X} + c),$$

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 $\mathrm{L} \subseteq \mathbb{R}$. Ceci montre que l'extension $\mathbb{Q} \subseteq \mathrm{L}$ n'est pas quasi-galoisienne.

21.3. P résoluble par radicaux $\Rightarrow$ Gal(P/k) résoluble. — Armé des trois propositions précédentes, on peut maintenant démontrer le théorème 21.5. Soient k un sous-corps de $\mathbb{C}$ et K le sous-corps engendré par les racines dans $\mathbb{C}$ d'un polynôme $\mathrm{P} \in k[\mathrm{X}]$ de degré $\geqslant 1$. On suppose l'équation $\mathrm{P}(x) = 0$ résoluble par radicaux, c.-à-d., que K est contenu dans une extension radicale L de k. Donc, il existe des entiers $n_1, \ldots, n_r \geqslant 1$ et $a_1, \ldots, a_r \in \mathrm{L}$, tels que, posant $\mathrm{L}_0 = k$ et $\mathrm{L}_i = \mathrm{L}_{i-1}[a_i]$, on ait $a_i^{n_i} \in \mathrm{L}_{i-1}$ pour $i = 1, \ldots, r$.

Notons n le ppcm des n_i. Alors, K est contenu dans la tour

$$k = \mathrm{L}_0 \subseteq \cdots \subseteq \mathrm{L}_r,$$

où chaque extension $\mathrm{L}_i/\mathrm{L}_{i-1}$ est **radicale élémentaire d'exposant divisant** n.

Il est commode de s'autoriser aussi l'indice -1 et de poser $k = \mathrm{L}_{-1} = \mathrm{L}_0$. Soit ξ une racine primitive de l'unité d'ordre n. Posons

$$\mathrm{L}'_{-1} = k \quad \text{et} \quad \mathrm{L}'_i = \mathrm{L}_i[\xi] \quad \text{pour } i = 0, \ldots, r.$$

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

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

De plus, d'après la proposition 21.11, l'extension $k \subseteq \mathrm{L}'_0 = k[\xi]$ est galoisienne, de groupe de Galois abélien (un sous-groupe de $(\mathbb{Z}/n\mathbb{Z})^\times$).

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

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

De plus, chaque extension $k \subseteq \mathrm{L}_i''$ est galoisienne, car L_i'' est un corps de décomposition sur k du polynôme $(\mathrm{X}^n-1)\mathrm{P}_1\cdots\mathrm{P}_i$. Alors, il résulte de la proposition 21.13 que chaque extension $\mathrm{L}_{i-1}'' \subseteq \mathrm{L}_i''$ 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

$$k = \widetilde{\mathrm{L}}_{-1} \subseteq \mathrm{L}_0'' = \widetilde{\mathrm{L}}_0 \subseteq \widetilde{\mathrm{L}}_1 \subseteq \cdots \subseteq \widetilde{\mathrm{L}}_{\mathrm{N}} = \mathrm{L}_r'',$$

où :

a) pour $i = 1, \ldots, \mathrm{N}$, l'extension $\widetilde{\mathrm{L}}_i/\widetilde{\mathrm{L}}_{i-1}$, est **radicale élémentaire d'exposant divisant** n, et donc **galoisienne**, d'après la proposition 21.9, puisque L_0'' contient $\mu_n(\mathbb{C})$.

b) L'extension $k \subseteq \mathrm{L}_0'' = k[\xi]$ est galoisienne, de groupe de Galois abélien, d'après la proposition 21.11.

c) L'extension $k \subseteq \widetilde{\mathrm{L}}_{\mathrm{N}} = \mathrm{L}_r''$ est galoisienne.

Notons $\mathrm{G} = \mathrm{Gal}(\widetilde{\mathrm{L}}_{\mathrm{N}}/k)$ son groupe de Galois et, pour $i = -1, 0, \ldots, \mathrm{N}$, notons G_i le fixateur de $\widetilde{\mathrm{L}}_i$. Alors,

$$\mathrm{G} = \mathrm{G}_{-1} \supseteq \mathrm{G}_0 \supseteq \cdots \supseteq \mathrm{G}_{\mathrm{N}} = \{1\}.$$

D'après le théorème d'Artin, chaque G_i est le groupe de Galois de $\widetilde{\mathrm{L}}_{\mathrm{N}}$ sur $\widetilde{\mathrm{L}}_i$. De plus, comme l'extension $\widetilde{\mathrm{L}}_i \subseteq \widetilde{\mathrm{L}}_{i+1}$ est galoisienne alors, d'après le point 5) du théorème principal de la théorie de Galois 17.18, G_{i+1} est un sous-groupe normal de G_i et $\mathrm{G}_i/\mathrm{G}_{i+1}$ est isomorphe à $\mathrm{Gal}(\widetilde{\mathrm{L}}_{i+1}/\widetilde{\mathrm{L}}_i)$, dont on a vu qu'il était abélien pour $i = -1$, et cyclique pour $i = 0, \ldots, \mathrm{N}$. Par conséquent, G est résoluble !

Finalement, comme $k \subseteq \mathrm{K} \subseteq \widetilde{\mathrm{L}}_{\mathrm{N}}$ et l'extension $k \subseteq \mathrm{K}$ est galoisienne, alors, d'après le point 5) du théorème 17.18, à nouveau, $\mathrm{Gal}(\mathrm{K}/k)$ est isomorphe au quotient G/H, où H désigne le fixateur dans G de K. Par conséquent, d'après le corollaire 19.38, $\mathrm{Gal}(\mathrm{K}/k) = \mathrm{Gal}(\mathrm{P}/k)$ est résoluble. Ceci achève la démonstration du théorème 21.5.

21.4. Un exemple de polynôme $\mathrm{P} \in \mathbb{Q}[\mathrm{X}]$ non résoluble par radicaux. —

***Proposition 21.15* (Critère d'Eisenstein).** — *Soit* $\mathrm{P} \in \mathbb{Z}[\mathrm{X}]$ *un polynôme unitaire de degré* $n \geqslant 1$. *Écrivons* $\mathrm{P} = \mathrm{X}^n + \sum_{i=0}^{n-1} a_i \mathrm{X}^i$. *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* $\mathbb{Z}[\mathrm{X}]$ *et aussi dans* $\mathbb{Q}[\mathrm{X}]$.

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

le chapitre 4, Proposition 9.42. 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 $\geqslant 1$ 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 $d \in \{1, \dots, n\}$ 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 21.16. — Le critère d'Eisenstein s'étend sans difficulté en remplaçant $\mathbb{Z}$ par un anneau factoriel quelconque.

Théorème 21.17. — *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 20.4, 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 19.56, 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 corollaire 19.25 que $G = S_5$. Comme S_5 n'est pas résoluble, d'après le théorème 19.41, le théorème 21.5 montre que P n'est pas résoluble par radicaux sur $\mathbb{Q}$. □

21.5. Compléments sur le critère de résolubilité. — Pour établir la réciproque du théorème 21.5, on utilise les deux théorèmes suivants, qui sont intéressants en eux-mêmes.

Théorème 21.18. — *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 $k \subseteq \mathrm{K}$ galoisienne, et on pose $\mathrm{G} = \mathrm{Gal}(\mathrm{K}/k)$. Alors l'extension $\mathrm{L} \subseteq \mathrm{KL}$ est aussi galoisienne, et son groupe de Galois s'identifie au sous-groupe de* G *fixant les éléments de $\mathrm{K} \cap \mathrm{L}$.*

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

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 21.5, 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 21.20. — *Soient k un corps de caractéristique 0 et* K *un corps de décomposition sur k d'un polynôme non-constant $\mathrm{P} \in k[\mathrm{X}]$. On pose $\mathrm{G} = \mathrm{Gal}(\mathrm{P}/k) = \mathrm{Gal}(\mathrm{K}/k)$. Alors l'équation $\mathrm{P}(x) = 0$ est résoluble par radicaux ssi* G *est résoluble.*

22. Constructions à la règle et au compas

(16) Des références pour cette section sont : [**Esc**, Chap. 5 & 9], [**ChL**, §§ 5.1, 5.2], [**Ti**, Ch.12, Appendix], [**Ja1**, §§ 4.2 & 4.11].

(16) Cette section n'a pas été traitée en cours.

22.1. Trois motivations. — Considérons les questions suivantes. On se suppose muni d'un compas et d'une règle non graduée.

Duplication du cube. Soit donné un cube C, d'arête de longeur a. Est-il possible de construire à la règle et au compas un segment tel que le volume du cube correspondant soit le **double** de celui de C ? C.-à-d., peut-on construire à la règle et au compas, à partir du segment de longeur a donné, un segment de longeur $\sqrt[3]{2}\,a$? La réponse est **NON**, comme on le verra ci-dessous, car le polynôme minimal sur $\mathbb{Q}$ de $\sqrt[3]{2}$ est X^3-2, de degré 3.

Trisection de l'angle. Soit donné un angle α, c.-à-d., sur le cercle « trigonométrique » de centre 0 et de rayon 1, on se donne les points de coordonnées $(1,0)$ et $(\cos\alpha,\sin\alpha)$; est-il possible de construire à la règle et au compas le point de coordonnées $(\cos\theta,\sin\theta)$, où $\theta=\alpha/3$?

À nouveau, la réponse est **NON** en général. En effet, posant $z=e^{i\theta}$ on a :

$$\cos 3\theta=\tfrac{z^3+\bar z^3}{2}=\cos^3\theta+3\cos\theta(i\sin\theta)^2=\cos^3\theta+3\cos\theta(\cos^2\theta-1)$$
$$=4\cos^3\theta-3\cos\theta.$$

Donc, $x=2\cos\theta$ est racine de l'équation

$$\mathrm{X}^3-3\mathrm{X}-2a=0,$$

où $a=\cos 3\theta=\cos\alpha$. En général, ce polynôme de degré 3 est irréductible dans $\mathrm{K}[\mathrm{X}]$, où $\mathrm{K}=\mathbb{Q}(a)$. Par exemple, si $\alpha=2\pi/3$ (resp. $\pi/3$) alors $2\cos(2\pi/3)=-1$ (resp. 1) et le polynôme

$$\mathrm{P}=\mathrm{X}^3-3\mathrm{X}+1\qquad\text{resp.}\quad\mathrm{X}^3-3\mathrm{X}-1$$

n'a pas de racines dans $\mathbb{Q}$. En effet, supposons que $r=p/q$ soit racine, avec p,q sans facteur commun et $q\geqslant 1$. Alors $p^3-3pq^2\pm q^3=0$ montre que q divise p, d'où $q=1$, puis $p(p^2-3)=\pm1$ entraîne $p=\pm1$, mais alors $p(p^2-3)=\mp2$, une contradiction.

Donc P n'a pas de racines dans $\mathbb{Q}$, donc est irréductible dans $\mathbb{Q}[\mathrm{X}]$, et d'après les résultats qu'on verra plus bas ceci montre que les angles $\alpha=2\pi/3$ et $\pi/3$ (c.-à-d., 120 et 60 degrés) ne sont pas trisectables à la règle et au compas.

Polygones réguliers. On sait construire à la règle et au compas un hexagone régulier : partant d'un point arbitraire du cercle unité, par exemple $(1,0)$, il suffit de reporter avec le compas le rayon du cercle. En ne prenant qu'un point sur deux de l'hexagone, on obtient bien sûr un triangle régulier.

D'autre part, comme on peut construire à la règle et au compas la médiatrice d'un segment et la bissectrice d'un angle, on voit que si on peut construire à la règle et au compas le polygone régulier à n côtés, alors on peut aussi construire celui à $2n$, $4n$, …, 2^sn côtés, pour tout $s\geqslant 1$.

Définition 22.1. — Pour tout entier $m\geqslant 0$, posons $\mathrm{F}_m=2^{2^m}+1$. Un nombre premier p est appelé un **nombre premier de Fermat** si $p=\mathrm{F}_m$, pour un

certain entier $m \geqslant 0$. Ainsi,

$$\mathrm{F}_0 = 3, \quad \mathrm{F}_1 = 5, \quad \mathrm{F}_2 = 17, \quad \mathrm{F}_3 = 259, \quad \mathrm{F}_4 = 65537$$

sont premiers. Par contre, Euler a montré que

$$\mathrm{F}_5 = 641 \cdot 6\,700\,417.$$

Actuellement, on sait que $\mathrm{F}_6, \ldots, \mathrm{F}_{32}$ ne sont pas premiers. On ignore s'il y a d'autres nombres premiers de Fermat autres que $\mathrm{F}_0, \ldots, \mathrm{F}_4$!

Théorème 22.2. — *Soit n un entier $\geqslant 3$. Le polygone régulier à n côtés est constructible à la règle et au compas si et seulement si n est le produit d'une puissance arbitraire de 2 et de nombres premiers de Fermat deux à deux distincts.*

Pour les petites valeurs de n, ceci donne le tableau suivant.

3	oui	12	oui	21	non
4	oui	13	non	22	non
5	oui	14	non	23	non
6	oui	15	oui	24	oui
7	non	16	oui	25	non
8	oui	17	oui	34	oui
9	non	18	non	51	oui
10	oui	19	non	68	oui
11	non	20	oui	85	oui

Pour la construction explicite du pentagone régulier, voir [**Esc**, Ex. 5.2], et pour le polygone régulier à 17 côtés, voir [**Ca**, Chap. 4] ou [**Co**, Chap. 2].

22.2. Description du problème et traduction en théorie de Galois. — Le problème donné est donc le suivant. On dispose d'un compas et d'une règle non graduée (mais arbitrairement longue, de même que le compas). On suppose donné un ensemble $\mathscr{E}$ de points de $\mathbb{R}^2$, de cardinal au moins 2. On choisit de façon arbitraire deux points, O et A ; on prend O comme origine et la longueur de OA comme longueur unité. On peut construire à la règle et au compas la perpendiculaire Δ à la droite (OA) passant par O, et choisir sur cette droite le point B tel que $\overrightarrow{i} = \overrightarrow{\mathrm{OA}}$ et $\overrightarrow{j} = \overrightarrow{\mathrm{OB}}$ forment une base orthonormée. Relativement à ce repère, chaque point $p \in \mathscr{E}$ a des coordonnées (x_p, y_p).

Définition 22.3. — 1) On note $\underline{\mathscr{C}}$ l'ensemble des points de $\mathbb{R}^2$ qui sont constructibles à la règle et au compas à partir de $\mathscr{E}$.

2) On note $\mathscr{K}$ l'ensemble des coordonnées des points de $\underline{\mathscr{C}}$. C'est un sous-ensemble de $\mathbb{R}$, appelé **ensemble des nombres contructibles** (à la règle et au compas) à partir de $\mathscr{E}$.

3) Si $\mathscr{E}$ n'a que deux points, ce qui équivaut à se donner des points $\mathrm{O} = (0,0)$ et $\mathrm{A} = (1,0)$ (et donc aussi $\mathrm{B} = (0,1)$, c.-à-d., un repère $(\mathrm{O}, \overrightarrow{i}, \overrightarrow{j})$), on parle alors de **nombres constructibles**.

Observons que l'on peut construire à la règle et au compas : la médiatrice d'un segment, la bissectrice d'un angle, et, étant donné une droite Δ et un point p, la perpendiculaire puis la parallèle à Δ passant par p.

Lemme 22.4. — *Si $t \in \mathbb{R}$ est un nombre constructible (à partir de $\mathscr{E}$), alors les points $(t,0)$ et $(0,t)$ appartiennent à $\underline{\mathscr{C}}$.*

Démonstration. — Supposons que t soit la 1ère coordonnée d'un point $p \in \underline{\mathscr{C}}$. Alors la projection orthogonale de p sur l'axe $\mathrm{O}\overrightarrow{i}$ est constructible, donc $(t,0) \in \underline{\mathscr{C}}$. On peut alors reporter au compas la longueur $|t|$ sur l'axe $\mathrm{O}\overrightarrow{j}$ pour obtenir les points $(0, \pm t)$. □

Proposition 22.5. — *L'ensemble $\mathscr{K}$ des nombres constructibles (à partir de $\mathscr{E}$) est un* **sous-corps** *de $\mathbb{R}$.*

Démonstration. — Si x, y sont constructibles alors $\underline{\mathscr{C}}$ contient $(x,0)$ et $(0,y)$. D'une part, on peut reporter au compas la longueur $|y|$ pour obtenir $(x \pm y, 0)$. D'autre part, soit Δ la droite joignant le point $(0,1)$ au point $(x,0)$. Si $y \neq 0$ alors la parallèle à Δ passant par le point $(y,0)$ coupe l'axe $\mathrm{O}\overrightarrow{i}$ au point $(x/y, 0)$. Ceci montre que $x \pm y$ et x/y (si $y \neq 0$) sont constructibles, donc $\mathscr{K}$ est bien un sous-corps de $\mathbb{R}$. □

Notation 22.6. — Notons k_0 le sous-corps de $\mathbb{R}$ engendré par les coordonnées des points de $\mathscr{E}$ (donnés au départ). (Ainsi, si $\mathscr{E}$ n'a que deux points, ce qui équivaut à se donner des points $\mathrm{O} = (0,0)$ et $\mathrm{A} = (1,0)$, alors $k_0 = \mathbb{Q}$).

Théorème 22.7. — *Soit $\alpha \in \mathbb{R}$. Les conditions suivantes sont équivalentes :*

1) *α est constructible à la règle et au compas à partir de $\mathscr{E}$;*

2) *α est contenu dans une tour d'extensions quadratiques de k_0, c.-à-d., il existe une tour*

$$k_0 = \mathrm{K}_0 \subseteq \mathrm{K}_1 \subseteq \cdots \subseteq \mathrm{K}_r$$

telle que $[\mathrm{K}_i : \mathrm{K}_{i-1}] = 2$ pour tout i, et $\alpha \in \mathrm{K}_r$.

Démonstration. — 1) ⇒ 2). Voyons comment construire de nouveaux points à partir de points existants, à coefficients dans un sous-corps k_1 dont on suppose qu'il vérifie la condition 2).

a) Si on a des points $p_0 = (x_0, y_0)$ et $p_1 = (x_0 + x_1, y_0 + y_1)$, on peut construire le point $(r,0)$ où r est la longueur du segment p_0p_1, c.-à-d.,

$$r = \sqrt{x_1^2 + y_1^2},$$

c.-à-d., on prend la racine carrée d'un élément de k_1.

b) Toute droite D entre deux points à coordonnées dans k_1 est définie par une équation

$$aX + bY + c = 0, \qquad \text{avec} \quad a, b, c \in k_1.$$

Si D_1 est une autre droite, d'équation $a'X + b'Y + c' = 0$, et sécante à D en un point $p = (x, y)$, alors (x, y) est l'unique solution du système linéaire à coefficients dans k_1 :

$$\begin{cases} aX + bY = -c\,; \\ a'X + b'Y = -c'\,; \end{cases}$$

et donc l'on a $x, y \in k_1$.

c) Si $\mathscr{C}$ est un cercle, centré en un point $p_0 = (x_0, y_0)$ à coordonnées dans k_1 et passant par le point $p_1 = (x_1, y_1)$ à coordonnées dans k_1 également, alors l'équation de $\mathscr{C}$ est

$$(*) \qquad (X - x_0)^2 + (Y - y_0)^2 = (x_1 - x_0)^2 + (y_1 - y_0)^2 = \mu \in k_1.$$

Supposons que $\mathscr{C}$ rencontre la droite D (en deux points distincts ou un point double si D est tangente à $\mathscr{C}$), et soit $q = (x, y)$ un point d'intersection. Quitte à échanger x et y, on peut supposer que $y = \alpha x + \beta$, avec $\alpha, \beta \in k_1$, et alors x est racine d'une équation quadratique

$$X^2 - bX + c = 0,$$

dont on sait, de plus, que son déterminant $\Delta = b^2 - 4c$ est $\geqslant 0$ puisque x est une racine réelle. Donc x et y appartiennent à l'extension quadratique

$$k_1[\sqrt{\Delta}\,].$$

d) Considérons enfin un deuxième cercle $\mathscr{C}'$, d'équation

$$(*') \qquad (X - x_0')^2 + (Y - y_0')^2 = (x_1' - x_0')^2 + (y_1' - y_0')^2 = \mu' \in k_1,$$

et supposons que $\mathscr{C}$ et $\mathscr{C}'$ se rencontrent (en deux points distincts, ou un point double si $\mathscr{C}$ et $\mathscr{C}'$ sont tangents). Soit $q = (x, y)$ un point d'intersection. Alors, en soustrayant $(*')$ de $(*)$, on obtient que (x, y) sont solutions de $(*)$ et de l'équation linéaire

$$(x_0' - x_0)(2X - x_0 - x_0') + (y_0' - y_0)(2Y - y_0 - y_0') = \mu - \mu',$$

et l'on est ainsi ramené au cas c) précédent. Ceci achève la preuve de l'implication 1) $\Rightarrow$ 2).

Réciproquement, montrons que 2) $\Rightarrow$ 1). Par récurrence sur la hauteur de la tour (= le nombre r d'extensions), il suffit de montrer que si $\alpha \in \mathbb{R}$ est racine d'une équation quadratique

$$(\dagger) \qquad X^2 - bX + c = 0,$$

où b, c sont dans un sous-corps k_1 de $\mathbb{R}$, alors α est constructible sur k_1 (c.-à-d., à partir des points à coordonnées dans k_1). Comme α est une racine réelle de (†), le discriminant $\Delta = b^2 - 4c \in k_1$ est $\geqslant 0$ et donc

$$\alpha = \frac{b \pm \sqrt{\Delta}}{2}.$$

Par conséquent, α est constructible à partir de k_1 si et seulement si $\sqrt{\Delta}$ l'est. On se ramène ainsi à montrer l'assertion suivante :

$$\text{si } c \in k_1 \cap \mathbb{R}_+^*, \text{ alors } \sqrt{c} \text{ est constructible sur } k_1.$$

Or, on peut construire le point $\mathrm{P} = (0, c+1)$, puis le milieu $\mathrm{I} = (0, (c+1)/2)$ du segment OP, puis le cercle $\mathscr{C}$ de centre I et de rayon $\mathrm{IO} = \mathrm{IP} = (c+1)/2$. Soit A le point $(1, 0)$ et soit $\mathrm{Q} = (1, y)$ le point d'intersection de la droite $\mathrm{X} = 1$ avec le cercle $\mathscr{C}$, avec $y > 0$. Alors

$$\left(\frac{c+1}{2}\right)^2 = \mathrm{IQ}^2 = \mathrm{IA}^2 + \mathrm{AQ}^2 = \left(\frac{c-1}{2}\right)^2 + y^2,$$

d'où $y^2 = \left(\frac{c+1}{2}\right)^2 - \left(\frac{c-1}{2}\right)^2 = c$. Ceci montre que $y = \sqrt{c}$ est constructible sur k_1. Le théorème est démontré. □

Corollaire 22.8. — **Si** $\alpha \in \mathbb{R}$ *est constructible sur le sous-corps* k_0, **alors** *le degré de* α *sur* k_0 *est une puissance de* 2.

Démonstration. — D'après le théorème précédent, $k_0[\alpha]$ est contenu dans le terme K_r d'une tour d'extensions quadratiques. Par multiplicativité des degrés,

$$2^r = [\mathrm{K}_r : k_0] = [\mathrm{K}_r : k_0[\alpha]] \cdot \deg_{k_0}(\alpha),$$

donc $\deg_{k_0}(\alpha)$ est un diviseur de 2^r, donc un certain 2^s avec $s \leqslant r$. □

Remarque 22.9. — La condition « $\deg_{k_0}(\alpha) = 2^s$ » est donc une condition **nécessaire** de constructibilité (c.-à-d., si $\deg_{k_0}(\alpha) \neq 2^s$ alors α n'est **pas** constructible).

En particulier, ceci explique l'impossibilité de réaliser à la règle et au compas la duplication du cube, ou la trisection d'un angle arbitraire (par exemple, $2\pi/3$).

Remarque 22.10. — **Mais attention**, ce n'est pas une condition suffisante ! En effet, on a le théorème suivant.

Théorème 22.11. — *Soient* $\alpha \in \mathbb{C}$ *et* k_0 *un sous-corps de* $\mathbb{C}$. *Les conditions suivantes sont équivalentes :*

1) α *est constructible à la règle et au compas sur* k_0 *;*

2) α *est contenu dans une extension galoisienne* K *de* k_0 *telle que* $[\mathrm{K} : k_0] = 2^t$, *pour un certain* $t \in \mathbb{N}$.

Démonstration. — 2) ⇒ 1). Supposons $\alpha \in \mathrm{K}$, où K/k_0 est extension galoisienne de degré 2^t. Alors, le groupe de Galois $\mathrm{G} = \mathrm{Gal}(\mathrm{K}/k_0)$ est un 2-groupe. D'après le corollaire 19.54, il existe une suite décroissante de sous-groupes

$$\mathrm{G} = \mathrm{G}_0 \rhd \mathrm{G}_1 \rhd \mathrm{G}_2 \rhd \cdots \rhd \mathrm{G}_{r+1} = \{1\}$$

telle que $\mathrm{G}_i/\mathrm{G}_{i+1} \cong \mathbb{Z}/2\mathbb{Z}$ pour $i = 0, 1, \ldots, r$. Considérons les corps intermédiaires associés :

$$k_0 = \mathrm{K}_0 \subset \mathrm{K}_1 \subset \cdots \subset \mathrm{K}_r = \mathrm{K}.$$

Alors, chaque $\mathrm{K}_i/\mathrm{K}_{i-1}$ est de degré 2, c.-à-d., une extension quadratique. Donc $\alpha \in \mathrm{K}_r$ est constructible sur k_0.

1) ⇒ 2). Supposons α constructible sur k_0, c.-à-d., il existe une tour d'extensions quadratiques

$$k_0 = \mathrm{L}_0 \subset \mathrm{L}_1 \subset \cdots \subset \mathrm{L}_r$$

telle que $\alpha \in \mathrm{L}_r$. D'après la preuve du théorème 21.5, donnée au § 21.3, cette tour est contenue dans une tour d'extensions quadratiques

$$k_0 = \widetilde{\mathrm{L}}_0 \subset \widetilde{\mathrm{L}}_1 \subset \cdots \subset \widetilde{\mathrm{L}}_{\mathrm{N}}$$

où, de plus, $\widetilde{\mathrm{L}}_{\mathrm{N}}$ est galoisienne sur k_0, de degré 2^{N}. Ceci prouve que 1) ⇒ 2).

Dans ce cas particulier où chaque $\mathrm{L}_i/\mathrm{L}_{i-1}$ est quadratique, la tour $(\widetilde{\mathrm{L}}_j)_{j=1}^{\mathrm{N}}$ est facile à construire explicitement. Pour $i = 1, \ldots, r$, écrivons

$$\mathrm{L}_i = \mathrm{L}_{i-1}[\sqrt{\xi_i}], \qquad \text{où} \quad \xi_i \in \mathrm{L}_{i-1}.$$

Chaque $\mathrm{L}_i/\mathrm{L}_{i-1}$ est galoisienne, de groupe $\{1, \tau_i\}$, où τ_i est l'involution définie par

$$\tau_i(a + b\sqrt{\xi_i}) = a - b\sqrt{\xi_i}, \qquad \forall\, a, b \in \mathrm{L}_{i-1}.$$

L'extension L_2/k_0 n'est pas nécessairement galoisienne, mais le polynôme

$$\mathrm{P}_2 := (\mathrm{X}^2 - a_2)(\mathrm{X}^2 - \tau_1(a_2)) \in \mathrm{L}_1[\mathrm{X}]$$

est invariant par τ_1 donc appartient à $k_0[\mathrm{X}]$. Ses racines sont $\pm\sqrt{a_2}$ et $\pm\sqrt{\tau_1(a_2)}$. Par conséquent,

$$\widetilde{\mathrm{L}}_2 = \mathrm{L}_2[\sqrt{\tau_1(a_2)}] = \mathrm{L}_1[\sqrt{a_2}, \sqrt{\tau_1(a_2)}]$$

est une extension galoisienne de k_0, puisque c'est le corps de décomposition sur k_0 du polynôme $\mathrm{P}_1\mathrm{P}_2$, où $\mathrm{P}_1 = \mathrm{X}^2 - a_1$.

De plus, $[\widetilde{\mathrm{L}}_2 : \mathrm{L}_2]$ égale 1 ou 2, donc $\widetilde{\mathrm{L}}_2$ est de degré 4 ou 8 sur k_0. Notons Γ_2 son groupe de Galois. Alors

$$\mathrm{P}_3 := \prod_{g \in \Gamma_2} (\mathrm{X}^2 - g(a_3)) \in \mathrm{L}_2[\mathrm{X}]$$

est invariant par Γ_2, donc appartient à k_0. Par conséquent,

$$\widetilde{\mathrm{L}}_3 = \widetilde{\mathrm{L}}_2[\sqrt{g(a_3)} \mid g \in \Gamma_2]$$

est galoisienne sur k_0, car corps de décomposition de $P_1P_2P_3$. De plus, le degré de $\widetilde{L}_3$ sur $\widetilde{L}_2$ est une puissance de 2 ; en effet, si on numérote $g_1, \dots, g_n$ les éléments de Γ_2 (avec, disons, $g_1 = \mathrm{id}$), alors on a la tour

$$\widetilde{L}_2 \subset \widetilde{L}_2[\sqrt{a_3}\,] \subseteq \widetilde{L}_2[\sqrt{a_3}, \sqrt{g_2(a_3)}] \subseteq \cdots \subseteq \widetilde{L}_2[\sqrt{a_3}, \cdots, \sqrt{g_n(a_3)}] = \widetilde{L}_3,$$

où à chaque étape l'extension est de degré 2 ou 1. Par conséquent, le degré de $\widetilde{L}_3$ sur k_0 est une puisance de 2. En poursuivant ainsi, on plonge ainsi la tour de départ dans une tour

$$k_0 = \widetilde{L}_0 \subset \widetilde{L}_1 \subset \cdots \subset \widetilde{L}_N$$

où chaque $\widetilde{L}_j$ est galoisienne sur k_0, de degré une puissance de 2. □

Remarque 22.12. — Soit $P \in \mathbb{Q}[X]$ un polynôme irréductible de degré 4, dont le groupe de Galois est S_4 (ou A_4), et ayant une racine réelle α. Alors, le sous-corps K de $\mathbb{C}$ engendré par les racines de P est de degré 24 (resp. 12) sur $\mathbb{Q}$. D'autre part, P est le polynôme minimal de α sur $\mathbb{Q}$, mais α n'est pas constructible sur $\mathbb{Q}$ car toute extension galoisienne $L/\mathbb{Q}$ contenant α contient aussi K donc le degré $[L : \mathbb{Q}]$ est divisible par 3.

22.3. Polygones réguliers. — Pour finir, on va démontrer le théorème 22.2.

Définition 22.13. — Soit p un nombre premier. On pose

$$\Phi_p(X) = \sum_{i=0}^{p-1} X^i = X^{p-1} + \cdots + X + 1,$$

et, pour tout $n \geqslant 1$,

$$\Phi_{p^n}(X) = \Phi_p(X^{p^{n-1}}) = X^{(p-1)p^{n-1}} + \cdots + X^{p^{n-1}} + 1.$$

Alors, chaque Φ_{p^n} est de degré $(p-1)p^{n-1}$.

Comme $X^p - 1 = (X-1)\Phi_p$ alors, pour tout $n \in \mathbb{N}^*$ on a

$$X^{p^n} - 1 = (X^{p^{n-1}} - 1)\Phi_p(X^{p^{n-1}}) = (X^{p^{n-1}} - 1)\Phi_{p^n},$$

d'où, par récurrence sur n, l'égalité :

$$(*) \qquad X^{p^n} - 1 = (X-1)\Phi_p \cdots \Phi_{p^{n-1}}\Phi_{p^n}.$$

Proposition 22.14. — *Chaque Φ_{p^n} est irréductible dans $\mathbb{Q}[X]$.*

Démonstration. — D'après le lemme des contenus de Gauss, il suffit de montrer que Φ_{p^n} est irréductible dans $\mathbb{Z}[X]$. Supposons qu'on ait une égalité

$$(\dagger) \qquad \Phi_{p^n} = PQ, \qquad \text{avec } P, Q \in \mathbb{Z}[X], \text{ non inversibles.}$$

Comme Φ_{p^n} est unitaire, on peut supposer P et Q unitaires, de degrés $a > 0$ et $b > 0$, respectivement.

Réduisons l'égalité (†) modulo p. Comme

$$\Phi_{p^n} \equiv (\Phi_p)^{p^{n-1}} \equiv (\mathrm{X}-1)^{p^{n-1}} \mod p,$$

on en déduit que $\mathrm{P} = (\mathrm{X}-1)^a + p\mathrm{A}$ et $\mathrm{Q} = (\mathrm{X}-1)^b + p\mathrm{B}$, avec $\mathrm{A}, \mathrm{B} \in \mathbb{Z}[\mathrm{X}]$. Alors, (†) donne

$$\Phi_{p^n} = p^2\mathrm{AB} \mod (\mathrm{X}-1),$$

et évaluant en $\mathrm{X} = 1$ on obtient

$$p = \Phi_{p^n}(1) = p^2\mathrm{A}(1)\mathrm{B}(1),$$

une contradiction. Ceci montre que Φ_{p^n} est irréductible. La proposition est démontrée. □

Corollaire 22.15. — *Soit $\xi \in \mathbb{C}$ une racine de l'unité primitive d'ordre p^n. Alors le polynôme minimal de ξ sur $\mathbb{Q}$ est Φ_{p^n}. Par conséquent, l'extension galoisienne $\mathbb{Q}[\xi]/\mathbb{Q}$ est de degré $(p-1)p^n$.*

Démonstration. — ξ est racine de $\mathrm{X}^{p^n} - 1$ mais pas de $\mathrm{X}^{p^{n-1}} - 1$, donc ξ est racine de Φ_{p^n}. Comme ce dernier est irréductible et unitaire, c'est le polynôme minimal de ξ sur $\mathbb{Q}$. Donc l'extension $\mathbb{Q}[\xi]/\mathbb{Q}$ est de degré $(p-1)p^n$, et on a déjà vu qu'elle est galoisienne (Prop. 21.11). □

Proposition 22.16. — *Soient $\mathrm{N} \geqslant 3$ et $\xi = e^{2i\pi/\mathrm{N}}$. On pose $\varphi(\mathrm{N}) = \deg_{\mathbb{Q}}(\xi)$. Alors l'extension*

$$\mathbb{Q} \subset \mathbb{Q}[\cos(2\pi/\mathrm{N})]$$

est galoisienne, de degré $\varphi(\mathrm{N})/2$.

Démonstration. — ξ est une racine de l'unité primitive d'ordre N et l'on a

$$\xi = \cos(2\pi/\mathrm{N}) + i\,\sin(2\pi/\mathrm{N}), \qquad \xi^{-1} = \overline{\xi} = \cos(2\pi/\mathrm{N}) - i\,\sin(2\pi/\mathrm{N}).$$

Posons $c = \cos(2\pi/\mathrm{N})$. Alors ξ et ξ^{-1} sont les deux racines du polynôme

$$\mathrm{X}^2 - 2c\mathrm{X} + 1.$$

Par conséquent, le degré d de $\mathbb{Q}[\xi]$ sur $\mathbb{Q}[c]$ est égal à 2 où 1. Mais ce ne peut être 1, car $\mathbb{Q}[c] \subseteq \mathbb{R}$ tandis que $\xi \notin \mathbb{R}$, d'où $\mathbb{Q}[c] \neq \mathbb{Q}[\xi]$ et donc $d > 1$. Donc $d = 2$, et par multiplicativité des degrés on obtient que

$$[\mathbb{Q}[\cos(2\pi/\mathrm{N}) : \mathbb{Q}] = \frac{[\mathbb{Q}[\xi] : \mathbb{Q}]}{2}.$$

Enfin, d'après la Proposition 21.11, l'extension $\mathbb{Q}[\xi]/\mathbb{Q}$ est galoisienne, de groupe de Galois G abélien. Comme $\overline{\xi} = \xi^{-1}$ alors la conjugaison complexe induit un automorphisme τ de $\mathrm{K} := \mathbb{Q}[\xi]$, non trivial puisque $\tau(\xi) \neq \xi$. Alors le sous-corps fixe

$$\mathrm{L} = \mathrm{K}^{\tau}$$

contient $\mathbb{Q}[\cos(2\pi/\mathrm{N})]$ et comme $[\mathrm{K} : \mathrm{L}] = 2$ d'après le théorème d'Artin, on a

$$\mathbb{Q}[\cos(2\pi/\mathrm{N})] = \mathrm{K}^{\tau}.$$

Comme G est abélien, le sous-groupe $\{1, \tau\}$ est normal, et donc l'extension $\mathbb{Q} \subset \mathbb{Q}[\cos(2\pi/\mathrm{N})]$ est galoisienne. La proposition est démontrée. □

Comme on peut construire à la règle et au compas la bissectrice d'un angle, on voit que si on peut construire à la règle et au compas le polygone régulier à n côtés, alors on peut aussi construire celui à $2^s n$ côtés, pour tout $s \geqslant 1$. Évidemment, on peut construire à la règle et au compas un carré (et aussi le « polygone régulier à deux côtés », en définissant celui-ci comme un diamètre du cercle) ; donc on peut construire les polygones réguliers à 2^s côtés, pour tout $s \geqslant 1$.

Proposition 22.17. — *Soient p un nombre premier impair et $n \in \mathbb{N}^*$. Alors $\cos(2\pi/p^n)$ est constructible sur $\mathbb{Q}$ si et seulement si $n = 1$ et*

$$p = 2^{2^m} + 1 \qquad \textit{pour un certain } m \geqslant 0.$$

Démonstration. — D'après ce qui précède, le degré sur $\mathbb{Q}$ de $c := \cos(2\pi/p^n)$ est

$$d := \frac{(p-1)p^{n-1}}{2}.$$

Si c est constructible alors, d'après le corollaire 22.8, $d = 2^{s-1}$, pour un certain $s \geqslant 1$, et donc $n = 1$, car sinon d serait divisible par p. Donc, on a

$$p = 2^s + 1.$$

Ceci entraîne, de plus, que $s = 2^m$ pour un certain $m \in \mathbb{N}$. En effet, écrivons $s = 2^m(2r+1)$. Appliquant l'égalité

$$1 - \mathrm{X} + (-\mathrm{X})^2 + \cdots + (-\mathrm{X})^{2r} = \frac{1 - (-\mathrm{X})^{2r+1}}{1 + \mathrm{X}} = \frac{1 + \mathrm{X}^{2r+1}}{1 + \mathrm{X}}$$

à $\mathrm{X} = 2^{2^m}$, on obtient

$$p = (2^{2^m} + 1)(1 - \mathrm{X} + \cdots)$$

et comme p est premier ceci entraîne que $p = 2^{2^m} + 1$ (et $r = 0$).

Réciproquement, supposons que $p = 2^{2^m} + 1$ soit un nombre premier de Fermat. Alors l'extension

$$\mathbb{Q} \subset \mathbb{Q}[\cos(2\pi/p)]$$

est galoisienne, de degré $d = 2^{2^m - 1}$, donc $\cos(2\pi/p)$ est constructible. La proposition est démontrée. □

Remarquons enfin que si on peut construire le polygone régulier à N côtés, on peut construire celui à d côtés, pour tout diviseur d de N. En effet, écrivons $\mathrm{N} = rd$; si on a construit le polygone régulier à N cotés, alors en ne joignant que les sommets de d en d, on obtient le polygone régulier à $r = \mathrm{N}/d$ côtés. On déduit donc de la proposition 22.17 le corollaire suivant.

Corollaire 22.18. — *Si le polygone régulier à* N *côtés est constructible à la règle et au compas, alors la décomposition de* N *est facteurs premiers est :*

$$\mathrm{N} = 2^s p_1 \cdots p_n,$$

où les p_i sont des nombres premiers de Fermat deux à deux distincts.

Pour achever la preuve du théorème 22.2, il suffit de faire les deux observations suivantes. Soit A le point $(1, 0)$.

1) Si l'on peut construire $\cos(\theta)$, on peut construire le point $\mathrm{P} = e^{i\theta}$ du cercle trigonométrique. Reportant la distance AP, on peut construire les points $e^{ir\theta}$, pour tout $r \in \mathbb{Z}$, et donc $\cos(r\theta)$ est constructible pour tout $r \in \mathbb{Z}$.

2) Supposons qu'on puisse construire les polygones réguliers à m et n côtés, où $m, n \in \mathbb{N}^*$ sont premiers entre eux. D'après le théorème de Bézout, il existe $r, s \in \mathbb{Z}$ tels que

$$rm + sn = 1.$$

Alors, partant de $\mathrm{A} = (1, 0)$ et reportant r fois l'angle $2\pi/n$, puis s fois l'angle $2\pi/m$, on obtient l'angle

$$2\pi \left(\frac{r}{n} + \frac{s}{m} \right) = 2\pi \frac{rm + sn}{mn} = \frac{2\pi}{mn}.$$

Ceci montre que le polygone régulier à mn côtés est constructible.

On a donc achevé la démonstration du théorème 22.2, que l'on récrit ci-dessous.

Théorème 22.19. — *Soit* N *un entier* $\geqslant 3$. *Le polygone régulier à* N *côtés est constructible à la règle et au compas si et seulement si* N *est le produit d'une puissance arbitraire de* 2 *et de nombres premiers de Fermat deux à deux distincts.*

TABLE DES MATIÈRES

VIII. Extensions normales, séparables, galoisiennes. Corps finis

IX. Groupes et polynômes symétriques, résolution d'équations

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.

[Ca] J.-C. Carrega, Théorie des corps – La règle et le compas, Hermann, 1981, 2ème édition 1989.

[ChL] A. Chambert-Loir, Algèbre corporelle, Éditions de l'École Polytechnique, 2005.

[Co] H. S. M. Coxeter, Introduction to Geometry, 2nd edition, Wiley, 1969.

[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.

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

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

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

[Fu] W. Fulton, Algebraic Curves, Benjamin, 1969.

[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.

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

[Ne04] J. Nekovář, 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.

[Re] M. Reid, Undergraduate commutative algebra, Cambridge Univ. Press, 1995.

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

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

[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.