# Chapitre 10

# Groupes et équations résolubles

Version du 4 janvier 2005

Dans ce chapitre, tous les groupes considérés sont finis, et tous les corps considérés sont des sous-corps de $\mathbb{C}$.

## 10.1 Groupes résolubles et non-résolubilité de $S_n$ pour $n \geq 5$

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

### 10.1.1 Groupes résolubles

**Définition 10.1.1** *$G$ est résoluble s'il existe une suite finie de sous-groupes*

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

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

**Définition 10.1.2** *1) Pour $x, y \in G$, on définit leur commutateur $[x, y] := xyx^{-1}y^{-1}$. On a $[x, y] = 1$ ssi $xy = yx$, c.-à-d., ssi $x$ et $y$ commutent.*

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

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

**Lemme 10.1.1** 1) *On a $D(G) = \phi(D(G))$ pour tout automorphisme de $G$. En particulier, $D(G)$ est un sous-groupe normal de $G$.*

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

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

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

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

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

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

Ceci prouve 4). □

**Définition 10.1.3** *On pose $D^0(G) = G$, $D^1(G) = D(G)$ et pour $i \geq 1$ on définit $D^{i+1}(G) = D(D^i(G))$. D'après ce qui précède, chaque $D^{i+1}(G)$ est normal dans $D^i(G)$ et le quotient $D^i(G)/D^{i+1}(G)$ est abélien. La suite*

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

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

**Proposition 10.1.2** *$G$ est résoluble ssi il existe $r \geq 0$ tel que $D^r(G) = \{1\}$.*

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

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

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

**Corollaire 10.1.3** *Soient $G$ un groupe, $H$ un sous-groupe arbitraire, $H'$ un sous-groupe normal, et $G' = G/H'$.*

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

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

*Démonstration.* Notons $\pi$ la projection $G \to G'$. En procédant par récurrence, on déduit du lemme 10.1.1 (points 2. et 3.) que $D^i(H) \subseteq D^i(G)$ et $\pi(D^i(G)) = D^i(G')$ pour tout $i \geq 0$. Par conséquent, si $G$ est résoluble, $H$ et $G'$ le sont aussi.

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

**Exemples 10.1.1** 1) Le groupe symétrique $S_3$ est résoluble car $A_3 \cong \mathbb{Z}/3$ et $S_3/A_3 \cong \{\pm 1\}$.

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

### 10.1.2 Propriétés des groupes symétriques $S_n$

**Notation** On représente en général un élément $\tau$ 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,

$$\begin{pmatrix} 123456 \\ 321654 \end{pmatrix}$$

est un élément de $S_6$. Pour certaines permutations, on utilise une écriture plus condensée. Soient $i \neq j$ dans $\{1, \ldots, n\}$ ; on note $(ij)$ la permutation qui échange $i$ et $j$ et laisse les autres nombres inchangés. Plus généralement, on dit que $\tau$ est un $r$-cycle ($r \geq 2$) 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 $\tau = (i_1 i_2 \cdots i_r)$. Par exemple, dans $S_6$, (253) et (1635) désignent, respectivement, les permutations suivantes :

$$\begin{pmatrix} 123456 \\ 152436 \end{pmatrix}, \qquad \begin{pmatrix} 123456 \\ 625413 \end{pmatrix}.$$

Si $\tau$ 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 $r$.

**Théorème 10.1.4 (Générateurs de $S_n$)** *Pour tout $n \geq 2$, $S_n$ est engendré par les transpositions $(12), (23), \cdots, (n-1, n)$.*

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

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

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

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

### Conjugaison et signature des cycles

On rappelle la définition du morphisme signature $\varepsilon : S_n \to \{\pm 1\}$, *cf.* 9.4.1. Pour tout $i$, on voit facilement que le couple $(i, i+1)$ est la seule inversion de $s_i$, et donc $\varepsilon(s_i) = -1$.

**Théorème 10.1.5** *Soit $r \leq n$. Tous les $r$-cycles de $S_n$ sont conjugués, et sont de signature $(-1)^{r-1}$.*

*Démonstration.* Soit $c = (i_1 i_2 \cdots i_r)$ un $r$-cycle arbitraire et soit $c_0$ le $r$-cycle $(12 \cdots r)$. Choisissons une bijection de $\{r+1, \ldots, n\}$ sur $\{1, \ldots, n\} \setminus \{i_1, \ldots, i_r\}$ et soit $\tau$ la permutation définie par $\tau(k) = i_k$ pour $k \leq r$ et $\tau(k) = \phi(k)$ pour $k > r$. Alors, on vérifie facilement que

$$\tau c_0 \tau^{-1} = c.$$

Ceci prouve la première assertion. En particulier, on a $\varepsilon(c) = \varepsilon(c_0)$. Par conséquent, il suffit de calculer $\varepsilon(c_0)$. Or, on voit facilement que

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

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

**Théorème 10.1.6 (Générateurs de $A_n$)** *On a $A_2 = \{1\}$ et, pour $n \geq 3$, $A_n$ est engendré par les produits de deux transpositions et aussi par les 3-cycles.*

*Démonstration.* Il est clair que $A_2 = \{1\}$. Supposons $n \geq 3$ et soit $\sigma \in A_n$. D'après le théorème 10.1.4, on peut écrire $\sigma$ comme un produit

$$s_{i_1} s_{i_2} \cdots s_{i_N}.$$

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

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

appartient au sous-groupe engendré par les produits de deux transpositions. Ceci prouve la 1ère assertion.

D'après le théorème 10.1.5, tout 3-cycle appartient à $A_n$. Donc, pour établir la 2ème 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 $\sigma$ 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. □

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

**Proposition 10.1.7** *Si $n \geq 5$, tout 3-cycle appartient à $D(A_n)$. Par conséquent, on a $A_n = D(A_n) = D^i(A_n)$, pour tout $i \geq 1$.*

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

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

Comme $(acd)$, resp. $(bce)$, est l'inverse de $(adc)$, resp. $(bec)$, alors $\sigma$ est le commutateur de $(acd)$ et $(bec)$, donc appartient à $D(A_n)$. Calculons les images

par $\sigma$ 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, $\sigma$ laisse inchangés les autres nombres. Donc, $\sigma = (abc)$ !

Comme les 3-cycles engendrent $A_n$, d'après le théorème 10.1.6, ceci montre que $A_n = D(A_n)$, et donc $A_n = D^i(A_n)$ pour tout $i \geq 1$. La proposition est démontrée. □

**Corollaire 10.1.8** *Pour $n \geq 5$, $A_n$ et $S_n$ ne sont pas résolubles.*

*Démonstration.* Soit $n \geq 5$. $A_n$ n'est pas résoluble, puisque $A_n = D^i(A_n)$ pour tout $i \geq 1$. Par conséquent, $S_n$ ne l'est pas non plus, d'après le corollaire 10.1.3. Plus précisément, comme tout commutateur est de signature 1, on a $D(S_n) \subseteq A_n$ pour tout $n$, et l'égalité $A_n = D(A_n)$ entraîne a fortiori $A_n = D(S_n)$. □

**Remarque 10.1.1** En fait, on a $D(S_n) = A_n$ pour tout $n$. C'est clair pour $n = 2$, et pour $n \geq 3$ il suffit de montrer que tout 3-cycle $(ijk)$ est un commutateur dans $S_n$. C'est bien le cas, car $(ijk) = (jk)(ij)(jk)(ij)$.

**Définition 10.1.4** *On dit qu'un groupe $G$ est simple s'il est non abélien et si ses seuls sous-groupes distingués sont $\{1\}$ et $G$. Dans ce cas, on a nécessairement $D(G) = G$. En particulier, un groupe simple n'est pas résoluble.*

**Remarque 10.1.2** On peut montrer, en fait, que $A_n$ est simple pour $n \geq 5$. Voir, par exemple, [Pe1, §I.8] ou [BR, p.188].

## 10.2 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.

### 10.2.1 Extensions radicales

**Définition 10.2.1** *Une suite finie d'extensions de corps $k = K_0 \subseteq K_1 \subseteq \cdots \subseteq K_r$ s'appelle une tour d'extensions (ou une tour de corps).*

**Définition 10.2.2** *Soit $L$ une extension algébrique de $k$ contenue dans $\mathbb{C}$. Nous dirons que l'extension $k \subseteq L$ est :*

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

*2) radicale s'il existe une tour*

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

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

**Définition 10.2.3** *Soit $P \in k[X]$ de degré $\geq 1$ et soit $K$ le sous-corps de $\mathbb{C}$ engendré par $k$ et les racines de $P$ dans $\mathbb{C}$. On dit que $P$ (ou l'équation $P(x) = 0$) est résoluble par radicaux sur $k$ s'il existe une extension radicale $k \subseteq L$ contenant $K$ c.-à-d., telle que $k \subseteq K \subseteq L$.*

**Remarque 10.2.1** Comme $\mathbb{C}$ est algébriquement clos, $P$ y est scindé, et donc $K$ est un corps de décomposition de $P$ sur $k$. De plus, comme $P$ est séparable, puisque $\mathrm{car}(k) = 0$, l'extension $k \subseteq K$ est galoisienne. On rappelle que son groupe de Galois est désigné par $\mathrm{Gal}(P/k)$.

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

**Théorème 10.2.1** *Si $P$ est résoluble par radicaux, alors le groupe $\mathrm{Gal}(P/k)$ est résoluble.*

**Remarque 10.2.2** 1) Grâce à ce théorème, on pourra donner des exemples d'équations non résolubles par radicaux, en montrant que le groupe de Galois correspondant n'est pas résoluble.

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

3) L'idée de la démonstration du théorème est très simple, et peut s'expliquer comme suit. Avec les notations précédentes, on suppose $K$ contenu dans une extension radicale $L$. Supposons de plus que chaque extension $L_i \subseteq L_{i+1}$ soit galoisienne, pour $i = 0, \ldots, r-1$, et que $k \subseteq L_r = L$ le soit aussi. Soit $G = \mathrm{Gal}(L/k)$ et notons $G_i$ le fixateur dans $G$ de $L_i$. Alors les hypothèses entraînent que

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

et que chaque $G_i/G_{i+1}$ est abélien. Donc, $G$ est résoluble. Enfin, $k \subseteq K \subseteq L$ et l'extension $k \subseteq K$ est galoisienne. Par conséquent, d'après le théorème 7.5.7, $\mathrm{Gal}(P/k)$ est un groupe quotient de $G$, donc est aussi résoluble.

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

### 10.2.2 Adjonction de racines de l'unité

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

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

**Définition 10.2.4** *Soit $L$ une extension algébrique de $K$ contenue dans $\mathbb{C}$. Nous dirons que l'extension $K \subseteq L$ est radicale élémentaire* **d'exposant divisant** *$n$ s'il existe $a \in L^\times$ et $n \geq 1$ tels que $L = K[a]$ et $a^n \in K$.*

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

**Proposition 10.2.2** *Soient $K$ un sous-corps de $\mathbb{C}$ et $K \subseteq L$ une extension radicale élémentaire d'exposant divisant $n$, c.-à-d., $L = K[a]$, avec $a^n \in K$. On suppose que $K$ contient une racine primitive d'ordre $n$ de l'unité $\xi$. Alors :*

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

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

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

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

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

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

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

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

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

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

**Lemme 10.2.3** *Soit $n$ un entier $\geq 2$. Le groupe des éléments inversibles de l'anneau commutatif $\mathbb{Z}/n\mathbb{Z}$ est formé des classes $a + n\mathbb{Z}$ telles que $a$ soit premier à $n$. On notera ce groupe $(\mathbb{Z}/n\mathbb{Z})^\times$ ou $U(n)$.*

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

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

**Proposition 10.2.4 (Extensions cyclotomiques)** *Soient $K \subseteq \mathbb{C}$ et $\xi$ une racine primitive de l'unité d'ordre $n$. L'extension $K \subseteq K[\xi]$ est galoisienne et son groupe de Galois est isomorphe à un sous-groupe de $(\mathbb{Z}/n\mathbb{Z})^\times$.*

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

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

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

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

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

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

**Remarque 10.2.3** 1) Le groupe $G := \mathrm{Gal}(K[\xi]/K)$ dépend du corps $K$. Par exemple, si $K$ contient déjà $\xi$, alors $K = K[\xi]$ et $G = \{1\}$.

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

Le dernier ingrédient dans la démonstration du théorème 10.2.1 est le suivant.

**Proposition 10.2.5** *Considérons des extensions de degré fini $k \subseteq K \subseteq L$, avec $\mathrm{car}(k) = 0$. On suppose :*

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

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

*Soit $P$ le polynôme minimal de $a$ sur $k$ et soit $\Omega$ un corps de décomposition de $P$ sur $K$. Alors, d'une part, l'extension $k \subseteq \Omega$ est galoisienne et, d'autre part, il existe une tour*

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

*où chaque extension $K_{i-1} \subseteq K_i$ est radicale élémentaire d'exposant divisant $n$.*

*Démonstration.* Posons $P = \mathrm{Irr}_k(a)$. Rappelons que, puisque $\mathrm{car}(k) = 0$, tout polynôme est séparable. D'autre part, d'après le lemme 7.4.2, $K$ est un corps de décomposition sur $k$ d'un polynôme (séparable !) $Q$. Alors, on voit que $\Omega$ est un corps de décomposition sur $k$ du polynôme $QP$. Par conséquent, d'après le second théorème fondamental 7.4.4, l'extension $k \subseteq \Omega$ est galoisienne. Ceci prouve le 1er point.

Montrons maintenant que l'extension $K \subseteq \Omega$ vérifie la propriété annoncée. Soient $a = a_1, \ldots, a_m$ les racines de $P$ dans $\Omega$ (c.-à-d., les conjugués sur $k$ de $a$ dans $\Omega$). Posons $K_0 = K$ et $K_i = K_{i-1}[a_i]$, pour $i = 1, \ldots, m$. Montrons que chaque extension $K_{i-1} \subseteq K_i$ est radicale élémentaire d'exposant divisant $n$. Pour $i = 1$, c'est l'hypothèse $a^n \in K$. Fixons $i \geq 2$. Il existe, d'après la proposition 7.3.2, un $k$-isomorphisme $\tau_i : k[a] \xrightarrow{\sim} k[a_i]$. Comme $\Omega$ est un corps de décomposition de $QP$ sur $k$ alors, d'après le premier théorème fondamental 7.3.5, $\tau_i$ se prolonge en un élément $\sigma_i$ de $G := \mathrm{Aut}_k(\Omega)$. Enfin, comme l'extension $k \subseteq K$ est galoisienne, alors $g(K) = K$, pour tout $g \in G$, d'après le théorème principal de la théorie de Galois 7.5.7 (point 3.). Par conséquent, on obtient que $a_i^n = \sigma_i(a^n)$ appartient à $K$ donc, a fortiori, à $K_{i-1}$. Ceci prouve que l'extension $K_{i-1} \subseteq K_i$ est radicale élémentaire, d'exposant divisant $n$. La proposition est démontrée. □

**Remarque 10.2.4 ZZ** 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 $\mathbb{Q} \subseteq \mathbb{Q}[\sqrt{2}]$ et $\mathbb{Q}[\sqrt[4]{2}$ sont galoisiennes, mais

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

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

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

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

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

### 10.2.3 Démonstration du théorème 10.2.1

Armé des trois propositions précédentes, on peut maintenant démontrer le théorème 10.2.1. Soient $k$ un sous-corps de $\mathbb{C}$ et $K$ le sous-corps engendré par les racines dans $\mathbb{C}$ d'un polynôme $P \in k[X]$ de degré $\geq 1$. On suppose l'équation $P(x) = 0$ résoluble par radicaux, c.-à-d., que $K$ est contenu dans une extension radicale $L$ de $k$. Donc, il existe des entiers $n_1, \ldots, n_r \geq 1$ et $a_1, \ldots, a_r \in L$, tels que, posant $L_0 = k$ et $L_i = L_{i-1}[a_i]$, on ait $a_i^{n_i} \in L_{i-1}$ pour $i = 1, \ldots, r$. De façon plus condensée, on dira que $K$ est contenu dans la tour

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

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

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

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

De plus, d'après la proposition 10.2.4, l'extension $k \subseteq L'_0 = k[\xi]$ est galoisienne, de groupe de Galois abélien.

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

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

De plus, chaque extension $k \subseteq L''_i$ est galoisienne, car $L''_i$ est un corps de décomposition sur $k$ du polynôme $(X^n - 1)P_1 \cdots P_i$. Alors, il résulte de la proposition 10.2.5 que chaque extension $L''_{i-1} \subseteq L''_i$ se raffine en une tour d'extensions radicales élémentaires d'exposant divisant $n$. En mettant bout à bout ces tours et en renumérotant, de la façon évidente, tous les corps apparaissant dans la grande tour ainsi obtenue, on obtient une tour

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

où chaque extension $\widetilde{L}_{i-1} \subseteq \widetilde{L}_i$, pour $i = 1, \ldots, N$ est radicale élémentaire d'exposant divisant $n$, et donc galoisienne, d'après la proposition 10.2.2, puisque $L''_0$ contient $\mu_n(\mathbb{C})$. De plus, l'extension $k \subseteq L''_0 = k[\xi]$ est galoisienne, de groupe abélien, d'après la proposition 10.2.4.

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

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

D'après le théorème d'Artin, chaque $G_i$ est le groupe de Galois de $\widetilde{L}_N$ sur $\widetilde{L}_i$. De plus, comme l'extension $\widetilde{L}_i \subseteq \widetilde{L}_{i+1}$ est galoisienne alors, d'après le point 3. du théorème principal de la théorie de Galois 7.5.7, $G_{i+1}$ est un sous-groupe normal de $G_i$ et $G_i/G_{i+1}$ est isomorphe à $\mathrm{Gal}(\widetilde{L}_{i+1}/\widetilde{L}_i)$, dont on a vu qu'il était abélien pour $i = -1$, et cyclique pour $i = 0, \ldots, N$. Par conséquent, $G$ est résoluble !

Finalement, comme $k \subseteq K \subseteq \widetilde{L}_N$ et l'extension $k \subseteq K$ est galoisienne, alors, d'après le point 3. du théorème 7.5.7, à nouveau, $\mathrm{Gal}(K/k)$ est isomorphe au quotient $G/H$, où $H$ désigne le fixateur dans $G$ de $K$. Par conséquent, d'après le corollaire 10.1.3, $\mathrm{Gal}(K/k) = \mathrm{Gal}(P/k)$ est résoluble. Ceci achève la démonstration du théorème 10.2.1.

## 10.3 Application : un exemple de polynôme $P \in \mathbb{Q}[X]$ non résoluble par radicaux

### 10.3.1 Deux générateurs de $S_n$

**Théorème 10.3.1** *Soit $n \geq 2$ et soient $\tau$ une transposition et $c$ un $n$-cycle dans $S_n$. Alors $S_n$ est engendré par $\tau$ et $c$.*

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

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

On en déduit que $\sigma_k := c^k(12)c^{-k}$ est la transposition $(k+1, k+2)$. En effet, si $j \notin \{k+1, k+2\}$ alors $c^{-k}(j) \notin \{1, 2\}$ et donc $\sigma_k(j) = j$. D'autre part, $\sigma_k(k+1) = c^k(2) = k+2$, et $\sigma_k(k+2) = c^k(1) = k+1$.

Donc, $H$ contient les transpositions $\tau = (12)$, et $(i, i+1)$ pour $i = 2, \ldots, n-1$. Or, d'après le théorème 10.1.4, ces transpositions engendrent $S_n$. Donc on obtient $H = S_n$ dans ce cas.

Maintenant, soient $\tau = (ij)$ et $c$ arbitraires. Comme $c^k(i)$ décrit $\{1, \ldots, n\}$ lorsque $k$ décrit $\{1, \ldots, n\}$, on peut supposer, quitte à remplacer $c$ par une

puissance $c^k$, que $c(i) = j$. On peut alors "renuméroter" les éléments de l'ensemble $E := \{1, \ldots, n\}$ pour se ramener au 1er cas. Explicitement, lorsque $k$ décrit $0, 1, \ldots, n-1$, les éléments $c^k(i)$ décrivent $E$ ; on peut donc considérer la bijection $\phi$ de $E$ définie par : $\phi(1) = i$, $\phi(2) = c(i) = j$, et $\phi(r) = c^{r-1}(i)$ pour tout $r = 2, \ldots, n$. Alors, l'application $\theta : \sigma \mapsto \phi^{-1}\sigma\phi$ est un automorphisme du groupe $S_n$, qui envoie $H$ sur le sous-groupe de $S_n$ engendré par $\theta((ij))$ et $\theta(c)$.

Or, on vérifie facilement que $\theta((ij)) = (12)$ et, pour $k = 1, \ldots, n$, l'on a

$$\phi^{-1}c\phi(k) = \phi^{-1}\left(c(c^{k-1}(i))\right) = \phi^{-1}\left(c^k(i)\right) = k + 1,$$

(avec la convention que $n+1 = 1$). Ceci montre que $\theta(c)$ est le cycle $(12\ldots n)$. On déduit alors du 1er cas que $H = S_n$. Le théorème est démontré. □

### 10.3.2 Polynômes irréductibles de $\mathbb{Z}[X]$ : le critère d'Eisenstein

Soit $P \in \mathbb{Z}[X]$ un polynôme unitaire de degré $n \geq 1$. Écrivons $P = X^n + \sum_{i=0}^{n-1} a_i X^i$.

**Proposition 10.3.2 (Critère d'Eisenstein)** *S'il existe un nombre premier $p$ divisant chaque $a_i$ mais tel que $p^2$ ne divise pas $a_0$, alors $P$ est irréductible dans $\mathbb{Z}[X]$ et aussi dans $\mathbb{Q}[X]$.*

*Démonstration.* Si $P$ est irréductible dans $\mathbb{Z}[X]$, il résulte du Lemme des contenus de Gauss que $P$ est aussi irréductible dans $\mathbb{Q}[X]$ ; on a vu cela dans le chapitre 5, Proposition 5.5.6. 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 $\geq 1$ 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 $\pi$ désigne la projection. Comme $A$ est factoriel et $X$ irréductible, ceci entraîne que $\pi(Q) = \lambda X^d$ et $\pi(R) = \lambda^{-1}X^{n-d}$, pour un certain $d \in \{1, \ldots, n\}$ et $\lambda \in \mathbb{F}_p^\times$. On en déduit que $p$ divise le terme constant de $Q$ et de $R$, et alors l'égalité $P = QR$ entraîne que $p^2$ divise $a_0$, une contradiction. Cette contradiction montre que $P$ est irréductible dans $\mathbb{Z}[X]$. La proposition est démontrée. □

**Remarque 10.3.1** Le critère d'Eisenstein s'étend sans difficulté en remplaçant $\mathbb{Z}$ par un anneau factoriel quelconque.

### 10.3.3 Le polynôme $P = X^5 - 10X + 5$

**Théorème 10.3.3** *Le polynôme $P = X^5 - 10X + 5$ n'est pas résoluble par radicaux sur $\mathbb{Q}$.*

*Démonstration.* Soit $K$ le sous-corps de $\mathbb{C}$ engendré par les racines de $P$ et soit $G = \mathrm{Gal}(K/\mathbb{Q})$. C'est un sous-groupe de $S_5$, d'après le théorème 9.4.7, 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 9.3.2, $G$ 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 $\alpha$ et une fois entre $\alpha$ et $+\infty$.

Donc $P$ a exactement 3 racines réelles, appelons-les $x_1, x_2, x_3$, et deux racines complexes (non-réelles) conjuguées, $x_4$ et $x_5 = \overline{x_4}$. Par conséquent, la conjugaison complexe $z \mapsto \overline{z}$, induit un $\mathbb{Q}$-automorphisme de $K$, c.-à-d., un élément de $G$, dont l'image dans $S_5$ est la transposition $\tau = (45)$. Comme on a vu plus haut que $G$ contient aussi un 5-cycle, il résulte du théorème 10.3.1 que $G = S_5$. Comme $S_5$ n'est pas résoluble, d'après le corollaire 10.1.8, le théorème 10.2.1 montre que $P$ n'est pas résoluble par radicaux sur $\mathbb{Q}$. □

*Fin du cours*

## 10.4 Quelques résultats sans démonstrations

### 10.4.1 La réciproque du théorème 10.2.1

Pour établir la réciproque du théorème 10.2.1, on utilise les deux théorèmes suivants, qui sont intéressants en eux-mêmes.

**Théorème 10.4.1** *Soient $k$ un corps arbitraire, $K$ et $L$ deux extensions de degré fini de $k$, contenues dans une extension $\Omega$ de $k$. On note $KL$ le sous-corps de $\Omega$ engendré par $K$ et $L$ ; on l'appelle extension composée de $K$ et $L$. On suppose l'extension $k \subseteq K$ galoisienne, et on pose $G = \mathrm{Gal}(K/k)$. Alors l'extension $L \subseteq KL$ est aussi galoisienne, et son groupe de Galois s'identifie au sous-groupe de $G$ fixant les éléments de $K \cap L$.*

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

**Théorème 10.4.2 (Extensions cycliques)** *Soient $n \geq 2$ et $K \subset L$ une extension galoisienne de degré $n$. On suppose que $K$ contient une racine primitive de l'unité d'ordre exactement $n$, et que $\mathrm{Gal}(L/K) \cong \mathbb{Z}/n\mathbb{Z}$. Alors il existe $a \in L$ tel que $L = K[a]$ et $a^n \in K$, et le polynôme minimal de $a$ sur $K$ est $X^n - a^n$.*

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

En utilisant les deux théorèmes précédents, on peut établir la réciproque du théorème 10.2.1, 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 10.4.3** *Soient $k$ un corps de caractéristique $0$ et $K$ un corps de décomposition sur $k$ d'un polynôme non-constant $P \in k[X]$. On pose $G = \mathrm{Gal}(P/k) = \mathrm{Gal}(K/k)$. Alors l'équation $P(x) = 0$ est résoluble par radicaux ssi $G$ est résoluble.*

## 10.5 Des regrets

### 10.5.1 Constructions à la règle et au compas

Mon regret principal est de n'avoir pas eu le temps de traiter ce sujet très classique. Je renvoie à [Esc, Chap. 5], pour la définition des nombres constructibles à la règle et au compas (à partir de deux points donnés dans le plan). Les deux résultats principaux sont les suivants.

**Théorème 10.5.1** *Un nombre $\alpha \in \mathbb{C}$ est constructible à la règle et au compas (à partir d'un segment donné, pris comme longueur unité), ssi $\alpha$ est contenu dans une tour d'extensions quadratiques, c.-à-d., s'il existe une tour*

$$\mathbb{Q} = K_0 \subseteq K_1 \subseteq \cdots \subseteq K_r$$

*telle que $[K_i : K_{i-1}] = 2$ pour tout $i$, et $\alpha \in K_r$. En particulier, d'après la multiplicativité des degrés, le degré de $\alpha$ sur $\mathbb{Q}$ doit être une puissance de 2.* (*Cette conditon est nécessaire, mais pas suffisante.*)

**Corollaire 10.5.2 (Impossibilité de la duplication du cube)**
*Étant donné un segment de longueur 1, il n'est pas possible de construire à la règle et au compas un segment tel que le volume du cube correspondant soit le double de celui du cube unité. C.-à-d., le nombre $\sqrt[3]{2}$ n'est pas constructible à la règle et au compas.*

*Démonstration.* Le polynôme minimal sur $\mathbb{Q}$ de $\sqrt[3]{2}$ est $X^3 - 2$, qui est de degré 3. □

**Définition 10.5.1** *Pour tout entier $m \geq 0$, posons $F_m = 2^{2^m} + 1$. Un nombre premier $p$ est appelé un nombre premier de Fermat si $p = F_m$, pour un certain entier $m \geq 0$. Ainsi,*

$$F_0 = 3, \quad F_1 = 5, \quad F_2 = 17, \quad F_3 = 259$$

*sont premiers, ainsi que $F_4 = 65537$. Par contre, Euler a montré que $F_5$ est divisible par 641. Actuellement, on sait que $F_6, \ldots, F_{16}$ ne sont pas premiers. On ignore s'il y a d'autres nombres premiers de Fermat autres que $F_0, \ldots, F_4$ !*

**Théorème 10.5.3** *Soit $n$ un entier $\geq 3$. Le polygone régulier à $n$ côtés est constructible à la règle et au compas ssi $n$ est le produit d'une puissance arbitraire de 2 et de nombres premiers de Fermat deux à deux distincts.*

Pour tout ce qui précède, voir [Esc], Propositions 5.5 et 5.7, Exercices 5.2 et 9.7, ou [ChL, §§5.1, 5.2], [Ti, Ch.12, Appendix], [Ja1, §§4.2 & 4.11].

### 10.5.2 Autres regrets

De n'avoir pas eu le temps de démontrer le théorème de Sylow, ni le théorème des zéros de Hilbert...

**FIN**

# Table des matières

# Bibliographie


[ALF] J.-M. Arnaudiès, J. Lelong-Ferrand, Cours de mathématiques, Tome 1, Algèbre (3ème édition), Dunod, 1978.

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

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

[Bla] A. Blanchard, Les corps non commutatifs, P.U.F., 1972.

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

[BR] A. Bouvier, D. Richard, Groupes (2ème édition revue et corrigée), Hermann, 1979.

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

[ChL] A. Chambert-Loir, A field guide to algebra, Springer, 2005.

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

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

[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.

[Kri] J.-L. Krivine, Théorie des ensembles, Cassini, 1998.

[Ku] E. Kunz, Introduction to commutative algebra and algebraic geometry, Birkhäuser, 1985.

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

[Laf] J.-P. Lafon, Les formalismes fondamentaux de l'algèbre commutative, Hermann, 1974.

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

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

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

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

[SD] H.P.F. Swinnerton-Dyer, A brief guide to algebraic number theory, C.U.P., 2001.

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