Antoine Chambert-Loir

ALGÈBRE CORPORELLE

Antoine Chambert-Loir
E-mail : antoine.chambert-loir@univ-rennes1.fr
IRMAR, Université de Rennes 1, Campus de Beaulieu, 35042 Rennes Cedex.
Centre de Mathématiques, École polytechnique, 91128 Palaiseau Cedex.

Version du 22 mars 2004, 13h35
Une version à jour est disponible sur le Web à l'adresse http://www.math.polytechnique.fr/~chambert/teach/algebre.pdf

— Il conviendrait donc, Glaucon, de prescrire cette étude par une loi, et de persuader à ceux qui doivent remplir les plus hautes fonctions publiques de se livrer à la science du calcul, non pas superficiellement, mais jusqu'à ce qu'ils arrivent, par la pure intelligence, à connaître la nature des nombres ; et de cultiver cette science non pas pour la faire servir aux marchands, mais pour l'appliquer à la guerre, et pour faciliter la conversion de l'âme du monde de la génération vers la vérité et l'essence.
— Très bien dit. Platon, *La république, Livre VII*

J'ai fait en analyse plusieurs choses nouvelles.
Évariste Galois, Lettre à A. Chevalier (29 mai 1832)

Table des matières

Présentation vii

1. Extensions de corps 1
Constructions à la règle et au compas, 1 ; *Corps*, 3 ; *Extensions de corps*, 8 ; *Quelques impossibilités classiques*, 14 ; *Fonctions symétriques des racines*, 18 ; *Appendice : transcendance de* e *et* π, 20 ; *Exercices*, 24.

2. « Mais où sont mes racines ? » 29
Anneau des restes, 29 ; *Extensions de décomposition*, 32 ; *Corps algébriquement clos ; clôture algébrique*, 33 ; *Appendice : structure des anneaux de polynômes*, 37 ; *Appendice : anneaux quotients*, 40 ; *Appendice : théorème de Puiseux*, 42 ; *Exercices*, 46.

3. Théorie de Galois 51
Homomorphismes d'une extension dans une clôture algébrique, 51 ; *Groupe d'automorphismes d'une extension*, 54 ; *Le groupe de Galois comme groupe de permutations des racines*, 59 ; *Discriminant, résolvantes*, 63 ; *Corps finis*, 66 ; *Exercices*, 68.

4. Un peu de théorie des groupes 75
Groupes (rappels de définitions), 75 ; *Sous-groupes*, 76 ; *Opération d'un groupe sur un ensemble*, 78 ; *Sous-groupes distingués, groupes quotients*, 79 ; *Groupes résolubles, nilpotents*, 82 ; *Groupe symétrique, alterné*, 85 ; *Groupes de matrices*, 89 ; *Exercices*, 92.

5. Applications 97
Constructibilité à la règle et au compas, 97 ; *Cyclotomie*, 98 ; *Extensions composées*, 103 ; *Extensions cycliques*, 106 ; *Les équations de degrés inférieur à* 4, 108 ; *Résolubilité par radicaux*, 113 ; *Comment (ne pas) calculer des groupes de Galois*, 117 ; *Spécialisation des groupes de Galois*, 120 ; *L'équation générique et le théorème d'irréductibilité de Hilbert*, 127 ; *Exercices*, 133.

6. Équations différentielles 139
Corps différentiels, 139 ; *Extensions différentielles. Construction de dérivations*, 142 ; *Équations différentielles*, 146 ; *Extensions de Picard-Vessiot*, 148 ; *Le groupe de Galois différentiel. Exemples*, 151 ; *La correspondance de Galois différentielle*, 156 ; *Extensions élémentaires*, 157 ; *Appendice : théorème des zéros de Hilbert*, 163 ; *Exercices*, 165.

Problèmes d'examen 167
Problème de révision (2002), 167 ; *Contrôle classant (2002)*, 168 ; *Session de rattrapage (2002)*, 171 ; *Contrôle classant (2003)*, 171.

Bibliographie 175

Index 177

Présentation

Voici un petit cours d'algèbre dans lequel l'accent est mis sur la structure de *corps*, d'où son titre.

Il y est question d'équations, polynomiales ou différentielles, et de la structure algébrique de leurs solutions. On sait par exemple résoudre explicitement les équations polynomiales de degré 2, 3 ou 4 (Cardan, Ferrari, etc.) à l'aide de formules algébriques et d'extractions de racines n-ièmes, mais le cas du degré 5 a résisté longtemps, jusqu'à ce qu'Abel montre en 1826 qu'une équation de degré 5 générale ne peut être résolue de la sorte.

Peu après, Galois a défini le groupe d'une équation polynomiale comme le groupe des permutations de ses racines (disons complexes) qui préservent toutes les identités algébriques à coefficients rationnels que ces racines vérifient. Par exemple, on sait bien que les fonctions symétriques élémentaires des racines sont (au signe près) les coefficients du polynôme. En général, il n'y en a pas d'autre, mais parfois si et le groupe de l'équation en est d'autant plus petit.

Et Galois a compris comment ce groupe de symétrie conditionne la résolubilité de l'équation. Il a défini à l'occasion la notion de *groupe résoluble* et établi que si le groupe de l'équation est résoluble, on peut exprimer ses racines par radicaux, et sinon non.

Expliquer tout ceci nous mènera sur d'intéressants chemins. Vous apprendrez par exemple pourquoi d'antiques problèmes de constructions à la règle et au compas n'ont effectivement pas de solution, mais inversement vous saurez pourquoi (et découvrirez peut-être comment) l'on peut construire certains polygones réguliers.

Il y a une théorie analogue pour les équations différentielles linéaires homogènes et nous introduirons un groupe analogue. Ce sera alors un groupe de matrices. Vous apprendrez aussi pourquoi certains calculs explicites de primitives, tels celui de $\int \exp(x^2)$, sont sans espoir.

Au menu figurent également quelques théorèmes d'analyse : la transcendance du nombre π, le fait que le corps des nombres complexes est algébriquement clos, ainsi que le théorème de Puiseux qui montre comment paramétrer les racines d'une équation polynomiale dont les coefficients peuvent varier.

Dans chaque chapitre, je propose quelques exercices. Vous en ferez vraisemblablement certains en petites classes. Je vous encourage à passer un peu de temps à les chercher. C'est en effet un excellent moyen d'assimiler les nouvelles notions introduites dans ce cours. Ne vous inquiétez pas, certains sont même faciles !

Quelques illustrations, tirées du *Web*, ont pour vocation d'égayer ce livre. J'ai trouvé les reproductions de timbres à l'adresse *http://jeff560.tripod.com/* — ceux que cela intéresse seront ravis de feuilleter le livre [**13**] — tandis que les photos proviennent de l'archive *MacTutor History of Mathematics* à l'adresse *http://www-groups.dcs.st-andrews.ac.uk/~history/*. J'encourage ceux d'entre vous qui sont intéressés par l'histoire des mathématiques à la fréquenter. La lecture du petit livre [**4**] d'A. Dahan et J. Peiffer est aussi vivement recommandée.

Et maintenant, commençons...

1

Extensions de corps

*Nous partons du problème géométrique des constructions à la règle et au compas. Nous introduisons ensuite les notions de corps et d'extensions de corps, et enfin celle d'extension algébrique. Cela fournit rapidement des résultats d'*impossibilité *pour quelques problèmes classiques. Nous verrons plus tard que la théorie de Galois fournit un critère définitif permettant de décider si une construction est ou n'est pas réalisable à la règle et au compas.*

1.1. Constructions à la règle et au compas

Pour les Grecs de l'antiquité, nombres et mesures de longueurs étaient deux concepts intimement liés. C'est ainsi qu'ils se sont posés le problème de *constructions géométriques* de nombres remarquables. Les outils qu'ils se donnaient étaient en général une règle et un compas, mais, notamment quand ils n'y arrivaient pas, il leur arriva d'admettre des mécanismes qui tracent des courbes plus générales (cf. [**4**] ainsi que les notes de [**9**]).

Formalisons le problème du point de vue mathématique.

DÉFINITION 1.1.1. — *Soit un ensemble Σ de points du plan $\mathbf{R}^2$. On dit qu'un point P est* constructible à la règle et au compas *à partir de Σ s'il existe un entier n et une suite de points $(P_1,\dots,P_n)$ tels que $P_n = P$ et tels que pour tout $i \in \{1;\dots;n\}$, notant $\Sigma_i = \Sigma \cup \{P_1;\dots;P_{i-1}\}$, l'une des propositions suivantes soit vérifiée :*

– il existe 4 points A, B, A' et $B' \in \Sigma_i$ tels que P_i soit l'intersection des deux droites non parallèles (AB) et $(A'B')$;

– il existe quatre points A, B, C, et $D \in \Sigma_i$ tels que P_i soit l'un des (au plus) deux points d'intersection de la droite (AB) et du cercle de centre C et de rayon $[CD]$;

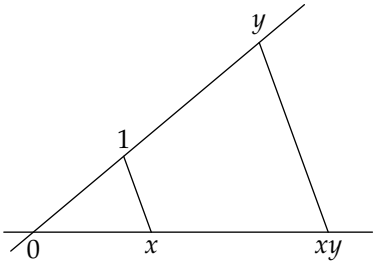
– il existe quatre points O, M, O' et $M' \in \Sigma_i$ tels que P_i soit l'un des (au plus) deux points d'intersection des cercles distincts respectivement de centre O et de rayon $[OM]$, et de centre O' et de rayon $[O'M']$.

DÉFINITION 1.1.2. — *Considérons une partie* Σ *de* $\mathbf{R}$. *Un réel* x *est dit* constructible à la règle et au compas *à partir de* Σ *si c'est l'abscisse d'un point du plan qui est constructible à la règle et au compas à partir des points* $(\xi, 0)$ *pour* $\xi \in \Sigma$. *Un nombre complexe est dit constructible à partir de* Σ *si sa partie réelle et sa partie imaginaire le sont.*

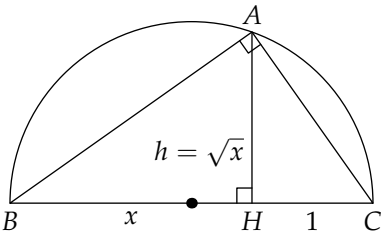
THÉORÈME 1.1.3. — *Soit* Σ *une partie de* $\mathbf{R}$ *contenant* 0 *et* 1. *L'ensemble* $\mathcal{C}_\Sigma$ *des nombres réels constructibles à partir de* Σ *vérifie les propriétés suivantes :*

a) *si* x *et* y *sont dans* $\mathcal{C}_\Sigma$, $x+y$, $x-y$, xy *sont dans* $\mathcal{C}_\Sigma$;
b) *si* x *et* y *sont dans* $\mathcal{C}_\Sigma$, $y \neq 0$, *alors* x/y *est dans* $\mathcal{C}_\Sigma$;
c) *si* $x > 0$ *est dans* $\mathcal{C}_\Sigma$, $\sqrt{x}$ *aussi.*

Démonstration. — Elle repose sur des arguments de géométrie élémentaire (du lycée) et peut se résumer en une série de figures. L'addition et la soustraction sont assez évidentes. La stabilité par multiplication et racine carrée est conséquence des figures 1(a) et 1(b). La stabilité par division se voir aussi sur la figure 1(a) car si x et xy sont connus, la figure permet d'en déduire y. □



(a) Construction du produit ou du quotient de deux nombres (théorème de Thalès)



(b) Construction de la racine carrée d'un nombre (théorème de Pythagore)

Exercice 1.1.4. — Ces figures supposent tout de même que l'on puisse construire des points hors de l'axe des abscisses. Le vérifier. Vérifiez aussi que vous savez construire les droites parallèle ou perpendiculaire à une droite donnée passant par un point fixé.

Dans la définition 1.1.1 de point constructible, les cercles sont de centre un point construit et passent par un autre point construit : on ne reporte pas les longueurs. Expliquer cependant comment construire le cercle de centre un point donné et de rayon la distance entre deux autres points.

Remarque 1.1.5. — Montrer que toute construction à la règle et au compas pourrait ne se faire qu'au compas seul (théorème de Mohr-Mascheroni). C'est un résultat de pure géométrie, voir par exemple [**5**] pour une solution.

1.2. Corps

DÉFINITION 1.2.1. — *Un* corps *(commutatif) est un ensemble K muni de deux lois internes $+$ et $\times$ et de deux éléments 0 et 1 distincts vérifiant les propriétés suivantes :*

a) $(K,+,0)$ *est un groupe commutatif*[(1)] *;*

b) $(K\setminus\{0\},\times,1)$ *est un groupe commutatif;*

c) *la loi $\times$ est distributive par rapport à la loi $+$: pour tous a, b et c dans K, $a\times(b+c)=a\times b+a\times c$.*

On note souvent ab le produit $a\times b$. On note aussi K^* l'ensemble $K\setminus\{0\}$.

Exemples 1.2.2. — a) les nombres rationnels $\mathbf{Q}$, les nombres réels $\mathbf{R}$ ou les nombres complexes $\mathbf{C}$ forment un corps ;

b) l'ensemble des nombres (réels ou complexes) constructibles à partir de $\{0;1\}$ est un corps qui contient le corps des nombres rationnels $\mathbf{Q}$.

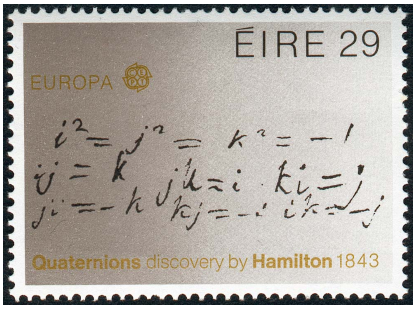
c) Si p est un nombre premier, l'ensemble $\mathbf{Z}/p\mathbf{Z}$ des entiers modulo p est un corps ; il est fini de cardinal p.

d) Si K est un corps, l'ensemble $K(X)$ des fractions rationnelles à coefficients dans K, muni des lois usuelles, est encore un corps.

e) Si Ω est un ouvert connexe de $\mathbf{C}$, l'ensemble des fonctions méromorphes dans Ω est un corps.

Un *sous-corps* d'un corps F est une partie de F contenant 0, 1, stable par $+$ et $\times$ de sorte que ces lois la munissent d'une structure de corps.

On considère parfois des *corps non-commutatifs* : cela signifie qu'on ne demande pas à la loi $\times$ d'être commutative. Bien entendu, la loi $+$ ne cesse pas de l'être.



Exemple 1.2.3. — L'espace vectoriel $\mathbf{H}=\mathbf{R}^4$ dont la base canonique est notée 1, i, j, k admet une unique structure de corps non-commutatif pour laquelle la loi $+$ est l'addition usuelle et la loi $\times$ vérifie les relations : $\mathrm{i}^2=\mathrm{j}^2=\mathrm{k}^2=-1$, $\mathrm{ij}=\mathrm{k}$. C'est le corps des quaternions, découvert par Hamilton.

DÉFINITION 1.2.4. — *Soit K un corps et S une partie de K. Le corps engendré par S dans K est le plus petit sous-corps de K contenant S.*

C'est l'ensemble des éléments de K de la forme

$$\frac{P(s_1,\dots,s_n)}{Q(s_1,\dots,s_n)},$$

(1) Voir le début du chapitre 4 pour des rappels de théorie des groupes.

où $P,Q \in \mathbf{Z}[X_1,\dots,X_n]$ sont des polynômes à coefficients entiers, $s_1,\dots,s_n$ des éléments de S tels que $Q(s_1,\dots,s_n) \neq 0$. Soit F un sous-corps de K et soit $x_1,\dots,x_n$ des éléments de K ; on note $F(x_1,\dots,x_n)$ le sous-corps de K engendré par F et les x_j.

Exercice 1.2.5. — L'ensemble des nombres complexes de la forme $x+\mathrm{i}y$ avec $x,\ y \in \mathbf{Q}$ est le sous-corps de $\mathbf{C}$ engendré par i.

Une structure plus faible que celle de corps, mais néanmoins très importante, est celle d'*anneau*.

DÉFINITION 1.2.6. — *Un anneau (commutatif) est un ensemble A muni de deux lois $+$ et $\times$ et de deux éléments 0 et 1 tels que*

– *$(A,+,0)$ est un groupe commutatif ;*
– *la loi $\times$ est commutative et associative ;*
– *pour tout $a \in A$, $a \times 1 = 1 \times a = a$;*
– *la loi $\times$ est distributive par rapport à la loi $+$: pour tous a, b, $c \in A$, $a \times (b+c) = a \times b + a \times c$.*

Un sous-anneau *d'un anneau A est une partie de A contenant 0 et 1, que les lois $+$ et $\times$ laissent stables et munissent d'une structure d'anneau.*

Un élément a d'un anneau A est dit inversible *s'il existe $b \in A$ tel que $ab = 1$. S'il existe, un tel élément est nécessairement unique et est appelé* inverse *de a.*

Exemples 1.2.7. — *a*) Un corps est un anneau. Plus précisément, un corps est un anneau dont tout élement non nul est inversible.

b) L'ensemble $\mathbf{Z}$ des entiers, $\mathbf{Z}/n\mathbf{Z}$ des entiers modulo un entier n sont des anneaux. L'anneau $\mathbf{Z}$ est un sous-anneau du corps des rationnels.

c) Si A est un anneau dans lequel $0 = 1$, alors $A = \{0\}$ (anneau nul, d'intérêt limité).

d) Si A est un anneau, l'ensemble $A[X]$ des polynômes à coefficients dans A est un anneau. L'anneau A en est un sous-anneau.

e) Si I est un intervalle de $\mathbf{R}$, l'ensemble des fonctions continues sur I est un anneau. De même pour les fonctions dérivables, de classe $\mathcal{C}^k$, $\mathcal{C}^\infty$, analytiques, etc.

f) L'ensemble des éléments de $\mathbf{C}$ de la forme $x+iy$ avec x et y dans $\mathbf{Z}$, muni des lois de $\mathbf{C}$, est un anneau (*anneau des entiers de Gauß*).

g) L'ensemble des éléments de $\mathbf{H}$ de la forme $x1+yi+zj+tk$ avec $x,\ y,\ z,\ t \in \mathbf{Z}$ est aussi un anneau, mais dont la multiplication n'est pas commutative.

DÉFINITION 1.2.8. — *Si A et B sont deux anneaux, un* homomorphisme *d'anneaux est une application $f : A \to B$ vérifiant les propriétés suivantes :*

a) *pour tous a et $b \in A$, $f(a+b) = f(a) + f(b)$;*
b) *pour tous a et $b \in A$, $f(ab) = f(a)f(b)$;*
c) *$f(0) = 0$ et $f(1) = 1$.*

Un *homomorphisme de corps* est un homomorphisme d'anneaux d'un corps dans un autre. Un *isomorphisme* est un homomorphisme bijectif. L'image d'un morphisme d'anneaux $A \to B$ est un sous-anneau de B ; l'image d'un morphisme de corps $K \to L$ est un sous-corps de L.

LEMME 1.2.9. — *Soit $f : A \to B$ un homomorphisme d'anneaux. Soit $I = f^{-1}(0)$ l'ensemble des $a \in A$ tels que $f(a) = 0$. Alors, I vérifie les propriétés suivantes :*

- $0 \in I$;
- *si a et $b \in I$, $a + b \in I$;*
- *si $a \in A$ et $b \in I$, $ab \in I$.*

De plus, f est injective si et seulement si $I = \{0\}$.

DÉFINITION 1.2.10. — *Une partie I d'un anneau A vérifiant les propriétés du lemme précédent est appelée* idéal. *Si $f : A \to B$ est un homomorphisme d'anneau, l'idéal $f^{-1}(0)$ est appelé* noyau *de f et noté* $\operatorname{Ker} f$.

Je renvoie au paragraphe 2.4 pour plus de détails sur la structure algébrique des anneaux de polynômes.

DÉFINITION 1.2.11. — *Un anneau non nul A est dit* intègre *si pour tous a et $b \in A \setminus \{0\}$, $ab \neq 0$.*

Exercice 1.2.12. — a) Les corps, l'anneau $\mathbf{Z}$ des entiers relatifs sont des anneaux intègres.

b) Un sous-anneau d'un anneau intègre est un anneau intègre.

c) Soit n un entier $\geqslant 2$. L'anneau $\mathbf{Z}/n\mathbf{Z}$ est intègre si et seulement si n est un nombre premier.

Pour tout anneau intègre A, on peut construire un corps contenant (un anneau isomorphe à) A tel que tout élément de K soit le quotient de deux éléments de A : c'est le *corps des fractions* de A. Le principe est le même que celui qui permet d'obtenir le corps des nombres rationnels à partir de l'anneau des entiers relatifs. On définit un ensemble K comme l'ensemble des classes d'équivalences de l'ensemble $\mathcal{F} = A \times (A \setminus \{0\})$ pour la relation d'équivalence

$$(a, b) \sim (c, d) \Leftrightarrow ad = bc.$$

(*Exercice* : montrer que c'est effectivement une relation d'équivalence.) On note a/b la classe du couple (a, b). On définit une addition et une multiplication sur K par le calcul des fractions habituel, en posant

$$\frac{a}{b} + \frac{c}{d} = \frac{ad + bc}{bd} \quad \text{et} \quad \frac{a}{b}\frac{c}{d} = \frac{ac}{bd}.$$

(*Exercice* : vérifier qu'elles sont bien définies, c'est-à-dire que $(ad + bc)/bd$ et ab/cd ne dépendent pas des choix des représentants des fractions a/b et c/d.) Muni de ces

deux lois, K est un corps commutatif, son zéro est l'élément $0/1$ tandis que son élément unité est $1/1$; l'application $A \to K$ qui associe à a l'élément $i(a) = a/1$ est un homomorphisme d'anneaux. (*Exercice* : vérifier ces assertions.) L'homomorphisme i est injectif : par définition de la relation d'équivalence, si $i(a) = a/1 = 0/1$, on en déduit $1a = 0\,1$, d'où $a = 0$. Alors, on remarque que pour tous $(a, b) \in \mathcal{F}$,

$$\frac{a}{b} = \frac{a}{1}\frac{1}{b} = i(a)\,i(b)^{-1}.$$

Autrement dit, tout élément de K est le quotient de deux éléments de A. Le fait que i soit injectif permet d'identifier un élément $a \in A$ et son image $i(a) \in K$.

Exemples 1.2.13. — Le corps des fractions de l'anneau $\mathbf{Z}$ est le corps des nombres rationnels. Celui de l'anneau $K[X]$ des polynômes à coefficients dans un corps K est le corps $K(X)$ des fractions rationnelles.

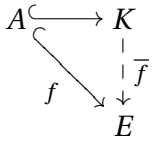
Si Ω est un ouvert connexe de $\mathbf{C}$, l'anneau des fonctions holomorphes sur Ω est intègre (cela résulte du principe des zéros isolés) et son corps des fractions est le corps des fonctions méromorphes sur cet ouvert. C'est un théorème d'analyse assez délicat qui repose sur la possibilité de construire explicitement une fonction holomorphe ayant un ensemble de zéros prescrit (produits de Weierstraß, voir par exemple [**11**], théorème 15.12).

Le corps des fractions possède une propriété importante.

PROPOSITION 1.2.14. — *Soit A un anneau intègre, K son corps des fractions. Soit E un corps. Pour tout homomorphisme injectif $f : A \to E$, il existe un unique homomorphisme $\overline{f} : K \to E$ tel que $\overline{f}(a) = f(a)$ pour $a \in A$.*

Remarquons que si $a/b = c/d$, alors $ad = bc$, donc $f(a)f(d) = f(b)f(c)$, puis $f(a)/f(b) = f(c)/f(d)$. Ainsi, on peut poser, si $x = a/b$ est un élément de K, $\overline{f}(x) = f(a)/f(b)$. On montre alors que $\overline{f}$ est un homomorphisme de corps. Les détails de la démonstration sont aussi fastidieux que ceux de la construction du corps des fractions. (*Exercice…*)

On peut représenter la proposition par un diagramme



où la flèche pointillée $\overline{f} : K \to E$ est celle dont l'existence est affirmée par la proposition. Une terminologie courante, un peu pompeuse, pour ce genre d'énoncés est « propriété universelle ».

PROPOSITION-DÉFINITION 1.2.15. — *Soit A un un anneau. Il existe un unique homomorphisme d'anneaux $f : \mathbf{Z} \to A$.*

Supposons que f n'est pas injectif. Si A est intègre, le plus petit élément strictement positif de $\operatorname{Ker} f$ *est un nombre premier dont* $\operatorname{Ker} f$ *est l'ensemble des multiples. Si A est un corps, ce nombre premier est appelé* caractéristique de A.

Si f est injectif et si A est un corps, on dit qu'il est de caractéristique nulle. Dans ce cas, f s'étend en un homomorphisme de corps $g\colon \mathbf{Q} \to A$.

Démonstration. — Commençons par définir f. On pose d'abord $f(0) = 0$ et $f(1) = 1$. Si $n \geqslant 2$, on définit par récurrence $f(n) = f(n-1)+1$. Enfin, si $n \geqslant 1$, on pose $f(-n) = -f(n)$. Comme ces relations sont vérifiées si f est un homomorphisme d'anneaux, cela prouve l'unicité d'un tel homomorphisme $\mathbf{Z} \to A$.

Montrons alors que f est un homomorphisme d'anneaux c'est-à-dire que sont vérifiées les relations $f(m+n) = f(m)+f(n)$ et $f(mn) = f(m)f(n)$. Elles sont en fait vraies pour exactement la même raison que celle qui fait que les entiers relatifs forment un anneau et se démontrent par récurrence.

Établissons pour m et $n \geqslant 0$ la relation $f(m+n) = f(m)+f(n)$. Elle est vraie si $n = 0$. Si elle est vraie pour n, alors

$$\begin{aligned} f(m+(n+1)) &= f((m+n)+1) = f(m+n)+1 \\ &= f(m)+f(n)+1 = f(m)+f(n+1) \end{aligned}$$

donc elle est vraie pour $n+1$. Cela la prouve par récurrence. Si $m \geqslant 0$ et $n < 0$, mais $m+n \geqslant 0$, on a

$$\begin{aligned} f(m+n)-f(m)-f(n) &= f(m+n)-f(m)+f(-n) \\ &= f((m+n)+(-n))-f(m) = f(m)-f(m) = 0. \end{aligned}$$

On démontre de même les autres cas. Établissons maintenant que l'on a $f(mn) = f(m)f(n)$ pour tous m et n. C'est vrai pour $n = 0$ et si c'est vrai pour n,

$$\begin{aligned} f(m(n+1)) &= f(mn+m) = f(mn)+f(m) = f(m)f(n)+f(m) \\ &= f(m)(f(n)+1) = f(m)f(n+1), \end{aligned}$$

donc c'est vrai pour $n+1$, puis pour tout $n \geqslant 0$ par récurrence. Si $n \leqslant 0$,

$$f(mn) = f(-m(-n)) = -f(m(-n)) = -f(m)f(-n) = f(m)f(n)$$

donc c'est aussi vrai pour tout $n \leqslant 0$.

Supposons maintenant que A soit intègre et que f ne soit pas injective et soit n le plus petit entier > 0 tel que $f(n) = 0$. Si n n'est pas premier, on peut écrire $n = ab$ où a et b sont deux entiers vérifiant $1 \leqslant a < n$ et $1 \leqslant b < n$. Par suite, $0 = f(n) = f(ab) = f(a)f(b)$. Comme l'anneau A est supposé intègre, on a donc $f(a) = 0$ ou $f(b) = 0$, ce qui contredit la minimalité de l'entier n.

L'image de tout multiple de n est 0. Considérons réciproquement un entier m tel que $f(m) = 0$. La division euclidienne de m par n s'écrit $m = qn+r$ avec $0 \leqslant r < n$. On a $f(r) = f(m-qn) = f(m)-qf(n) = 0$. Par minimalité de n, $r = 0$ et m est multiple de n.

Si f est injective et si A est un corps, f s'étend d'après la propriété universelle (prop. 1.2.14) en un homomorphisme de $\mathbf{Q}$ dans A. □

Remarque 1.2.16. — Soit K un corps de caractéristique p et $f\colon \mathbf{Z} \to K$ l'homomorphisme étudié ci-dessus. Si m et n sont deux entiers congrus modulo p, $m-n$ est multiple de p, si bien que $f(m-n)=0$, d'où $f(m)=f(n)$. L'homomorphisme $\mathbf{Z}\to K$ induit une application naturelle $\mathbf{Z}/p\mathbf{Z}\to K$ qui est un homomorphisme de corps.

Ainsi, tout corps « reçoit » un (et un seul) des corps $\mathbf{Z}/p\mathbf{Z}$ (pour p premier) et $\mathbf{Q}$, dont l'image est appelée *sous-corps premier*definesous-corps !premier.

PROPOSITION 1.2.17. — *Soit p un nombre premier et soit A un anneau tel que $p1_A = 0_A$ (par exemple un corps de caractéristique p). Alors, pour tous a et b dans A, on a*

$$(a+b)^p = a^p + b^p.$$

Par suite, l'application $\varphi\colon A\to A$ définie par $\varphi(a)=a^p$ est un homomorphisme d'anneaux.

Démonstration. — D'après la formule du binôme de Newton, on a

$$(a+b)^p = a^p + b^p + \sum_{n=1}^{p-1}\binom{p}{n}a^n b^{p-n}.$$

Or, lorsque $1\leqslant n\leqslant p-1$, $\binom{p}{n} = p!/n!(p-n)!$ est une fraction dont le numérateur $p!$ est multiple du nombre premier mais, et c'est là qu'on utilise que p est un nombre premier, dont le dénominateur n'est pas multiple de p. Comme $\binom{p}{n}$ est un entier, c'est un multiple de p et l'on a $\binom{p}{n}1_A = 0$, d'où $(a+b)^p = a^p + b^p$. □

DÉFINITION 1.2.18. — *Si K est un corps de caractéristique p, l'homomorphisme $\varphi\colon K\to K$, $x\mapsto x^p$ est appelé* homomorphisme de Frobenius.

1.3. Extensions de corps

DÉFINITION 1.3.1. — *La donnée d'un homomorphisme de corps $j\colon E\to F$ est appelée* extension de corps.

Remarquons qu'un tel j est toujours injectif : si en effet $x\neq 0$, on a

$$j(x)\,j(1/x) = j(1) = 1 \neq 0,$$

donc $j(x)\neq 0$. La plupart du temps, j est parfaitement déterminé par le contexte et peut être sous-entendu. On dit alors plus simplement que F est une extension de E. C'est notamment le cas quand $E\subset F$ et j est l'inclusion. On dit alors « soit $E\subset F$ une extension de corps ». Quitte à remplacer E par son image (bijective) dans F par l'homomorphisme j, c'est essentiellement le cas général.

Si $j\colon E\to F$ est une extension de corps, F est naturellement muni d'une structure de E-espace vectoriel : la loi d'addition est celle de F et la multiplication externe $E\times F\to F$ est définie par $e\cdot f = j(e)f$.

DÉFINITION 1.3.2. — *Si $j\colon E \to F$ est une extension, son* degré *est la dimension de F comme E-espace vectoriel. On le note $[F:E]$.*

L'extension $j\colon E \to F$ est dite finie *si $[F:E] \neq +\infty$.*

Remarque 1.3.3. — Cette notation $[F:E]$ est abusive : elle ne fait pas intervenir j alors qu'elle en dépend ! Par exemple, si $E = \mathbf{C}(X)$, $F = \mathbf{C}(Y)$, l'extension $j_1\colon E \to F$ définie par $P(X) \mapsto P(Y)$ est de degré 1 (c'est un isomorphisme) alors que $j_2\colon E \to F$ définie par $P(X) \mapsto P(Y^2)$ est de degré 2. Lorsque E est un sous-corps de F, ce qui est un cas assez fréquent, il n'y a pas de risque de confusion.

Exemples 1.3.4. — a) L'inclusion de corps $\mathbf{R} \subset \mathbf{C}$ est une extension finie : $\mathbf{C}$ est un $\mathbf{R}$-espace vectoriel de dimension 2 (la famille $\{1, i\}$ en est une base) et $[\mathbf{C}:\mathbf{R}] = 2$.

b) Si K est un corps, l'extension $K \subset K(X)$ n'est pas finie. En effet, $K(X)$ contient la famille libre infinie des X^n (pour $n \in \mathbf{N}$).

Remarque 1.3.5. — L'inclusion de corps $\mathbf{Q} \subset \mathbf{R}$ n'est pas non plus finie. En effet, le produit de deux ensembles dénombrable est dénombrable. Comme $\mathbf{Q}$ est dénombrable, il suit par récurrence que tout $\mathbf{Q}$-espace vectoriel de dimension finie est dénombrable. Cependant, le corps des nombres réels ne l'est pas, si bien que $[\mathbf{R}:\mathbf{Q}] = +\infty$. (Le même argument permet de montrer que $\mathbf{R}$ n' pas de base dénombrable sur $\mathbf{Q}$.)

Il est aussi possible d'exhiber des familles infinies de nombres réels qui soient linéairement indépendantes sur $\mathbf{Q}$. Par exemple, si α est un nombre transcendant, la famille $\{1, \alpha, \alpha^2, \ldots\}$ est libre sur $\mathbf{Q}$. Voir aussi l'exercice 1.6 pour un exemple plus explicite.

THÉORÈME 1.3.6. — *Soit $j\colon E \to F$ et $k\colon F \to G$ deux extensions de corps. Alors, $(k \circ j)\colon E \to G$ est une extension finie si et seulement si $j\colon E \to F$ et $k\colon F \to G$ sont finies et l'on a alors la relation*

$$[F:E]\,[G:F] = [G:E].$$

Démonstration. — Soit $x_1, \ldots, x_m$ une base de F comme E-espace vectoriel et soit $y_1, \ldots, y_n$ une base de G comme F-espace vectoriel. Un élément de $z \in G$ s'écrit $z = \sum_{i=1}^{n} a_i y_i$ avec $a_1, \ldots, a_n \in F$. Ainsi, chaque a_i se décompose sous la forme $a_i = \sum_{j=1}^{m} a_{i,j} x_j$, si bien que

$$y = \sum_{i=1}^{n} \sum_{j=1}^{m} a_{i,j} x_i y_j$$

et la famille des $(x_i y_j)_{\substack{1 \leqslant i \leqslant m \\ 1 \leqslant j \leqslant n}}$ engendre G comme E-espace vectoriel.

Montrons qu'en fait, c'en est une base. Soient donc des éléments $a_{i,j}$ de E tels que $\sum_{i,j} a_{i,j} x_i y_j = 0$. Comme la famille (y_j) est une base de G comme F-espace vectoriel,

les éléments de F, $\sum_{i=1}^{m} a_{i,j}x_i$, sont tous nuls. Comme la famille des (x_i) forme une base de F comme E-espace vectoriel, les $a_{i,j}$ sont tous nuls, cqfd.

Finalement, la dimension de G comme E-espace vectoriel est égale à mn, c'est-à-dire au produit de la dimension de G comme F-espace vectoriel par celle de F comme E-espace vectoriel, ce qui démontre le théorème. □

DÉFINITION 1.3.7. — *Soit $j\colon E \to F$ une extension de corps. Un élément $x \in F$ est dit* algébrique *sur E s'il existe un polynôme non nul $P \in E[X]$ tel que $P(x) = 0$.*

Il est dit transcendant *sinon.*

Une telle extension est dite algébrique *si tout élément de F est algébrique sur E.*

Un nombre complexe est dit algébrique ou transcendant s'il l'est sur le corps des nombres rationnels.

Exemples 1.3.8. — a) Considérons l'extension de corps $\mathbf{R} \subset \mathbf{C}$. Un élément $z = x + iy$ de $\mathbf{C}$, avec x et y dans $\mathbf{R}$, vérifie l'équation $(z-x)^2 + y^2 = 0$, si bien que z est algébrique sur $\mathbf{R}$.

b) Le réel $\sqrt{2}$ est algébrique sur $\mathbf{Q}$, ainsi que le nombre complexe $\sqrt{2} + i\sqrt[3]{3} + \sqrt[5]{5}$.

c) Le réel $\sum_{n=0}^{\infty} 10^{-n!}$ est transcendant (Liouville, 1844) ; voir l'exercice 1.2.

d) L'ensemble des polynômes à coefficients rationnels est dénombrable, si bien que l'ensemble des nombres complexes algébriques est dénombrable. Il existe en particulier des nombres transcendants (Cantor, 1874).

e) Les réels $e \approx 2{,}718\ldots$, $\pi \approx 3{,}14159$ sont transcendants sur $\mathbf{Q}$ (théorèmes de Hermite, 1873, et de Lindemann, 1882).

f) On ne sait pas si π est algébrique sur le sous-corps de $\mathbf{R}$ engendré par e (formé des $P(e)$ pour P décrivant $\mathbf{Q}(X)$).

Soit $j\colon E \to F$ une extension de corps et soit x un élément de F. L'application $\varphi_x\colon E[X] \to F$ qui à un polynôme $P = a_0 + \cdots + a_n X^n$ associe l'élément

$$(j(P)(x)) = j(a_0) + j(a_1)x + \cdots + j(a_n)x^n$$

est à la fois un homomorphisme de E-espaces vectoriels et un homomorphisme d'anneaux. Son image est ainsi non seulement un sous-espace vectoriel de F, mais aussi un sous-anneau de F, sous-anneau qu'on note $E[x]$. C'est le sous-anneau de F engendré par x sur E. (Lorsqu'il n'y a pas de confusion possible, on note $P(x)$ ce qu'on devrait noter $j(P)(x)$.) On va voir tout de suite (proposition 1.3.9) que si x est algébrique sur E, le sous-anneau $E[x]$ de F est en fait un corps, donc s'identifie au sous-corps $E(x)$ engendré par x sur E.

Plus généralement, si $x_1, \ldots, x_n$ sont des éléments de F, on note $E[x_1, \ldots, x_n]$ le *sous-anneau de F engendré par les x_i sur E*. C'est l'ensemble des $P(x_1, \ldots, x_n) \in F$

pour P parcourant $E[X_1,\dots,X_n]$. Le *sous-corps de F engendré par les x_i sur E*, noté $E(x_1,\dots,x_n)$, en est donc le corps des fractions.

La proposition suivante fournit une caractérisation extrêmement pratique des éléments algébriques en termes de l'anneau $E[x]$.

PROPOSITION 1.3.9. — *Soit $j\colon E\to F$ une extension et soit x un élément de F*

a) Si x est transcendant sur E, φ_x est un isomorphisme et $E[x]$ est un E-espace vectoriel de dimension infinie.

b) si x est algébrique sur E, il existe un unique polynôme unitaire de degré minimal $P\in E[X]$ tel que $P(x)=0$. Alors, P est irréductible et $\dim_E E[x]=\deg P$. *De plus, tout polynôme $Q\in E[X]$ tel que $Q(x)=0$ est multiple de P.*

Rappelons qu'on dit qu'un polynôme non constant $P\in E[X]$ est irréductible s'il n'est pas le produit de deux polynômes non constants à coefficients dans E.

DÉFINITION 1.3.10. — *Ce polynôme est appelé* polynôme minimal *de x sur E. Ses autres racines sont les* conjugués *de x. Son degré est appelé* degré *de x sur E.*

Démonstration. — a) Si x est transcendant, φ_x est injective par définition, surjective par construction, donc un isomorphisme. En particulier, $\dim_E E[x]=+\infty$.

b) Soit $P\in E[X]$ un polynôme unitaire de degré minimal tel que $P(x)=0$. Soit A un polynôme de $E[X]$ tel que $A(x)=0$. Notons $A=PQ+R$ la division euclidienne de A par P, de sorte que $\deg R<\deg P$. On a alors $R(x)=A(x)-P(x)Q(x)=0$. Si R n'est pas nul, de coefficient dominant noté r, le polynôme R/r est unitaire, de degré strictement inférieur à celui de P et annule x, ce qui contredit le choix de P. Par suite, $R=0$ et A est multiple de P. (Autrement dit, avec la terminologie du paragraphe 2.4, P est le *générateur unitaire de l'idéal des polynômes de $E[X]$ qui annulent x*.) Cela implique l'unicité d'un polynôme unitaire P de degré minimal tel que $P(x)=0$. En effet, soit $A\in E[X]$ un polynôme unitaire tel que $A(x)=0$ et soit Q le quotient de A par P. Comme A et P sont unitaires, Q aussi. Si $\deg Q=0$, on a nécessairement $Q=1$ et $A=P$. Si $\deg Q>0$, $\deg A>\deg P$.

Si $d=\deg P$, l'argument que nous venons de faire montre que φ_x induit un homomorphisme injectif $\varphi_{x,d}$ de $E[X]_{<d}$ (polynômes de degrés $<d$) dans $E[x]$. Toujours par division euclidienne, $\varphi_{x,d}$ est surjectif : si $A\in E[X]$ et si $A=PQ+R$ est la division euclidienne de A par P (avec $\deg R<d$), on a

$$\varphi_x(A)=A(x)=P(x)Q(x)+R(x)=R(x)$$

appartient à $\operatorname{Im}\varphi_{x,d}$. Par suite, $\dim_E E[x]=d$.

Il reste à montrer que P est irréductible. Mais, si $P=QR$ pour deux polynômes non constants Q et R dans $E[X]$, on a

$$Q(x)R(x)=P(x)=0$$

donc $Q(x) = 0$ ou $R(x) = 0$. Comme Q et R sont non constants et comme $\deg Q + \deg R = \deg P$, on a $\deg Q < \deg P$ et $\deg R < \deg P$, ce qui contredit encore la minimalité du degré de P. □

En voici une première application.

COROLLAIRE 1.3.11. — *Toute extension finie de corps est algébrique.*

Démonstration. — Soit $j : E \to F$ une extension finie de corps. Pour tout $x \in F$, $E[x]$ est un E-sous-espace vectoriel de F, donc est de dimension $\leqslant \dim_E F$, donc finie. D'après la proposition précédente, x est algébrique sur E. □

L'application qui suit est peut-être plus frappante :

THÉORÈME 1.3.12. — *Soit $j : E \to F$ une extension de corps. Soit x et y deux éléments de F algébriques sur E. Alors, $x+y$, xy sont algébriques sur E. Si $x \neq 0$, $1/x$ est algébrique sur E et appartient même à $E[x]$.*

En particulier, tout élément de $E[x]$ est algébrique sur E.

COROLLAIRE 1.3.13. — *L'ensemble des éléments de F qui sont algébriques sur E est un sous-corps de F.*

Démonstration. — Considérons le sous-anneau $E[x,y]$ de F engendré par x et y sur E ; il est formé des $P(x,y)$ pour P parcourant $E[X,Y]$. C'est un E-espace vectoriel de dimension finie : en effet, si $1, x, \ldots, x^{m-1}$ et $1, y, \ldots, y^{n-1}$ engendrent $E[x]$ et $E[y]$ respectivement, la famille des $x^i y^j$ avec $0 \leqslant i < m$ et $0 \leqslant j < n$ est une partie génératrice de $E[x,y]$.

Ceci dit, les sous-anneaux $E[x+y]$ et $E[xy]$ sont tous deux contenus dans $E[x,y]$. Ils sont donc de dimension finie et la proposition précédente permet donc d'affirmer que $x+y$ et xy sont algébriques sur E.

Supposons maintenant que $x \neq 0$ et montrons que $1/x$ est algébrique sur E. Considérons une relation $a_0 + a_1 x + \cdots + a_d x^d = 0$, où les a_i sont des éléments de E non tous nuls. Divisons cette relation par x^d. On obtient

$$a_0 (1/x)^d + a_1 (1/x)^{d-1} + \cdots + a_d = 0,$$

ce qui prouve que $1/x$ est algébrique sur E.

Montrons qu'en fait $1/x$ appartient à $E[x]$. Soit r le plus petit entier tel que $a_r \neq 0$, de sorte que $a_0 = \cdots = a_{r-1} = 0$. On a alors $a_r x^r + \cdots + a_d x^d = 0$, soit en divisant par $x^r \neq 0$,

$$a_r + a_{r+1} x + \cdots + a_d x^{d-r} = 0.$$

Divisons encore cette relation par $a_r x$. On obtient

$$\frac{1}{x} = -\frac{a_{r+1}}{a_r} - \frac{a_{r+2}}{a_r} x - \cdots - \frac{a_d}{a_r} x^{d-r-1},$$

d'où $1/x \in E[x]$, ce qu'il fallait démontrer. □

COROLLAIRE 1.3.14. — *Un élément $x \in F$ est algébrique sur E si et seulement si l'anneau $E[x]$ est un sous-corps de F.*

Démonstration. — Si l'inverse $x \neq 0$ appartient à $E[x]$, il existe un polynôme $P \in E[X]$ tel que $1/x = P(x)$. Alors, x est racine du polynôme non nul $1 - XP(X)$ donc est algébrique. Réciproquement, soit a un élément non nul de $E[x]$. D'après le théorème précédent, il est algébrique et son inverse dans F appartient à $E[a]$. Comme $E[a] \subset E[x]$, $E[x]$ est un corps. (Pour une autre démonstration, voir l'exercice 1.1.) □

Remarque 1.3.15. — Soit $j : E \to F$ une extension finie de corps et soit $x \in F$. D'après les corollaires précédents, x est algébrique sur E et $E[x]$ est un sous-corps de F, d'où une extension composée $E \to E[x] \to F$. D'après le théorème 1.3.6, $[F : E] = [F : E[x]]\,[E[x] : E]$. Or, le degré de l'extension $E \to E[x]$ est précisément égal au degré de x. Il en résulte que le degré (sur E) de tout élément de F *divise* le degré de l'extension $[F : E]$.

Un autre corollaire de ce genre d'idées est la « transitivité » du caractère algébrique.

THÉORÈME 1.3.16. — *Soit $j : E \to F$ et $k : F \to G$ deux extensions de corps. Si un élément $x \in G$ est algébrique sur F et si F est algébrique sur E, alors x est algébrique sur E.*

En particulier, si $E \to F$ et $F \to G$ sont des extensions algébriques, la composée $E \to G$ est une extension algébrique.

Démonstration. — Soit $P \in F[X]$ le polynôme minimal de x sur F. On l'écrit $P = X^n + a_{n-1}X^{n-1} + \cdots + a_0$. Les a_j sont dans F, donc sont algébriques sur E. Par récurrence, le sous-anneau $F_0 = E[a_0, \ldots, a_{n-1}]$ de F est un corps et une extension finie de E. Par construction, x est algébrique sur F_0 si bien que l'extension $F_0 \to F_0[x]$ est finie. D'après le théorème 1.3.6, l'extension $E \to F_0[x]$ est finie, ce qui prouve bien que x est algébrique sur E. □

Remarque 1.3.17. — Si $A \to B$ est un homomorphisme d'anneaux, on dit parfois que B est une *A-algèbre*. Outre les extensions de corps (si $E \to F$ est une extension de corps, F est ainsi une E-algèbre), un cas particulier important est fourni par les anneaux de polynômes $K[X_1, \ldots, X_n]$ sur un corps K. Si K est un corps, un anneau A contenant K et tel qu'il existe des éléments $x_1, \ldots, x_n$ dans A de sorte que $A = K[x_1, \ldots, x_n]$ est appelé *K-algèbre de type fini*.

La proposition 1.3.9 montre en particulier que si $A = K[x]$ est un corps, alors A est algébrique sur K. Le *théorème des zéros de Hilbert* que nous démontrerons au paragraphe 6.8 (théorème 6.8.1) généralise ce fait à toutes les K-algèbres de type fini, pas seulement celles qui sont engendrées par un seul élément.

1.4. Quelques impossibilités classiques

Nous voulons maintenant montrer comment les résultats précédents permettent d'affirmer qu'un certain nombre de constructions géométriques sont *impossibles*.

Revenons tout d'abord sur les nombres constructibles. Comme l'ensemble des nombres constructibles est un corps, il revient au même de dire que x est constructible à partir d'une partie Σ contenant 0 et 1 que de dire qu'il est constructible à partir du corps engendré par Σ dans $\mathbf{R}$. En particulier, être constructible à partir de $\{0;1\}$ et l'être à partir de $\mathbf{Q}$ sont deux notions équivalentes.

THÉORÈME 1.4.1 (Wantzel, 1837). — *Soit E un sous-corps de $\mathbf{R}$. Un réel x est constructible à la règle et au compas à partir de E si et seulement s'il existe un entier n et une suite de sous-corps de $\mathbf{R}$,*

$$E = E_0 \subset E_1 \subset \cdots \subset E_n$$

tels que pour tout $i \in \{1;\ldots;n\}$, $[E_i : E_{i-1}] = 2$ et tels que $x \in E_n$.

Avant de faire la démonstration, il nous faut détailler la structure des extensions de degré 2 : elles sont obtenues par « adjonction d'une racine carrée ». On les appelle aussi *extensions quadratiques*.

PROPOSITION 1.4.2. — *Soit E un sous-corps de $\mathbf{R}$ (plus généralement un corps de caractéristique différente de 2) et soit $j : E \to F$ une extension de degré 2. Alors, il existe un élément $a \in F \setminus E$ tel que $a^2 \in E$ et $F = E[a]$.*

Démonstration. — Soit x un élément de F qui n'est pas dans E. La famille $(1,x)$ est alors libre sur E donc est une base de F comme E-espace vectoriel. La famille $(1,x,x^2)$ est alors liée et il existe trois éléments a, b, c de E non tous nuls tels que l'on ait $ax^2+bx+c=0$. Comme la famille $(1,x)$ est libre, $a \neq 0$, d'où la relation classique

$$\left(x+\frac{b}{2a}\right)^2 = \frac{b^2-4ac}{4a^2}.$$

Posons $\delta = 2ax+b$, de sorte que $\delta^2 = b^2-4ac$ appartient à E (c'est le discriminant du polynôme aX^2+bX+c). Comme $x = \delta/2a$, la famille $(1,\delta)$ est une base de F sur E. □

Démonstration du théorème de Wantzel. — La démonstration repose sur la forme des équations des droites et des cercles qui interviennent dans la construction, ainsi que sur leur résolution explicite.

Tout d'abord, une droite passant par deux points $A = (a,b)$ et $A' = (a',b')$ dont les coordonnées sont dans K possède une équation à coefficients dans K, à savoir

$$\det\begin{pmatrix} 1 & 1 & 1 \\ x & a & a' \\ y & b & b' \end{pmatrix} = 0.$$

De même, le cercle de rayon MM' et de centre O, avec $M = (a,b)$, $M' = (a',b')$ et $O = (a'',b'')$ des points du plans dont les coordonnées sont dans K, a une équation de la forme

$$x^2 + y^2 + Ax + By + C = 0,$$

avec A, B, C dans K, comme on le voit en développant l'équation de ce cercle

$$(x-a'')^2 + (y-b'')^2 = (a-a')^2 + (b-b')^2.$$

Les formules explicites pour les coordonnées du point d'intersection P de deux droites concourantes montrent que celles-ci sont des expressions rationnelles en les coefficients des équations des droites. Les coordonnées du point d'intersection P de deux droites non parallèles (AA') et (BB') telles que A, A', B, B' aient leurs coordonnées dans K sont donc dans K.

Si P nécessite une intersection droite/cercle, on obtient les équations polynomiales de degré 2

$$x^2 + y^2 + Ax + By + C = 0 \quad \text{et} \quad Dx + Ey + F = 0$$

avec A, B, C, D, E, $F \in K$. Supposant par exemple $E \neq 0$ et éliminant y, on obtient une équation du second degré pour x à coefficients dans K ; notons Δ son discriminant (il appartient à K). Ainsi, x, puis y, appartiennent à l'extension $K(\sqrt{\Delta})$ qui de degré 2 sur K.

Si P nécessite une intersection cercle/cercle, on se ramène au cas précédent cercle/droite en soustrayant les deux équations de cercles. (Du point de vue géométrique, la droite qui apparaît est l'*axe radical* des deux cercles. Si les cercles se coupent, c'est celle qui passe par leurs deux points d'intersections.)

Par récurrence sur le nombre d'étapes, tout nombre constructible à partir du sous-corps E est de la forme indiquée dans l'énoncé du théorème.

Réciproquement, si $x \in E_n$, bout d'une chaîne d'extensions de degré 2, on démontre que x est constructible. Il suffit de montrer que si $E \subset F$ est une extension de degré 2, tout élément de F est constructible à partir de E. D'après la proposition 1.4.2, il existe un élément δ de F tel que $F = E[\delta]$ et $\delta^2 \in E$. D'après le théorème 1.1.3, $\delta = \pm\sqrt{\delta^2}$ est constructible. Toujours d'après cette proposition, tout élément de $\mathbf{R}$ de la forme $x + y\delta$ est constructible à partir de E, si bien que tout élément de F est constructible à partir de E. □

Exercice 1.4.3. — Étendre le théorème de Wantzel aux nombres complexes.

COROLLAIRE 1.4.4. — *Soit E un sous-corps de $\mathbf{R}$ et soit x un réel constructible à la règle et au compas à partir de E. Alors, x est algébrique et est de degré (sur E) une puissance de 2.*

Démonstration. — Soit $E = E_0 \subset E_1 \subset \cdots \subset E_n \subset \mathbf{R}$ une chaîne d'extensions quadratiques avec $x \in E_n$. Par récurrence, la multiplicativité des degrés implique que

$$[E_n : E] = [E_n : E_1][E_1 : E_0] = 2[E_n : E_1] = \cdots = 2^n.$$

Considérant les extensions $E \subset E[x] \subset E_n$, le degré de $E[x]$ sur E doit diviser 2^n ; c'est donc une puissance de 2. □

Nous pouvons maintenant démontrer l'impossibilité de constructions longtemps — et vainement — cherchées.

THÉORÈME 1.4.5 (Doublement du cube). — *Le réel $\sqrt[3]{2}$ n'est pas constructible à la règle et au compas à partir de* $\mathbf{Q}$.

Il n'est donc pas possible de construire à la règle et au compas le côté d'un cube dont le volume serait le double de celui du cube unité. La légende veut que ce problème provienne d'une requête du dieu grec Apollon, qui aurait demandé aux habitants de Delos de lui construire un autel deux fois plus grand.

Démonstration. — Posons $\alpha = \sqrt[3]{2}$. Il suffit de montrer que α n'est pas de degré une puissance de 2. Comme α est annulé par le polynôme $X^3 - 2$, il est de degré $\leqslant 3$ et il suffit donc de montrer que $X^3 - 2$ est irréductible sur $\mathbf{Q}$. Si ce n'était pas le cas, il aurait une racine dans $\mathbf{Q}$ (lemme 1.4.9). Or, les racines de $X^3 - 2$ dans $\mathbf{C}$ sont α, $\alpha \exp(2i\pi/3)$ et $\alpha \exp(-2i\pi/3)$. Seul α est réel. Si α était rationnel, écrivons le sous la forme d'une fraction irréductible a/b. On a alors $a^3 = 2b^3$, si bien que a est pair. Posons $a = 2a'$. On a alors $b^3 = 4(a')^3$, ce qui montre que b est aussi pair. Comme cela contredit l'hypothèse que a et b sont premiers entre eux, α n'est pas rationnel et le polynôme $X^3 - 2$ est irréductible sur $\mathbf{Q}$. □

Le problème de la trisection de l'angle est plus subtil. À partir du point de coordonnées $(\cos(\alpha), \sin(\alpha))$ du cercle unité, il s'agit de construire le point de coordonnées $(\cos(\alpha/3), \sin(\alpha/3))$.

Remarquons que $\sin(\alpha)$ est constructible à partir du corps $\mathbf{Q}(\cos(\alpha))$, puisque l'on a $\sin^2(\alpha) = 1 - \cos^2(\alpha)$. Ainsi, il revient au même de dire que $\cos(\alpha/3)$ est constructible sur le corps $\mathbf{Q}(\cos(\alpha), \sin(\alpha))$ ou sur le corps $\mathbf{Q}(\cos(\alpha))$. En outre, si l'on suppose que $\cos(\alpha/3)$ est constructible sur le corps $\mathbf{Q}(\cos(\alpha/3))$, $\sin(\alpha/3)$ le sera aussi. Ainsi, on peut trisecter l'angle α si et seulement si $\cos(\alpha/3)$ est constructible à partir du corps $\mathbf{Q}(\cos(\alpha))$.

Comme $\cos(3x) = 4\cos^3(x) - 3\cos(x)$, $2\cos(\alpha/3)$ est une racine du polynôme

$$X^3 - 3X - 2\cos(\alpha),$$

les deux autres étant $\cos(\alpha/3 + 2\pi/3)$ et $\cos(\alpha/3 + 4\pi/3)$. Si le polynôme $X^3 - 3X - 2\cos(\alpha)$ est irréductible sur le corps $\mathbf{Q}(\cos(\alpha))$, le degré de $\cos(\alpha/3)$ sur $\mathbf{Q}(\cos(\alpha))$ est égal à 3 et l'angle α n'est pas trisectable. Sinon, il résulte du lemme 1.4.9 que ce polynôme

a une racine dans $\mathbf{Q}(\cos(\alpha))$; le degré de $\cos(\alpha/3)$ est alors 1 ou 2 et $\cos(\alpha/3)$ est constructible. On a ainsi démontré le théorème :

THÉORÈME 1.4.6 (Trisection de l'angle). — *Soit α un réel. Le réel* $\cos(\alpha/3)$ *est constructible à la règle et au compas à partir de* $\{0;1;\cos(\alpha)\}$ *si et seulement si le polynôme* $X^3-3X-2\cos(\alpha)$ *n'est pas irréductible sur le corps* $\mathbf{Q}(\cos(\alpha))$.

Démonstration. — Si ce polynôme est irréductible, $\cos(\alpha/3)$ n'est pas constructible à partir de $\cos(\alpha)$. S'il n'est pas irréductible, il s'écrit comme produit P_1P_2 de deux polynômes à coefficients dans $\mathbf{Q}(\cos(\alpha))$ de degrés 1 et 2 respectivement. Si $P_1(\cos(\alpha/3))=0$, $\cos(\alpha)$ appartient à $\mathbf{Q}(\cos(\alpha))$ donc est constructible à partir de $\cos(\alpha)$. Si $P_2(\cos(\alpha/3))=0$, $\cos(\alpha/3)$ est de degré 2 sur $\mathbf{Q}(\cos(\alpha))$ donc est constructible à partir de $\cos(\alpha)$. □

Exemple 1.4.7. — L'angle $\pi/9$ n'est pas constructible à la règle et au compas. Comme $\cos(\pi/3)=1/2$, il suffit de voir que le polynôme $P=X^3-3X-1$ est irréductible sur $\mathbf{Q}$. S'il ne l'est pas, il a d'après le lemme 1.4.9 une racine dans $\mathbf{Q}$; considérons une telle racine, mise sous forme d'une fraction irréductible a/b. On a donc $a^3-3ab^2-b^3=0$. Si p est un nombre premier qui divise a, il divise $b^3=a(a^2-3b^2)$, donc il divise b. Comme a et b sont premiers entre eux, $a=\pm1$. De même, si p est un nombre premier qui divise b, il divise $a^3=b^2(3a+b)$, donc il divise a. Ainsi, $b=\pm1$. Par suite, les seules racines possibles rationnelles de P sont $+1$ et -1 ; puisque $P(1)=-3$ et $P(-1)=1$, P n'a pas de racine dans $\mathbf{Q}$, donc est irréductible sur $\mathbf{Q}$.

Cela montre qu'on ne peut construire à la règle et au compas un polygone régulier à 9 côtés. Dans le chapitre 5, nous déterminerons les polygones réguliers que l'on peut construire à la règle et au compas (théorème 5.2.2).

THÉORÈME 1.4.8 (Quadrature du cercle). — *Le réel $\sqrt{\pi}$ n'est pas constructible.*

En termes plus classiques, il n'est pas possible de construire à la règle et au compas le côté d'un carré dont l'aire serait celle du disque unité.

Démonstration. — Si $\sqrt{\pi}$ était constructible, il serait algébrique sur $\mathbf{Q}$, donc π aussi. Or, d'après le théorème de Lindemann, π est transcendant. □

Terminons en rappelant un lemme utilisé plusieurs fois.

LEMME 1.4.9. — *Soit K un corps. Un polynôme $P\in K[X]$ de degré 2 ou 3 est irréductible sur K si et seulement s'il n'a pas de racine dans K*

Démonstration. — Si P a une racine $a\in K$, soit $P=(X-a)Q+R$ la division euclidienne de P par $X-a$. Le polynôme R est de degré $<\deg(X-a)=1$ donc est constant. Comme on a $P(a)=R(a)=0$, $R=0$ et $P=(X-a)Q$. Puisque $\deg Q=\deg P-1\geqslant 1$, P n'est pas irréductible.

Dans l'autre sens, si P n'est pas irréductible, écrivons $P = QR$ pour deux polynômes non constants Q et R dans $K[X]$. Comme $\deg Q + \deg R = \deg P \leqslant 3$, l'un des deux $\deg Q$ ou $\deg R$ est égal à 1 et a automatiquement une racine dans K. Par conséquent, P a une racine dans K. □

1.5. Fonctions symétriques des racines

Rappelons que le groupe des permutations (bijections) de l'ensemble fini $\{1;\dots;n\}$ est noté $\mathfrak{S}_n$. C'est un groupe fini de cardinal $n!$.

DÉFINITION 1.5.1. — *Un polynôme $P \in A[X_1,\dots,X_n]$ en n indéterminées à coefficients dans un anneau A est dit* symétrique *si pour toute permutation $\sigma \in \mathfrak{S}_n$, on a*

$$P(X_{\sigma(1)},\dots,X_{\sigma(n)}) = P(X_1,\dots,X_n).$$

Les exemples les plus connus sont la somme $S_1(X) = X_1 + \cdots + X_n$ et le produit $S_n(X) = X_1 \dots X_n$. Plus généralement, on introduit les *polynômes symétriques élémentaires* par

$$S_p(X) = \sum_{1 \leqslant i_1 < \cdots < i_p \leqslant n} X_{i_1} \dots X_{i_p}, \qquad 1 \leqslant p \leqslant n.$$

Il est important de remarquer que les $S_p(X)$ sont les coefficients du polynôme $(T - X_1)\dots(T - X_n)$ (polynôme en T à coefficients dans $A[X_1,\dots,X_n]$) ; en effet, on a

$$(T - X_1)\dots(T - X_n) = T^n - S_1 T^{n-1} + S_2 T^{n-2} + \cdots + (-1)^n S_n.$$

Il existe bien d'autres polynômes symétriques : par exemple, les polynômes de Newton

$$N_p(X) = X_1^p + \cdots + X_n^p.$$

On a $N_1 = S_1$,

$$\begin{aligned} N_2(X) &= X_1^2 + \cdots + X_n^2 \\ &= (X_1 + \cdots + X_n)^2 - 2(X_1X_2 + X_1X_3 + \cdots + X_{n-1}X_n) \\ &= S_1^2 - 2S_2, \end{aligned}$$

et plus généralement, $N_p(X)$ s'exprime comme un polynôme à coefficients entiers en $S_1(X),\dots,S_n(X)$.

PROPOSITION 1.5.2. — *Pour tout entier $p \geqslant 1$, il existe un polynôme à coefficients entiers $P_p \in \mathbf{Z}[T_1,\dots,T_n]$ tel que l'on ait*

$$N_p(X_1,\dots,X_n) = P_p(S_1(X),\dots,S_n(X)).$$

Démonstration. — Introduisons le polynôme $\Pi = (T-X_1)\dots(T-X_n)$ et soit M sa matrice compagnon. C'est une matrice carrée $n \times n$ à coefficients dans le sous-anneau $\mathbf{Z}[S_1,\dots,S_n]$ de $\mathbf{Z}[X_1,\dots,X_n]$, de polynôme minimal Π et de polynôme caractéristique Π aussi. Comme son polynôme caractéristique est scindé dans le corps $\mathbf{Q}(X_1,\dots,X_n)$, elle est triangularisable dans ce corps, de valeurs propres $X_1,\dots,X_n$. En particulier, N_p est la trace de C^p. Comme C est à coefficients dans l'anneau $\mathbf{Z}[S_1,\dots,S_n]$, ses puissances aussi, et leur trace a fortiori. Cela montre l'existence du polynôme P_p. □

Ce que nous avons démontré pour les sommes de Newton est en fait valable pour tout polynôme symétrique.

THÉORÈME 1.5.3. — *Pour tout polynôme symétrique $P \in A[X_1,\dots,X_n]$, il existe un unique polynôme $Q \in A[Y_1,\dots,Y_n]$ tel que*

$$P(X_1,\dots,X_n) = Q(S_1(X),\dots,S_n(X)).$$

Démonstration. — On démontre l'existence de Q par récurrence sur le degré de P et sur le nombre de variables n. Si $n=1$, on a $S_1 = X_1$ et on pose $Q = P$. Si $\deg P = 0$, P est constant et on choisit pour Q cette constante. Supposons le résultat vérifié en $(n-1)$ variables ou en degrés $< m$ et soit P un polynôme symétrique de degré m. Le polynôme P_0 en $(n-1)$ variables défini par

$$P_0(X_1,\dots,X_{n-1}) = P(X_1,\dots,X_{n-1},0)$$

est symétrique. Il existe par récurrence un polynôme

$$Q_0 \in A[Y_1,\dots,Y_{n-1}]$$

tel que

$$P_0(X_1,\dots,X_{n-1}) = Q_0(S_1(X),\dots,S_{n-1}(X)).$$

Dans cette dernière formule, il s'agit des polynômes symétriques en $(n-1)$ variables, mais il est facile de constater que l'on a (on indique en exposant le nombre de variables) :

$$S_p^{(n-1)}(X_1,\dots,X_{n-1}) = S_p^{(n)}(X_1,\dots,X_{n-1},0)$$

et plus généralement,

$$S_p^{(n)}(X_1,\dots,X_n) = S_p^{(n-1)}(X_1,\dots,X_{n-1}) + X_n S_{p-1}^{(n-1)}(X_1,\dots,X_{n-1}).$$

Alors,

$$P_1(X) = P(X_1,\dots,X_n) - Q_0(S_1(X),\dots,S_{n-1}(X))$$

est un polynôme symétrique et lorsqu'on remplace X_n par 0, on obtient le polynôme nul. Cela implique que P_1 est multiple de X_n : le coefficient d'un monôme $X_1^{i_1}\dots X_n^{i_n}$ sont nuls dès que $i_n = 0$. Comme il est symétrique, le coefficient de $X_1^{i_1}\dots X_n^{i_n}$ est nul dès que l'un des i_j est nul. Ainsi, chaque monôme non nul de P_1 est multiple de $S_n = X_1\dots X_n$ et par suite P_1 aussi. On peut donc écrire $P_1 = S_n P_2$ pour $P_2 \in A[X_1,\dots,X_n]$.

Le polynôme P_2 est encore symétrique mais de degré $< m$. Par récurrence, il s'écrit $Q_2(S_1,\dots,S_n)$. Finalement, on a

$$P(X) = Q_0(S_1,\dots,S_n) + P_1(X) = Q_0(S_1,\dots,S_n) + S_n Q_2(S_1,\dots,S_n)$$

et il suffit de poser $Q = Q_0 + S_n Q_2$.

Démontrons maintenant l'unicité. Il suffit de démontrer que si un polynôme $Q \in A[Y_1,\dots,Y_n]$ vérifie $Q(S_1,\dots,S_n) = 0$, alors $Q = 0$. Si $n = 1$, c'est évident. Supposons le résultat d'unicité démontré pour $(n-1)$ variables. On le démontre alors pour n variables par récurrence sur le degré de Q. Spécialisant X_n sur 0, on a en particulier

$$0 = Q(S_1(X_1,\dots,X_{n-1},0),\dots,S_n(X_1,\dots,X_{n-1},0)) = Q(S_1^{(n-1)},\dots,S_{n-1}^{(n-1)},0),$$

ce qui implique par récurrence que $Q(Y_1,\dots,Y_{n-1},0) = 0$. Ainsi, Q est multiple de Y_n et on conclut par récurrence sur le degré de Q. □

Un polynôme symétrique important est le *discriminant* :

$$D = \prod_{i<j} (X_i - X_j)^2.$$

Pour constater qu'il est symétrique, il est peut-être plus simple de l'écrire

$$D = (-1)^{n(n-1)/2} \prod_{i\neq j} (X_i - X_j)$$

et de remarquer que si $\sigma \in \mathfrak{S}_n$, l'application $(i,j) \mapsto (\sigma(i),\sigma(j))$ est une bijection de l'ensemble des couples d'entiers distincts dans lui-même. Ainsi, $\sigma(D) = D$.

1.6. Appendice : transcendance de e et π

Nous démontrons dans ce paragraphe la transcendance de e et π. Comme les nombres e et π ne sont pas du ressort de l'algèbre mais de l'analyse, il n'est pas étonnant que la démonstration mette en jeu des outils analytiques, en l'occurrence concentrés dans le lemme suivant.

LEMME 1.6.1. — *Soit f un polynôme à coefficients réels ; notons m son degré. Pour tout nombre complexe z, l'intégrale (complexe)*

$$I(f;z) = \int_0^1 z\mathrm{e}^{z(1-u)} f(zu)\,du$$

vérifie

$$I(f;z) = \mathrm{e}^z \sum_{j=0}^{m} f^{(j)}(0) - \sum_{j=0}^{m} f^{(j)}(z).$$

De plus, on a la majoration

$$\big|I(f;z)\big| \leqslant |z|\,\mathrm{e}^{|z|} \sup_{u\in[0,1]} \big|f(zu)\big|.$$

Démonstration. — Intégrons par partie dans la définition de $I(f;z)$. On obtient

$$\begin{aligned} I(f;z) &= \left[-\mathrm{e}^{z(1-u)}f(zu)\right]_0^1 + \int_0^1 \mathrm{e}^{z(1-u)}zf'(zu)\,du \\ &= -f(z) + \mathrm{e}^z f(0) + I(f';z), \end{aligned}$$

d'où le résultat par récurrence sur le degré de f. Pour obtenir la majoration de $\left|I(f;z)\right|$, il suffit d'intégrer sur $[0,1]$ l'inégalité

$$\left|z\mathrm{e}^{z(1-u)}f(zu)\right| \leqslant |z|\,\mathrm{e}^{|z|}\sup_{u\in[0,1]}\left|f(zu)\right|,$$

valable pour tout $u \in [0,1]$. □

LEMME 1.6.2. — *Soit f un polynôme à coefficients entiers. Pour tout entier $n \geqslant 0$, il existe un polynôme f_n à coefficients entiers tels que $f^{(n)} = n!f_n$.*

Démonstration. — Par linéarité, il suffit de démontrer ce lemme pour $f = X^m$. Dans ce cas, $f^{(n)} = m(m-1)\dots(m-n+1)X^{m-n}$. Le polynôme $f_n = \binom{m}{n}X^{m-n}$ est à coefficients entiers et vérifie $f^{(n)} = n!f_n$. □

THÉORÈME 1.6.3 (Hermite). — e *est transcendant.*

Démonstration. — Raisonnons par l'absurde. Si e n'est pas transcendant, il existe des entiers $a_0,\dots,a_n$ tels que

$$a_0 + a_1\mathrm{e} + \cdots + a_n\mathrm{e}^n = 0.$$

Quitte à diviser cette relation par une puissance de e, on peut en outre supposer que $a_0 \neq 0$.

Soit p un nombre premier fixé pour l'instant ; soit $f(x) = x^{p-1}(x-1)^p\dots(x-n)^p$ et introduisons

$$J_p = a_0I(f;0) + a_1I(f;1) + \cdots + a_nI(f;n).$$

On a donc

$$J_p = -\sum_{i=0}^{n} a_i \sum_{j=0}^{np+p-1} f^{(j)}(i).$$

C'est en particulier un entier.

De plus, si $i \in \{1,\dots,n\}$, i est racine de f à l'ordre p, si bien que $f^{(j)}(i) = 0$ pour $j < p$, tandis que pour $j \geqslant p$, c'est un multiple de $p!$. En revanche, $i = 0$ est racine de f d'ordre $p-1$. Il en résulte que $f^{(j)}(0) = 0$ pour $j < p-1$, et est multiple de $p!$ pour $j \geqslant p$, mais

$$f^{(p-1)}(0) = (p-1)!(-1)^p\dots(-n)^p = (-1)^{np}(p-1)!(n!)^p.$$

Charles Hermite (1822–1901)

Ainsi, il existe un entier N tel que

$$J_p = (-1)^{np+1} a_0 (p-1)!(n!)^p + p!N.$$

En particulier, si $p > n$ et ne divise pas a_0 (c'est là qu'on utilise que $a_0 \neq 0$), $J_p/(p-1)!$ est un entier non nul modulo p, donc est non nul, donc est au moins égal à 1 en valeur absolue. On a ainsi $|J_p| \geqslant (p-1)!$. Or, il existe un réel c tel que $|J_p| \leqslant c^p$ pour tout p. L'inégalité obtenue $c^p \geqslant (p-1)!$ contredit alors la formule de Stirling

$$p! \sim p^p \mathrm{e}^{-p} \sqrt{2\pi p}$$

quand p tend vers l'infini. □

Passons maintenant à la transcendance de π. Si f est un polynôme et $g\colon \mathbf{C} \to \mathbf{C}$ une fonction, on notera

$$\sum_{f(\alpha)=0} g(\alpha)$$

la somme $g(\alpha_1) + \cdots + g(\alpha_n)$ où les α_j sont les racines de f, répétées autant de fois que leur multiplicité.

LEMME 1.6.4. — *Soit f un polynôme à coefficients entiers, de coefficient dominant a. Alors, pour tout $n \geqslant 0$,*

$$a^n \sum_{f(\alpha)=0} \alpha^n \in \mathbf{Z}.$$

Démonstration. — Soit m le degré de f et notons A la matrice compagnon de polynôme minimal f/a. Par construction, $aA \in M_m(\mathbf{Z})$. Par suite, $a^n A^n$ est à coefficients entiers et sa trace est un entier. Or, les valeurs propres de $a^n A^n$ sont les $(a\alpha)^n$, α parcourant les racines de f, avec multiplicités. Le lemme est donc démontré. □

PROPOSITION 1.6.5. — *Soit f un polynôme à coefficients entiers tel que $f(0) \neq 0$. Alors, $\sum_{f(\alpha)=0} e^{\alpha}$ n'est pas un entier non nul.*

Démonstration. — Soit $N = \sum_{f(\alpha)=0} e^{\alpha}$ et supposons par l'absurde que N est entier. Notons a le coefficient dominant de f. Soit p un nombre premier, fixé temporairement, définissons $g(x) = x^{p-1} f^p(x)$. C'est un polynôme de degré $m = p(1+\deg f) - 1$. Posons alors

$$J_p = \sum_{f(\alpha)=0} I(g;\alpha).$$

On a ainsi

$$J_p = N\left(\sum_n g^{(n)}(0)\right) - \sum_n \left(\sum_{f(\alpha)=0} g^{(n)}(\alpha)\right).$$

Si $f(\alpha)=0$, α est zéro de g à l'ordre p, si bien que $g^{(n)}(\alpha)=0$ pour $n<p$. D'autre part, si $n\geqslant p$, les deux lemmes précédents impliquent que $g_n=g^{(n)}/p!$ est un polynôme à coefficients entiers de degré $m-n$ et que

$$a^{m-n}\sum_{f(\alpha)=0} g^{(n)}(\alpha)$$

est entier, multiple de $p!$. D'autre part, $g^{(n)}(0)=0$ pour $n<p-1$, est multiple de $p!$ pour $n\geqslant p$ mais

$$g^{(p-1)}(0)=(p-1)!f(0)^p.$$

Ainsi, il existe un entier M tel que

$$\frac{a^{m-p}}{(p-1)!}J_p=a^{m-p}Nf(0)^p+pM.$$

Le second membre de cette égalité est entier. De plus, si le nombre premier p ne divise pas $aNf(0)$, il n'est pas multiple de p. Il est en particulier non nul, et par conséquent au moins égal à 1 en valeur absolue ! Ainsi,

$$\left|J_p\right|\geqslant(p-1)!a^{p-m}=(p-1)!a^{1-p\deg f}.$$

Or, la majoration de l'intégrale I dans le lemme 1.6.1 implique qu'il existe un réel $c>0$ tel que l'on ait

$$\left|J_p\right|\leqslant c^p$$

pour tout p.

Lorsque p tend vers l'infini, la formule de Stirling rend ces deux inégalités sont incompatibles. La proposition est donc démontrée. □

THÉORÈME 1.6.6 (Lindemann). — *π est transcendant.*

Démonstration. — Si π était algébrique, $i\pi$ aussi. Soit alors f un polynôme irréductible à coefficients entiers tel que $f(i\pi)=0$. Notons $\alpha_1,\ldots,\alpha_n$ ses racines. De l'équation

$$1+e^{i\pi}=0,$$

on déduit

$$\prod_{f(\alpha)=0}(1+e^{\alpha})=(1+e^{\alpha_1})\ldots(1+e^{\alpha_n})=0.$$

Développons cette égalité. Il vient

$$\sum_{\varepsilon\in\{0;1\}^n}\exp(\sum\varepsilon_j\alpha_j)=0.$$

Or, les $\sum\varepsilon_j\alpha_j=0$ sont les racines du polynôme

$$F_0=\prod_{\varepsilon\in\{0;1\}^n}(X-\sum_j\varepsilon_j\alpha_j)$$

dont les coefficients s'expriment comme des polynômes symétriques en les α_j. D'après le théorème sur les fonctions symétriques élémentaires, ce sont donc des

polynômes en les fonctions symétriques élémentaires des α_j, donc en les coefficients de f. Ce sont donc des nombres rationnels. Il existe par suite un entier N tel que $NF_0 \in \mathbf{Z}[X]$. Soit $q \geqslant 1$ la multiplicité de la racine 0 dans F_0. On pose alors $F = NF_0/X^q$. C'est un polynôme à coefficients entiers et $F(0) \neq 0$. De plus, on a

$$0 = \sum_{\varepsilon \in \{0;1\}^n} \exp(\sum \varepsilon_j \alpha_j) = q + \sum_{F(\beta)=0} e^{\beta}.$$

Ceci contredit la proposition précédente. □

Exercices

Exercice 1.1. — **a)** Soit A un anneau intègre fini. Montrer que A est un corps. Exemples ?

b) Soit F un anneau intègre et $E \subset F$ un sous-corps de sorte que F soit un E-espace vectoriel de dimension finie. Montrer que F est un corps.

Exercice 1.2 (Critère de Liouville). — **a)** Soit α un nombre complexe qui est algébrique sur $\mathbf{Q}$. Notons d son degré. Montrer qu'il existe un polynôme $P \in \mathbf{Z}[X]$ de degré d tel que $P(\alpha) = 0$ et $P'(\alpha) \neq 0$.

Montrer qu'il existe un réel $c > 0$ tel que pour tout couple $(p, q) \in \mathbf{Z} \times \mathbf{N}^*$, on a

$$\left| \alpha - \frac{p}{q} \right| \geqslant \frac{c}{q^d}.$$

b) Montrer que le réel

$$\alpha = \sum_{n=1}^{\infty} 10^{-n!}$$

est transcendant sur $\mathbf{Q}$.

Exercice 1.3. — Soit $\mathbf{C}(z)$ le corps des fractions rationnelles à coefficients complexes. Soit Ω un ouvert connexe de $\mathbf{C}$ et $\mathcal{H}(\Omega)$ le corps des fonctions méromorphes sur Ω. Soit $j : \mathbf{C}(z) \to \mathcal{H}(\Omega)$ l'homomorphisme de corps naturel.

a) Soit $f \in \mathbf{C}(z)$ une fraction rationnelle non constante qui n'a pas de pôle dans Ω. Montrer que $\exp(f) \in \mathcal{H}(\Omega)$ n'appartient pas à $\mathbf{C}(z)$.

b) Si f est un élément de $\mathbf{C}(z) \setminus \mathbf{C}$, montrer que $\exp(f)$ est transcendant sur F. (Raisonner par l'absurde et, notant N le degré de $\exp(f)$ sur $\mathbf{C}(z)$, dériver une relation algébrique $\sum_{n=0}^{N} p_n(z) \exp(nf(z)) = 0$.)

c) Si $f_1, \ldots, f_n$ sont des éléments non constants distincts de $\mathbf{C}(z)$, montrer que $\exp(f_1), \ldots, \exp(f_n)$ sont linéairement indépendants sur $\mathbf{C}(z)$. (Raisonner par récurrence sur n. Considérer une relation de dépendance linéaire $\sum_{i=1}^{n} p_i(z) \exp(f_i(z)) = 0$. Si $p_n \neq 0$, la diviser par $p_n(z)$ puis dériver.)

Exercice 1.4. — **a)** Soit $P = X^n + a_{n-1}X^{n-1} + \cdots + a_0$ un polynôme de degré n à coefficients complexes. Montrer que toute racine $z \in \mathbf{C}$ de P vérifie

$$|z| \leqslant 1 + |a_0| + \cdots + |a_{n-1}|.$$

b) Soit $f : \mathbf{C} \to \mathbf{C}$ une fonction *entière*, c'est-à-dire une fonction holomorphe définie sur tout le plan complexe. Supposons que f soit algébrique sur le corps $\mathbf{C}(z)$ des fonctions rationnelles. Montrer qu'il existe un entier $n \geqslant 0$ et un nombre réel c tel que pour tout $z \in \mathbf{C}$, on ait

$$\big|f(z)\big| \leqslant c(1 + |z|^n).$$

c) (*suite*) Soit $f(z) = \sum_{j=0}^{\infty} c_j z^j$ le développement en série de f en l'origine. Montrer que la fonction g définie par $g(z) = \sum_{j=0}^{\infty} c_{j+n} z^j$ est entière et bornée. Déduire du théorème de Liouville sur les fonctions entières bornées que f est un polynôme.

Exercice 1.5. — Soit P un polynôme unitaire de $\mathbf{Z}[X]$. Si $a \in \mathbf{Q}$ est une racine de P, montrer que $a \in \mathbf{Z}$.

Exercice 1.6. — **a)** Soit $E \subset F$ une extension quadratique. Soit $x \in F \setminus E$ tel que $x^2 \in E$ et soit $a \in E$. Si a est un carré dans F, montrer que ou bien a est un carré dans E, ou bien ax^2 est un carré dans E.

b) Soit $p_1, \ldots, p_n$ des nombres premiers distincts. On considère les deux propriétés :

a$_n$) le corps $\mathbf{Q}(\sqrt{p_1}, \ldots, \sqrt{p_n})$ est de degré 2^n sur $\mathbf{Q}$;

b$_n$) un élément $x \in \mathbf{Q}$ est un carré dans $\mathbf{Q}(\sqrt{p_1}, \ldots, \sqrt{p_n})$ si et seulement s'il existe une partie $I \subset \{1; \ldots; n\}$ telle que $x \prod_{i \in I} p_i$ est un carré dans $\mathbf{Q}$.

Montrer que la conjonction de a$_n$ et de b$_n$ implique a$_{n+1}$, et que la conjonction de a$_n$ et b_{n-1} entraîne b$_n$. En déduire par récurrence sur n qu'elles valent pour tout entier n.

c) Montrer que la famille $\{\sqrt{2}, \sqrt{3}, \sqrt{5}, \sqrt{7}, \ldots\}$ des racines des nombres premiers est libre sur $\mathbf{Q}$.

Exercice 1.7. — Soit p un nombre premier et considérons le polynôme $P = X^n + X + p$, où $n \geqslant 2$.

a) Supposons $p \neq 2$. Montrer que toute racine complexe de P vérifie $|z| > 1$.

b) Toujours pour $p \neq 2$, montrer que P est irréductible dans $\mathbf{Z}[X]$.

c) Supposons maintenant $p = 2$. Si n est pair, montrer que P est irréductible dans $\mathbf{Z}[X]$. Si n est impair, montrer que $X + 1$ divise P et que $P/(X+1)$ est irréductible dans $\mathbf{Z}[X]$.

d) Plus généralement, tout polynôme $P = a_n X^n + \cdots + a_1 X + a_0$ tel que $|a_0|$ soit un nombre premier strictement supérieur à $|a_1| + \cdots + |a_n|$ est irréductible.

Exercice 1.8. — Soit $P = X^n + a_{n-1}X^{n-1} + \cdots + a_0$ un polynôme unitaire dans $\mathbf{Z}[X]$ tel que $a_0 \neq 0$ et

$$|a_{n-1}| > 1 + |a_{n-2}| + \cdots + |a_0|.$$

a) À l'aide du théorème de Rouché en théorie des fonctions d'une variable complexe, montrer que P a exactement une racine complexe de valeur absolue $\geqslant 1$.

b) Montrer que P est irréductible dans $\mathbf{Z}[X]$ (*théorème de Perron*).

Exercice 1.9 (Contenu d'un polynôme). — Si P est un polynôme à coefficients entiers, on note $\mathrm{ct}(P)$ le pgcd de ses coefficients.

a) Soit P et Q deux polynômes de $\mathbf{Z}[X]$. Soit p est un nombre premier qui divise tous les coefficients de PQ, montrer en réduisant modulo p que p divise $\mathrm{ct}(P)$ ou $\mathrm{ct}(Q)$.

b) Montrer que pour tous polynômes P et Q dans $\mathbf{Z}[X]$, on a $\mathrm{ct}(PQ) = \mathrm{ct}(P)\,\mathrm{ct}(Q)$.

c) Soit P un polynôme unitaire de $\mathbf{Z}[X]$ et soit Q un polynôme unitaire de $\mathbf{Q}[X]$ qui divise P dans $\mathbf{Q}[X]$. Montrer que Q est à coefficients entiers.

Exercice 1.10 (Critère d'Eisenstein). — *Soit p un nombre premier et soit $A = a_nX^n + \cdots + a_0$ un polynôme à coefficients entiers tels que a) p divise $a_0, \ldots, a_{n-1}$; b) p ne divise pas a_n ; c) p^2 ne divise pas a_0. Alors, A est irréductible dans $\mathbf{Q}[X]$.*

On raisonne par l'absurde en supposant que A n'est pas irréductible dans $\mathbf{Q}[X]$.

a) Montrer à l'aide du lemme de Gauß qu'il existe deux polynômes non constants B et C dans $\mathbf{Z}[X]$ tels que $A = BC$.

b) On note $B = b_dX^d + \cdots + b_0$. En réduisant modulo p, montrer que p divise $b_0, \ldots, b_{d-1}$.

c) En déduire que p^2 divise a_0, d'où une contradiction.

d) Montrer que le polynôme

$$\frac{X^p - 1}{X - 1} = X^{p-1} + \cdots + 1$$

est irréductible dans $Q[X]$. (Faire le changement de variables $X = Y + 1$.)

Exercice 1.11. — Montrer que l'ensemble des nombres complexes constructibles est un sous-corps de $\mathbf{C}$ qui est stable par l'opération de racine carrée.

Exercice 1.12. — On trouve dans un ouvrage de géométrie de 1833, *Traité du compas (Traité élémentaire de tous les traits servant aux Arts et Métiers et à la construction des Bâtiments)* de Zacharie [**14**], la construction suivante.

> *Construire un eptagone régulier, c'est-à-dire une figure à sept côtés égaux.*
>
> D'un point quelconque tracez une circonférence ; tirez le diamètre AB, divisez ce diamètre en sept parties égales (voyez la figure 45), aux points 1, 2, 3, 4, 5, 6, 7 ; des points A et B, pris pour centre, et avec une ouverture de compas égale au diamètre AB, tracez des arcs qui se couperont en C ; du point d intersection C, tirez la ligne $C5$, que vous prolongerez jusqu'à la circonférence, au point D ; tirez la ligne BD, elle sera le côté de l'eptagone ; portez avec le compas la longueur de la ligne BD sur la circonférence, aux points E, F, G, H, I et vous aurez l'eptagone demandé.

Faire une figure et dire ce qui ne va pas.

Exercice 1.13. — Soit P le polynôme $X^4 - X - 1$.

a) Montrer qu'il a exactement deux racines réelles. On les notes x_1 et x_2. On note x_3 et x_4 les deux racines complexes conjuguées.

b) Montrer qu'il est irréductible sur $\mathbf{Q}$.

c) On cherche à écrire $P(X) = (X^2 + aX + b)(X^2 + cX + d)$. Exprimer b, c et d en fonction de a. En déduire un polynôme Q de degré 3 tel que, a étant fixé, ce système a une solution si et seulement si $Q(a^2) = 0$.

d) Montrer que Q est irréductible sur $\mathbf{Q}$.

e) Montrer que a appartient à $\mathbf{Q}(x_1, x_2)$. En déduire que x_1 et x_2 ne sont pas tous deux constructibles à la règle et au compas.

Exercice 1.14 (Formules de Newton). — **a)** Montrer les formules suivantes, qui relient sommes de Newton et fonctions symétriques élémentaires dans $\mathbf{Z}[X_1, \ldots, X_n]$:

$$\text{si } m \leqslant n, \qquad N_m - N_{m-1}S_1 + \cdots + (-1)^{m-1} N_1 S_{m-1} + (-1)^m m S_m = 0 ;$$
$$\text{si } m > n, \qquad N_m - N_{m-1}S_1 + \cdots + (-1)^n N_{m-n} S_n = 0.$$

b) En déduire que tout polynôme symétrique de $\mathbf{Q}[X_1, \ldots, X_n]$ s'écrit de manière unique comme un polynôme en les sommes de Newton $N_1, \ldots, N_n$. Qu'en est-il dans un corps de caractéristique $p > 0$?

Exercice 1.15. — Soit G un groupe abélien fini, noté multiplicativement. On dit qu'un élément $g \in G$ est d'ordre d si d est le plus petit entier $\geqslant 1$ tel que $g^d = 1$.

a) Soit g et h deux éléments de G d'ordres m et n premiers entre eux. Montrer que gh est d'ordre mn.

b) Plus généralement, si G possède deux éléments d'ordres m et n, montrer qu'il existe un élément de G d'ordre $\mathrm{ppcm}(m, n)$.

c) Montrer qu'il existe un entier $d \geqslant 1$ et un élément $g \in G$ tel que a) g soit d'ordre d ; b) pour tout $h \in G$, $h^d = 1$.

Exercice 1.16. — Soit E un corps et soit G un sous-groupe fini de E^*. Montrer que G est cyclique. (Considérer un couple (d, g) comme dans l'exercice 1.15 et montrer que $G \simeq \mathbf{Z}/d\mathbf{Z}$, g étant un générateur.)

Exercice 1.17. — Soit $j : K \to E$ une extension de corps et soit $x_1, \ldots, x_n$ des éléments de E. Montrer l'équivalence des propriétés suivantes :

a) les x_i sont algébriques sur K ;
b) $K[x_1, \ldots, x_n]$ est de dimension finie sur K ;
c) $K[x_1, \ldots, x_n]$ est un corps ;
d) $K(x_1, \ldots, x_n)$ est de dimension finie sur K.

L'implication (3) $\Rightarrow$ (4) nécessite le théorème 6.8.1 (théorème des zéros de Hilbert).

Exercice 1.18. — On appelle degré, poids et degré partiel d'un monôme $X_1^{i_1} \ldots X_n^{i_n}$ les expressions $i_1 + \cdots + i_n$, $i_1 + 2i_2 + \cdots + n i_n$ et $\max(i_1, \ldots, i_n)$. Le degré, le poids et le degré partiel d'un polynôme P, notés respectivement $\deg(P)$, $w(P)$ et $\delta(P)$, sont par définition le maximum des degrés, poids et degrés partiels de ses monômes non nuls.

a) Calculer le degré, le poids et le degré partiel des polynômes symétriques élémentaires $S_1, \ldots, S_n$.

b) Soit $P \in \mathbf{Z}[X_1, \ldots, X_n]$ un polynôme symétrique. D'après le théorème 1.5.3, il existe un unique polynôme $Q \in \mathbf{Z}[X_1, \ldots, X_n]$ tel que $P = Q(S_1, \ldots, S_n)$. En revenant à la preuve par récurrence du théorème 1.5.3, démontrer que $\deg(P) = w(Q)$ et $\delta(P) = \deg(Q)$.

2

« Mais où sont mes racines ? »

Le point de vue qui prédomine au premier chapitre est celui des nombres et des éventuelles équations algébriques dont ils sont les solutions. Dans celui-ci, nous renversons les rôles et nous intéressons aux équations polynomiales et à leurs racines éventuelles. En généralisant la construction des nombres complexes à partir de celle des nombres réels, nous montrons comment créer les racines d'un polynôme qui n'en a pas assez !

2.1. Anneau des restes

Soit K un corps et P un polynôme non constant de $K[X]$. Notons d son degré. Munissons l'espace vectoriel E des polynômes de degré $< d$ d'une structure d'anneau de la façon suivante :

– l'addition, l'élément 0 sont fournis par la structure d'espace vectoriel ;
– l'élément 1 est le polynôme constant 1 ;
– si A et B sont deux polynômes de E, on définit $A*B$ comme le reste de la division euclidienne du polynôme AB par le polynôme P.

Montrons que cela définit effectivement un anneau. Il est tout d'abord clair que $(E,+,0)$ est un groupe abélien. La loi interne $(E,*,1)$ est commutative, l'élément 1 est neutre : $1*A = A*1$ est le reste de la division euclidienne de A par P, donc est A puisque $\deg A < d = \deg P$. Montrons qu'elle est associative. Pour cela, écrivons les divisions euclidiennes $AB = PQ_1 + A*B$, et $(A*B)C = PQ_2 + (A*B)*C$, de sorte que

$$ABC = (PQ_1 + A*B)C = PQ_1C + PQ_2 + (A*B)*C = P(Q_1C + Q_2) + (A*B)*C,$$

ce qui prouve que $(A*B)*C$ est le reste de la division euclidienne de ABC par P. De même, $A*(B*C)$ est le reste de la division euclidienne de ABC par P, donc est égal à $(A*B)*C$, ce qui prouve l'associativité. La distributivité se montre de même : si l'on a les deux divisions euclidiennes $AB = PQ_1 + A*B$ et $AC = PQ_2 + A*C$, on en déduit

$$A(B+C) = AB + AC = P(Q_1 + Q_2) + A*B + A*C.$$

Ainsi, $A*B+A*C$ est le reste de la division euclidienne de $A(B+C)$ par P, donc est égal à $A*(B+C)$ par définition.

Remarquons que l'application $a \mapsto a$ (l'élément $a \in K$ a pour image le polynôme constant a) est un homomorphisme d'anneaux $K \to E$.

DÉFINITION 2.1.1. — *L'anneau ainsi construit est noté* $K[X]/(P)$.

C'est *l'anneau des restes des divisions euclidiennes* par P. Bien entendu, on ne va pas traîner le symbole $*$ de multiplication trop longtemps : dès qu'on sera habitué à ce nouvel anneau, on notera la multiplication comme d'habitude — c'est-à-dire qu'on ne la notera pas.

PROPOSITION 2.1.2. — *Soit P un polynôme non constant de $K[X]$. Les propriétés suivantes sont équivalentes :*

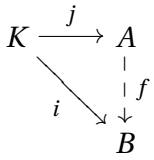
a) *l'anneau $K[X]/(P)$ est un corps ;*
b) *l'anneau $K[X]/(P)$ est intègre ;*
c) *le polynôme P est irréductible dans $K[X]$.*

Démonstration. — L'implication (1) $\Rightarrow$ (2) est évidente. Supposons (2). Si $P = QR$ dans $K[X]$, pour deux polynômes Q et R de degrés $< \deg P$, on a $Q*P = 0$ dans $K[X]/(P)$, ce qui contredit le fait que $K[X]/(P)$ soit intègre ; par suite, P est irréductible dans $K[X]$, d'où (3). Supposons enfin (3). Soit A un polynôme non nul de $K[X]/(P)$ et montrons qu'il a un inverse dans $K[X]/(P)$. Comme P est irréductible et A non multiple de P, ils sont premiers entre eux et la relation de Bézout (corollaire 2.4.2) fournit deux polynômes U et V dans $K[X]$ tels que $UA+VP = 1$. Si $U = PQ+U_1$ est la division euclidienne de U par P, on a alors $U_1 * A = 1$, ce qui prouve que A est inversible. □

Soit P un polynôme irréductible de $K[X]$ et considérons donc l'extension de corps que nous venons de construire $j : K \to K[X]/(P)$. Notons x le polynôme X dans $K[X]/(P)$. Par construction, pour tout polynôme $A \in K[X]$, $A(x)$ est le reste de la division euclidienne du polynôme $A(X)$ par le polynôme P. En particulier, $P(x) = 0$. Autrement dit, *nous venons de créer une extension du corps K dans lequel le polynôme P a une racine.* Le théorème suivant affirme que c'était même la « meilleure » façon de le faire : cet anneau $K[X]/(P)$ vérifie en effet une *propriété universelle.*

THÉORÈME 2.1.3. — *Soit K un corps et P un polynôme de $K[X]$. Notons A l'anneau $K[X]/(P)$ et $j : K \to A$ l'homomorphisme d'anneaux canonique. Soit $i : K \to B$ un homomorphisme d'anneaux et y un élément de B tel que $P(y) = 0$. Alors, il existe un* unique *homomorphisme d'anneaux $f : A \to B$ tel que pour $fj = i$ et $f(x) = y$.*

On représente cela parfois par un diagramme



où la flèche pointillée $f\colon A \to B$ est celle dont l'existence est affirmée par le théorème.

L'idée de la démonstration n'est pas compliquée. Il faut comprendre ce qu'on a fait en construisant $K[X]/(P)$. On est parti de l'anneau $K[X]$ dans lequel on a un élément X supplémentaire, mais qui ne vérifie rien du tout ; en particulier, il n'est pas racine de P. Simplement, on a changé intelligemment les règles de calcul en imposant $P(x) = 0$ *et* toutes les conséquences de cette annulation.

Démonstration. — Si $f(x) = y$, on doit avoir $f(Q(x)) = Q(y)$ pour tout polynôme $Q \in K[X]$, et en particulier pour tout polynôme de degré $< \deg P$. Cela montre qu'il existe au plus un tel homomorphisme f et que s'il existe, il est donné par l'application

$$f\colon K[X]/(P) \to B, \quad Q(X) \mapsto Q(y).$$

(Rappelons qu'un élément de $K[X]/(P)$ *est* un polynôme de degré $< \deg P$.) Définissons ainsi f. Il faut maintenant vérifier que c'est un homomorphisme d'anneaux. C'est évidemment un homomorphisme de K-espaces vectoriels qui vérifie $fj = i$. De plus, si Q et R sont deux polynômes de $K[X]$ de degrés $< \deg P$, écrivons la division euclidienne de QR par P, soit $QR = PS + Q * R$. Alors, puisque $P(y) = 0$ dans B,

$$f(Q*R) = (Q*R)(y) = (Q*R)(y) + P(y)S(y) = (QR)(y) = Q(y)R(y) = f(Q)f(R),$$

ce qui prouve que f est un homomorphisme d'anneaux. □

Pour résumer la construction de ce paragraphe, introduisons une définition.

DÉFINITION 2.1.4. — *Si $i\colon E \to F$ et $j\colon E \to F'$ sont deux extensions de E, un* homomorphisme d'extensions *de F dans F' est un homomorphisme de corps $f\colon F \to F'$ tel que $fi = j$.*

Un *isomorphisme d'extensions* est un homomorphisme bijectif.

THÉORÈME 2.1.5. — *Soit K un corps et P un polynôme irréductible à coefficients dans K. Il existe une extension finie de corps $K \to K_1$, une racine x de P dans K_1 telle que*

a) *$K_1 = K[x]$;*

b) *Si $K \to L$ est une extension de corps, l'ensemble des homomorphismes d'extensions de K_1 dans L est en bijection avec l'ensemble des racines de P dans L, la bijection étant donnée par $f \mapsto f(x)$.*

2.2. Extensions de décomposition

DÉFINITION 2.2.1. — *Soit K un corps et P un polynôme non constant de $K[X]$. Une* extension de décomposition *de P est une extension de corps $j\colon K \to E$ telle que :*

a) Dans E, P soit un produit de facteurs de degré 1 : si d est le degré de P et c son coefficient dominant, il existe des x_i dans E tels que $P = c\prod_{i=1}^{d}(X - x_i)$;

b) E soit le corps engendré par les x_i : $E = K(x_1, \dots, x_d)$.

Autrement dit, une extension de décomposition d'un polynôme irréductible P est une extension qui contient toutes « les » racines de P (c'est la condition a) et qui est « minimale » (c'est la condition b).

THÉORÈME 2.2.2. — *Soit K un corps et P un polynôme non constant de $K[X]$.*

a) Il existe une extension de décomposition de P ;

b) Deux telles extensions sont isomorphes : si $j\colon K \to E$ et $j'\colon K \to E'$ sont deux extensions de décomposition de P, il existe un isomorphisme de corps $f\colon E \to E'$ tel que $fj = j'$.

Démonstration. — Commençons par une remarque très simple : soit $K \to E$ une extension de décomposition de P et soit α une des racines de P dans E. On peut ainsi écrire $P = (X - \alpha)Q$ où Q est un polynôme à coefficients dans $K[\alpha]$. Alors, E est une extension de décomposition du polynôme Q sur $K[\alpha]$. Cette remarque ouvre la voie à la démonstration : réciproquement, si on sait construire $K[\alpha]$, on obtiendra une extension de décomposition E par récurrence. Et justement, on sait construire $K[\alpha]$: c'est le résultat de la section précédente.

On démontre a) et b) par récurrence sur le degré de P. Lorsque $\deg P = 1$, il suffit de poser $E = K$. Soit $Q \in K[X]$ un facteur irréductible de P. D'après le théorème 2.1.5, il existe une extension $K \to K_1$ et un élément $x_1 \in K_1$ tel que a) $Q(x_1) = 0$; b) $K_1 = K[x_1]$. Soit alors P_1 le quotient de P par $X - x_1$ dans $K_1[X]$. Par récurrence, P_1 admet une extension de décomposition sur K_1, soit $K_1 \to E$. La composée de ces extensions $K \to E$ est une extension de corps dans laquelle P est produit de facteurs de degré 1. De plus, si $x_2, \dots, x_d$ sont les racines de P_1 dans E (on a noté $d = \deg P$), on a

$$E = K_1[x_2, \dots, x_d] = K[x_1][x_2, \dots, x_d] = K[x_1, \dots, x_d]$$

si bien que E est engendré par les x_i sur K. C'est donc une extension de décomposition de P sur K.

Soit $K \to E'$ une autre extension de décomposition de P et construisons un isomorphisme d'extensions de E dans E'. Par hypothèse, le facteur irréductible Q de P choisi dans la construction de E a une racine x_1' dans E'. Il existe ainsi d'après le théorème 2.1.5 un homomorphisme d'extensions f_1 de K_1 dans le sous-corps $K_1' = K[x_1']$ de E'. Comme il est surjectif, c'est même un isomorphisme et par cet isomorphisme,

le polynôme P_1 est envoyé sur le polynôme $P_1' = P/(X - x_1')$. Par récurrence, il existe un isomorphisme $f : E \to E'$ qui prolonge l'isomorphisme $f_1 : K_1 \to K_1'$. □

2.3. Corps algébriquement clos ; clôture algébrique

DÉFINITION 2.3.1. — *On dit qu'un corps K est* algébriquement clos *si tout polynôme non constant de $K[X]$ a une racine dans K.*

Par récurrence sur le degré, il revient au même de demander que *tout polynôme soit scindé dans K*. Les constructions de ce chapitre montrent aussi qu'un corps est algébriquement clos si et seulement s'*il n'a pas d'extension algébrique non triviale* (c'est-à-dire : si $j : K \to E$ est une extension algébrique, j est un isomorphisme). Un sens est clair : si K est algébriquement clos et si $j : K \to E$ est une extension algébrique, soit x un élément de E, soit P son polynôme minimal. Par hypothèse, P est scindé dans K : il existe des éléments $x_1, \dots, x_n$ de K tels que $P = (X - x_1) \dots (X - x_n)$. Puisque $P(x) = 0$, x est l'un des x_i (c'est-à-dire en fait l'un des $j(x_i)$). Ainsi, j est surjectif et donc un isomorphisme. Dans l'autre sens, soit P un polynôme non constant de $K[X]$ et soit Q un facteur irréductible de P. On a montré que l'anneau de restes $K[X]/(Q)$ est une extension algébrique de K de degré $\deg Q$. Si K n'a pas d'extension algébrique non triviale, cela implique $\deg Q = 1$, si bien que Q a une racine dans K, et donc P aussi.

DÉFINITION 2.3.2. — *Une* clôture algébrique *d'un corps K est une extension algébrique $j : K \to \Omega$ où Ω est un corps algébriquement clos.*

THÉORÈME 2.3.3 (Steinitz, 1910). — *Tout corps admet une clôture algébrique ; deux clôtures algébriques sont isomorphes.*

Il y a dans la nature deux types de clôtures algébriques : celles qu'on peut voir, comme celle du corps des nombres réels (le corps des nombres complexes) et celles qui sont construites par un procédé transfini comme dans la démonstration du théorème d'existence d'une clôture algébrique.

THÉORÈME 2.3.4. — *Le corps $\mathbf{C}$ des nombres complexes est algébriquement clos.*

Contrairement aux apparences, c'est un théorème d'analyse. Nous en donnons trois démonstrations. La première est courte et franchement analytique. La seconde est d'apparence algébrique mais l'analyse est cachée dans le théorème des valeurs intermédiaires. La troisième est topologique.

Démonstration (première). — Soit $P \in \mathbf{C}[X]$ un polynôme non constant. Supposons qu'il n'a pas de racine dans $\mathbf{C}$. Écrivons $P = a_n X^n + \dots + a_0$, donc $a_n \neq 0$ et $n \geqslant 1$.

Alors, si $z \in \mathbf{C}$ est de module > 1, on a

$$\begin{aligned} |P(z)| &\geqslant |a_n|\,|z|^n - (|a_0| + \cdots + |a_{n-1}|)\,|z|^{n-1} \\ &\geqslant \left|z^n\right| \left(|a_n| - \frac{1}{|z|}(|a_0| + \cdots + |a_{n-1}|) \right). \end{aligned}$$

En particulier, $|P(z)|$ tend vers $+\infty$ quand $|z|$ tend vers $+\infty$. Il en résulte que la fonction $1/|P|$ est holomorphe sur $\mathbf{C}$ (car P ne s'annule pas) et bornée, ce qui implique qu'elle est constante ; contradiction. □

Démonstration (deuxième). — Soit $P \in \mathbf{C}[X]$ un polynôme non constant. Le polynôme $Q(X) = P(X)\overline{P}(X)$ est à coefficients réels. Si nous démontrons qu'il a une racine complexe z, alors ou bien $P(z) = 0$, ou bien $P(\overline{z}) = \overline{\overline{P}(z)} = 0$ et P a une racine complexe. Il suffit donc de démontrer que tout polynôme non constant $P \in \mathbf{R}[X]$ a une racine complexe, ce que nous allons faire par récurrence sur la plus grande puissance de 2, $v_2(P)$, qui divise le degré de P.

Si cette puissance est 0, c'est-à-dire si $\deg P$ est impair, les limites de $P(x)$ lorsque $x \to \pm\infty$ sont $+\infty$ et $-\infty$ (laquelle précisément dépend du signe du coefficient dominant de P). D'après le théorème des valeurs intermédiaires, P a une racine réelle.

Supposons le résultat établi pour les polynômes P tels que $v_2(P) < n$ et soit P un polynôme de $\mathbf{R}[X]$ vérifiant $v_2(P) = n$. Soit Ω une extension de $\mathbf{C}$ dans lequel P est scindé et notons $(\xi_i)_{1 \leqslant i \leqslant \deg P}$ ses racines. Soit c un réel. Posons, si $1 \leqslant i < j < \deg P$, $z_{i,j;c} = \xi_i + \xi_j + c\xi_i\xi_j$ et considérons le polynôme unitaire $Q \in \Omega[X]$ dont les racines sont les $z_{i,j;c}$. Tout d'abord, $\deg Q = \deg P(\deg P - 1)/2$, donc $v_2(Q) = v_2(P) - 1$. De plus, Q est à *coefficients réels*. En effet, ces coefficients sont donnés par des polynômes à coefficients réels en les ξ_i, polynômes manifestement invariants par toute permutation des variables. D'après le théorème sur les polynômes symétriques, les coefficients de Q s'expriment comme des polynômes à coefficients réels en les polynômes symétriques élémentaires de ξ_i, c'est-à-dire en les coefficients de P. Ainsi, les coefficients de Q sont réels. Par récurrence, Q a au moins une racine $z_{i,j}$ dans $\mathbf{C}$.

Ceci est vrai pour toute valeur de c. Comme $\mathbf{R}$ est infini, il existe au moins un couple (i, j) et deux réels $c \neq c'$ tels que $\xi_i + \xi_j + c\xi_i\xi_j$ et $\xi_i + \xi_j + c'\xi_i\xi_j$ soient tous deux des nombres complexes, d'où on déduit que $a = \xi_i + \xi_j$ et $b = \xi_i\xi_j$ appartiennent à $\mathbf{C}$. Ils sont alors racines du polynôme $R = X^2 - aX + b$, dont le discriminant $\Delta = a^2 - 4b$ est un nombre complexe. Il nous suffit de montrer que Δ est un carré dans $\mathbf{C}$ pour en déduire que les deux racines de R, à savoir ξ_i et ξ_j, sont des nombres complexes.

Écrivons $\Delta = p + \mathrm{i}q$. L'équation $(x + \mathrm{i}y)^2 = \Delta$ équivaut aux équations

$$x^2 - y^2 = p \quad \text{et} \quad 2xy = q,$$

d'où $(x^2+y^2)^2 = p^2+q^2$ et $x^2+y^2 = \sqrt{p^2+q^2}$. On en déduit pour x^2 et y^2 les valeurs (positives) suivantes :

$$x^2 = \frac{1}{2}\big(p+\sqrt{p^2+q^2}\big) \quad \text{et} \quad y^2 = \frac{1}{2}\big(-p+\sqrt{p^2+q^2}\big),$$

d'où les valeurs de x et y en prenant garde au signe de q.

Cela montre que ξ_i et ξ_j sont des nombres complexes et que le polynôme initial P a une racine dans $\mathbf{C}$.

Par récurrence, le théorème est démontré. □

Démonstration (troisième). — Si $z \in \mathbf{C}$, on notera $\nu(z)$ le cardinal de l'ensemble fini $P^{-1}(z)$. Le but est de montrer que $\nu(0) > 0$ et on va en fait montrer que $\nu(z) > 0$ pour tout $z \in \mathbf{C}$.

Soit $\Delta \subset \mathbf{C}$ l'ensemble des $z \in \mathbf{C}$ tels que $P'(z) = 0$, $U = \complement\Delta$ et $V = \complement P(\Delta)$. Les ensembles U et V sont les complémentaires d'ensembles finis de $\mathbf{C}$ donc sont ouverts et connexes.

Si $u = x + \mathrm{i}y$ et $P(u) = A(x,y) + \mathrm{i}B(x,y)$, on montre facilement (à partir des relations de Cauchy) que

$$\big|P'(u)\big|^2 = \det\begin{pmatrix} \partial A/\partial x & \partial B/\partial x \\ \partial A/\partial y & \partial B/\partial y \end{pmatrix}.$$

D'après le théorème des fonctions implicites, si $P'(u) \neq 0$, P définit un difféomorphisme d'un voisinage de u sur un voisinage de $P(u)$.

Soit en particulier $z \in V$. Pour tout $u \in P^{-1}(z)$, on a $P'(u) \neq 0$. Cela implique qu'il existe un voisinage Ω de z tel que pour tout $w \in \Omega$, $\nu(w) \geqslant \nu(z)$. En particulier, l'ensemble V^+ des $z \in V$ tels que $\nu(z) > 0$ est *ouvert* dans V.

Montrons qu'il est aussi fermé : soit (z_j) une suite de points de V tels que $\nu(z_j) > 0$ et qui converge vers $z \in V$. Choisissons pour tout j un élément $u_j \in \mathbf{C}$ tel que $z_j = P(u_j)$. Comme la suite (z_j) est bornée et comme $|P(u)|$ tend vers $+\infty$ lorsque $|u| \to +\infty$, la suite (u_j) est bornée. Elle possède donc une valeur d'adhérence $u \in \mathbf{C}$. Comme P définit une fonction continue, $P(u)$ est valeur d'adhérence de la suite $(P(u_j))$: on a nécessairement $P(u) = z$ et $\nu(z) > 0$. Ainsi, V^+ est fermé dans V.

Puisque V est connexe et que V^+ en est un ouvert fermé non vide, $V^+ = V$. Autrement dit, $\nu(z) > 0$ pour tout $z \in V$.

Si $z \notin V$, il existe par définition $u \in \Delta$ tel que $P(u) = 0$ et $\nu(z) > 0$. Finalement, $\nu(z) > 0$ pour tout $z \in \mathbf{C}$. □

À partir d'un corps algébriquement clos, on fabrique facilement la clôture algébrique de n'importe lequel de ses sous-corps.

PROPOSITION 2.3.5. — *Soit Ω un corps algébriquement clos et soit K un sous-corps de Ω. Soit $\overline{K}$ l'ensemble des éléments de Ω qui sont algébriques sur K. Alors, $K \subset \overline{K}$ est une clôture algébrique de K.*

Par exemple, l'ensemble des nombres algébriques dans $\mathbf{C}$ est une clôture algébrique de $\mathbf{Q}$.

Démonstration. — a) Par construction, tout élément de $\overline{K}$ est algébrique sur K. L'extension $K \subset \overline{K}$ est donc algébrique.

b) Soit $P \in \overline{K}[X]$ un polynôme non constant. Montrons qu'il a une racine dans $\overline{K}$. Comme $\overline{K} \subset \Omega$ et comme Ω est algébriquement clos, P a une racine x dans Ω. L'élément x est algébrique sur $\overline{K}$ et puisque $\overline{K}$ est algébrique sur K, x est algébrique sur K (théorème 1.3.16). Ainsi, $x \in \overline{K}$ et P a une racine dans $\overline{K}$, ainsi qu'il fallait démontrer. □

La démonstration du théorème de Steinitz n'est absolument pas éclairante et repose sur un argument de « récurrence transfinie » (donc nécessite l'axiome du choix dès que le corps n'est pas dénombrable !) On a vu comment rajouter les racines d'un polynôme. Il faut maintenant faire cela avec chacun, ce qui nécessite un peu d'ordre.

Démonstration du théorème de Steinitz. — Soit K le corps dont on veut construire une clôture algébrique. Nous allons construire une extension algébrique $K \to \Omega$ de K dans laquelle chaque polynôme de $K[X]$ est scindé. Alors, Ω est une clôture algébrique de K. Soit en effet un polynôme $P = X^n + a_{n-1}X^{n-1} + \cdots + a_0$ à coefficients dans Ω, qu'on peut supposer irréductible. Chacun des a_i étant algébrique sur K, le sous-corps $L = K[a_0, \ldots, a_{n-1}] \subset \Omega$ qu'ils engendrent définit une extension finie de K. Nécessairement, P est irréductible dans $L[X]$. Soit ainsi $L \to L[X]/(P)$ une extension algébrique finie dans laquelle le polynôme P a une racine α, de polynôme minimal P. Comme L est algébrique sur K, α est algébrique sur K. Il a ainsi un polynôme minimal $Q \in K[X]$. Comme $Q(\alpha) = 0$, Q est multiple de P dans $L[X]$. Mais par construction, Q est scindé dans Ω. Par suite, P aussi. Ainsi, Ω est bien une extension algébriquement close de K.

La méthode pour construire Ω, consiste à « rajouter » patiemment les racines de chaque polynôme irréductible de $K[X]$. Pour le faire, munissons l'ensemble $\mathcal{E}$ des polynômes irréductibles d'un *bon ordre* $\prec$, c'est-à-dire d'un ordre total tel que toute partie non vide admette un plus petit élément. L'ordre standard sur $\mathbf{N}$ est un bon ordre. L'existence d'un tel ordre sur tout ensemble équivaut à l'axiome du choix, ou au lemme de Zorn. Si K est dénombrable, l'ensemble des polynômes irréductibles est dénombrable et les énumérer fournit un bon ordre. Une fois choisi un tel ordre, le principe de récurrence s'énonce et se démontre (quasiment) de la même façon que pour les récurrences sur $n \in \mathbf{N}$: Soit $(X, \prec)$ un ensemble muni d'un bonne ordre et $\mathcal{P}$ une propriété des éléments de X. Supposons que soit vérifiée l'assertion : « soit $x \in X$, si pour tout $y \in X$, $y \prec x$, $\mathcal{P}(y)$ est vérifiée, alors $\mathcal{P}(x)$ est vérifiée », alors $\mathcal{P}(x)$ est satisfaite pour tout $x \in X$. (Démonstration : sinon, l'ensemble des $x \in X$ tels que $\mathcal{P}(x)$ n'est pas vérifiée admet un plus petit élément x_0. Par définition, pour tout $y \prec x_0$, $\mathcal{P}(y)$ est vraie. D'après l'assertion entre guillemets, $\mathcal{P}(x_0)$ est vraie, ce qui est une contradiction.)

On montre maintenant l'existence d'une famille d'extensions algébriques $j_P \colon K \to \Omega_P$, pour $P \in \mathcal{E}$, dans laquelle P est scindé, et d'homomorphismes $j_P^Q \colon \Omega_Q \to \Omega_P$ si P, Q sont deux polynômes de $\mathcal{E}$ avec $Q \prec P$ de sorte que l'on ait $j_P = j_P^Q \circ j_Q$. (Cela veut en fait dire que Ω_P est une extension non seulement de K mais de tous les Ω_Q qui précèdent.)

Pour établir ceci par récurrence, il faut faire deux constructions si $P \in \mathcal{E}$:

– la première, que je ne veux pas définir formellement, est la *limite inductive* $\Omega_{\prec P}$ de toutes les extensions Ω_Q avec $Q \prec P$. C'est essentiellement la réunion de ces corps : pour calculer dans $\Omega_{\prec P}$, on choisit un Ω_Q où tout est défini et on fait les calculs là. En utilisant les homomorphismes $j_{Q'}^Q$, on voit

que le résultat des calculs est essentiellement indépendant de l'endroit où on les a faits. On dispose alors d'homomorphismes $j_{\prec P}^{Q}\colon \Omega_Q \to \Omega_{\prec P}$.

– la seconde consiste à rajouter au corps $\Omega_{\prec P}$ toutes les racines de P : on définit Ω_P comme une extension de décomposition du polynôme P sur le corps $\Omega_{\prec P}$, d'où un homomorphisme de corps $j_P^{\prec P}\colon \Omega_{\prec P} \to \Omega_P$ qui composé avec les $j_{\prec P}^{Q}$ fournit les homomorphismes $j_P^Q\colon \Omega_Q \to \Omega_P$ cherchés.

Une fois l'existence de ces (Ω_P, j_P^Q) obtenue, on peut alors définir Ω comme la limite inductive des Ω_P.

Pour démontrer que deux clôtures algébriques sont isomorphes, nous utiliserons un théorème du chapitre suivant. Soit $K \to \Omega'$ une clôture algébrique de K. Nous voulons montrer qu'il existe un K-homomorphisme de la clôture algébrique Ω que nous venons de construire dans Ω'. On montre par récurrence qu'il existe pour tout $P \in \mathcal{E}$ un K-homomorphisme $\alpha_P\colon \Omega_P \to \Omega'$ tel que $\alpha_P \circ j_P^Q = \alpha_Q$ pour $Q \prec P$. C'est vrai pour $P = \min \mathcal{E}$ puisqu'alors $\Omega_P = K$. Fixons maintenant $P \in \mathcal{E}$. En combinant tous les homomorphismes $\alpha_Q\colon \Omega_Q \to \Omega'$, pour $Q \prec P$ et $Q \neq P$, ond définit un K-homomorphisme $\alpha_{\prec P}\colon \Omega_{\prec P} \to \Omega'$. Comme le corps Ω_P est une extension de décomposition du polynôme P sur le corps $\Omega_{\prec P}$, il résulte du théorème 3.1.6 que l'homomorphisme $\alpha_{\prec P}$ s'étend en un K-homomorphisme $\alpha_P\colon \Omega_P \to \Omega'$.

Mis bout à bout, les α_P définissent un K-homomorphisme $\alpha\colon \Omega \to \Omega'$. Comme tout homomorphisme de corps, α est injectif. Montrons qu'il est surjectif. Soit x un élément de Ω'. Par définition, x est algébrique sur K. Soit P son polynôme minimal dans $K[X]$. Comme Ω est une clôture algébrique de K, P est scindé dans Ω. Écrivons ainsi $P = \prod_{i=1}^{n} (X - x_i)$ dans $\Omega[X]$. Alors,

$$0 = P(x) = \prod_{i=1}^{n} (x - \alpha(x_i))$$

si bien que x est l'un des $\alpha(x_i)$ et α est surjectif. C'est un isomorphisme, ce qu'il fallait démontrer. □

2.4. Appendice : structure des anneaux de polynômes

Rappelons qu'un *idéal* d'un anneau A est un sous-groupe abélien $I \subset A$ tel que si $a \in A$ et $b \in I$, $ab \in I$. Si a est un élément de A, l'*idéal principal* engendré par a est l'ensemble des ab pour b décrivant A. On le note aA ou (a). On dit inversement que a est un *générateur* de l'idéal (a).

THÉORÈME 2.4.1. — *Si I est un idéal de $K[X]$, il existe un polynôme $P \in K[X]$ tel que $I = (P)$.*

Un anneau intègre dans lequel tout idéal est principal est en général appelé *anneau principal.*

Démonstration. — On refait essentiellement l'argument de la proposition 1.3.9 (qui en est un cas particulier : prendre pour I l'ensemble des $P \in K[X]$ tel que $P(x) = 0$). Si $I = \{0\}$, on pose $P = 0$. Sinon, soit $d \geqslant 0$ le plus petit degré d'un élément non nul de I et soit $P \in I$ un polynôme de degré d. Comme I est un idéal, pour tout $Q \in K[X]$, on a $PQ \in I$, donc $(P) \subset I$. Réciproquement, soit A un élément de I et introduisons la division euclidienne $A = PQ + R$ de A par P. On a $PQ \in I$, si bien que $R = A - PQ$

appartient à I. Par définition, $\deg R < \deg P$. Le choix de P implique $R = 0$, d'où $A = PQ \in (P)$. □

Remarquez qu'un idéal non nul de $K[X]$ a plusieurs générateurs. Cependant, si P et Q sont deux polynômes non nuls qui engendrent le même idéal, il existe $\lambda \in K^*$ tel que $Q = \lambda P$. En particulier, un idéal non nul possède un unique générateur *unitaire*.

COROLLAIRE 2.4.2. — *Soit A et B deux polynômes. L'ensemble I des polynômes de la forme $AP + BQ$, avec P et Q dans $K[X]$, est un idéal de $K[X]$. Si D est un générateur de cet idéal, alors*

a) *il existe U et V tels que $D = AU + BV$;*
b) *D divise A et B ;*
c) *tout polynôme C divisant à la fois A et B divise D.*

Ainsi, D est un *plus grand diviseur commun* de A et B. Il est bien défini à un scalaire près, si bien qu'on conviendra d'appeler pgcd de A et B l'unique générateur de I qui est unitaire. Rappelons qu'on dit que deux polynômes A et B sont *premiers entre eux* si leurs seuls diviseurs communs sont les polynômes constants. D'après ce résultat, cela revient à dire qu'il existe deux polynômes U et V tels que $AU + BV = 1$: c'est le « théorème de Bézout ».

Démonstration. — Comme I est l'ensemble des $AP + BQ$ pour P, Q décrivant $K[X]$ et comme $D \in I$, il existe U et V dans $K[X]$ tels que $D = AU + BV$, d'où a).

Comme $A = A \cdot 1 + B \cdot 0$, $A \in I$ et il existe $P \in K[X]$ tel que $A = PD$. De même, il existe $Q \in K[X]$ tel que $B = QD$. Ainsi, A et B sont tous deux multiples de D, d'où b).

Enfin, si C divise A et B, écrivons $A = CP$ et $B = CQ$ pour deux polynômes P et Q. La relation $D = AU + BV$ entraîne $D = CPU + CQV = C(PU + QV)$, si bien que C divise D. □

De cela, on déduit que le pgcd de deux polynômes ne dépend pas du corps dans lequel on le calcule :

PROPOSITION 2.4.3. — *Soit $K \subset L$ une extension de corps, A et B deux polynômes de $K[X]$. Alors, le pgcd de A et B dans $L[X]$ est égal au pgcd dans $L[X]$.*

Démonstration. — Soit D le pgcd de A et B dans $K[X]$ et E le pgcd de A et B dans $L[X]$. Comme D divise tout autant A et B dans $L[X]$ qu'il les divise dans $K[X]$, D divise E. Pour montrer l'autre divisibilité, considérons U et V dans $K[X]$ tels que $D = AU + BV$. Comme E divise A et B, il divise nécessairement D ! Puisqu'on a pris soin de choisir D et E unitaires, ils sont égaux. □

On déduit aussi de la relation de Bézout le « lemme de Gauss », qui est le point crucial dans la démonstration de la factorialité des anneaux de polynômes.

LEMME 2.4.4 (Lemme de Gauss). — *Soit P un polynôme irréductible de $K[X]$. Soit A et B deux polynômes de $K[X]$ tels que P divise AB. Alors, P divise A ou P divise B.*

Démonstration. — Supposons que P ne divise pas A. Comme P est irréductible, ses seuls diviseurs sont les polynômes constants $\lambda \in K^*$ et les multiples λP pour $\lambda \in K^*$. Parmi ceux-ci seuls les polynômes constants divisent A, si bien que A et P sont premiers entre eux. Par suite, il existe U et V tels que $AU + PV = 1$. Multiplions cette relation par B ; on obtient $ABU + PBV = B$. Comme P divise AB, on peut écrire $AB = PQ$. Alors, $B = P(QU + BV)$ est multiple de P, cqfd. □

THÉORÈME 2.4.5. — *Tout polynôme non nul A de $K[X]$ admet une décomposition en facteurs irréductibles : $A = a\prod_{i=1}^{m} P_i^{n_i}$ où $a \in K^*$, $m \geqslant 0$ et où, pour tout i, P_i est un polynôme irréductible unitaire et n_i un entier $\geqslant 1$.*

De plus, si $A = a'\prod_{j=1}^{m'} Q_j^{n'_j}$ est une autre décomposition, on a $a = a'$, $m = m'$ et il existe une permutation σ de $\{1;\ldots;m\}$ telle que pour tout i, $P_i = Q_{\sigma(i)}$ et $n_i = n'_{\sigma(i)}$.

On dit que l'anneau $K[X]$ est un *anneau factoriel.*

Démonstration. — L'existence d'une telle décomposition se fait par récurrence sur le degré de A. Si A est irréductible, on écrit $A = aP$ avec P irréductible unitaire et a le coefficient dominant de A. Sinon, on peut écrire $A = A_1A_2$ pour deux polynômes A_1 et A_2 de degrés strictement inférieurs à $\deg A$, et on conclut par récurrence.

L'unicité est le point important. On peut encore raisonner par récurrence. En considérant les coefficients dominants, on obtient $a = a'$. Ensuite, comme P_1 est irréductible et divise A, il divise l'un des Q_j, notons le $Q_{\sigma(1)}$. Puisque $Q_{\sigma(1)}$ est irréductible, nécessairement P_1 et $Q_{\sigma(1)}$ sont multiples l'un de l'autre ; comme ils sont unitaires, ils sont égaux. On applique l'hypothèse de récurrence à A/P_1 ce qui permet de conclure. □

Donnons maintenant la définition générale d'un anneau factoriel.

DÉFINITION 2.4.6. — *Soit A un anneau intègre. On dit qu'un élément a dans A est* irréductible *si* a) *a n'est pas inversible ;* b) *pour tous x et y dans A tels que $a = xy$, x ou y est inversible dans A.*

On dit que l'anneau A est factoriel *si*

a) *pour tout élément non nul $a \in A$, il existe un entier $r \geqslant 0$, des éléments irréductibles $p_1, \ldots, p_r$ et un élément inversible u tels que $a = up_1 \ldots p_r$* (existence d'une décomposition en facteurs irréductibles) *;*

b) *si $a = up_1 \ldots p_r$ et $a = vq_1 \ldots q_s$ sont deux décompositions en facteurs irréductibles, alors $r = s$, il existe une permutation σ de $\{1; \ldots; r\}$, des éléments inversibles u_j ($1 \leqslant j \leqslant r$) tels que pour tout j, $q_j = u_j p_{\sigma(j)}$* (« unicité » de la décomposition en facteurs irréductibles).

THÉORÈME 2.4.7 (Gauss). — *Si A est un anneau factoriel, $A[X]$ aussi.*

La démonstration commence par décrire les éléments irréductibles de $A[X]$: outre les éléments irréductibles de A, ce sont les polynômes de $A[X]$ dont les coefficients sont premiers entre eux et qui sont irréductibles en tant que polynômes à coefficients dans le corps des fractions de A. Elle utilise ensuite une variante du lemme de Gauss (lemme 2.4.4). Pour l'énoncer, appelons *contenu* de $A[X]$ le pgcd de ses coefficients. Alors, *si P et Q sont deux polynômes de $A[X]$, le contenu de leur produit PQ est égal au produit des contenus de P et Q.*

COROLLAIRE 2.4.8. — *Les anneaux $\mathbf{Z}[X_1, \ldots, X_n]$ et, si K est un corps, $K[X_1, \ldots, X_n]$, sont factoriels.*

2.5. Appendice : anneaux quotients

Dans ce paragraphe, j'explique comment généraliser la construction de l'anneau des restes faite au paragraphe 2.1.

La situation est la suivante. On se donne un anneau A et un idéal I de A ; le but est de construire un *anneau quotient* qui sera noté A/I et un homomorphisme d'anneau surjectif $\pi : A \to A/I$ de noyau I. Ainsi, deux éléments a et b auront même image dans A/I si et seulement si leur différence $a - b$ appartient à I : on dit alors que a et b sont dans la même *classe modulo I*. (Exercice : vérifier que cela fait bien une relation d'équivalence.) Au §2.1, nous avons traité le cas où $A = K[X]$ et $I = (P)$ est l'idéal engendré par un polynôme $P \in K[X]$. Dans ce cas, la division euclidienne fournit un représentant privilégié de chaque classe modulo I. Lorsque $A = \mathbf{Z}$ et $I = (n)$, on a encore un représentant privilégié, par exemple les entiers de $\{0; \ldots; n-1\}$. Ce sera le cas dans tout *anneau euclidien*, mais pas en général. On ne se laisse pas arrêter par cette difficulté : le choix du représentant n'a strictement aucune importance et on peut choisir un représentant de chaque classe, fixé une fois pour toute. Une manière plus élégante (?) consiste à définir A/I comme *l'ensemble des classes d'équivalences modulo I*. Si $a \in A$,

notons $\overline{a}$ la classe de a dans A/I. L'application $\pi\colon A \to A/I$ est tout simplement définie par $\pi(a) = \overline{a}$. Paradoxalement, plutôt que de choisir un représentant par classe, on manipule ainsi toute la classe.

Dire que π est un homomorphisme d'anneaux revient à dire que l'addition et la multiplication sur A/I sont définies de sorte à être compatibles avec celles de A. Il faut ainsi vérifier que si $\overline{a} = \overline{b}$ et $\overline{c} = \overline{d}$, alors $\overline{a+c} = \overline{b+d}$ et $\overline{ac} = \overline{bd}$. Or, $(b+d)-(a+c) = (b-a)+(c-d)$ et $bd-ac = (b-a)d + a(d-c)$ sont la somme de deux éléments de I donc appartiennent à I. Les autres axiomes se vérifient de la même façon.

Si I est un idéal de A, il est alors intéressant de traduire en termes de l'idéal I les propriétés algébriques que peuvent avoir l'anneau quotient A/I.

PROPOSITION 2.5.1. — a) *L'anneau A/I est nul si et seulement si $A = I$;*

b) *l'anneau A/I est intègre si et seulement si $I \neq A$ et si pour tous x et y dans $A \setminus I$, $xy \notin I$;*

c) *l'anneau A/I est un corps si et seulement si $I \neq A$ et si les seuls idéaux de A contenant I sont I et A.*

Dans le cas b), on dit que I est un *idéal premier* ; dans le cas c), que c'est un *idéal maximal.*

PROPOSITION 2.5.2. — *Soit A un anneau principal qui n'est pas un corps. Ses idéaux premiers sont* a) *l'idéal nul* (0) *;* b) *les idéaux (p) engendrés par un élément irréductible.*

Parmi ceux-ci, seul l'idéal nul n'est pas maximal.

Concernant l'existence d'idéaux maximaux dans un anneau général, on a les théorèmes suivants.

THÉORÈME 2.5.3 (Krull). — *Soit A un anneau. Tout idéal de A distinct de A est contenu dans un idéal maximal.*

Démonstration. — Soit I un idéal de A, $I \neq A$. Soit $\mathcal{F}$ l'ensemble des idéaux J de A tels que $I \subset J$ et $J \neq A$. Munissons $\mathcal{F}$ d'un bon ordre $\prec$ dont I soit l'élément minimal. On définit alors par récurrence une famille croissante d'idéaux de $\mathcal{F}$ de la façon suivante. Si $\mathfrak{a} = I = \min(\mathcal{F})$, on pose $I_\mathfrak{a} = I$. Soit maintenant $\mathfrak{a} \in \mathcal{F}$ et supposons défini l'idéal $I_\mathfrak{a} J$. Soit $\mathfrak{b} = s(\mathfrak{a})$ le successeur de $\mathfrak{a}$ dans $(\mathcal{F}, \prec)$. Si $I_\mathfrak{a} \subset \mathfrak{b}$, on définit $I_\mathfrak{b} = \mathfrak{b}$. Sinon, on pose $I_\mathfrak{b} = I_\mathfrak{a}$. Par récurrence, tous ces idéaux sont distincts de A et contiennent I.

La réunion des idéaux $I_\mathfrak{a}$ est alors un idéal J de A. Montrons que c'est un idéal maximal qui contient I. Tout d'abord, $J \neq A$. Sinon, on aurait $1 \in J = \bigcup I_\mathfrak{a}$ et il existerait $\mathfrak{a} \in \mathcal{F}$ tel que $1 \in I_\mathfrak{a}$, ce qui est absurde. Ensuite, si $\mathfrak{b} \neq A$ est un idéal de A qui contient J, il contient I, donc est dans $\mathcal{F}$. Comme $J = \bigcup I_\mathfrak{a}$ est contenu dans $\mathfrak{b}$, chacun des $I_\mathfrak{a}$ l'est et en particulier $I_\mathfrak{b} \subset \mathfrak{b}$. Par construction, on a alors $I_\mathfrak{b} = \mathfrak{b}$ et $J = \mathfrak{b}$. Cela prouve que J est maximal. □

COROLLAIRE 2.5.4. — *Soit A un anneau. Un élément de A est inversible si et seulement si il n'appartient à aucun idéal maximal de A.*

Démonstration. — Soit $I = (a)$ l'idéal engendré par un élément $a \in A$. Si a est inversible, il existe $b \in A$ tel que $ab = 1$, d'où $1 \in I$. Alors, pour tout $x \in A$, $x = 1x \in I$ donc $I = A$. Ainsi, I n'est contenu dans aucun idéal maximal, donc a n'appartient à aucun idéal maximal. Réciproquement, si a n'est pas inversible, $I \neq A$. Il existe d'après le théorème 2.5.3 un idéal maximal qui contient I. Cet idéal maximal contient a. □

2.6. Appendice : théorème de Puiseux

Le théorème de Puiseux auquel cet appendice est consacré peut être appréhendé de deux manières différentes :

– du point de vue analytique, il montre que les solutions d'une équation polynômiale dont les coefficients sont des fonctions holomorphes (des séries entières) peuvent être *paramétrées* et fournissent des fonctions holomorphes en un paramètre $t^{1/n}$;

– du point de vue algébrique, il décrit explicitement la clôture algébrique du corps des fonctions méromorphes dans un voisinage de 0.

Si $r > 0$, soit $\mathcal{A}(r)$ l'ensemble des fonctions continues sur le disque fermé $\overline{D}(0,r) \subset \mathbf{C}$ dont la restriction au disque ouvert $D(0,r)$ est holomorphe. C'est un anneau ; en vertu du principe des zéros isolés, il est intègre. Si $f \in \mathcal{A}(r)$, posons $\|f\| = \sup_{|z| \leqslant r} |f(z)|$. C'est une norme sur $\mathcal{A}(r)$ qui définit la topologie de la convergence uniforme. Une limite uniforme de fonctions continues est continue, une limite uniforme de fonctions holomorphes est holomorphe. Par suite, cette norme fait de $\mathcal{A}(r)$ un espace de Banach, et même une *algèbre de Banach* car on a l'inégalité $\|fg\| \leqslant \|f\| \, \|g\|$.

Une fonction f dans $\mathcal{A}(r)$ a un développement en série entière

$$f(z) = \sum_{n=0}^{\infty} a_n z^n,$$

qui converge pour $|z| < r$, comme on peut le voir, par exemple, à l'aide des estimées de Cauchy des dérivées des fonctions analytiques. Deux fonctions distinctes ont des développements distincts, ce qui nous permet d'identifier les éléments de $\mathcal{A}(r)$ à leur série entière. Un mot concernant la notation : nous allons manipuler des polynômes à coefficients dans $\mathcal{A}(r)$, c'est-à-dire des polynômes dont les coefficients sont des *fonctions*. Nous noterons X l'indéterminée polynomiale, et z l'argument des fonctions dans $\mathcal{A}(r)$. Par exemple, dans le théorème ci-dessous, l'expression $P(z^e, X)$ est le polynôme de $\mathbf{C}[X]$ obtenu en évaluant en z^e chaque coefficient du polynôme $P \in \mathcal{A}(r)[X]$.

THÉORÈME 2.6.1 (Puiseux). — *Soit P un polynôme unitaire de degré n à coefficients dans $\mathcal{A}(r)$. Il existe un entier $e \geqslant 1$, un réel $\rho \in]0; r^{1/e}]$, un entier $e \geqslant 1$ et des séries $x_1, \dots, x_n \in \mathcal{A}(\rho)$ telles que*

$$P(z^e, X) = \prod_{i=1}^{n} (X - x_i(z)).$$

En particulier, les n racines du polynôme $P(t)$ sont paramétrées sous la forme de séries $x_i(z^{1/e})$ en une puissance fractionnaire de z. Donnons quelques exemples simples qui montrent à la fois la nécessité d'introduire une telle puissance fractionnaire et aussi que le rayon de convergence des solutions peut être inférieur à celui des coefficients de l'équation :

a) les racines de $P = X^2 - 2zX - 1$ sont

$$x_1(z) = z + \sqrt{1+z^2} = 1 + z + \sum_{n=1}^{\infty} \binom{1/2}{n} z^{2n}$$

et

$$x_2(z) = z - \sqrt{1+z^2} = -1 + z + \sum_{n=1}^{\infty} \binom{1/2}{n} (-1)^n z^{2n},$$

deux séries entières qui convergent pour $|z| < 1$.

b) les racines de $P = X^2 - z(1+z)$ sont

$$\pm z^{1/2}\sqrt{1+z} = \pm \sum_{n=0}^{\infty} \binom{1/2}{n} (z^{1/2})^{2n+1},$$

deux séries convergentes pour $|z| < 1$. Dans ce cas, on a $e = 2$.

La démonstration du théorème 2.6.1 se fait par récurrence sur n.

PROPOSITION 2.6.2. — *Soit $P \in \mathcal{A}(r)[X]$ un polynôme unitaire de degré n. On suppose qu'il existe deux polynômes unitaires Q_0 et $R_0 \in \mathbf{C}[X]$ de degrés $< n$, premiers entre eux, tels que $P(0) = Q_0 R_0$. Alors, il existe $\rho \in]0; r]$ et deux polynômes unitaires Q et R à coefficients dans $\mathcal{A}(\rho)$, tels que $Q(0, X) = Q_0(X)$, $R(0, X) = R_0(X)$ et $P = QR$.*

Démonstration. — C'est une application du théorème des fonctions implicites, dans sa version holomorphe. Nous allons cependant la présenter à l'aide du théorème de point fixe de Banach.

Posons $P_0 = P(0)$ et soit $P_1 \in \mathcal{A}(r)[X]$ tel que $P = P_0 + zP_1$. Soit $m = \deg Q_0$, $p = \deg R_0$; on a $m + p = n$. Cherchons Q et R sous la forme $Q = Q_0 + zU$ et $R = R_0 + zV$ avec U de degré $< m$ et V de degré $< p$. L'équation $P = QR$ se récrit ainsi

$$P_1 = UR_0 + VQ_0 + zUV.$$

Si a est un entier, identifions les polynômes de degré $< a$ à $\mathbf{C}^a$ et considérons l'application linéaire $\varphi\colon \mathbf{C}^m \times \mathbf{C}^p \to \mathbf{C}^{m+p}$ définie par $\varphi(U, V) = UR_0 + VQ_0$. Elle est *injective* :

en effet, si $\varphi(U,V)=0$, R_0 divise VQ_0 mais est premier à Q_0, donc divise V. Comme $\deg V < p = \deg Q_0$, cela impose $V=0$. De même $U=0$. Ainsi, φ est un isomorphisme. Son inverse est une application linéaire $\varphi^{-1}\colon \mathbf{C}^{m+p} \to \mathbf{C}^m \times \mathbf{C}^p$.

Identifions de même $\mathcal{A}(r)^a$ aux polynômes de degré $< a$ à coefficients dans $\mathcal{A}(r)$. Alors, par les mêmes formules, l'application φ^{-1} s'étend en un isomorphisme $\Phi^{-1}\colon \mathcal{A}(r)^{m+p} \to \mathcal{A}(r)^m \times \mathcal{A}(r)^p$, inverse de l'application linéaire $\Phi\colon \mathcal{A}(r)^m \times \mathcal{A}(r)^p \to \mathcal{A}(r)^{m+p}$ donnée par $\Phi(U,V) = UR_0 + VQ_0$, U et V désignant des polynômes de $\mathcal{A}(r)[X]$ de degré respectivement $< m$ et $< p$. L'équation $P = QR$ devient alors

$$(U,V) = \Phi^{-1}(P_1 - zUV).$$

Désignons par $T(U,V)$ le second membre de cette équation.

Si a est un entier, munissons $\mathcal{A}(r)^a$ de la norme donnée par $\|(f_1,\dots,f_a)\| = \|f_1\| + \cdots + \|f_a\|$. C'est encore un espace de Banach. Les applications linéaires Φ et Φ^{-1} sont continues, lipschitziennes, pour ces normes : en fait, leurs constantes de Lipschitz sont les mêmes que celles de φ et φ^{-1}, à condition de munir $\mathbf{C}^a$ de la norme $\|(z_1,\dots,z_a)\| = |z_1| + \cdots + |z_a|$. Posons $A = \|\Phi^{-1}\|$.

Pour tous $U \in \mathcal{A}(r)^m$ et $V \in \mathcal{A}(r)^p$, on a $\|UV\| \leqslant \|U\|\,\|V\|$. En effet, si $U = f_0 + f_1X + \cdots + f_{m-1}X^{m-1}$ et $V = g_0 + g_1X + \cdots + g_{p-1}X^{p-1}$,

$$\|UV\| = \sum_{j=0}^{m+p-1} \left\| \sum_{k+\ell=j} f_k g_\ell \right\| \leqslant \sum_{j=0}^{m+p-1} \sum_{k+\ell=j} \|f_k\|\,\|g_\ell\| \leqslant \sum_{k=0}^{m-1} \|f_k\| \sum_{\ell=0}^{p-1} \|g_\ell\| \leqslant \|U\|\,\|V\|.$$

L'application T de $\mathcal{A}(r)^m \times \mathcal{A}(r)^p$ dans lui-même vérifie alors

$$\|T(U,V)\| \leqslant A\|P_1\| + Ar\|U\|\,\|V\|.$$

Ainsi, si $R > A\|P_1\|$ et si $r < r_1 = (R - A\|P_1\|)/AR^2$, la boule B_R définie par $\|U\| + \|V\| \leqslant R$ est stable par T.

De plus, si (U,V) et $(U',V') \in B_R$,

$$\begin{aligned}
\|T(U,V) - T(U',V')\| &= \|\Phi^{-1}(-tUV + tU'V')\| \\
&\leqslant Ar\|UV - U'V'\| \\
&\leqslant Ar\|U(V-V') + V'(U-U')\| \\
&\leqslant ArR\big(\|U-U'\| + \|V-V'\|\big).
\end{aligned}$$

Autrement dit, si $r < r_2 = 1/AR$, T est contractante.

Il reste à remarquer que l'on peut fixer $R > A\|P_1\|$ puis choisir $\rho < \min(r_1, r_2)$. Alors, l'application T de $\mathcal{A}(\rho)^m \times \mathcal{A}(\rho)^p$ dans lui-même laisse stable la boule B_R définie par $\|U\| + \|V\| \leqslant R$ et y définit une application contractante. D'après le théorème du point fixe de Banach, elle y a un unique point fixe, d'où la factorisation $P = QR$ dans l'anneau $\mathcal{A}(\rho)[X]$. □

Cette première étape (proposition 2.6.2) va nous permettre de supposer que $P(0)$ a une unique racine. Supposons en effet que l'on ait une factorisation $P(0) = \prod_j (X - z_j)^{n_j}$, où les z_j sont *distincts*. Cette factorisation s'étend par récurrence en une factorisation $P = \prod_j P_j$, avec $P_j \in \mathcal{A}(\rho)[X]$ et $P_j(0,X) = (X - z_j)^{n_j}$, pour un certain réel $\rho > 0$. Supposons que chaque P_j vérifie le théorème de Puiseux, c'est-à-dire qu'il existe pour tout j un entier $e_j \geqslant 1$ et des fonctions $x_{j,i} \in \mathcal{A}(\rho_j)$, $1 \leqslant i \leqslant n_j$, telles que

$$P_j(z^{e_j}, X) = \prod_{j=1}^{n_j} (X - x_{j,i}(z)).$$

Posons alors $e = \mathrm{ppcm}(e_1, \dots, e_j, \dots)$ et $f = j = e/e_j$, de sorte que

$$P(z^e, X) = \prod_j P_j\big((z^{f_j})^{e_j}, X\big) = \prod_j \prod_{i=1}^{n_j} \big(X - x_{j,i}(z^{f_j})\big),$$

ce qui prouve le théorème de Puiseux pour P, avec $\rho = \min(\rho_j^{1/f_j})$.

On suppose donc que $P(0)$ a une unique racine α. Quitte à remplacer le polynôme $P = X^n + a_1 X^{n-1} + \dots$ par le polynôme $P(X - a_1/n)$, on peut aussi supposer que P n'a pas de terme en X^{n-1}, c'est-à-dire que la somme des racines de $P(z,X)$ est nulle. En particulier, la somme des racines de $P(0,X)$ est nulle, donc $\alpha = 0$ et $P(0,X) = X^n$.

La proposition suivante fait intervenir l'ordre d'annulation en 0 d'un élément de $\mathcal{A}(r)$: si $f(z) = \sum_{n \geqslant 0} a_n z^n$, c'est le plus petit entier n tel que $a_n \neq 0$; c'est aussi la plus grande puissance de z qui divise f. On le note $v(f)$.

PROPOSITION 2.6.3. — *Soit $P = X^n + a_2 X^{n-2} + \dots + a_n$ un polynôme unitaire à coefficients dans $\mathcal{A}(r)$. Soit $\nu = \min_{2 \leqslant j \leqslant n} v(a_j)/j$; écrivons $\nu = m/e$ où m et e sont deux entiers positifs premiers entre eux. Alors, il existe un polynôme unitaire Q, de degré n, à coefficients dans $\mathcal{A}(r^{1/e})$ tel que*

$$z^{mn} Q(z,X) = P(z^e, z^m X).$$

En $z = 0$, on a $Q(0,X) \neq X^n$.

Avant d'établir cette proposition, terminons la démonstration du théorème de Puiseux. Comme $Q(0,X) \neq X^n$ et comme la somme de ses racines est nulle, les racines de $Q(0,X)$ ne sont pas toutes égales. La proposition 2.6.2 permet de factoriser Q sous la forme RS (dans un certain $\mathcal{A}(\rho)$). Par récurrence, il existe un entier $f \geqslant 1$, un réel ρ et des séries $y_j(z) \in \mathcal{A}(\rho)$ telles que

$$Q(z^f, X) = \prod_{j=1}^{n} (X - y_j(z)).$$

Alors,

$$P(z^{ef}, t^m X) = z^{mn} \prod_{j=1}^{n} (X - y_j(z^f))$$

et

$$P(z^{ef}, X) = \prod_{j=1}^{n} (X - z^m y_j(z^f)),$$

si bien que les $x_j = z^m y_j(z^f)$ sont les séries cherchées.

Démonstration de la proposition 2.6.3. — Dans le développement

$$P(z^e, z^m X) = \sum_{j=0}^{n} a_j(z^e) z^{m(n-j)} X^{n-j},$$

le coefficient $a_j(z^e)z^{m(n-j)}$ est une série dont l'ordre d'annulation en 0 est égal à $ev(a_j) + m(n-j) = mn + e(v(a_j) - jv) \geqslant mn$. Il existe ainsi une série $b_j \in \mathcal{A}(r^{1/e})$ telle que $a_j(z^e)z^{m(n-j)} = z^{mn} b_j(z)$. De plus, si j est choisi de sorte que $v(a_j)/j = v$, on a $v(b_j) = 0$, ce qui signifie $b_j(0) \neq 0$. Autrement dit, $Q(0, X) \neq X^n$. □

Exercices

Exercice 2.1. — **a)** Soit $d_1, \ldots, d_r$ des entiers positifs. Montrer que $d_1! \ldots d_r!$ divise $(d_1 + \cdots + d_r)!$.

b) En suivant les étapes de la construction d'une extension de décomposition d'un polynôme de degré d,, montrer que c'est une extension finie et que son degré divise $d!$.

Exercice 2.2. — Soit p un nombre premier, $p \geqslant 3$.

a) Montrer que $\prod_{a \in (\mathbf{Z}/p\mathbf{Z})^*} a = -1$ (*théorème de Wilson*). — Indication : dans le produit, regrouper a et $1/a$ lorsqu'ils sont différents.

b) Si $a \in (\mathbf{Z}/p\mathbf{Z})^*$, notons $S_a = \{a, -a, 1/a, -1/a\}$. Montrer que pour a et b dans $(\mathbf{Z}/p\mathbf{Z})^*$, soit $S_a = S_b$, soit $S_a \cap S_b = \emptyset$.

c) Calculer le cardinal de S_a suivant que $a^2 = \pm 1$ ou non. En déduire que -1 est un carré dans $(\mathbf{Z}/p\mathbf{Z})^*$ si et seulement si $p \equiv 1 \pmod 4$. Pouvez-vous donner une formule pour une racine de carrée de -1, quand elle existe ?

Exercice 2.3. — Un corps algébriquement clos est infini.

Exercice 2.4. — Soit K un corps, p un nombre premier et a un élément de K. Montrer que le polynôme $X^p - a$ est réductible sur K si et seulement s'il a une racine dans K. (Si $X^p - a = P(X)Q(X)$, que peut valoir $P(0)$?)

Exercice 2.5. — Pour $n \in \mathbf{N}^*$, soit $\Phi_n \in \mathbf{C}[X]$ le polynôme unitaire dont les racines sont simples, égales aux racines primitives n-ièmes de l'unité dans $\mathbf{C}$.

a) Montrer que $\prod_{d|n} \Phi_d = X^n - 1$. En déduire par récurrence que pour tout $n \geqslant 1$, $\Phi_n \in \mathbf{Z}[X]$.

Soit ζ une racine primitive n-ième de l'unité et soit $P \in \mathbf{Q}[X]$ son polynôme minimal (unitaire) sur $\mathbf{Q}$.

b) Montrer que P est à coefficients entiers et qu'il divise Φ_n.

c) Soit p un nombre premier ne divisant pas n. Montrer qu'il existe $b \in \mathbf{Z}[\zeta]$ tel que $P(\zeta^p) = pb$. Si $P(\zeta^p) \neq 0$, montrer en dérivant le polynôme $X^n - 1$ qu'il existe $c \in \mathbf{Z}[\zeta]$ tel que $n\zeta^{n-1} = pc$. En déduire une contradiction et donc que $P(\zeta^p) = 0$.

d) Montrer que $P = \Phi_n$, c'est-à-dire que le polynôme Φ_n est irréductible sur $\mathbf{Q}$.

Exercice 2.6. — Soit A l'anneau $\mathbf{Z}[i]$.

a) Montrer que pour tous a et b dans A, $b \neq 0$, il existe q et r dans A tels que $a = bq + r$ et $|r| < |q|$.

b) Montrer que A est principal. En particulier, il est factoriel.

c) Soit p un nombre premier. Montrer que l'on est dans l'un des cas suivants : 1) ou bien p est irréductible dans A ; 2) ou bien il existe a et b dans $\mathbf{N}$ tels que $p = a^2 + b^2$ et $p = (a + ib)(a - ib)$ est une décomposition en facteurs irréductibles dans A.

d) Montrer que les nombres premiers congrus à 3 modulo 4 sont irréductibles dans A. Montrer que 2 ne l'est pas.

e) Soit p un nombre premier. Construire un isomorphisme d'anneaux entre A/pA et l'anneau $(\mathbf{Z}/p\mathbf{Z})[X]/(X^2 + 1)$. En déduire que p est irréductible dans A si et seulement si le polynôme $X^2 + 1$ n'a pas de racine dans le corps $\mathbf{Z}/p\mathbf{Z}$. Montrer que c'est le cas si p est congru à 1 modulo 4.

Exercice 2.7 (Tout entier est somme de quatre carrés). — Soit $\mathbf{H}$ le corps non commutatif des quaternions. C'est $\mathbf{Q}^4$, de base canonique notée $(1, i, j, k)$ avec la multiplication définie par $i^2 = j^2 = k^2 = -1$ et $ij = k$.

a) Si $z = a + bi + cj + dk \in \mathbf{H}$, on pose $\overline{z} = a - bi - cj - dk$ et $N(z) = z\overline{z}$. Montrer que $N(z) = a^2 + b^2 + c^2 + d^2$ et que $N(zz') = N(z)N(z')$. En déduire que l'ensemble des entiers qui sont somme de quatre carrés d'entiers est stable par multiplication.

b) Montrer que l'ensemble A_0 des $x + yi + zj + tk \in \mathbf{H}$ avec x, y, z, $t \in \mathbf{Z}$ est un sous-anneau (non commutatif) de H.

c) Soit $\varepsilon = (1 + i + j + k)/2$. Calculer ε^2. En déduire que l'ensemble A des $a \in \mathbf{H}$ tels que $a \in A_0$ ou $a - \varepsilon \in A_0$ est un sous-anneau de $\mathbf{H}$. Si $z \in A$, montrer que $N(z) \in \mathbf{N}$. Montrer que $z \in A$ est inversible si et seulement si $N(z) = 1$.

d) Montrer que A est un anneau euclidien. En déduire que tout idéal (à gauche) de A est principal (de la forme Az pour $z \in A$).

e) Soit p un nombre premier impair. Montrer qu'il existe des entiers a, b non tous deux multiples de p tels que $a^2 + b^2 + 1 = 0$ modulo p. Soit I l'idéal à gauche de A engendré par p et $1 + ai + bj$. Si $I = Az$, montrer que $N(z) = p$. En déduire que p est somme de quatre carrés

d'entiers. (Si $z \in A_0$, c'est fini. Sinon, montrer qu'il existe $u = \frac{1}{2}(\pm 1 \pm i \pm j \pm k) \in A^*$ et $b \in A_0$ tels que $z = u + 2b$; remarquer que zu^{-1} appartient à A_0.)

f) Montrer que pour tout entier $n \geqslant 0$, il existe des entiers a, b, c, d tels que $n = a^2 + b^2 + c^2 + d^2$.

Exercice 2.8. — Montrer que les seuls idéaux d'un corps sont lui-même et l'idéal nul. Réciproquement, montrer qu'un anneau (non nul) n'ayant que ces deux idéaux est un corps.

Exercice 2.9. — Soit A le sous-anneau $\mathbf{Z}[\sqrt{-5}]$ de $\mathbf{C}$.

a) Montrer que tout élément de A s'écrit de manière unique sous la forme $a + b\sqrt{-5}$ avec a et b dans $\mathbf{Z}$. Montrer que l'application N de A dans $\mathbf{Z}$ qui à $a + b\sqrt{-5}$ associe $a^2 + 5b^2$ vérifie $N(xy) = N(x)N(y)$.

b) Montrer qu'un élément $x \in A$ est inversible si et seulement si $N(x) = \pm 1$.

c) Montrer que les éléments 2, 3, $1 + \sqrt{-5}$ et $1 - \sqrt{-5}$ sont irréductibles dans A.

d) Montrer que A n'est pas factoriel.

Exercice 2.10. — Soit A un anneau.

a) Soit I et J deux idéaux de A. Montrer que l'ensemble $I + J$ formé des sommes $a + b$ avec $a \in I$ et $b \in J$ est un idéal de A.

b) Soit I un idéal de A. Soit R_I l'ensemble des $a \in A$ tels qu'il existe $n \in \mathbf{N}$ de sorte que $a^n \in I$. Montrer que R_I est un idéal de A contenant I. Si $I \neq A$, montrer que $R_I \neq A$.

c) Si $A = \mathbf{Z}$, $I = (12)$, calculer R_I.

Exercice 2.11. — Soit K un corps.

a) Montrer que les deux polynômes X et Y de $K[X, Y]$ sont premiers entre eux.

b) Soit $I = (X, Y)$ l'idéal de $K[X, Y]$ engendré par X et Y. Montrer que tout polynôme $P \in I$ vérifie $P(0, 0) = 0$. En déduire qu'il n'existe pas U et V dans $K[X, Y]$ tels que $UX + VY = 1$.

c) Montrer que l'application $A \to K$, $P \mapsto P(0, 0)$ est un homomorphisme d'anneaux de noyau I. En déduire que I est un idéal maximal de $K[X, Y]$.

Exercice 2.12. — On dit qu'un anneau A est *noethérien* si tout idéal de A est engendré par un nombre fini d'éléments.

a) Si K est un corps, montrer que $K[X]$ est noethérien.

b) Si A est un anneau noethérien et I un idéal de A, montrer que l'anneau quotient A/I est noethérien.

c) Montrer qu'un anneau est noethérien si et seulement si toute suite croissante d'idéaux est stationnaire.

Exercice 2.13 (Théorème de Hilbert). — Soit A un anneau noethérien. On pose $B = A[X]$. Le but de l'exercice est de montrer que B est un anneau noethérien. Soit donc I un idéal de $A[X]$.

Pour tout entier n, soit J_n l'idéal de A engendré par les coefficients dominants des polynômes $P \in I$ qui sont de degré n.

a) Montrer que pour tout n, $J_n \subset J_{n+1}$. En déduire qu'il existe un entier N tel que pour $n \geqslant N$, $J_n = J_N$.

b) Si n est un entier, montrer qu'il existe des polynômes $P_{n,1}, \ldots, P_{n,m_n} \in I$ de degré n dont les coefficients dominants engendrent J_n.

c) Montrer que les polynômes $P_{n,j}$ pour $n \leqslant N$ et $1 \leqslant j \leqslant m_n$ engendrent I. (On pourra procéder par récurrence sur le degré : si I_0 désigne l'idéal de B engendré par ces polynômes, et si P est un polynôme de I de degré n, construire un polynôme P_n de I_0 tel que $P - P_0$ soit de degré $\leqslant n-1$.)

d) Si K est un corps, montrer que $K[X_1, \ldots, X_n]$ est un anneau noethérien. De même, montrer que $\mathbf{Z}[X_1, \ldots, X_n]$ est un anneau noethérien.

Exercice 2.14. — Dans un anneau factoriel, les éléments irréductibles engendrent des idéaux premiers.

3

Théorie de Galois

C'est dans ce chapitre qu'est établie la correspondance de Galois. Découverte en 1832, elle permet de comprendre toutes les sous-extensions d'une extension de décomposition d'un polynôme (séparable) en termes d'un sous-groupe du groupe des permutations des racines de ce polynôme.

Ce chapitre est le cœur de ce cours. Nous verrons plus tard de nombreuses applications de cette bijection. Jointe à l'étude (abstraite) des extensions dont le groupe associé est cyclique, elle fournit en effet la clef du problème de résolubilité par radicaux ainsi que des constructions à la règle et au compas.

3.1. Homomorphismes d'une extension dans une clôture algébrique

Dans ce paragraphe, on étudie la situation suivante : soit $j\colon K \to L$ une extension algébrique finie et soit $i\colon K \to \Omega$ une clôture algébrique de K. Existe-t-il des homomorphismes d'extensions de L dans Ω, c'est-à-dire, des homomorphismes de corps $f\colon L \to \Omega$ tels que $f \circ j = i$. Autrement dit peut-on *étendre* l'homomorphisme i de K à L ? Un tel f sera appelé *K-homomorphisme* de L dans Ω. Nous avons déjà étudié un cas dans le théorème 2.1.5 : lorsque L est de la forme $K[X]/(P)$ pour un polynôme irréductible P.

DÉFINITION 3.1.1. — *On dit qu'une extension $j\colon K \to L$ est monogène s'il existe $x \in L$ tel que $L = K[x]$.*

PROPOSITION 3.1.2 (Corollaire du théorème 2.1.5). — *Soit $j\colon K \to L$ une extension monogène, $x \in L$ tel que $L = K[x]$, P son polynôme minimal. Soit $i\colon K \to \Omega$ une clôture algébrique de K. Alors, l'ensemble des K-homomorphismes de L dans Ω et l'ensemble des racines de P dans Ω sont en bijection par l'application $f \mapsto f(x)$. En particulier, leur nombre est non nul, inférieur ou égal à $[L\colon K]$.*

Remarque 3.1.3. — Remarquons que chacun de ces homomorphismes permet de considérer Ω comme une clôture algébrique de L. Mais ces façons sont toutes différentes, et c'est pour cela que j'ai tenu à présenter systématiquement les extensions

de corps comme des homomorphismes injectifs et non comme l'inclusion d'un sous-corps. Néanmoins, une fois *fixé* un tel homomorphisme, on peut sans dommage remplacer L par son image dans Ω ce qui ramène à la situation peut-être plus rassurante $K \subset L \subset \Omega$.

Nous dirons qu'un polynôme $P \in K[X]$ est *séparable* si ses racines dans une clôture algébrique de K sont simples.

LEMME 3.1.4. — *Soit K un corps. Un polynôme $P \in K[X]$ est séparable si et seulement si P et P' sont premiers entre eux dans $K[X]$.*

Démonstration. — Soit Ω une clôture algébrique de P. Par définition, P est séparable si et seulement si P et P' sont premiers entre eux dans $\Omega[X]$. D'après le corollaire 2.4.3, cela équivaut à ce qu'ils soient premiers entre eux dans $K[X]$. □

Si $K \to L$ est une extension algébrique, on dira enfin qu'un élément $\alpha \in L$ est *séparable* sur K si son polynôme minimal est séparable.

LEMME 3.1.5. — *Soit $K \to L$ une extension algébrique, Ω une clôture algébrique de L. Si $\alpha \in \Omega$ est séparable sur K, il est séparable sur L.*

Rappel : dans la situation du lemme, α est algébrique sur L et l'extension $K \to L$ est algébrique, si bien que α est algébrique sur K (théorème 1.3.16).

Démonstration. — Soit P le polynôme minimal de α sur L et Q son polynôme minimal sur K. Comme $Q(\alpha) = 0$, Q est multiple de P. Puisque α est supposé séparable sur K, Q est à racines simples dans Ω. Il en est donc de même de P. □

THÉORÈME 3.1.6. — *Soit K un corps, $j : K \to L$ une extension finie et $i : K \to \Omega$ une clôture algébrique. Alors, le nombre N de K-homomorphismes distincts de L dans Ω vérifie $1 \leqslant N \leqslant [L : K]$. De plus, on a équivalence des trois propriétés suivantes :*

a) *$N = [L : K]$;*

b) *il existe des éléments $x_1, \ldots, x_n \in L$ qui sont séparables sur K tels que $L = K[x_1, \ldots, x_n]$;*

c) *tout élément de L est séparable sur K.*

Une extension $K \to L$ qui vérifie ces dernières propriétés est dite *séparable*.

Démonstration. — Comme L est une extension finie de K, il existe des éléments $x_1, \ldots, x_n \in L$ tels que $L = K[x_1, \ldots, x_n]$. La démonstration se fait alors par récurrence sur n. Lorsque $n = 1$, L est une extension monogène et la proposition 3.1.2 affirme que N est égal au nombre de racines distinctes dans Ω du polynôme minimal de x_1. Ce polynôme étant de degré $[L : K]$, on en déduit les deux faits :

– l'entier N est compris entre 1 et $[L : K]$;
– il vaut $[L : K]$ si et seulement si x_1 est séparable sur K.

Supposons que $x_1 \notin K$ et posons alors $L_1 = K[x_1]$. Chaque K-homomorphisme de L_1 dans Ω, c'est-à-dire chaque racine du polynôme minimal de x_1, permet de considérer Ω comme une clôture algébrique de L_1. L'extension $L_1 \subset L$ est de degré inférieur à $[L : K]$. Par récurrence, pour chacun d'entre eux, le nombre de L_1-homomorphismes de L dans Ω est compris entre 1 et $[L : L_1]$. Finalement, on a construit ainsi des K-homomorphismes distincts de L dans Ω, en nombre compris entre 1 et $[L : K]$. Réciproquement, tout K-homomorphisme de L dans Ω est obtenu de la sorte, ce qui prouve la première partie du théorème.

La démonstration précédente montre qu'on a l'égalité $N = [L : K]$, si et seulement si x_1 est séparable sur K, x_2 est séparable sur $K[x_1]$, etc. D'après le lemme 3.1.5, si les x_i sont tous séparables sur K, cette condition est vérifiée, donc $N = [L : K]$. Supposons maintenant que $N = [L : K]$ et montrons que tout élément x de L est séparable sur K. Il suffit pour cela d'appliquer l'argument précédent à la famille $(x, x_1, \ldots, x_n)$: si $N = [L : K]$, alors x est séparable sur K. Cela montre que l'extension $K \to L$ est séparable. □

DÉFINITION 3.1.7. — *On dit qu'un corps K est* parfait *si tout polynôme irréductible de $K[X]$ a autant de racines distinctes dans une clôture algébrique que son degré.*

Ainsi, la définition et le théorème 3.1.6 entraînent que les propriétés suivantes sont équivalentes :

a) K est un corps parfait ;
b) tout polynôme irréductible de $K[X]$ est séparable ;
c) tout élément d'une clôture algébrique de K est séparable sur K ;
d) toute extension algébrique de K est séparable ;
e) pour toute extension $K \to L$, le nombre de K-homomorphismes de L dans une extension algébriquement close de K est exactement égal à $[L : K]$.

PROPOSITION 3.1.8. — *Toute extension algébrique d'un corps parfait est un corps parfait.*

Démonstration. — C'est une reformulation du lemme 3.1.5. Soit K un corps parfait, $K \to L$ une extension finie de K. Un élément algébrique sur L est algébrique sur K. Par hypothèse, il est séparable sur K, donc aussi sur L grâce au lemme. □

Nous terminons ce paragraphe par une caractérisation des corps parfaits qui ne fait pas intervenir les extensions.

PROPOSITION 3.1.9. — *Les corps parfaits sont* a) *les corps de caractéristique nulle ;* b) *les corps de caractéristique $p > 0$ dont l'homomorphisme de Frobenius est bijectif.*

En particulier, les corps finis sont parfaits.

Démonstration. — Soit P un polynôme irréductible de $K[X]$. Les racines multiples de P dans une clôture algébrique Ω sont exactement les racines communes de P et de

P', c'est-à-dire les racines de leur pgcd D. Comme P est irréductible, ce pgcd est ou bien 1, ou bien P. S'il est égal à 1, toutes les racines sont simples. S'il est égal à P, toutes les racines sont multiples. Dans ce cas, P divise P' ; mais le degré de P' est au plus égal à $\deg P - 1$. Cela implique $P' = 0$.

En caractéristique nulle, c'est bien sûr impossible : si le coefficient dominant de P est aX^n (avec $n = \deg P$), le coefficient dominant de P' est naX^{n-1} et $na \neq 0$, donc $\deg P' = n - 1$. Les corps de caractéristique nulle sont donc parfaits.

En revanche, si K est de caractéristique $p > 0$, $P' = 0$ signifie que les seuls coefficients non nuls de P sont ceux des termes dont le degré est multiple de p. Ainsi, $P = a_n X^{pn} + a_{n-1} X^{p(n-1)} + \cdots + a_0$ est un polynôme en X^p. Supposons que l'homomorphisme de Frobenius de K est surjectif. Pour tout n, il existe alors $b_n \in K$ tel que $\varphi(b_n) = b_n^p = a_n$. Alors,

$$P = b_n^p X^{pn} + b_{n-1}^p X^{p(n-1)} + \cdots + b_0^p = \left(b_n X^n + \cdots + b_0\right)^p,$$

ce qui contredit l'irréductibilité de P. Un tel corps est donc parfait. Réciproquement, si l'homomorphisme de Frobenius de K n'est pas surjectif, soit $a \in K$ qui n'est pas la puissance p-ième d'un élément de K. Soit P le polynôme $P = X^p - a$. Soit b une racine p-ième de a dans Ω, de sorte que $P = (X - b)^p$ dans $\Omega[X]$: la racine de P est donc de multiplicité p. Si $P = QR$ pour deux polynômes non constants, disons unitaires, Q et R dans $K[X]$, on a nécessairement $Q = (X - b)^m$ et $R = (X - b)^{p-m}$ dans $\Omega[X]$, m étant un entier compris entre 1 et $p - 1$. En développant Q, on voit que $mb \in K$, donc que $b \in K$ puisque m est non nul dans K, contradiction. Par suite, P est irréductible et le corps K n'est pas parfait. □

3.2. Groupe d'automorphismes d'une extension

DÉFINITION 3.2.1. — *Soit $j : K \to L$ une extension de corps. Un* K-automorphisme de L *est un automorphisme de corps qui est un homomorphisme d'extensions.*

L'ensemble des K-automorphismes de L forme un groupe, noté $\mathrm{Aut}(L/K)$. Dans le cas particulier important où K est un sous-corps de L, un K-automorphisme de L n'est rien d'autre qu'un automorphisme de L dont la restriction à K est l'identité.

L'intérêt de cette notion vient de la remarque suivante — évidente mais cruciale : si σ est un K-automorphisme de L et $P \in K[X]$, alors, pour tout $x \in L$, $\sigma(P(x)) = P(\sigma(x))$. Par suite, σ permute les racines de P.

Exemples 3.2.2. — a) Considérons l'extension $\mathbf{R} \subset \mathbf{C}$. Soit σ un $\mathbf{R}$-automorphisme de $\mathbf{C}$. Si $z = a + ib \in \mathbf{C}$, avec a, $b \in \mathbf{R}$,

$$\sigma(z) = \sigma(a + ib) = \sigma(a) + \sigma(ib) = a + \sigma(i)b.$$

Comme

$$\sigma(i)^2 = \sigma(i^2) = \sigma(-1) = -1,$$

on a $\sigma(i) = \pm i$, d'où deux automorphismes : l'identité et la conjugaison complexe.

b) Soit ω le réel $\sqrt[3]{2}$ et considérons l'extension $\mathbf{Q} \subset \mathbf{Q}(\omega)$. Comme tout élément de $\mathbf{Q}(\omega)$ s'écrit $a + b\omega + c\omega^2$, avec $a, b, c \in \mathbf{Q}$, un $\mathbf{Q}$-automorphisme σ de $\mathbf{Q}(\omega)$ est déterminé par l'image de ω. Or,

$$\sigma(\omega)^3 = \sigma(\omega^3) = \sigma(2) = 2,$$

et l'équation $x^3 = 2$ n'a qu'une racine, ω, dans $\mathbf{R}$, donc a fortiori dans $\mathbf{Q}(\omega)$. Par conséquent, $\mathrm{Aut}(\mathbf{Q}(\omega)/\mathbf{Q}) = \{\mathrm{id}\}$.

c) On a $\mathrm{Aut}(\mathbf{R}/\mathbf{Q}) = \{\mathrm{id}\}$.

d) Tout $\mathbf{C}$-automorphisme de $\mathbf{C}(X)$ est de la forme $P \mapsto P((aX+b)/(cX+d))$ pour une matrice $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$ dans $\mathrm{GL}(2, \mathbf{C})$, bien déterminée à multiplication par un scalaire près. Par suite, $\mathrm{Aut}(\mathbf{C}(X)/\mathbf{C}) = \mathrm{PGL}(2, \mathbf{C})$.

Remarque 3.2.3. — Soit $K \to L$ une extension finie et soit $\sigma : L \to L$ un K-homomorphisme. Alors, σ est injectif, comme tout homomorphisme de corps. Par suite, $\sigma(L)$ est un K-espace vectoriel de dimension $[L : K]$, et donc $[\sigma(L) : K] = [L : K]$. Puisque $\sigma(L) \subset L$, on a $\sigma(L) = L$ et σ est surjectif. Cela montre que σ est un K-automorphisme de L.

PROPOSITION 3.2.4. — *Soit $j : K \to L$ une extension finie. Alors,* $\mathrm{Aut}(L/K)$ *est de cardinal au plus égal à* $[L : K]$. *S'il y a égalité, l'extension $K \to L$ est séparable.*

Démonstration. — Soit $i : L \to \Omega$ une clôture algébrique de L. Tout K-automorphisme $\sigma \in \mathrm{Aut}(L/K)$ détermine un K-homomorphisme $i \circ \sigma : L \to \Omega$. D'après le théorème 3.1.6, le nombre de tels homomorphismes est inférieur ou égal à $[L : K]$ et s'il est égal, l'extension est séparable. La proposition en résulte. □

DÉFINITION 3.2.5. — *On dit qu'une extension finie $K \to L$ est* galoisienne *si* $\mathrm{Aut}(L/K)$ *est de cardinal* $[L : K]$. *Le groupe* $\mathrm{Aut}(L/K)$ *est alors appelé* groupe de Galois *de l'extension et est noté* $\mathrm{Gal}(L/K)$.

D'après la proposition 3.2.4, une extension galoisienne est nécessairement séparable.

Énonçons maintenant le *théorème principal* de la théorie de Galois.

THÉORÈME 3.2.6 (Correspondance de Galois). — *Soit $K \subset L$ une extension finie galoisienne de groupe de Galois $G = \mathrm{Gal}(L/K)$.*

a) Pour tout sous-groupe $H \subset G$, l'ensemble $L^H = \{x \in L ; \forall \sigma \in H,\ \sigma(x) = x\}$ est un sous-corps de L contenant K. En outre, $[L^H : K]$ est égal à l'indice $(G : H)$ de H dans G.

b) Pour tout sous-corps E tel que $K \subset E \subset L$, l'extension $E \subset L$ est galoisienne de groupe $\mathrm{Gal}(L/E) = \{\sigma \in \mathrm{Gal}(L/K) ; \forall x \in E,\ \sigma(x) = x\}$.

c) Les applications $H \mapsto L^H$ et $E \mapsto \mathrm{Gal}(L/E)$ sont des bijections décroissantes, réciproques l'une de l'autre, entre l'ensemble des sous-groupes de G et l'ensemble des sous-corps de L contenant K.

La démonstration de ce théorème passe par deux autres énoncés.

PROPOSITION 3.2.7. — *Soit $K \subset L$ une extension finie. Les conditions suivantes sont équivalentes :*

a) l'extension $K \subset L$ est galoisienne ;

b) l'extension $K \to L$ est séparable et tout K-homomorphisme de L dans une clôture algébrique de L a pour image L ;

c) l'extension $K \to L$ est séparable et tout polynôme irréductible de $K[X]$ qui a une racine dans L est scindé dans L ;

d) il existe un polynôme $P \in K[X]$ scindé à racines simples dans L dont $K \subset L$ est une extension de décomposition.

Démonstration. — Fixons dans toute la preuve une clôture algébrique $i : L \to \Omega$ de L.

Supposons *a)*. Tout élément $\sigma \in \mathrm{Gal}(L/K)$ détermine un K-homomorphisme de L dans Ω, à savoir $i \circ \sigma$. Comme le nombre de ces homomorphismes est majoré par $[L : K]$, ils sont tous obtenus ainsi, d'où *b)*.

Réciproquement, si l'extension $K \subset L$ est séparable, les K-homomorphismes de L dans Ω sont au nombre de $[L : K]$. Si *b)* est vérifié, ces homomorphismes sont d'image L, donc définissent des K-automorphismes distincts de L. Par suite, $\mathrm{Aut}(L/K)$ a pour cardinal au moins $[L : K]$ et l'extension $K \subset L$ est galoisienne.

Supposons toujours *b)* et soit P un polynôme irréductible de $K[X]$ qui a une racine ω dans L. Notons $E = K[\omega] \subset L$ le sous-corps de L engendré par cette racine. Pour toute racine α de P, il existe un unique K-homomorphisme de E dans Ω tel que $\omega \mapsto \alpha$. Un tel homomorphisme s'étend alors en un K-homomorphisme $\sigma : L \to \Omega$ tel que $\sigma(\omega) = \alpha$. Par hypothèse, $\sigma(L) = L$. Il en résulte que $\alpha \in L$ et donc que P est scindé dans L.

Supposons *c)* et soit $x_1, \ldots, x_n$ des éléments de L tels que $L = K[x_1, \ldots, x_n]$. Leurs polynômes minimaux $P_i \in K[X]$ sont irréductibles et ont une racine dans L. Ils sont donc scindés dans L et comme $K \to L$ est séparable, leurs racines sont simples dans L. Le polynôme $P = \mathrm{ppcm}(P_1, \ldots, P_n)$ a les mêmes racines que $P_1 \ldots P_n$ mais avec multiplicité 1 et L est une extension de décomposition de P.

Supposons enfin que L est une extension de décomposition d'un tel polynôme P et montrons que l'extension $K \subset L$ est galoisienne. Il suffit de montrer que tout K-homomorphisme de L dans Ω est d'image L. Or, par un K-homomorphisme $\sigma : L \to \Omega$, les racines $x_1, \ldots, x_n$ de P ont pour image des racines de P. Par suite, ces images sont dans L. Comme $L = K[x_1, \ldots, x_n]$, $\sigma(L) \subset L$. Comme σ est injectif, $[\sigma(L) : K] = [L : K]$ et $K = L$. □

PROPOSITION 3.2.8 (Lemme d'Artin). — *Soit L un corps et soit G un groupe fini d'automorphismes de L. Soit $K = L^G$ l'ensemble des $x \in L$ tels que $\sigma(x) = x$ pour tout $\sigma \in G$. Alors, K est un sous-corps de L tel que $[L:K] = \operatorname{card} G$. En particulier, l'extension $K \subset L$ est galoisienne de groupe G.*

Démonstration. — Vérifions rapidement que K est un sous-corps de L. Si $\sigma \in G$, $\sigma(0) = 0$ et $\sigma(1) = 1$ donc 0 et 1 appartiennent à K. Si x et $y \in K$, on a, pour tout $\sigma \in G$, les relations $\sigma(x+y) = \sigma(x) + \sigma(y) = x + y$, $\sigma(-x) = -\sigma(x) = -x$, $\sigma(1/x) = \sigma(1)/\sigma(x) = 1/x$ (si $x \neq 0$) et $\sigma(xy) = \sigma(x)\sigma(y) = xy$. Par suite, $x+y$, xy, $-x$, $1/x$ (pour $x \neq 0$) appartiennent à K, ce qui montre que K est un sous-corps de L.

Emil Artin (1898–1962)

Supposons que $[L:K] > \operatorname{card} G$. Posons alors $n = 1 + \operatorname{card} G$ et soit $a_1, \ldots, a_n$ des élements de L linéairement indépendants sur K. Puisque $n > \operatorname{card} G$, le système de $\operatorname{card} G$ équations à n inconnues

$$\sum_{j=1}^{n} \sigma(a_i) x_i = 0, \qquad \sigma \in G$$

possède des solutions non triviales $(x_1, \ldots, x_n)$. Choisissons en une dont le nombre de coefficients non nuls m est minimal. Quitte à renuméroter, on peut supposer qu'il s'agit de $x_1, \ldots, x_m$. Par linéarité, on peut aussi supposer $x_m = 1$, d'où les relations

$$\sum_{j=1}^{m-1} \sigma(a_i) x_i + \sigma(a_m) = 0, \qquad \sigma \in G.$$

Soit $\tau \in G$ et appliquons τ à la relation précédente pour $\tau^{-1} \circ \sigma$. On obtient

$$\sum_{j=1}^{m-1} \sigma(a_i) \tau(x_i) + \sigma(a_m) = 0, \qquad \sigma \in G,$$

d'où, si l'on soustrait la relation pour σ,

$$\sum_{j=1}^{m-1} \sigma(a_i)(\tau(x_i) - x_i) = 0, \qquad \sigma \in G.$$

Par minimalité de m, il en résulte que $\tau(x_i) = x_i$ pour tout i et tout τ. Par suite, les x_i appartiennent à K et la relation $\sum_{j=1}^{m} a_j x_j = 0$ implique que les a_i sont linéairement dépendants sur K, ce qui est absurde.

Ainsi, $[L:K] \leqslant \operatorname{card} G$ et en particulier, l'extension $K \subset L$ est finie. Les éléments de G s'identifient manifestement à des K-automorphismes de L. D'après la proposition 3.2.4, on a $\operatorname{card} G \leqslant [L:K]$, d'où finalement l'égalité. □

Nous pouvons maintenant démontrer le théorème fondamental de la théorie de Galois. Soit $K \subset L$ une extension finie galoisienne de groupe de Galois G.

Soit H un sous-groupe de G. D'après la proposition 3.2.8, l'extension $L^H \subset L$ est galoisienne de groupe de Galois H. Il est évident que $K \subset L^H$. De plus,

$$[L^H : K] = \frac{[L:K]}{[L:L^H]} = \frac{\operatorname{card} G}{\operatorname{card} H} = (G:H).$$

Inversement, soit E un sous-corps de L contenant K. Puisque $K \subset L$ est galoisienne, c'est une extension de décomposition d'un polynôme $P \in K[X]$ scindé à racines simples dans L. Par suite, $E \subset L$ est aussi une extension de décomposition de ce polynôme P et est du même coup galoisienne. Son groupe de Galois est évidemment un sous-groupe de G, nécessairement égal à

$$H = \{\sigma \in G;\ \forall x \in E,\ \sigma(x) = x\}.$$

(Par définition, un élément de $\mathrm{Gal}(L/E)$ appartient à H ; réciproquement, un élément de H définit un E-automorphisme de L, donc un élément de $\mathrm{Gal}(L/E)$.) En particulier, $\operatorname{card} H = [L:E]$ et

$$(G:H) = \frac{\operatorname{card} G}{\operatorname{card} H} = \frac{[L:K]}{L:E]} = [E:K].$$

Par la première partie du théorème, l'extension $L^H \subset L$ est galoisienne de groupe H. Mais L^H contient E. Comme ces deux corps ont même degré sur K, à savoir $(G:H)$, ils sont égaux. Il en résulte que $H \mapsto L^H$ et $E \mapsto \mathrm{Gal}(L/E)$ sont des bijections réciproques l'une de l'autre.

Le mot « décroissantes » signifie juste les deux faits évidents suivants : *a*) si $H \subset H'$, alors $L^{H'} \subset L^H$ et *b*) si $E \subset E'$, alors $\mathrm{Gal}(L/E')$ est un sous-groupe de $\mathrm{Gal}(L/E)$.

PROPOSITION 3.2.9. — *Soit $K \subset L$ une extension finie galoisienne de groupe $G = \mathrm{Gal}(L/K)$. Soit H un sous-groupe de G.*

a) *Si $\sigma \in \mathrm{Gal}(L/K)$, on a $\sigma(L^H) = L^{\sigma H \sigma^{-1}}$.*

Soit alors $N_G(H) = \{\sigma \in \mathrm{Gal}(L/K);\ \sigma H \sigma^{-1} = H\}$ le normalisateur de H dans $\mathrm{Gal}(L/K)$. Ses éléments sont les $\sigma \in \mathrm{Gal}(L/K)$ tels que $\sigma(L^H) \subset L^H$.

b) *En restreignant à L^H un élément de $N_G(H)$, on définit un morphisme de groupe surjectif $N_G(H) \to \mathrm{Aut}(L^H/K)$ dont le noyau est H. En particulier, l'extension $K \subset L^H$ est galoisienne si et seulement si H est un sous-groupe distingué de G. On a alors $\mathrm{Gal}(L^H/K) = G/H$*

Démonstration. — *a*) Un élément $x \in L$ appartient à L^H si et seulement si $h(x) = x$ pour tout $h \in H$. Par suite, $y = \sigma(x)$ appartient à $\sigma(L^H)$ si et seulement si $h\sigma^{-1}(y) = \sigma^{-1}(y)$ pour tout $h \in H$, c'est-à-dire $\sigma h \sigma^{-1}(y) = y$ pour tout $h \in H$, soit encore $y \in L^{\sigma H \sigma^{-1}}$.

b) Comme l'extension $K \subset L$ est galoisienne, tout K-homomorphisme $L^H \to L^H$ est la restriction à L^H d'un K-homomorphisme $L \to L$, c'est-à-dire d'un élément $\sigma \in$

$\mathrm{Gal}(L/K)$. Un tel σ vérifie $\sigma(L^H) = L^H$ si et seulement si $\sigma H \sigma^{-1} = H$, d'où un homomorphisme surjectif $N_G(H) \to \mathrm{Aut}(L^H/K)$. Le noyau de cet homomorphisme s'identifie aux $\sigma \in N_G(H)$ tels que $\sigma(x) = x$ pour tout $x \in L^H$, c'est-à-dire à H. On a donc construit un isomorphisme $N_G(H)/H \simeq \mathrm{Aut}(L^H/K)$.

En particulier, l'extension $K \subset L^H$ est galoisienne si et seulement si $[L^H : K] = (N_G(H) : H)$, c'est-à-dire, puisque $[L^H : K] = (G : H)$ si et seulement si $G = N_G(H)$, c'est-à-dire H distingué dans G. □

Enfin, si $K \subset L$ n'est pas une extension galoisienne, la théorie de Galois permet tout de même de dire quelque chose des extensions intermédiaires, grâce à la proposition suivante, corollaire de la proposition 3.2.7.

PROPOSITION 3.2.10. — *Soit K un corps, Ω une clôture algébrique de K et soit L une extension finie séparable de K contenue dans Ω. Il existe alors une plus petite extension $L \subset L^{\mathrm{g}}$ contenue dans Ω telle que l'extension $K \subset L^{\mathrm{g}}$ soit galoisienne.*

Démonstration. — Considérons des éléments x_i de L tels que $L = K[x_1, \ldots, x_n]$; ils sont donc séparables et pour tout i, le polynôme minimal P_i de x_i est séparable. Il suffit de définir L^{g} comme le sous-corps de Ω engendré par les racines des P_i. C'est une extension de décomposition du polynôme séparable $\mathrm{ppcm}(P_1, \ldots, P_n)$, donc c'est une extension galoisienne. Par ailleurs, toute extension finie E de L qui est galoisienne comme extension de K contient les racines de P_i, si bien que $E \subset L^{\mathrm{g}}$. La proposition est ainsi démontrée. □

D'après le théorème de Galois, tout sous-corps E de L^{g} contenant K correspond à un sous-groupe de $\mathrm{Gal}(L^{\mathrm{g}}/K)$, à savoir $\mathrm{Gal}(L^{\mathrm{g}}/E)$. En particulier, L correspond au sous-groupe $\mathrm{Gal}(L^{\mathrm{g}}/L)$. Si E est contenu dans L, $\mathrm{Gal}(L^{\mathrm{g}}/E)$ contient $\mathrm{Gal}(L^{\mathrm{g}}/L)$. Ainsi, l'ensemble des extensions $K \subset E \subset L$ est en bijection avec l'ensemble des sous-groupes de $\mathrm{Gal}(L^{\mathrm{g}}/K)$ contenant $\mathrm{Gal}(L^{\mathrm{g}}/L)$. Puisqu'un groupe fini n'a qu'un nombre fini de sous-groupes, il s'ensuit que si $K \subset L$ est une extension finie séparable, il n'y a qu'un nombre fini de corps E tels que $K \subset E \subset L$. Ce résultat assez surprenant peut être *faux* si l'extension $K \subset L$ n'est pas supposée séparable, voir l'exercice 3.9.

3.3. Le groupe de Galois comme groupe de permutations des racines

Le paragraphe précédent considérait le point de vue d'une extension galoisienne « abstraite », choisie a priori. On démontrait en particulier que c'est une extension de décomposition d'un polynôme. D'un autre côté, les problèmes concrets sont plutôt dans l'autre sens : partant d'un polynôme, éventuellement irréductible, que dire du corps engendré par ses racines dans une extension algébriquement close ?

Le lemme suivant est évident, mais il ne faut pas le perdre de vue. Il affirme que si $K \subset L$ est une extension de décomposition d'un polynôme séparable $P \in K[X]$, $\mathrm{Gal}(L/K)$ permute les racines de $\mathcal{P}$, et un élément de $\mathrm{Gal}(L/K)$ est déterminé par son action sur ces racines.

LEMME 3.3.1. — *Soit K un corps, $P \in K[X]$ un polynôme séparable et $K \subset L$ une extension de décomposition de P. Soit $\mathcal{R} \subset L$ l'ensemble des racines de P dans L.*

a) *Pour tout K-automorphisme $\sigma \in \mathrm{Gal}(L/K)$ et toute racine $x \in \mathcal{R}$, on a $\sigma(x) \in \mathcal{R}$.*

b) *La restriction d'un automorphisme dans $\mathrm{Gal}(L/K)$ à $\mathcal{R}$ induit une permutation de $\mathcal{R}$ et l'homomorphisme qui s'en déduit, $\mathrm{Gal}(L/K) \to \mathfrak{S}(\mathcal{R})$, est injectif.*

Démonstration. — a) Si σ appartient à $\mathrm{Gal}(L/K)$ et si $x \in L$, on a $\sigma(P(x)) = P(\sigma(x))$. En particulier, si $P(x) = 0$, $P(\sigma(x)) = 0$, ce qui signifie $\sigma(x) \in \mathcal{R}$.

b) Considérons maintenant l'application $\mathrm{Gal}(L/K) \to \mathfrak{S}(\mathcal{R})$. Elle est bien définie : puisque $\mathcal{R}$ est un ensemble stable par $\sigma \in \mathrm{Gal}(L/K)$, la restriction de σ à $\mathcal{R}$ est une application injective. Puisque $\mathcal{R}$ est fini, $\sigma|_{\mathcal{R}}$ est nécessairement bijective donc définit une permutation de $\mathcal{R}$. Il est alors évident que cette application est un homomorphisme de groupes.

Supposons que pour tout $x \in \mathcal{R}$, on ait $\sigma(x) = x$. L'ensemble L^σ formé des $a \in L$ tels que $\sigma(a) = a$ est une sous-extension de L. Par hypothèse, elle contient les racines de P qui, par définition d'une extension de décomposition, engendrent L. Par suite, $L^\sigma = L$. On a ainsi $\sigma(a) = a$ pour tout $a \in L$, ce qui signifie $\sigma = \mathrm{id}_L$, cqfd. □

Rappelons qu'on dit qu'un groupe G opérant sur un ensemble X opère *transitivement* si pour tous x et y dans X, il existe $g \in G$ tel que $g \cdot x = y$.

PROPOSITION 3.3.2. — *Soit K un corps, $P \in K[X]$ un polynôme séparable et $K \subset L$ une extension de décomposition de P. L'action de $\mathrm{Gal}(L/K)$ sur les racines de P est transitive si et seulement si le polynôme P est irréductible.*

Démonstration. — Notons $\mathcal{R}$ l'ensemble des racines de P dans L. Si P n'est pas irréductible, on peut écrire $P = QR$ où Q et R sont deux polynômes qu'on peut supposer premiers entre eux, P étant séparable. Par suite, on peut décomposer $\mathcal{R}$ en la réunion disjointe des racines de Q et de R : $\mathcal{R} = \mathcal{R}_1 \cup \mathcal{R}_2$, où $\mathcal{R}_1$ et $\mathcal{R}_2$ sont non vides et disjoints. Si $x \in \mathcal{R}_1$ et $\sigma \in \mathrm{Gal}(L/K)$, $Q(\sigma(x)) = \sigma(Q(x)) = \sigma(0) = 0$, donc $\sigma(x) \in \mathcal{R}_1$. En particulier, $\sigma(x) \notin \mathcal{R}_2$. Par suite, si x_1 et x_2 sont deux éléments de $\mathcal{R}_1$ et $\mathcal{R}_2$ respectivement, il n'existe pas d'élément $\sigma \in \mathrm{Gal}(L/K)$ tel que $\sigma(x_1) = x_2$.

Supposons dans l'autre sens que P est irréductible et soit x, y, deux racines de P. Les sous extensions $K \subset K[x]$ et $K \subset K[y]$ sont toutes deux monogènes engendrées par une racine de P. Il existe ainsi un unique K-isomorphisme $f : K[x] \to K[y]$ tel que $f(x) = y$. Le corps L est alors une extension de décomposition du polynôme P sur les deux corps isomorphes $K[x]$ et $K[y]$. D'après le théorème 2.2.2, on peut prolonger f

en un K-automorphisme $\sigma : L \to L$. Un tel σ est un élément de $\mathrm{Gal}(L/K)$ et l'on a bien $\sigma(x) = y$. □

On le voit dans la démonstration de la proposition précédente, la détermination « concrète » d'un élément d'un groupe de Galois est malaisée car il faut procéder par étapes. Chaque étape est en revanche très simple puisque dans le cadre d'une extension monogène. Le théorème de l'élément primitif que nous démontrons maintenant affirme qu'en fait, toute extension séparable est monogène !

THÉORÈME 3.3.3 (Théorème de l'élément primitif). — *Soit K un corps et $K \subset L$ une extension finie séparable. Il existe $x \in L$ tel que $L = K[x]$.*

Démonstration. — La démonstration doit distinguer deux cas, suivant que le corps K est fini ou infini.

Supposons pour commencer que le corps K soit fini. Dans ce cas, le corps L est aussi fini et son groupe multiplicatif L^* est cyclique (exercice 1.16). Si x est un générateur de L^*, on a alors $L = K[x]$.

Supposons maintenant que K soit infini et introduisons une extension finie M de L telle que $K \subset M$ est galoisienne, par exemple la clôture galoisienne de $K \subset L$. D'après la théorie de Galois, les sous-corps de M contenant K correspondent à des sous-groupes de $\mathrm{Gal}(M/K)$. Comme ce groupe est fini, il n'a qu'un nombre fini de sous-groupes. Par suite, il n'y a qu'un nombre fini de corps E tels que $K \subset E \subset M$. A fortiori, il n'y a qu'un nombre fini de corps E de la forme $E = K[x]$ tels que $K \subset E \subset L$. Notons les $E_1, \ldots, E_n$.

Tout élément de L appartient à un tel sous-corps : x appartient à $K[x]$. Cela montre que L est la réunion des E_i. En particulier, le K-espace vectoriel L est réunion finie des sous-K-espaces vectoriels E_i. D'après le lemme suivant, l'un de ces sous-espaces est égal à L. Il existe ainsi $x \in L$ tel que $L = K[x]$. □

LEMME 3.3.4. — *Soit K un corps infini, V un K-espace vectoriel de dimension finie et $V_1, \ldots, V_n$ une famille finie de sous-espaces vectoriels de V distincts de V. Alors, $\bigcup_{i=1}^{n} V_i \neq V$.*

Démonstration. — On raisonne par récurrence sur n, le résultat étant clair pour $n = 1$. Par récurrence, $V_1 \cup \cdots \cup V_{n-1} \neq V$. Soit ainsi $x \in V$ n'appartenant pas à V_i pour $i \leqslant n-1$. Si x n'appartient pas à V_n, c'est gagné. Sinon, puisque $V_n \neq V$, on peut choisir $y \in V$ n'appartenant pas à V_n. Considérons les éléments $x + ty$ de V, t parcourant K. On va montrer qu'au plus un nombre fini d'entre eux appartient à la réunion des V_i.

Remarquons pour commencer qu'un indice i étant fixé, il existe au plus une valeur de t pour laquelle $x + ty \in V_i$. Si $x + ty$ et $x + t'y \in V_i$ pour deux valeurs de t et t' distinctes, leur différence $(t - t')y$ appartient à V_i, donc $y \in V_i$ puis $x = (x + ty) - ty \in V_i$. C'est absurde aussi bien pour $i < n$ ($x \notin V_i$) que pour $i = n$ ($y \notin V_n$). Ainsi, l'ensemble des t pour lesquels $x + ty$ appartient à l'un des V_i est fini de cardinal $\leqslant n$. Comme K

est infini, on peut choisir $t \in K$ tel que $x + ty \notin \bigcup_{i=1}^{n} V_i$, ce qui conclut la démonstration du lemme. □

L'approche que nous avons suivie pour présenter la théorie de Galois met l'accent sur la notion d'homomorphisme d'extensions. Le point crucial en est le « lemme d'Artin » (prop. 3.2.8).

Une autre approche est cependant possible et consiste à démontrer d'abord le théorème de l'élément primitif (théorème 3.3.3), sans utiliser la théorie de Galois. L'intérêt est bien sûr que le groupe de Galois d'une extension galoisienne définie par un élément primitif est très facile à visualiser : si $L = K[x]$ où x est une racine d'un polynôme irréductible $P \in K[X]$ scindé dans L, tout K-automorphisme de L est défini par l'image de x qui est l'une des racines y de P dans L. Cela fait pile poil le bon nombre.

Autre démonstration du théorème de l'élément primitif. — Par récurrence, il suffit de montrer qu'une extension engendrée par deux éléments l'est en fait par un seul. Le cas d'un corps fini se traite comme avant. Soit donc K un corps infini, L une extension finie séparable de K et x, y deux éléments de L tels que $L = K[x, y]$. Soit P et Q les polynômes minimaux de x et y sur K. Soit Ω une clôture algébrique de L et notons $x = x_1, \dots, x_n$ (resp. $y = y_1, \dots, y_m$) les racines distinctes de P (resp. Q) dans Ω. Comme K est infini, il existe $c \in K$ tel que pour tout $(i, j) \neq (1, 1)$, $x_i + cy_j \neq x_1 + cy_1$.

Posons $z = x + cy$ et montrons que $L = K[z]$. Le polynôme $R(Y) = P(z - cY)$ est à coefficients dans le corps $K[z]$ et s'annule en $Y = y$. D'autre part, si $j \neq 1$, $z - cy_j = x_1 + cy_1 - cy_j$ n'est par hypothèse pas racine de P, donc $R(y_j) \neq 0$, si bien que y est la seule racine commune à Q et à R. Comme Q est séparable, on a $Q(Y) = \prod_{j=1}^{m} (Y - y_j)$ et $\operatorname{pgcd}(Q, R) = Y - y$. Comme Q et R sont tous deux à coefficients dans $K[z]$, leur pgcd (choisi unitaire) aussi et $y \in K[z]$. Alors, $x = z - cy \in K[z]$, ce qui implique bien $L = K[z]$. □

Ceci fait, la plupart des récurrences deviennent inutiles, au moins si l'on se limite à l'étude des extensions séparables. On doit aussi démontrer autrement le lemme d'Artin.

Autre démonstration de la proposition 3.2.8. — On commence de même. Si $x \in L$, considérons son orbite par G c'est-à-dire l'ensemble $\mathcal{O}_x$ des $\sigma(x)$ pour $\sigma \in G$. Le polynôme

$$P_x = \prod_{y \in \mathcal{O}_x} (X - y)$$

est stable par σ, donc ses coefficients appartiennent à $K = L^G$. Comme il est à racines simples et que $P_x(x) = 0$, x est séparable. Par suite, l'extension $K \subset L$ est séparable. De plus, tout élément de L est de degré au plus $\operatorname{card} G$ sur K.

Montrons que l'extension $K \subset L$ est finie. Sinon, il existerait une suite croissante d'extensions finies $K \subset L_1 \subset L_2 \subset \ldots$, avec $L_i \subset L$ pour tout i telle que $[L_i : K]$ tende vers l'infini. D'après le théorème de l'élément primitif, chaque extension $K \subset L_i$ est monogène, puisqu'elle est finie et séparable, d'où $[L_i : K] \subset \operatorname{card} G$. Cette contradiction montre que l'extension $K \subset L$ est finie. Une nouvelle application du théorème de l'élément primitif entraîne qu'elle est de degré au plus $\operatorname{card} G$. Comme elle est de degré au moins $\operatorname{card} G$, on a l'égalité voulue. □

3.4. Discriminant, résolvantes

Nous allons commencer ce paragraphe en caractérisant les polynômes $P \in K[X]$ tels que le groupe de Galois d'une extension de décomposition de P est contenu dans le groupe alterné. Du point de vue de la théorie de Galois, c'est parfaitement naturel : si H est un sous-groupe de $\mathfrak{S}_n$, $H \cap \operatorname{Gal}(L/K)$ est un sous-groupe de $\operatorname{Gal}(L/K)$, donc correspond à une sous-extension $K \subset L' \subset L$. De plus, comme le sous-groupe alterné $\mathfrak{A}_n \subset \mathfrak{S}_n$ est distingué, savoir s'il contient le groupe de Galois ou pas ne dépendra pas de l'ordre choisi pour numéroter les racines.

Rappelons que l'on avait défini le discriminant comme un polynôme symétrique en n variables. D'après le théorème sur les fonctions symétriques élémentaires, il existe un unique polynôme $\Delta \in \mathbf{Z}[S_1, \ldots, S_n]$ tel que

$$D(X_1, \ldots, X_n) = \Delta(S_1, \ldots, S_n).$$

On définit maintenant le discriminant d'un polynôme en une variable,

$$P = a_n X^n + a_{n-1} X^{n-1} + \ldots a_1 X + a_0, \qquad a_n \neq 0.$$

par la formule

$$\operatorname{disc}(P) = a_0^{2n-2} \Delta(-a_1/a_0, a_2/a_0, \ldots, a_n/a_0).$$

Si $x_1, \ldots, x_n$ sont les racines de P dans une clôture algébrique de K, on a

$$\operatorname{disc}(P) = a_n^{2n-2} D(x_1, \ldots, x_n).$$

En particulier, $\operatorname{disc}(P) \neq 0$ si et seulement le polynôme P est séparable.

Exemples 3.4.1. — a) Si $P = aX^2 + bX + c$, les racines x et y vérifient $x + y = -b/a$ et $xy = c/a$, si bien que

$$\operatorname{disc}(P) = a^2(x-y)^2 = a^2(x^2 + y^2 - 2xy) = a^2((x+y)^2 - 4xy) = b^2 - 4ac.$$

b) On a

$$\operatorname{disc}(P) = (-1)^{n(n-1)/2} a_n^{n-2} \prod_{j=1}^{n} P'(x_j).$$

Si $y_1, \dots, y_{n-1}$ désignent les racines de P', on a

$$P'(x_j) = na_0 \prod_{k=1}^{n-1} (x_j - y_k),$$

si bien que

$$\operatorname{disc}(P) = (-1)^{n(n-1)/2} a_n^{2n-2} n^n \prod_{k=1}^{n-1} \prod_{j=1}^{n} (x_j - y_k).$$

Par suite, on a aussi

$$\operatorname{disc}(P) = (-1)^{n(n-1)/2} a_n^{n-1} n^n \prod_{k=1}^{n-1} P(y_k).$$

c) Pour $P = X^3 + pX + q$, $P' = 3X^2 + p$ a pour racines $\pm\sqrt{-p/3}$. On a ainsi

$$\begin{aligned}\operatorname{disc}(P) &= -27P(-\sqrt{-p/3})P(\sqrt{-p/3}) \\ &= -27\left(-\sqrt{-p/3}\frac{2p}{3} + q\right)\left(\sqrt{-p/3}\frac{2p}{3} + q\right) \\ &= -27q^2 - 4p^3.\end{aligned}$$

Si P est unitaire séparable de degré n, de racines $\{x_1, \dots, x_n\}$ dans une extension de décomposition L de K, notons

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

C'est ainsi un élément de L qui vérifie $d^2 = \operatorname{disc}(P)$. Si $\sigma \in \operatorname{Gal}(L/K)$, on a ainsi

$$\sigma(d) = \prod_{i<j} (\sigma(x_i) - \sigma(x_j)) = \prod_{i<j} (x_{\sigma(i)} - x_{\sigma(j)}),$$

où l'on a noté $\sigma(i)$ l'unique entier de $\{1; \dots; n\}$ tel que $\sigma(x_i) = x_{\sigma(i)}$. Alors,

$$\sigma(d)/d = \prod_{i<j} \begin{cases} 1 & \text{si } \sigma(i) < \sigma(j)\,; \\ -1 & \text{si } \sigma(i) > \sigma(j). \end{cases}$$

Autrement dit, $\sigma(d)/d$ est égal à (-1) puissance le nombre d'inversions de la permutation de $\{x_1; \dots; x_n\}$ associée à σ : c'est la signature de σ dans K (c'est-à-dire : $\sigma(d)/d = \varepsilon_\sigma 1_K$). On en déduit que d appartient à K si et seulement si la signature de tout élément de $\operatorname{Gal}(L/K)$ est égale à 1 dans K, c'est-à-dire si et seulement si

– ou bien la caractéristique du corps K est égale à 2 ;
– ou bien $\operatorname{Gal}(L/K)$ est un sous-groupe de $\mathfrak{A}_n$.

Nous avons ainsi démontré la proposition, caractéristique de ce que permet de démontrer la théorie de Galois :

PROPOSITION 3.4.2. — *Soit K un corps de caractéristique différente de 2. Le groupe de Galois d'un polynôme unitaire séparable P est contenu dans le groupe des permutations paires des racines si et seulement son discriminant est un carré dans K.*

Soit encore P un polynôme séparable unitaire à coefficients dans K, $K \subset L$ une extension de décomposition de P. Notons $x_1, \dots, x_n$ les racines de P dans L. Si f est un polynôme dans $K[X_1, \dots, X_n]$, l'expression $f(x_1, \dots, x_n)$ est a priori un élément de L.

On a déjà démontré que si f était un polynôme symétrique, alors f est un polynôme $g(S_1, \dots, S_n)$ en les polynômes symétriques élémentaires $S_1, \dots, S_n$. Comme les $S_j(x_1, \dots, x_n)$ sont, au signe près, les coefficients de P, $f(x_1, \dots, x_n)$ appartient à K. Plus généralement, si $f(X_{\sigma(1)}, \dots, X_{\sigma(n)}) = f(X_1, \dots, X_n)$ pour toute permutation σ dans un sous-groupe G de $\mathfrak{S}_n$, et si $\mathrm{Gal}(L/K) \subset G$, on aura de même $f(x_1, \dots, x_n) \in K$. Cela motive les considérations qui vont suivre.

Soit G un sous-groupe de $\mathfrak{S}_n$, f un polynôme dans $\mathbf{Z}[X_1, \dots, X_n]$ et soit H le sous-groupe de G formé des $\sigma \in G$ tels que

$$f(X_{\sigma(1)}, \dots, X_{\sigma(n)}) = f(X_1, \dots, X_n).$$

En fait, la formule ${}^{\sigma}f = f(X_{\sigma(1)}, \dots, X_{\sigma(n)})$ définit une action $[\sigma] : f \mapsto {}^{\sigma}f$ du groupe symmétrique $\mathfrak{S}_n$ sur l'anneau des polynômes $K[X_1, \dots, X_n]$. Remarquez que $[\sigma]$ est à la fois un automorphisme d'anneaux et de K-espace vectoriels. Si l'on restreint cette action au sous-groupe $G \subset \mathfrak{S}_n$, le groupe H n'est autre que le stabilisateur de f. Par suite, si $\sigma \in G$ et $\tau \in H$, ${}^{\sigma\tau}f = {}^{\sigma}({}^{\tau}f) = {}^{\sigma}f$ et ${}^{\sigma}f$ ne dépend que de la classe à droite de σ dans G/H. A fortiori, $f(x_{\sigma(1)}, \dots, x_{\sigma(n)})$ ne dépend aussi que de cette classe σH. On peut ainsi poser la définition :

DÉFINITION 3.4.3. — *On définit la* résolvante $R_G(f, P)$ *de P par rapport à f et G par :*

$$R_G(f, P) = \prod_{\sigma H \in G/H} (X - f(x_{\sigma(1)}, \dots, x_{\sigma(n)})).$$

(Le produit est sur un système arbitraire de représentants dans G des classes à droites modulo H.)

LEMME 3.4.4. — *C'est un polynôme de $K[X]$.*

Démonstration. — Comme c'est *a priori* un polynôme de $L[X]$, il suffit de vérifier que pour tout élément $\tau \in \mathrm{Gal}(L/K)$, $\tau(R_G(f, P)) = R_G(f, P)$. (L'action de $\mathrm{Gal}(L/K)$ sur les polynômes se fait coefficient par coefficient. Le polynôme est stabilisé si et seulement si chacun de ses coefficients l'est.) Or, rappelons que par définition, $\tau(x_j) = x_{\tau(j)}$ pour tout j, si bien que

$$\tau(f(x_{\sigma(1)}, \dots, x_{\sigma(n)})) = f(x_{\tau\sigma(1)}, \dots, x_{\tau\sigma(n)}).$$

Par suite,

$$\tau(R_G(f, P)) = \tau\Big(\prod_{\sigma \in G/H} (X - f(x_{\sigma(1)}, \dots, x_{\sigma(n)}))\Big) = \prod_{\sigma \in G/H} (X - f(x_{\tau\sigma(1)}, \dots, x_{\tau\sigma(n)})).$$

Comme $\mathrm{Gal}(L/K) \subset G$, lorsque $[\sigma]$ parcourt G/H, l'ensemble des classes à droite de G modulo H, $[\tau\sigma]$ aussi, si bien que $\tau(R_G(f, P)) = R_G(f, P)$. C'est ce qu'il fallait démontrer. □

Le discriminant apparaît maintenant comme un cas particulier de la construction générale de résolvante que nous venons d'étudier. En effet, le stabilisateur du polynôme $f = \prod_{i<j}(X_i - X_j)$ dans $G = \mathfrak{S}_n$ est par définition égal au groupe alterné $\mathfrak{A}_n$. De plus, $f(x_1,\dots,x_n) = d$ tandis que pour toute permutation impaire σ, $f(x_{\sigma(1)},\dots,x_{\sigma(n)}) = -d$. Ainsi,

$$R_{\mathfrak{S}_n}(f,P) = (X-d)(X+d) = X^2 - d^2 = X^2 - \mathrm{disc}(P).$$

La proposition 3.4.2 peut alors être reformulée comme suit : le groupe de Galois de P est contenu dans $\mathfrak{A}_n$ si et seulement si le polynôme $X^2 - \mathrm{disc}(P)$ est scindé à racines simples dans K.

Pour des résolventes plus générales, on a la proposition suivante :

PROPOSITION 3.4.5. — *Avec les notations précédentes, supposons que* $\mathrm{Gal}(L/K) \subset G$ *de sorte que* $R_G(f,P) \in K[X]$*, et supposons de plus que* $R_G(f,P)$ *admette une racine simple dans* K*. Alors,* $\mathrm{Gal}(L/K)$ *est conjugué dans* G *à un sous-groupe de* H *: il existe* $g \in G$ *tel que* $\mathrm{Gal}(L/K) \subset gHg^{-1}$.

Démonstration. — Pour tout $\sigma \in G$, notons $\alpha_\sigma = f(x_{\sigma(1)},\dots,x_{\sigma(n)})$. On a vu dans la démonstration précédente que pour tout $\tau \in \mathrm{Gal}(L/K)$, $\tau(\alpha_\sigma) = \alpha_{\tau\sigma}$. Soit $\sigma \in G$ tel que la racine simple de l'énoncé soit α_σ. Si α_σ appartient à K, cela signifie que pour tout $\tau \in \mathrm{Gal}(L/K)$, $\alpha_{\tau\sigma} = \tau(\alpha_\sigma) = \alpha_\sigma$. Comme α_σ est supposé être une racine simple de $R_G(f,P)$, pour tout $\tau \in \mathrm{Gal}(L/K)$, $\tau\sigma$ est dans la même classe à droite que σ modulo H : $\tau\sigma \in \sigma H$, autrement dit $\tau \in \sigma H\sigma^{-1}$. C'est ce qu'il fallait démontrer. □

Une généralisation de cette proposition, jointe à une liste convenable de (G,f), est utilisée par les ordinateurs pour déterminer explicitement les groupes de Galois des polynômes à coefficients entiers, au moins lorsque leur degré n'est pas trop élevé. (Les connaissances et les capacités des ordinateurs actuels permettent d'aller jusqu'au degré 23, dans l'implémentation de MAGMA.)

Évariste Galois (1811–1832)

3.5. Corps finis

Un corps fini est un corps qui n'a qu'un nombre fini d'éléments. Les corps finis offrent le double intérêt d'illustrer de manière simple et directe la théorie de Galois, sans pour autant cesser d'être un sujet d'étude arithmétique incroyablement riche. Ils ont été inventés par Gauss mais il n'a rien publié à ce sujet et Galois les a redécouvert plus tard.

Commençons par des remarques simples. Soit F un corps fini. Remarquons que l'homomorphisme canonique $\mathbf{Z} \to F$ ne peut pas être injectif, si bien que la caractéristique de F est un nombre premier p. En particulier, F contient le corps $\mathbf{F}_p = \mathbf{Z}/p\mathbf{Z}$. Alors, F est un $\mathbf{F}_p$-espace vectoriel, de dimension nécessairement finie. Si d désigne cette dimension, on a alors l'égalité $\operatorname{card} F = p^d$.

Notons $q = \operatorname{card} F = p^d$. L'ensemble F^* des éléments non nuls de F est un groupe pour la multiplication, de cardinal $q-1$. D'après le théorème de Lagrange (proposition 4.2.2), tout élément non nul de F vérifie $x^{q-1} = 1$. De manière équivalente, tout élément x de F vérifie $x^q = x$. Comme tout sous-groupe fini du groupe multiplicatif d'un corps, F^* est cyclique (voir l'exercice 1.16) et il existe un élément $x_1 \in F^*$ d'ordre $q-1$.

Si $F \to \Omega$ est un plongement de F dans une clôture algébrique de $\mathbf{F}_p$, les images des éléments de F^* sont des racines $(q-1)$-ièmes de l'unité. Réciproquement, l'ensemble des éléments $x \in \Omega$ qui vérifient $x^q = x$ est un ensemble fini, de cardinal exactement q car le polynôme $X^q - X$ est séparable (de dérivée -1). C'est de plus un sous-corps de Ω : si φ désigne l'automorphisme de Frobenius de Ω, c'est le sous-corps de Ω fixé par l'automorphisme φ^d.

Cette description montre aussi que deux corps finis de même cardinal q sont isomorphes : ils sont tous deux isomorphes au sous-corps de Ω formé des x tels que $x^q = x$.

Résumons :

PROPOSITION 3.5.1. — *Soit p un nombre premier et $q = p^d$ une puissance de p, l'ensemble des racines du polynôme $X^q - X$ dans une clôture algébrique de $\mathbf{F}_p$ est un corps fini de cardinal q. Tout corps fini de cardinal q lui est isomorphe.*

Passons maintenant aux extension de corps finis. Soit $E \to F$ une telle extension ; les deux corps E et F sont de même caractéristique p. Notons $\operatorname{card} E = p^e$, $\operatorname{card} F = p^f$. Comme F est un E-espace vectoriel de dimension finie, le cardinal de F est en fait une puissance de celui de E et e *divise* f. Posons $d = f/e$; c'est le degré $[F : E]$ de l'extension $E \to F$. Réciproquement, si E et F sont deux corps finis de cardinaux p^e et p^f avec $f = de$, il existe un homomorphisme $E \to F$: si Ω est une clôture algébrique de $\mathbf{F}_p$, E et F s'identifient aux sous-corps de Ω formés des x tels que $x^{p^e} = x$ et $x^{p^f} = x$ respectivement. Ainsi, on peut identifier E à un sous-corps de F, d'où l'homomorphisme cherché.

On suppose dans la suite que $E \subset F$. Soit $\Phi = \varphi^e : F \to F$ l'automorphisme de F donné par $x \mapsto x^{p^e}$. Il est l'identité sur E, donc définit un élément de $\operatorname{Gal}(F/E)$. Si $x_1 \in F^*$ est un élément d'ordre $p^f - 1$, on a $\Phi^j(x) = x^{p^{ej}}$, donc $\Phi^j(x) \neq x$ si $1 \leqslant ej < f$. Cela montre que les d éléments $\mathrm{id}, \Phi, \ldots, \Phi^{d-1}$ de $\operatorname{Gal}(F/E)$ sont distincts et $\operatorname{card}\operatorname{Gal}(F/E) \geqslant d$. Il en résulte que l'extension $E \to F$ est galoisienne, de groupe de Galois engendré par Φ et isomorphe à $\mathbf{Z}/d\mathbf{Z}$.

Nous avons ainsi démontré la proposition suivante :

PROPOSITION 3.5.2. — *Les extensions de corps finis sont galoisiennes, leur groupe de Galois est cyclique.*

Cela a une conséquence pratique importante sur l'action du groupe de Galois d'une extension de décomposition sur les racines. Pour simplifier, considérons un polynôme séparable $P \in \mathbf{F}_p[X]$, et soit F une extension de décomposition de P. Soit $\varphi\colon x \mapsto x^p$ l'automorphisme de Frobenius, générateur de $\mathrm{Gal}(F/\mathbf{F}_p)$. Si x est une racine de P, $\varphi(x)$ aussi. Numérotons les racines $\{x_1, x_2, \dots, x_n\}$ de P de sorte que la permutation induite par φ ait la décomposition en cycles

$$(x_1 \dots x_{n_1})(x_{n_1+1} \dots x_{n_1+n_2}) \dots (x_{n_1+\dots+n_{r-1}+1} \dots x_n).$$

(Il y a r cycles, de longueurs $n_1, \dots, n_r$, avec $n_1 + \dots + n_r = n$.) Comme $\mathrm{Gal}(F/\mathbf{F}_p)$ est engendré par φ, les racines de P dans un même cycle sont donc exactement les conjuguées d'une quelconque d'entre elles, d'où une factorisation de P en facteurs irréductibles de degrés $n_1, \dots, n_r$.

Cette remarque est surtout employée à rebours : les degrés des facteurs irréductibles du polynôme P permettent de déterminer les longueurs des cycles de la permutation de ses racines que définit l'automorphisme de Frobenius.

Notons aussi que pour calculer les n_j, il n'est pas besoin de factoriser complètement le polynôme P, mais il suffit de déterminer le nombre ν_d de facteurs de degré d donné. Par définition, ν_1 est le nombre de racines (distinctes car P est supposé séparable) de P dans $\mathbf{F}_p$; ce sont les racines communes à P et à $X^p - X$, si bien que ν_1 est le degré du polynôme $\mathrm{pgcd}(P, X^p - X)$. Puis, si $\mathbf{F}_{p^2}$ désigne une extension de $\mathbf{F}_p$ de cardinal p^2, ν_2 est la moitié du nombre de racines de P qui appartiennent à $\mathbf{F}_{p^2}$ mais pas à $\mathbf{F}_p$. Ainsi, $2\nu_2$ est le degré du pgcd de P et de $(X^{p^2} - X)/(X^p - X)$, qui est aussi le pgcd de $P/\mathrm{pgcd}(P, X^p - X)$ et $X^{p^2} - X$. Plus généralement, le nombre de racines de P dnas le corps $\mathbf{F}_{p^n}$ est égal à

$$\sum_{d|n} d\nu_d = \deg \mathrm{pgcd}(X^{p^n} - X, P).$$

Cela permet de calculer ν_d par récurrence.

Exercices

Exercice 3.1 (Principe de prolongement des identités algébriques)
Soit K un corps infini.

a) Si $P \in K[X_1,\dots,X_n]$ est non nul, montrer qu'il existe $(x_1,\dots,x_n) \in K^n$ tel que $P(x_1,\dots,x_n) \neq 0$.

b) Rappeler pourquoi l'anneau des polynômes $K[X_1,\dots,X_n]$ est intègre. En déduire une autre démonstration du lemme 3.3.4.

c) Soit P et Q deux polynômes de $K[X_1,\dots,X_n]$. On suppose que $Q \neq 0$ et que pour tous $(x_1,\dots,x_n) \in K^n$ tels que $Q(x_1,\dots,x_n) \neq 0$, $P(x_1,\dots,x_n) = 0$. Montrer que $P = 0$.

Exercice 3.2. — Soit K un corps.

a) Montrer qu'un polynôme $P \in K[X]$ est séparable si et seulement si c'est le produit de polynômes *irréductibles* séparables.

b) Soit $P_1,\dots,P_r$ des polynômes séparables dans $K[X]$. Montrer que leur ppcm et leur pgcd sont séparables.

Exercice 3.3. — Soit K le corps engendré par i et $\sqrt{2}$ dans $\mathbf{C}$ ($i^2 = -1$).

a) Montrer que $[K : \mathbf{Q}] = 4$. En donner un élément primitif ainsi que son polynôme minimal.

b) Déterminer les opérations possibles de $\mathrm{Gal}(K/\mathbf{Q})$ sur l'ensemble $\{\pm i, \pm\sqrt{2}\}$.
Montrer que $\mathrm{Gal}(K/\mathbf{Q}) \simeq (\mathbf{Z}/2\mathbf{Z})^2$.

c) Dresser la liste des sous-corps de K.

Exercice 3.4. — Soit $K \subset L$ une extension galoisienne de groupe de Galois G. Soit H un sous-groupe de G et $E = L^H$ l'extension de K associée. Montrer que la clôture galoisienne E^g de E est contenue dans L et déterminer le sous-groupe de G qui lui correspond par la théorie de Galois.

Exercice 3.5. — Soit K un corps, L une extension finie galoisienne de K. Soit $x \in L$ et y un conjugué de x, c'est-à-dire une racine du polynôme minimal de x sur K.

Montrer qu'il existe un élément $\sigma \in \mathrm{Gal}(L/K)$ tel que $\sigma(x) = y$. (D'ailleurs, combien en existe-t-il ?)

Exercice 3.6. — Soit K un corps et $K \subset L$ une extension galoisienne, extension de décomposition d'un polynôme irréductible séparable de degré n de $K[X]$. On note $x_1,\dots,x_n$ ses racines dans L et on considère $\mathrm{Gal}(L/K)$ comme un sous-groupe de $\mathfrak{S}_n$.

a) Si $i \in \{1;\dots;n\}$, soit H_i le sous-groupe de $\mathfrak{S}_n$ constitué des permutations σ telles que $\sigma(i) = i$. On pose $G_i = \mathrm{Gal}(L/K) \cap H_i$. Montrer que les G_i sont conjugués dans $\mathrm{Gal}(L/K)$ et que pour tout i, $(\mathrm{Gal}(L/K) : G_i) = n$. À quelles sous-extensions correspondent ces sous-groupes ?

b) Si $\mathrm{Gal}(L/K)$ est abélien, montrer que $L = K[x_1]$.

Exercice 3.7. — Soit $K \subset L$ une extension finie galoisienne et soit $x \in L$. On suppose que les éléments $\sigma(x)$, pour σ parcourant $\mathrm{Gal}(L/K)$, sont tous distincts. Montrer que $L = K(x)$.

Exercice 3.8. — Soit $K \to L$ une extension monogène et soit $\alpha \in L$ tel que $L = K[\alpha]$. Pour tout corps E tel que $K \subset E \subset L$, notons P_E le polynôme minimal de α sur E.

a) Montrer que $[L : E] = \deg P_E$.

b) Si E et E' sont des corps tels que $K \subset E' \subset E \subset L$, montrer que P_E divise $P_{E'}$.

c) Soit E un corps tel que $K \subset E \subset L$ et soit E' le sous-corps de E engendré par les coefficients de P_E. Montrer que $P_{E'} = P_E$. Conclure que $E' = E$.

d) Montrer qu'il y a un nombre fini de corps E tels que $K \subset E \subset L$.

Exercice 3.9. — **a)** Soit $K \to L$ une extension algébrique séparable. Soit n un entier tel que tout élément de L soit de degré au plus n sur K. Montrer que $[L : K] \leqslant n$. (*Considérer sinon une extension finie $L_1 \subset L$ telle que $[L_1 : K] > n$ et appliquer le théorème de l'élément primitif.*)

b) Soit p un nombre premier, $K = \mathbf{F}_p(X, Y)$ et soit L l'extension engendrée dans une clôture algébrique de K par $X^{1/p}$ et $Y^{1/p}$. Montrer que $[L : K] = p^2$ mais que tout élément de L est de degré au plus p. En particulier, l'extension $K \subset L$ n'est pas monogène.

Exercice 3.10. — Soit k un corps, $L = k(X_1, \ldots, X_n)$ le corps des fractions rationnelles en n variables et K le sous-corps de L engendré par les polynômes symétriques élémentaires $S_1, \ldots, S_n$.

a) Montrer que l'extension $K \subset L$ est galoisienne de groupe $\mathfrak{S}_n$.

b) Supposons que k est de caractéristique zéro. Montrer que $X_1 + 2X_2 + \cdots + nX_n$ engendre L sur K.

c) Soit $f \in L$ et soit H sont stabilisateur dans $\mathfrak{S}_n$, c'est-à-dire l'ensemble des $\sigma \in \mathfrak{S}_n$ tels que

$$f(X_1, \ldots, X_n) = f(X_{\sigma(1)}, \ldots, X_{\sigma(n)}).$$

Montrer que l'extension $K(f) \subset L$ est galoisienne de groupe H. (Montrer que f est un élément primitif de l'extension $K \subset L^H$.)

d) Déduire de la question précédente que toute fonction rationnelle $g \in L$ qui a même stabilisateur que f peut être exprimée comme une fonction rationnelle de f et des polynômes symétriques élémentaires (Lagrange, 1770, 60 ans avant Galois !).

Exemple explicite avec $n = 3$: $f = X_1X_2 + X_3$, $g = X_3$.

Exercice 3.11. — **a)** Soit G un groupe et F un corps. Soit $\sigma_1, \ldots, \sigma_n$ n homomorphismes distincts de G dans le groupe multiplicatif $F^\times$. Montrer que $\sigma_1, \ldots, \sigma_n$ sont linéairement indépendants : si $a_1, \ldots, a_n$ sont des éléments de F tels que $a_1\sigma_1 + \cdots + a_n\sigma_n = 0$, alors $a_1 = \cdots = a_n = 0$.

b) Soit E et F deux corps et $\sigma_1, \ldots, \sigma_n$ n homomorphismes de corps distincts $E \to F$. Montrer qu'ils sont linéairement indépendants sur F.

Exercice 3.12. — Soit $K \to \Omega$ une extension algébrique d'un corps parfait K et supposons que tout polynôme non constant dans $K[X]$ a une racine dans Ω.

a) Soit $K \to L$ une extension de décomposition d'un polynôme irréductible $P \in K[X]$. Montrer qu'il existe $\alpha \in L$ tel que $L = K(\alpha)$.

b) Soit Q le polynôme minimal de α sur K. En utilisant le fait que Q a une racine dans Ω, montrer qu'il existe un morphisme d'extensions $L \to \Omega$.

c) Conclure que P est scindé dans Ω, et donc que Ω est une clôture algébrique de K.

Exercice 3.13. — Soit K un corps et soit n un entier tel que $n \geqslant 2$. Soit $E = K[\zeta]$ une extension de K engendrée par une racine primitive n-ième de l'unité.

a) Montrer que l'ensemble des racines n-ième de l'unité dans E est un groupe cyclique d'ordre n, engendré par ζ.

b) Montrer que l'extension $K \to E$ est galoisienne.

c) Soit σ un élément de $\mathrm{Gal}(E/K)$. Montrer qu'il existe un entier d premier à n tel que $\sigma(\zeta) = \zeta^d$.

d) Construire un homomorphisme de groupes injectif $\varphi\colon \mathrm{Gal}(E/K) \to (\mathbf{Z}/n\mathbf{Z})^*$. En déduire que $\mathrm{Gal}(E/K)$ est un groupe abélien.

e) Quel est le groupe de Galois de $\mathbf{Q}(\zeta_n)/\mathbf{Q}$?

Exercice 3.14. — Soit p un nombre premier impair. On rappelle que $(\mathbf{Z}/p\mathbf{Z})^*$ est cyclique d'ordre $p-1$.

a) Montrer que pour tout $n \geqslant 1$, $(\mathbf{Z}/p^n\mathbf{Z})^*$ est cyclique d'ordre $(p-1)p^{n-1}$. (Si $a \in \mathbf{Z}$ est un élément dont la classe dans $\mathbf{Z}/p\mathbf{Z}$ engendre $(\mathbf{Z}/p\mathbf{Z})^*$, considérer $a^{p^n}(1+p)$.)

b) En déduire que pour tout $n \geqslant 1$ le corps cyclotomique $\mathbf{Q}(\zeta_{p^n})$ engendré par une racine primitive p^n-ième de l'unité possède un unique sous-corps K tel que $[K : \mathbf{Q}] = 2$.

c) Soit $\varepsilon\colon (\mathbf{Z}/p\mathbf{Z})^* \to \{\pm 1\}$ l'unique homomorphisme de groupes par lequel tout générateur de $(\mathbf{Z}/p\mathbf{Z})^*$ a pour image -1. On pose (*somme de Gauß*)

$$G = \sum_{k=1}^{p-1} \varepsilon(k) \exp(2\mathrm{i}k\pi/p).$$

Montrer que $G^2 = (-1)^{(p-1)/2}p$. Quel est le sous-corps K de la question précédente ?

Exercice 3.15. — Soit $F = \mathbf{F}_q$ un corps fini de cardinal q. Si $d \geqslant 1$, on note $\mathcal{I}_d$ l'ensemble des polynômes unitaires irréductibles de degré d dans $F[X]$; soit $N_d = \mathrm{card}\,\mathcal{I}_d$.

a) Soit $n \geqslant 1$. Montrer que le degré d'un polynôme irréductible qui divise $X^{q^n} - X$ est un diviseur de n. Réciproquement, si d divise n, montrer que tout polynôme de $\mathcal{I}_d$ divise $X^{q^n} - X$.

b) Montrer la relation

$$q^n = \sum_{d|n} dN_d.$$

c) Montrer que pour tout entier n,

$$N_n \geqslant \frac{1}{n} q^n \frac{q-2}{q-1}.$$

En particulier, $N_n \neq 0$.

d) Soit $\mu\colon \mathbf{N}^* \to \{0, 1, -1\}$ la fonction de Möbius définie par $\mu(n) = (-1)^r$ si n est le produit de r nombres premiers distincts, et $\mu(n) = 0$ sinon. Si f et g sont des fonctions de $\mathbf{N}^*$ dans $\mathbf{C}$, montrer que l'on a $f(n) = \sum_{d|n} g(d)$ pour tout n, si et seulement si $g(n) = \sum_{d|n} \mu(n/d) g(d)$ pour tout n (*formule d'inversion de Möbius*). En particulier,

$$N_n = \frac{1}{n} \sum_{d|n} \mu(n/d) q^d.$$

Exercice 3.16. — On s'intéresse dans cet exercice à la factorisation des polynômes cyclotomiques sur un corps fini $\mathbf{F}_q$ de cardinal q. Soit p sa caractéristique ; on note Ω une clôture algébrique de $\mathbf{F}_q$.

a) Si n est un entier premier à p et r un entier positif ou nul, montrer que l'on a $\Phi_{p^r n} = \Phi_n^{p^r-1}$ dans $\mathbf{F}_q[X]$.

b) Soit $\alpha \in \Omega^*$. Montrer qu'il existe un plus petit entier n tel que $\alpha^n = 1$. Montrer qu'il n'est pas multiple de p. Soit δ l'ordre de q dans le groupe $(\mathbf{Z}/n\mathbf{Z})^*$. Montrer alors que le polynôme minimal de α est de degré δ.

c) Soit $n \geqslant 2$ un entier premier à p. Montrer que le polynôme Φ_n est séparable dans $\mathbf{F}_q[X]$. Déduire de la question précédente que tous ses facteurs irréductibles sur $\mathbf{F}_q$ ont même degré, égal à l'ordre de q dans le groupe $(\mathbf{Z}/n\mathbf{Z})^*$.

d) Montrer que le polynôme X^4+1 est irréductible dans $\mathbf{Q}[X]$ mais que pour tout nombre premier p, il est réductible dans $\mathbf{F}_p[X]$. Généraliser.

Exercice 3.17. — **a)** Soit n et a deux entiers, et soit p un nombre premier qui divise $\Phi_n(a)$ sans diviser n. Montrer que $p \equiv 1 \pmod{n}$.

b) Soit n un entier. Montrer qu'il existe une infinité de nombres premiers de la forme $kn+1$. (*C'est un cas facile du théorème de Dirichlet selon lequel si n et m sont deux entiers premiers entre eux, il existe une infinité de nombres premiers de la forme $kn+m$.*)

Exercice 3.18. — Soit $\mathbf{F}$ un corps fini, q son cardinal et p sa caractéristique. Si $f \in \mathbf{F}[x_1,\dots,x_n]$, on pose $S(f) = \sum_{x\in\mathbf{F}^n} f(x)$.

a) Calculer $S(x_1^{i_1}\dots x_n^{i_n})$ en fonction de $(i_1,\dots,i_n)$.

b) Soit $f_1,\dots,f_r$ des polynômes de $\mathbf{F}[x_1,\dots,x_n]$ de degrés $d_1,\dots,d_r$ et soit V l'ensemble de leurs zéros communs dans $\mathbf{F}^n$.

Soit f le polynôme défini par $f = \prod_{i=1}^{r}(1-f_i^{q-1})$. Calculer $S(f)$ en fonction de $\operatorname{card} V$. En déduire que si $d_1+\cdots+d_r < n$, $\operatorname{card} V$ est multiple de p (*théorème de Chevalley–Warning*).

Exercice 3.19. — Soit $\mathbf{F}$ un corps fini ; on note q son cardinal.

a) Montrer que l'espace vectoriel $\mathbf{F}^2$ est réunion de $q+1$-droites vectorielles, mais pas moins. Plus généralement, combien faut-il d'hyperplans pour recouvrir $\mathbf{F}^n$?

b) Soit $H_1,\dots,H_d$ des hyperplans affines de $\mathbf{F}_q^n$ ne passant pas par l'origine et recouvrant $\mathbf{F}_q^n \setminus \{0\}$. Montrer que $d \geqslant n(q-1)$. Montrer que cette minoration est optimale en exhibant un tel recouvrement avec $d = n(q-1)$. (*Si f_i est une équation de H_i, poser $f = \prod_{i=1}^{d} f_i$ et considérer la quantité $S(f)$ introduite dans l'exercice 3.18.*)

Exercice 3.20. — Cet exercice est la base de l'algorithme de Berlekamp pour factoriser des polynômes sur des corps finis.

Soit P un polynôme séparable non constant à coefficients dans le corps fini $\mathbf{F}_p$. Notons R_P l'anneau $\mathbf{F}_p[X]/(P)$. Soit $P = \prod_{i=1}^{r} P_i$ la factorisation de P en polynômes irréductibles de $\mathbf{F}_p[X]$. Notons $n_i = \deg P_i$.

a) Montrer que l'anneau R_{P_i} est isomorphe au corps fini $\mathbf{F}_{p^{n_i}}$.

b) Si $A \in R_P$, on désigne par $\rho_i(A)$ le reste de la division euclidienne de A par P_i. Montrer que l'application $A \mapsto (\rho_1(A), \ldots, \rho_r(A))$ définit un isomorphisme d'anneaux $R_P \simeq \prod_{i=1}^{r} R_{P_i}$.

c) Si $A \in R_P$, posons $t(A) = A^p - A$. Montrer que t est un endomorphisme $\mathbf{F}_p$-linéaire de R_P, vu comme un $\mathbf{F}_p$-espace vectoriel et qu'il correspond, par les isomorphismes précédents, à l'application

$$\prod_{i=1}^{r} \mathbf{F}_{p^{n_i}} \to \prod_{i=1}^{r} \mathbf{F}_{p^{n_i}}, \qquad (a_1, \ldots, a_r) \mapsto (a_1^p - a_1, \ldots, a_r^p - a_r).$$

d) Montrer que le noyau de t est un sous-espace vectoriel de R_P de dimension r.

e) Soit a un élément du noyau de t. Montrer qu'il existe un polynôme unitaire $Q \in \mathbf{F}_p[X]$ de degré minimal tel que $Q(a) = 0$. Montrer que le polynôme Q est séparable et scindé sur $\mathbf{F}_p$.

f) (*suite*) Si $a \notin \mathbf{F}_p$, montrer que Q n'est pas irréductible. D'une factorisation partielle $Q = Q_1 Q_2$, montrer comment obtenir une factorisation partielle non triviale de P.

Exercice 3.21. — **a)** Soit p et q deux éléments d'un corps K. Montrer que le discriminant du polynôme $X^5 + pX + q$ est égal à $5^5 q^4 + 4^4 p^5$.

b) Généraliser la question précédente en calculant, pour tout entier $n \geqslant 2$, le discriminant du polynôme $X^n + pX + q$.

Exercice 3.22. — Soit p et q deux nombres premiers distincts. Soit F une extension de décomposition du polynôme $P = X^q - 1$ sur le corps $\mathbf{F}_p$.

a) L'automorphisme de Frobenius $\varphi \in \mathrm{Gal}(F/\mathbf{F}_p)$ induit une permutation des racines de P. Déterminer sa décomposition en cycles de supports disjoints.

b) Montrer que $\mathrm{Gal}(F/\mathbf{F}_p)$ est un sous-groupe du groupe alterné $\mathfrak{A}_q$ si et seulement si p est un carré dans $\mathbf{Z}/q\mathbf{Z}$.

Exercice 3.23. — Si $a \in (\mathbf{Z}/q\mathbf{Z})^*$, on note $\left(\frac{a}{q}\right) = 1$ si a est un carré dans $\mathbf{Z}/q\mathbf{Z}$ et -1 sinon (*symbole de Legendre*).

a) Si q est impair, montrer que $\left(\frac{a}{q}\right) = a^{(q-1)/2}$.

b) À l'aide des résultats de l'exercice 3.22, établir la loi de réciprocité quadratique (Gauß, 8 avril 1796) : si p et q sont deux nombres premiers impairs distincts,

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{(p-1)(q-1)/4}.$$

c) On suppose que p est un nombre premier impair. Soit ζ une racine primitive 8-ième de l'unité dans une clôture algébrique de $\mathbf{F}_p$. Soit $\alpha = \zeta + \zeta^{-1}$.

Calculer α^2. En déduire que 2 est un carré dans $\mathbf{F}_p$ si et seulement si $p \equiv \pm 1 \pmod 8$. Vérifier enfin que

$$\left(\frac{2}{p}\right) = (-1)^{(p^2-1)/8}.$$

Exercice 3.24 (Résultant et discriminant). — Soit

$$A = a_n(X - x_1)\dots(X - x_n) = a_n X^n + \cdots + a_0$$
$$B = b_m(X - y_1)\dots(X - y_m) = b_m X^m + \cdots + b_0,$$

deux polynômes scindés à coefficients dans un corps K.

a) Introduisons les deux matrices suivantes à coefficients dans K :

$$S = \begin{pmatrix} a_n & a_{n-1} & \dots & a_0 & & \\ & \ddots & & & \ddots & \\ & & a_n & a_{n-1} & \dots & a_0 \\ b_m & b_{m-1} & \dots & b_0 & & \\ & \ddots & & & \ddots & \\ & & b_m & b_{m-1} & \dots & b_0 \end{pmatrix}$$

où il y a m lignes de a puis n lignes de b, et

$$V = \begin{pmatrix} y_1^{n+m-1} & \dots & y_m^{n+m-1} & x_1^{n+m-1} & \dots & x_n^{n+m-1} \\ \vdots & & \vdots & \vdots & & \vdots \\ y_1 & \dots & y_m & x_1 & \dots & x_n \\ 1 & \dots & 1 & 1 & \dots & 1 \end{pmatrix}.$$

Le déterminant de S est appelé *résultant de A et B* et est noté $\mathrm{Res}(A,B)$. En calculant le produit SV puis en prenant les déterminants, montrer que

$$\mathrm{Res}(A,B) = a_n^m b_m^n \prod_{\substack{1\leqslant i\leqslant n \\ 1\leqslant j\leqslant m}} (x_i - y_j) = a_n^m \prod_{i=1}^{n} B(x_i) = (-1)^{mn} b_m^n \prod_{j=1}^{m} A(y_j),$$

au moins lorsque le polynôme AB est à racines simples.

b) À l'aide de l'exercice 3.1, montrer que les formules précédentes sont toujours valables.

c) Si $m = n-1$ et $B = A'$, montrer que

$$\mathrm{Res}(A,A') = (-1)^{n(n-1)/2} a_n \,\mathrm{disc}(A).$$

Exercice 3.25. — Soit $P = a_n X^n + a_{n-1}X^{n-1} + \cdots + a_0$ un polynôme de degré n à coefficients entiers. Montrer que le discriminant de P est un entier.. (Utiliser au choix l'exercice 1.18 ou l'exercice 3.24).

4

Un peu de théorie des groupes

Ce chapitre rappelle les notions essentielles de théorie des groupes qui interviennent en théorie de Galois. Je conseille de ne le lire qu'au fur et à mesure des besoins (c'est d'ailleurs dans cet esprit qu'il sera enseigné).

4.1. Groupes (rappels de définitions)

Un *groupe* est un ensemble G muni d'une opération interne $(g, g') \mapsto g * g'$ vérifiant les propriétés suivantes :

– il existe un élément $e \in G$ tel que pour tout $g \in G$, $e * g = g * e = g$ (existence d'un *élément neutre*) ;
– pour tout $g \in G$, il existe $g' \in G$ tel que $g * g' = g' * g = e$ (existence d'un *inverse*) ;
– pour tous g, g', g'' dans G, on a $g * (g' * g'') = (g * g') * g''$ (*associativité*).

De nombreuses autres notations existent pour la loi interne : outre $*$, citons $\cdot$, $\times$, $+$, $\bullet$, $*$, ., etc. Quand il ne peut pas y avoir de confusion, il est souvent courant de ne pas mettre de symbole et de noter tout simplement gg' le *produit* de deux éléments g et g' d'un groupe G. Surtout quand la loi est noté $\cdot$, l'inverse d'un élément g est noté g^{-1}. L'élément neutre peut aussi être noté e_G (s'il y a plusieurs groupes), 1 ou 1_G.

La notation additive $+$ n'est utilisée que pour les groupes *commutatifs*, c'est-à-dire les groupes dont deux éléments quelconques vérifient la relation $gg' = g'g$. Dans ce cas, l'élément neutre est noté 0 ou 0_G et l'inverse d'un élément g est notée $-g$. De tels groupes sont aussi appelés *abéliens*, en l'honneur du mathématicien norvégien Niels Henryk Abel.

Comme *exemples de groupes*, citons le groupe $\mathfrak{S}_n$ des permutations de l'ensemble $\{1, \ldots, n\}$ (la loi est la composition), le groupe $\mathbf{Z}$ des entiers relatifs (pour l'addition), l'ensemble des réels non nuls (pour la multiplication), tout espace vectoriel (pour l'addition), l'ensemble des matrices $n \times n$ inversibles (pour la multiplication), l'ensemble des matrices $n \times n$ orthogonales (encore pour la multiplication).

4.2. Sous-groupes

Si G et H sont deux groupes, un *homomorphisme de groupes* $f : G \to H$ est une application f telle que $f(gg') = f(g)f(g')$ pour tous g et g' dans G. Si $f : G \to H$ est un homomorphisme, $f(e_G) = e_H$ et, pour tout $g \in G$, $f(g^{-1}) = f(g)^{-1}$. Un *isomorphisme* est un homomorphisme bijectif.

Soit G un groupe. Une partie $H \subset G$ est un *sous-groupe* de G si $e_G \in H$, le produit de deux éléments quelconques de H est dans H, et l'inverse d'un élément de H est dans H. Alors, la loi de groupe de G se restreing en une loi interne sur H qui le munit d'une structure de groupe, d'élément neutre e_G. Si S est une partie d'un groupe G, $\langle S \rangle$ désigne le sous-groupe de G *engendré* par S : c'est le plus petit sous-groupe de G contenant S.

LEMME 4.2.1. — *Soit G un groupe et soit S une partie non-vide de G. Le sous-groupe $\langle S \rangle$ est l'ensemble de tous les produits $s_1 \dots s_n$, où $s_i \in S$ ou $s_i^{-1} \in S$ pour tout i.*

Démonstration. — Soit H l'ensemble de tous ces produits. Comme tout sous-groupe de G contenant S doit contenir ces produits, $H \subset \langle S \rangle$. Inversement, comme $S \subset H$, il suffit de montrer que H est un sous-groupe de G. L'inverse de d'un élément $s_1 \dots s_n$ de H est égal à $s_n^{-1} \dots s_1^{-1}$, donc appartient à H. De même, si $s_1 \dots s_n \in H$ et $t_1 \dots t_m \in H$, leur produit $s_1 \dots s_n t_1 \dots t_m$ appartient à H. Enfin, $e_G \in H$ (ou bien comme le produit d'une famille vide, ou bien en l'écrivant ss^{-1} pour $s \in S$). □

L'image $f(G)$ d'un morphisme de groupes $f : G \to H$ est un sous-groupe de H. L'image réciproque $f^{-1}(H')$ de tout sous-groupe $H' \subset H$ est un sous-groupe de G. En particulier, le *noyau* de f, formé des éléments $g \in G$ tels que $f(g) = e_H$, est un sous-groupe de G. Il est égal à $\{e_G\}$ si et seulement si f est injective.

Si un groupe G est fini, son *ordre* n'est autre que son cardinal. L'ordre d'un élément $g \in G$ est le plus petit entier $n \geqslant 1$ tel que $g^n = e$ (si un tel entier n'existe pas, g est dit d'ordre infini). C'est aussi l'ordre du sous-groupe $\langle g \rangle$ de G engendré par g. Remarquez aussi que $\langle g \rangle$ est isomorphe à $\mathbf{Z}/n\mathbf{Z}$ si g est d'ordre fini n, et est isomorphe à $\mathbf{Z}$ si g est d'ordre infini (*exercice*).

PROPOSITION 4.2.2 (Lagrange). — *Si G est un groupe fini et H un sous-groupe de G, l'ordre de H divise l'ordre de G. En particulier, l'ordre de tout élément de G divise l'ordre de G.*

On appelle alors *indice* de H dans G le quotient $\operatorname{card} G / \operatorname{card} H$; on le note $(G : H)$.

Démonstration. — Introduisons la relation sur G définie par $g \sim g'$ si et seulement s'il existe $h \in H$ tel que $g' = gh$. C'est une relation d'équivalence :

– réflexivité : comme $g = ge$ et $e \in H$, $g \sim g$ pour tout $g \in G$;

– symétrie : si $g \sim g'$, soit $h \in H$ tel que $g' = gh$. Alors, $g = g'h^{-1}$, d'où $g' \sim g$ puisque $h^{-1} \in H$;

– transitivité : si $g \sim g'$ et $g' \sim g''$, soit h et $h' \in H$ tels que $g' = gh$ et $g'' = g'h'$. On a alors $g'' = g(hh')$, donc $g \sim g''$ puisque H est un sous-groupe, donc $hh' \in H$.

La classe d'équivalence d'un élément $g \in G$ est l'ensemble gH des gh pour $h \in H$. Puisque G est un groupe, l'application $h \mapsto gh$ induit une bijection de H sur gH : toutes les classes d'équivalence sont en bijection. En particulier, si G est fini, *elles ont même cardinal,* celui de H.

L'ensemble G est réunion disjointe de ses classes d'équivalences pour cette relation. S'il y a N classes, on a donc $\operatorname{card} G = N \operatorname{card} H$ et le cardinal de H divise celui de G. □

Les classes gH introduites ci-dessus sont appelées *classes à droite* [1] de G selon H. On note G/H l'ensemble des classes à droite. On introduit de même une relation d'équivalence à gauche : $g \sim g'$ si et seulement si $g' = hg$. Les classes d'équivalence sont alors les parties Hg pour $g \in G$ et l'ensemble de ces classes, dites *à gauche* est noté $H\backslash G$. Dans le cas où G est fini, les deux ensembles G/H et $H\backslash G$ ont pour cardinal l'indice $(G : H)$ de H dans G.

La réciproque partielle du théorème de Lagrange est parfois attribuée à Cauchy.

PROPOSITION 4.2.3 (Lemme de Cauchy). — *Soit G un groupe fini et soit p un nombre premier qui divise l'ordre de G. Alors, il existe un élément de G qui est d'ordre p.*

Démonstration. — Le cas où G est abélien est une conséquence immédiate de l'exercice 1.15. On raisonne alors par récurrence sur l'ordre de G.

Notons Z le *centre* de G, ensemble des $g \in G$ tels que pour tout $h \in H$, $gh = hg$. Si p divise le cardinal de Z, on conclut ou bien par récurrence si $\operatorname{card} Z < \operatorname{card} G$, ou bien par le cas d'un groupe abélien si $\operatorname{card} Z = \operatorname{card} G$.

[1] Les classes à droites sont les orbites pour l'action de H par translation à droite dans G. Certains auteurs comme Lang [**7**] ou Bourbaki les appellent classes à gauche...

Si $x \in G$, notons $\mathcal{C}_x$ sa classe de conjugaison : c'est l'ensemble des gxg^{-1} pour g décrivant G. L'application de G dans $\mathcal{C}_x$ qui à g associe gxg^{-1} est surjective. Si $gxg^{-1} = hxh^{-1}$, alors $y = h^{-1}g$ vérifie $yx = xy$, et réciproquement. L'ensemble des tels y forme un sous-groupe G_x de G, le *centralisateur* de x dans G. Ainsi, le cardinal de $\mathcal{C}_x$ que multiplie celui de G_x est égal au cardinal de G :

$$\operatorname{card} \mathcal{C}_x = (G : G_x).$$

Écrivons que G est réunion de classes de conjugaison : soit $x_1, \dots, x_r \in G$ des éléments deux à deux non conjugués tels que tout élément de G soit conjugué à l'un des x_i. On a donc

$$\operatorname{card} G = \sum_{i=1}^{r} (G : G_{x_i}).$$

Remarquons qu'un élément de Z n'est conjugué qu'à lui-même. Cela signifie que dans cette somme, tous les éléments du centre apparaissent et l'on peut écrire

$$\operatorname{card} G = \operatorname{card} Z + \sum_{\substack{i=1 \\ x_i \notin Z}}^{r} (G : G_{x_i}).$$

Comme $\operatorname{card} G$ est multiple de p mais pas $\operatorname{card} Z$, l'un des $(G : G_{x_i})$ n'est pas multiple de p. Cela implique que p divise $\operatorname{card} G_{x_i}$. Puisque $x_i \notin Z$, $G_{x_i} \neq G$, donc $\operatorname{card} G_{x_i} < \operatorname{card} G$ et l'on conclut par récurrence. □

4.3. Opération d'un groupe sur un ensemble

Une *opération*, ou *action*, d'un groupe G sur un ensemble X est un homomorphisme de G dans le groupe $\mathfrak{S}(X)$ des permutations de X. Dans de nombreux cas, il n'y a pas de confusion sur l'homomorphisme dont il s'agit et on note $g \cdot x$, voire gx l'image de x par la permutation associée à g.

L'*orbite* $\mathcal{O}_x$ d'un élément $x \in X$ est l'ensemble des $g \cdot x$ pour g parcourant G. Le *stabilisateur* $\operatorname{Stab}_G(x)$ de x est l'ensemble des $h \in G$ tels que $hx = x$. C'est un sous-groupe de G. De plus, $gx = g'x$ si et seulement si on a $g'g^{-1}x = x$, soit $g'g^{-1} \in \operatorname{Stab}_G(x)$ ou encore $g' \in \operatorname{Stab}_G(x)$. Autrement dit, l'application $G \to X$ donnée par $g \mapsto gx$ induit une bijection entre l'ensemble $G/\operatorname{Stab}_G(x)$ des classes à droite suivant $\operatorname{Stab}_G(x)$ et l'orbite $\mathcal{O}_x$.

En particulier, si G est fini et opère sur un ensemble X,

$$\operatorname{card} \mathcal{O}_x = (G : \operatorname{Stab}_G(x)) = \frac{\operatorname{card} G}{\operatorname{card} \operatorname{Stab}_G(x)}$$

pour tout élément $x \in X$.

L'ensemble X est réunion des orbites de ses éléments. De plus, si x et y sont dans X, ou bien leurs orbites sont disjointes, ou bien elles sont égales. On peut alors choisir

un élément x_i par orbite, de sorte que X est la réunion disjointe des orbites des x_i. Si X est fini, son cardinal est en particulier la somme des cardinaux des orbites des x_i, c'est-à-dire

$$\boxed{\operatorname{card} X = \sum_i \operatorname{card} \mathcal{O}_{x_i} = \sum_i \frac{\operatorname{card} G}{\operatorname{card} \operatorname{Stab}_G(x_i)}.}$$

C'est *l'équation aux classes*. Elle est très importante car souvent on obtient rien qu'en la considérant (pour une action il est vraie bien choisie) des restrictions assez fortes sur les ordres de divers sous-groupes.

En fait, nous avons déjà fait usage de cette équation aux classes dans la preuve de la proposition 4.2.3, pour l'action par *conjugaison*, qui est l'action du groupe G sur lui-même définie par $g \cdot h = ghg^{-1}$. Le centralisateur d'un élément $g \in G$ n'est alors autre que le stabilisateur de g pour cette action.

Les translations à droite et à gauche sont deux autres exemples importants d'action d'un groupe G sur lui-même, définies respectivement par $g \cdot h = hg^{-1}$ et $g \cdot h = gh$. Une action d'un group se restreint naturellement en une action de n'importe lequel de ses sous-groupes. Ainsi, un sous-groupe $H \subset G$ agit sur G par translation à droite, ou à gauche. Il est facile de vérifier que les orbites de ces actions sont précisément les classes à droite, ou à gauche, de H dans G.

4.4. Sous-groupes distingués, groupes quotients

La notion de *sous-groupe distingué* que nous introduisons maintenant apparaît naturellement lorsqu'on veut faire des *quotients* dans la catégorie des groupes : n'importe quel sous-groupe n'est pas le noyau d'un homomorphisme de groupes. En effet, soit $\varphi : G \to G'$ un homomorphisme de groupes ; si g, $h \in G$, on a

$$\varphi(g^{-1}hg) = \varphi(g)^{-1}\varphi(h)\varphi(g).$$

En particulier, si $\varphi(h) = e$, on a

$$\varphi(g^{-1}hg) = \varphi(g)^{-1}e\varphi(g) = e.$$

D'où la définition :

DÉFINITION 4.4.1. — *Un sous-groupe H d'un groupe G est dit* distingué *si pour tout $g \in G$ et tout $h \in H$, $g^{-1}hg \in H$.*

PROPOSITION 4.4.2. — *Le noyau d'un homomorphisme de groupes est un sous-groupe distingué.*

Exemples 4.4.3. — *a*) Soit G un groupe. Les sous-groupes « triviaux » $\{1\}$ et G sont distingués dans G.

b) Si le groupe G est commutatif, tous ses sous-groupes sont distingués.

c) Soit Z l'ensemble des $g \in G$ tels que pour tout $h \in G$, $gh = hg$: le *centre* de G. C'est un sous-groupe distingué de G. En effet, si $h \in Z$ et $g \in G$, $g^{-1}hg = hg^{-1}g = h \in Z$.

d) Soit D le sous-groupe de G (*sous-groupe dérivé*) engendré par les expressions de la forme $g_1 g_2 g_1^{-1} g_2^{-1}$ avec g_1 et g_2 dans G (*commutateurs*). C'est un sous-groupe distingué de G. En effet, si $g \in G$ et $g_1 g_2 g_1^{-1} g_2^{-1}$ est un commutateur, on a

$$\begin{aligned} g^{-1}(g_1 g_2 g_1^{-1} g_2^{-1})g &= (g^{-1}g_1 g)(g^{-1}g_2 g)(g^{-1}g_1^{-1} g)(g^{-1}g_2^{-1} g) \\ &= (g^{-1}g_1 g)(g^{-1}g_2 g)(g^{-1}g_1 g)^{-1}(g^{-1}g_2 g)^{-1} \\ &= h_1 h_2 h_1^{-1} h_2^{-1} \end{aligned}$$

avec $h_1 = g^{-1}g_1 g$ et $h_2 = g^{-1}h_1 g$, donc est un commutateur. Notons D_0 l'ensemble des commutateurs dans G. Un élément d de D s'écrit $d_1 \dots d_n$ où les d_i sont des commutateurs (l'inverse d'un commutateur est encore un commutateur). Alors,

$$g^{-1} d g = (g^{-1} d_1 g) \dots (g^{-1} d_n g)$$

est d'après la remarque ci-dessus un produit de commutateurs, donc appartient à D, cqfd.

Exercice 4.4.4. — Montrer que $H \subset G$ est distingué si et seulement si $gH = Hg$.

La construction du *groupe quotient* d'un groupe par un sous-groupe distingué montre inversement que tout sous-groupe distingué est le noyau d'un homomorphisme surjectif. Soit G/H l'ensemble des classes à droite modulo H. On définit une loi interne sur G/H : si g et g' sont dans G, h et h' dans H, on a

$$(gh)(g'h') = gg'(g')^{-1} h g' h',$$

et, puisque H est distingué dans G, $(g')^{-1} h g'$ appartient à H, et donc $(g')^{-1} h g' h'$ aussi. Ainsi, la classe à droite de gg' modulo H ne dépend que des classes à droite de g et g' et l'on peut poser

$$(gH) * (g'H) = (gg')H.$$

Une fois établi que cette définition a un sens, c'est un pure exercice de routine que de vérifier qu'elle munit G/H d'une structure de groupe d'élément neutre $H = eH$, et que l'application $G \to G/H$ qui à $g \in G$ associe sa classe à droite gH est un homomorphisme surjectif de groupes. Par construction, son noyau est H.

La vertu des groupes quotients est aussi de jouir d'un *théorème de factorisation* (encore une « propriété universelle ») :

THÉORÈME 4.4.5. — *Soit G un groupe, H un sous-groupe distingué de G. Soit $f : G \to G'$ un homomorphisme de groupes dont le noyau contient H. Alors, il existe un unique homomorphisme de groupes $\varphi : G/H \to G'$ tel que pour tout $g \in G$, $\varphi(\pi(g)) = f(g)$. (Autrement dit, $\varphi \circ \pi = f$.)*

Le noyau de φ est égal à $\pi(\operatorname{Ker} f)$. Ainsi, φ est injectif si et seulement si $\operatorname{Ker} f = H$. *Enfin, φ est surjectif si et seulement si f l'est.*

Démonstration. — Si $\pi(g) = \pi(g')$, il existe $h \in H$ tel que $g = g'h$. Ainsi, $f(g) = f(g'h) = f(g')f(h) = f(g')$ puisque $H \subset \operatorname{Ker} f$. Cela signifie que l'application de G/H dans G' qui associe à une classe de G/H l'image par f de n'importe lequel de ses membres est bien définie. Notons φ cette application ; elle vérifie $\varphi \circ \pi = f$ par construction.

Il est alors tout aussi routinier qu'avant de vérifier que $\varphi\colon G/H \to G'$ est un homomorphisme de groupes. Une classe gH appartient au noyau de φ si et seulement si $f(g) = e$, c'est-à-dire si et seulement si $g \in \operatorname{Ker} f$. Ainsi, $\operatorname{Ker}\varphi = \pi(\operatorname{Ker} f)$. Dire que φ est injective signifie alors que $g \in \operatorname{Ker} f$ équivaut à $g \in H$, c'est-à-dire $H = \operatorname{Ker} f$. Enfin, si f est surjective, il est immédiat que φ l'est et réciproquement, si φ est surjective, f l'est aussi car π est surjectif. □

PROPOSITION 4.4.6. — *Soit G un groupe, H un sous-groupe distingué de G et $\pi\colon G \to G/H$ l'homomorphisme canonique de noyau H.*

a) *Si K est un sous-groupe de G/H, $\pi^{-1}(K)$ est un sous-groupe de G contenant H. Réciproquement, tout sous-groupe de G contenant H est de cette forme pour un unique sous-groupe de G/H, à savoir $\pi(H)$.*

b) *Si K est un sous-groupe distingué de G/H, alors l'application naturelle $G \to G/H \to (G/H)/K$ a pour noyau $\pi^{-1}(K)$ et induit un isomorphisme*

$$G/\pi^{-1}(K) \simeq (G/H)/K.$$

Démonstration. — *a*) Comme toute image réciproque d'un sous-groupe, $\pi^{-1}(K)$ est un sous-groupe de G. Il contient $\pi^{-1}(e) = H$. Inversement, soit K un sous-groupe de G contenant H. Alors, $\pi(K)$ est un sous-groupe de G/H et $\pi^{-1}(\pi(K))$ contient K. Pour montrer l'autre inclusion, soit $g \in \pi^{-1}(\pi(K))$. Alors $\pi(g) \in \pi(K)$, donc il existe $k \in K$ tel que $\pi(g) = \pi(k)$. Par suite, $h = gk^{-1}$ est un élément de $\operatorname{Ker}\pi = H$. Comme $H \subset K$, $g = hk \in K$.

b) L'application $f\colon G \to (G/H)/K$ est un morphisme de groupes, surjectif, comme composition de deux tels homomorphismes. De plus, un élément $g \in G$ apartient au noyau de f si et seulement si $\pi(g)$ appartient au noyau K du morphisme $G/H \to (G/H)/K$, si bien que $\operatorname{Ker} f = \pi^{-1}(K)$. Par suite, f induit un isomorphisme $G/\pi^{-1}(K) \simeq (G/H)/K$. □

DÉFINITION 4.4.7. — *On dit qu'un groupe G est* simple *s'il n'a pas de sous-groupe distingué non trivial.*

4.5. Groupes résolubles, nilpotents

Soit G un groupe. Si N est un sous-groupe distingué de G, on peut en un certain sens « approcher » la structure de groupe de G par la combinaison de celles de N et de G/N. Plus généralement, il peut être utile d'introduire des *suites distinguées* dans G, c'est-à-dire des suites de sous-groupes

$$\{1\} = G_0 \subset G_1 \subset \cdots \subset G_{n-1} \subset G_n = G$$

de G, telles que pour tout entier i tel que $1 \leqslant i \leqslant n$, G_{i-1} soit un sous-groupe distingué de G_i.

DÉFINITION 4.5.1. — *On dit qu'un groupe G est* résoluble *s'il possède une suite distinguée*

$$\{1\} = G_0 \subset G_1 \subset \cdots \subset G_{n-1} \subset G_n = G$$

telle que le groupe G_i/G_{i-1} soit commutatif pour tout i, $1 \leqslant i \leqslant n$.

Du point de vue de l'algèbre, c'est une notion très robuste :

PROPOSITION 4.5.2. — *Soit G un groupe, H un sous-groupe de G.*

a) *Si G est résoluble, H est résoluble ;*
b) *Si G est résoluble et si H est distingué, G/H est résoluble ;*
c) *Si H est résoluble, distingué et si G/H est résoluble, alors G est résoluble.*

Démonstration. — *a*) Considérons une suite de sous-groupes $G_0 \subset \ldots G_n$ comme dans la définition et posons $H_i = H \cap G_i$. Les H_i définissent une suite de sous-groupes de H. De plus, H_{i-1} est distingué dans H_i : si $g \in H_i$ et $h \in H_{i-1}$, $g^{-1}hg$ appartient à G_{i-1} (car $g \in G_i$, $h \in G_{i-1}$ et G_{i-1} est distingué dans G_i) et appartient aussi à H (car g et h appartiennent à H), donc appartient à H_{i-1}. Enfin, le groupe quotient H_i/H_{i-1} est commutatif. Pour le voir, considérons l'homomorphisme « naturel »

$$H_i \to G_i \to G_i/G_{i-1}$$

composé de l'inclusion $H_i \subset G_i$ et de la projection de G_i vers G_i/G_{i-1}. Son noyau est l'ensemble des $h \in H_i$ tels que $h \in G_{i-1}$, donc est H_{i-1}. Il en résulte par passage au quotient un homomorphisme *injectif*

$$H_i/H_{i-1} \to G_i/G_{i-1}.$$

Comme G_i/G_{i-1} est un groupe commutatif, tous ses sous-groupes le sont aussi et H_i/H_{i-1} étant isomorphe à un de ces sous-groupes est commutatif. Cela montre que H est résoluble.

b) Supposons de plus que H est distingué et montrons que G/H est résoluble. Pour tout i, soit H_i le sous-groupe engendré par H et G_i. On obtient ainsi une suite de sous-groupes de G contenant H :

$$H = H_0 \subset H_1 \subset \cdots \subset H_n = G$$

et pour tout i, H_{i-1} est distingué dans H_i. Considérons l'homomorphisme naturel

$$G_i \to H_i \to H_i/H_{i-1}.$$

Il est surjectif : un élément de H_i s'écrit

$$g_1 h_1 \dots g_m h_m$$

avec des $g_j \in G_i$ et $h_j \in H$. Puisque H_{i-1} contient H et que H est distingué dans G, donc dans H_i, sa classe dans H_i/H_{i-1} est égale à celle de $g_1 \dots g_m$ qui appartient à G_i. De plus, son noyau contient G_{i-1} si bien que G_i/G_{i-1} s'envoie surjectivement sur H_i/H_{i-1} qui est donc un quotient du groupe commutatif G_i/G_{i-1}. Il est donc en particulier commutatif. Alors, pour tout i, H_i définit un sous-groupe $\overline{H}_i = H_i/H$ de G/H ; $\overline{H}_{i-1}$ est distingué dans $\overline{H}_i$ et

$$\overline{H}_i/\overline{H}_{i-1} = H_i/H_{i-1},$$

ce qui montre que G/H est résoluble.

c) Puisque H est résoluble, il existe une suite de sous-groupes

$$\{1\} = H_0 \subset H_1 \subset \cdots \subset H_m = H$$

dont les quotients successifs sont commutatifs. Puisque G/H est résoluble, il existe une suite analogue de sous-groupes dans G/H :

$$\{1\} = K_0 \subset K_1 \subset \cdots \subset K_n = G/H.$$

Considérons alors la suite de sous-groupes de G :

$$\{1\} = H_0 \subset H_1 \subset \cdots \subset H_m = H = \pi^{-1}(K_0) \subset \pi^{-1}(K_1) \subset \cdots \subset \pi^{-1}(K_n) = G.$$

Chaque sous-groupe est distingué dans le suivant et les quotients successifs sont commutatifs : c'est clair pour les m premiers, et pour les n derniers, remarquons que si K_{i-1} est distingué dans K_i, l'homomorphisme composé

$$\pi^{-1}(K_i) \xrightarrow{\pi} K_i \to K_i/K_{i-1}$$

est surjectif et a pour noyau $\pi^{-1}(K_{i-1})$. Ainsi, $\pi^{-1}(K_{i-1})$ est distingué dans $\pi^{-1}(K_i)$ et

$$\pi^{-1}(K_i)/\pi^{-1}(K_{i-1}) \simeq K_i/K_{i-1}$$

qui est commutatif, d'où l'assertion. □

Pour les groupes finis, être résoluble coïncide avec une notion apparemment plus restrictive.

PROPOSITION 4.5.3. — *Soit G un groupe fini. Alors, G est résoluble si et seulement s'il possède une suite distinguée*

$$\{1\} = G_0 \subset G_1 \subset \cdots \subset G_{n-1} \subset G_n = G$$

telle que pour tout $i \in \{1,\dots,n\}$, le groupe G_i/G_{i-1} soit cyclique.

En particulier, si G est un groupe fini résoluble, il existe un sous-groupe distingué H de G tel que G/H soit isomorphe au groupe $\mathbf{Z}/d\mathbf{Z}$, pour un certain entier $d \geqslant 2$.

Démonstration. — Comme les groupes cycliques sont commutatifs, un groupe satisfaisant ce critère est résoluble. Réciproquement, montrons d'abord qu'un groupe fini commutatif possède une telle suite distinguée. Soit G un groupe fini abélien, il existe des éléments $x_1,\dots,x_r \in G$ tels que $G = \langle x_1,\dots,x_r\rangle$ (prendre par exemple tous les éléments de G). Tout sous-groupe d'un groupe commutatif étant distingué, la suite de sous-groupe

$$\{e_G\} \subset \langle x_1\rangle \subset \rangle x_1, x_2\rangle \subset \cdots \subset \langle x_1,\dots,x_r\rangle = G$$

est distinguée. De plus, si $1 \leqslant i \leqslant r$, le quotient $\langle x_1,\dots,x_i\rangle/\langle x_1,\dots,x_{i-1}\rangle$ est engendré par x_i donc est cyclique. Cela montre que la proposition est vraie pour un groupe abélien fini.

Montrons par récurrence qu'elle est vraie pour un groupe résoluble fini quelconque en supposant qu'elle vaut pour tout groupe fini résoluble de cardinal $< \operatorname{card} G$. Par hypothèse, G possède un sous-groupe distingué non trivial H tel que G/H soit commutatif. On peut alors trouver une suite distinguée dans H, à quotients cycliques,

$$\{e_G\} \subset G_1 \subset \cdots \subset G_m = H.$$

Par le cas abélien, le groupe G/H possède une suite distinguée à quotients cycliques, soit

$$\{e_{G/H}\} = K_0 \subset K_1 \subset \cdots \subset K_r = G/H.$$

Pour $1 \leqslant i \leqslant r$, définissons G_{m+i} comme l'image réciproque de K_i dans G. Alors, G_{m+i-1} est distingué dans G_{m+i} et le quotient G_{m+i}/G_{m+i-1}, isomorphe à K_i/K_{i-1}, est cyclique. La suite de sous-groupes

$$\{e_G\} \subset G_1 \subset \cdots \subset G_m \subset G_{m+1} \subset \cdots \subset G_{m+r} = G$$

est une suite distinguée satisfaisant la condition de l'énoncé. □

Une définition voisine donne un résultat un peu différent :

DÉFINITION 4.5.4. — *On dit qu'un groupe G est* nilpotent *s'il possède une suite distinguée*

$$\{1\} = G_0 \subset G_1 \subset \cdots \subset G_{n-1} \subset G_n = G$$

tels que pour tout i, G_i est distingué dans G et G_{i+1}/G_i est contenu dans le centre de G/G_i.

Un groupe nilpotent est automatiquement résoluble.

4.6. Groupe symétrique, alterné

Rappelons que $\mathfrak{S}_n$ désigne le groupe des permutations de l'ensemble $\{1;2;\dots;n\}$. Il est de cardinal $n!$. Une transposition de $\mathfrak{S}_n$ est une permutation qui échange deux éléments distincts et fixe tous les autres. Le cycle $(i_1 \dots i_m)$ est la permutation telle que $i_1 \mapsto i_2$, …, $i_{m-1} \mapsto i_m$ et $i_m \mapsto i_1$, tous les autres étant fixés. Sa longueur est m. (Un cycle de longueur 2 est donc une transposition.)

Il est facile de savoir si deux éléments du groupe symétrique $\mathfrak{S}_n$ sont conjugués. Rappelons que tout élément σ de $\mathfrak{S}_n$ se décompose en un produit de cycles de supports disjoints. On associe alors à σ la *partition* $\pi(\sigma)$ de n formée par la suite des longueurs des cycles qui interviennent, ordonnée par ordre croissant.

PROPOSITION 4.6.1. — *Deux permutations sont conjuguées si et seulement si elles définissent la même partition.*

En particulier, les transpositions sont toutes conjuguées entre elles, de même que les 3-cycles.

Démonstration. — Soit $(m_1;\dots;m_p)$ la partition associée à σ et à τ. On peut ainsi décomposer

$$\sigma = (i_{1,1} \dots i_{1,m_1}) \dots (i_{p,1} \dots, i_{p,m_p})$$

et pareil pour τ avec des entiers $j_{k,r}$. Soit γ la permutation qui envoie $i_{k,r}$ sur $j_{k,r}$. Alors, si $1 \leqslant r < m_k$, on a

$$\gamma\sigma\gamma^{-1}(j_{k,r}) = \gamma\sigma(i_{k,r}) = \gamma(i_{k,r+1}) = j_{k,r+1}$$

tandis que

$$\gamma\sigma\gamma^{-1}(j_{k,m_k}) = \gamma\sigma(i_{k,m_k}) = \gamma(i_{k,1}) = j_{k,1}.$$

ce qui montre que $\gamma\sigma\gamma^{-1} = \tau$, et donc que σ et τ sont conjuguées.

Réciproquement, c'est en fait le même calcul : si σ est comme ci-dessus et si γ est une permutation de $\mathfrak{S}_n$, on a

$$\gamma\sigma\gamma^{-1} = (\gamma(i_{1,1}) \dots \gamma(i_{1,m_1})) \dots (\gamma(i_{p,1}) \dots \gamma(i_{p,m_p}));$$

c'est une décomposition en cycles de supports disjoints et de longueurs $m_1, \dots, m_p$ ce qui montre que deux éléments conjugués ont même partition. □

Pour établir d'autres propriétés du groupe symétrique, nous aurons besoin de savoir qu'il est engendré par des familles spécifiques.

PROPOSITION 4.6.2. — *Le groupe $\mathfrak{S}_n$ est engendré par (au choix) :*

a) *les permutations $(i\ j)$;*

b) *les permutations* $(i\ i+1)$ *;*
c) *la permutation* $(1\,2)$ *et le cycle* $(1\,2\,\ldots\,n)$.

Démonstration. — *a*) On démontre ceci par récurrence sur l'entier k tel que σ fixe $k,\ k+1,\ \ldots,\ n$. Pour $k=1$, σ est l'identité donc c'est clair. Supposons que σ fixe $k+1,\ldots,n$, posons $j=\sigma(k)$ et considérons le produit $\tau=(j\ k)\circ\sigma$. C'est une permutation qui fixe $k+1,\ldots,n$ et telle que $\tau(k)=(j\ k)(\sigma(k))=(j\ k)(j)=k$. Par récurrence, τ appartient au sous-groupe engendré par toutes les transpositions, donc σ aussi.

b) Soit H le sous-groupe engendré par ces transpositions $(i\ i+1)$. En considérant pour $p<m$ dans $\{1;\ldots;n\}$ le produit

$$(m-1\ m)\circ(m-2\ m-1)\circ(p\ p+1),$$

on voit que H contient un élément τ tel que $\tau(p)=m$ et qui fixe les éléments $m+1,\ldots,n$. Le même argument qu'au *a*) montre alors que $H=\mathfrak{S}_n$.

c) Notons $\tau=(1\,2)$ et γ le cycle $(1\,2\,\ldots\,n)$ et H le sous-groupe de $\mathfrak{S}_n$ engendré par τ et γ. D'après un calcul que nous avons fait dans la démonstration de la proposition 4.6.1,

$$\gamma\tau\gamma^{-1}=\gamma(1\,,\,2)\gamma^{-1}=(\gamma(1)\,,\,\gamma(2))=(2\,,\,3),$$

et de même, $\gamma^{i-1}\tau\gamma^{1-i}=(i\,,\,i+1)$ pour tout entier i tel que $1\leqslant i\leqslant n-1$. Tous ces éléments appartiennent à H. D'après *b*), $H=\mathfrak{S}_n$. □

Nous allons en déduire la proposition intéressante qui montre qu'essentiellement, le seul homomorphisme de $\mathfrak{S}_n$ dans un groupe commutatif est fourni par la signature.

Pour être complet, rappelons la definition de la signature d'une permutation. La méthode la plus facile consiste à poser

$$\varepsilon(\sigma)=\prod_{1\leqslant i<j\leqslant n}\frac{\sigma(i)-\sigma(j)}{i-j}.$$

C'est un nombre rationnel de valeur absolue 1 (toutes les paires $\{i,j\}$ apparaissent au numérateur et au dénominateur), donc vaut ±1. Plus précisément, $\varepsilon(\sigma)=(-1)^{i(\sigma)}$, où $i(\sigma)$ désigne le nombre d'inversions de la permutation σ, c'est-à-dire le nombre de couples (i,j) avec $i<j$ tels que $\sigma(i)>\sigma(j)$.

On peut montrer directement que $\varepsilon(\sigma\tau)=\varepsilon(\sigma)\varepsilon(\tau)$, mais nous l'avons quasiment fait p. 64 du paragraphe 3.4. Considérons en effet le polynôme $d=\prod_{i<j}(X_i-X_j)$. Le même calcul que dans *loc. cit.*, où ${}^{\sigma}f=f(X_{\sigma(1)},\ldots,X_{\sigma(n)})$ désigne l'action d'une permutation $\sigma\in\mathfrak{S}_n$ sur un polynôme $f\in\mathbf{Q}[X_1,\ldots,X_n]$ montre que l'on a ${}^{\sigma}d=\varepsilon(\sigma)d$. Le fait que l'on a une action entraîne que ε est un morphisme de groupes, $\mathfrak{S}_n\to\{\pm1\}$.

Une permutation σ est dite paire ou impaire, suivant que $\varepsilon(\sigma)=1$ or -1. Les permutations paires forment un sous-groupe $\mathfrak{A}_n\subset\mathfrak{S}_n$, appelé *groupe alterné*. C'est le

noyau de ε, donc un sous-groupe distingué. La permutation $\sigma = (1,2)$ n'a qu'une inversion (pour le couple $(1,2)$), donc $\varepsilon(\sigma) = -1$. En particulier, la signature est un homomorphisme surjectif et le groupe alterné est d'indice 2 dans le groupe symétrique. Puisque deux transpositions sont conjuguées, la signature d'une transposition quelconque vaut -1.

PROPOSITION 4.6.3. — *Soit A un groupe commutatif et $f\colon \mathfrak{S}_n \to A$ un homomorphisme de groupes. Si $f \neq 0$ (l'homomorphisme qui envoie toute permutation sur l'élément neutre de A), il existe un unique élément $a \in A \neq \{0\}$ tel que $2a = 0$ et tel que pour tout $\sigma \in \mathfrak{S}_n$, $f(\sigma) = 0$ si $\varepsilon(\sigma) = 1$ et $f(\sigma) = a$ si $\varepsilon(\sigma) = -1$, où $\varepsilon(\sigma)$ désigne la signature de la permutation σ.*

Démonstration. — Puisque les transpositions sont conjuguées dans $\mathfrak{S}_n$ et que A est commutatif, elles ont même image par f. Notons a cette image. Puisqu'une transposition τ vérifie $\tau^2 = \mathrm{id}$, on a $2a = 2f(\tau) = f(\tau^2) = f(\mathrm{id}) = 0$. D'autre part, si un élément σ de $\mathfrak{S}_n$ est produit de m transpositions $\tau_1, \ldots, \tau_m$, on aura $f(\sigma) = f(\tau_1) + \cdots + f(\tau_m) = ma$. De même, on a $\varepsilon(\sigma) = (-1)^m$. Ainsi, si $\varepsilon(\sigma) = 1$, m est pair et $f(\sigma) = 0$, tandis que si $\varepsilon(\sigma) = -1$, m est impair et $f(\sigma) = a$. □

COROLLAIRE 4.6.4. — *Le sous-groupe dérivé de $\mathfrak{S}_n$ est le groupe alterné $\mathfrak{A}_n$, noyau de la signature.*

Démonstration. — Tout commutateur étant une permutation paire, le sous-groupe dérivé $D(\mathfrak{S}_n)$ est contenu dans $\mathfrak{A}_n$. Inversement, comme le sous-groupe dérivé est distingué dans $\mathfrak{S}_n$, on peut considérer le groupe quotient $A = \mathfrak{S}_n / D(\mathfrak{S}_n)$. Tout commutateur dans A est l'image d'un commutateur dans $\mathfrak{S}_n$ par l'homomorphisme surjectif canonique $\mathfrak{S}_n \to A$. Par suite, tout commutateur dans A est trivial et le groupe A est abélien. D'après la proposition 4.6.3, l'application map $\mathfrak{S}_n \to A$ se factorise par la signature, donc son noyau $D(\mathfrak{S}_n)$ contient $\mathfrak{A}_n$. On a donc l'égalité voulue. We therefore have equality. □

Nous allons maintenant jouer au même jeu dans le groupe alterné. Cette fois-ci, tout va reposer sur trois propriétés :

– les 3-cycles engendrent $\mathfrak{A}_n$;
– le carré du 3-cycle (123) est égal au 3-cycle (132) ;
– si $n \geqslant 5$, les 3-cycles sont conjugués dans $\mathfrak{A}_n$. (Ils le sont bien sûr toujours dans $\mathfrak{S}_n$.)

LEMME 4.6.5. — *Le groupe $\mathfrak{A}_n$ est engendré par les cycles de longueur 3.*

Démonstration. — Les transpositions engendrent $\mathfrak{S}_n$ et tout élément de $\mathfrak{A}_n$ est produit de transpositions, en nombre nécessairement pair. Il suffit ainsi de montrer que

tout produit de deux transpositions est un produit de 3-cycles. Or, la formule

$$(12)(13) = (132)$$

traite le cas de deux transpositions ayant un point commun, tandis que la formule

$$(12)(34) = (12)(23)(23)(34) = (123)(243)$$

règle celui de deux transpositions de supports disjoints. □

PROPOSITION 4.6.6. — *Si $n \geqslant 5$, tout homomorphisme du groupe alterné dans un groupe commutatif est nul.*

Démonstration. — Comme annoncé, montrons que les 3-cycles $\gamma = (123)$ et $\delta = (abc)$ sont conjugués dans $\mathfrak{A}_n$ dès que $n \geqslant 5$. Considérons une permutation quelconque σ de $\mathfrak{S}_n$ telle que $\sigma(1) = a$, $\sigma(2) = b$ et $\sigma(3) = c$. Conformément aux calculs faits plus haut pour le conjugué d'une permutation par une autre, cette transposition conjugue les deux 3-cycles :

$$\sigma\gamma\sigma^{-1} = \delta.$$

Si σ appartient à $\mathfrak{A}_n$, les deux 3-cycles sont conjugués dans $\mathfrak{A}_n$. Dans le cas contraire, montrons comment modifier σ *sous l'hypothèse que* $n \geqslant 5$. L'idée est simple : il suffit de multiplier σ par une transposition τ telle que $\tau\gamma\tau^{-1} = \gamma$. Par exemple, $\tau = (45)$ convient. (C'est là qu'on utilise que $n \geqslant 5$: on a dû faire intervenir deux éléments hors du 3-cycle (123).) Alors, on a

$$(\sigma\tau)\gamma(\sigma\tau)^{-1} = \sigma(\tau\gamma\tau^{-1})\sigma^{-1} = \sigma\gamma\sigma^{-1} = \delta,$$

ce qui prouve que γ et δ sont conjugués par $\sigma\tau \in \mathfrak{A}_n$.

Supposons maintenant $n \geqslant 5$ et considérons un homomorphisme $f : \mathfrak{A}_n \to A$ où A est un groupe commutatif. Puisque tous les 3-cycles sont conjugués, ils ont même image a dans A. D'autre part, le carré du 3-cycle (123) est le 3-cycle (132). Cela montre que $f((132)) = 2f((123))$, d'où $a = 2a$ et $a = 0$. Ainsi, f est nul sur les 3-cycles. Or, ceux-ci engendrent $\mathfrak{A}_n$. Donc $f = 0$. □

On en déduit immédiatement les deux corollaires.

COROLLAIRE 4.6.7. — *Si $n \geqslant 5$, le sous-groupe dérivé de $\mathfrak{A}_n$ est encore $\mathfrak{A}_n$.*

COROLLAIRE 4.6.8. — *Si $n \geqslant 5$, $\mathfrak{A}_n$ et $\mathfrak{S}_n$ ne sont pas résolubles.*

Remarque 4.6.9. — On peut démontrer plus généralement que pour tout entier $n \geqslant 5$, le groupe $\mathfrak{A}_n$ est simple, voir l'exercice 4.16.

4.7. Groupes de matrices

Soit k un corps. On note T le sous-groupe des matrices diagonales dans $\mathrm{GL}(n,k)$, B celui des matrices triangulaires supérieures et U celui des matrices triangulaires supérieures n'ayant que des 1 sur la diagonale.

PROPOSITION 4.7.1. — *Le groupe U est nilpotent. Le groupe dérivé de B est contenu dans U. En particulier, B est résoluble.*

Démonstration. — Un calcul montre que $D(B) \subset U$. Par suite, si on montre que U est nilpotent, U est résoluble, $D(B)$ aussi comme sous-groupe d'un groupe résoluble, donc B aussi.

Montrons que U est nilpotent. Soit $(C^m)_m$ la suite centrale descendante de U : $C^0 = U$ et $C^{m+1} = [C^m, U]$ est le sous-groupe engendré par les commutateurs $cuc^{-1}u^{-1}$ avec $u \in U$ et $c \in C^m$. On identifie matrices $n \times n$ et endomorphismes de k^n. On note $(e_1, \dots, e_n)$ la base canonique et pour $1 \leqslant i \leqslant n$, $V_i = \mathrm{vect}(e_1, \dots, e_i)$, $V_i = 0$ pour $i \leqslant 0$.

Soit pour $m \geqslant 0$, N_m l'ensemble des endomorphismes u de k^n tels que pour tout i, $u(V_i) \subset V_{i-m}$. Si $u \in N_m$ et $v \in N_p$, alors $u \circ v \in N_{m+p}$. Comme $N_m = 0$ pour $m \geqslant n$, en particulier, les endomorphismes de N_m sont nilpotents dès que $m \geqslant 1$.

Montrons par récurrence sur m que si une matrice c appartient à C^m, alors il existe $\gamma \in N_{m+1}$ tel que $c = \mathrm{id} + \gamma$. Il en résultera que $C^n = \{\mathrm{id}\}$. En particulier, U est nilpotent.

C'est vrai pour $m = 0$ par définition de U. Si c'est vrai pour $m - 1 \geqslant 0$, considérons un commutateur $cgc^{-1}g^{-1}$ avec $c \in C^{m-1}$ et $g \in U$. Écrivons $c = \mathrm{id} + u$ avec $u \in N_m$ et $g = \mathrm{id} + v$ avec $v \in N_1$. Alors, on a

$$g^{-1} = (\mathrm{id} + v)^{-1} = \mathrm{id} - v + v^2 - \dots \quad \text{et} \quad c^{-1} = (\mathrm{id} + u)^{-1} = \mathrm{id} - u + u^2 - \dots.$$

En particulier, il existe $v' \in N_2$ et $u' \in N_{2m}$ tels que

$$g^{-1} = \mathrm{id} - v + v' \quad \text{et} \quad c^{-1} = \mathrm{id} - u + u'.$$

Alors,

$$\begin{aligned} c^{-1}g^{-1} &= (\mathrm{id} - u + u')(\mathrm{id} - v + v') \\ &= \mathrm{id} - u + u' - v + uv - u'v + v' - uv' + u'v' \\ &= \mathrm{id} - u - v + \text{élément } w \text{ de } N_{m+1} \end{aligned}$$

(on a utilisé que $N_{2m} \subset N_{m+1}$ puisque $m \geqslant 1$) tandis que

$$cg = (\mathrm{id} + u)(\mathrm{id} + v) = \mathrm{id} + u + v + \text{élément } w' \text{ de } N_{m+1}.$$

En faisant le produit, on voit que

$$\begin{aligned} cgc^{-1}g^{-1} &= (\mathrm{id} + u + v + w')(\mathrm{id} - u - v + w) \\ &= \mathrm{id} + w + w' + (u + v + w')(-u - v + w) \end{aligned}$$

est la somme de id et d'un élément de N_{m+1}. La proposition est ainsi démontrée. □

La réciproque suivante est fondamentale pour la théorie algébrique des équations différentielles.

THÉORÈME 4.7.2 (Lie, Kolchin). — *Tout sous-groupe connexe résoluble de* $\mathrm{GL}(n,\mathbf{C})$ *est conjugué à un sous-groupe de* B.

La démonstration utilise le lemme (classique) suivant.

LEMME 4.7.3. — *Toute famille de matrices qui commutent deux à deux peut être mise sous-forme triangulaire dans une base convenable. En particulier, tout sous-groupe commutatif de* $\mathrm{GL}(n,\mathbf{C})$ *est conjugué à un sous-groupe de* B.

Démonstration. — On raisonne par récurrence sur l'entier n. Le cas $n=1$ étant trivial, supposons $n>1$.

Soit G une famille de matrices $n\times n$ à coefficients complexes qui commutent deux à deux. Si tout élément de G est scalaire, le résultat est manifestement vrai. Sinon, considérons un élément h de G distinct de l'identité et soit V un espace propre de h, de valeur propre $\lambda\in\mathbf{C}$. (En particulier, $d=\dim V\in\{1;\dots;n-1\}$.) Pour tout $g\in G$, on a

$$hg(v)=gh(v)=g(\lambda v)=\lambda g(v),$$

donc $g(v)\in V$. Ainsi, G laisse stable V. Cela signifie qu'il existe une base $(e_1,\dots,e_n)$ de $\mathbf{C}^n$ telle que $(e_1,\dots,e_d)$ soit une base de V et dans laquelle les matrices de G s'écrivent par blocs $\left(\begin{smallmatrix} g_1 & * \\ 0 & g_2\end{smallmatrix}\right)$ où $g_1\in\mathrm{GL}(d,\mathbf{C})$ et $g_2\in\mathrm{GL}(n-d,\mathbf{C})$. Les matrices g_1 commutent deux à deux (calcul par bloc du produit de deux matrices), de même que les matrices g_2. Par récurrence, il existe une base $f_1,\dots,f_d$ de $\mathrm{vect}(e_1,\dots,e_d)$ dans laquelle toutes ces matrices g_1 soient triangulaires supérieures. De même, il existe une base $f_{d+1},\dots,f_n$ de $\mathrm{vect}(e_{d+1},\dots,e_n)$ dans laquelle toutes les matrices g_2 soient triangulaires supérieures. Dans la base $(f_1?\dots,f_n)$ de $\mathbf{C}^n$, toutes les matrices de G sont triangulaires supérieures. □

Démonstration du théorème de Lie-Kolchin. — Soit V un sous-espace vectoriel de $\mathbf{C}^n$ qui est stable par tous les éléments de G, avec $0<\dim V<n$. Alors, on peut faire un changement de base de $\mathbf{C}^n$ qui commence par une base de V. Dans cette base, les éléments de G ont une matrice triangulaire par blocs : $\left(\begin{smallmatrix} g_1 & u \\ 0 & g_2\end{smallmatrix}\right)$. L'application $G\to\mathrm{GL}(V)$ telle que $g\mapsto g_1$ a pour image un sous-groupe résoluble de G. Quitte à bien choisir la base de V, on peut supposer par récurrence que toutes les matrices g_1 sont triangulaires supérieures. De même, quitte à bien choisir une base de $\mathbf{C}^n/V$, on peut supposer que toutes les matrices g_2 sont triangulaires supérieures. Dans la base de $\mathbf{C}^n$ obtenue, les matrices de G sont triangulaires supérieures.

Cette réduction nous permet de supposer (par récurrence sur n) qu'*aucun sous-espace vectoriel de* $\mathbf{C}^n$ *(sauf* 0 *et* $\mathbf{C}^n$*) n'est stable par tous les éléments de* G. On va montrer que cela implique $n=1$.

Raisonnons maintenant par récurrence sur le plus petit entier m tel que $D^m(G)=\{1\}$.

Si $D^1(G)=\{1\}$), *i.e.* si G est commutatif, le lemme 4.7.3 affirme que l'on peut choisir une base de $\mathbf{C}^n$ dans laquelle la matrice de tout élément de G est triangulaire supérieure. Si $P\in \mathrm{GL}(n,\mathbf{C})$ est la matrice de changement de bases correspondante, on a ainsi $P^{-1}GP\subset B$. La droite $\mathbf{C}e_1$ étant stable par P, la droite $\mathbf{C}(Pe_1)$ est stable par G, d'où $n=1$.

Supposons maintenant que l'on ait démontré que $n=1$ si $D^{m-1}(G)=\{1\}$ et considérons un sous-groupe $G\subset \mathrm{GL}(n,\mathbf{C})$ un sous-groupe tel que $D^m(G)=\{1\}$ mais $H=D^{m-1}(G)$ est un sous-groupe distingué commutatif non trivial.

Par récurrence, il existe ainsi une base de $\mathbf{C}^n$ dans laquelle les matrices de H sont triangulaires supérieures. On effectue ce changement de base en supposant désormais $H\subset B$. Le premier vecteur e_1 de cette base est un vecteur propre de tout élément $h\in H$. Soit alors $V\subset\mathbf{C}^n$ le sous-espace vectoriel engendré par tous les vecteurs $v\in\mathbf{C}^n$ qui sont vecteurs propres de chaque $h\in H$. Puisqu'il contient e_1, il n'est pas nul. Montrons qu'il est stable par G. En effet, si $h\in H$ et $g\in G$, on a pour $v\in V$ propre pour H,

$$\begin{aligned} h(g(v)) &= gg^{-1}hg(v)=g(g^{-1}hg)(v)\\ &= g(\lambda_{g^{-1}hg}(v)) && \text{car } g^{-1}hg\in H\\ &= \lambda_{g^{-1}hg}g(v)\end{aligned}$$

donc est vecteur propre pour H. Ainsi, $g(v)\in V$ et par linéarité, V est stable par G. D'après la première réduction cela implique que $V=\mathbf{C}^n$. Autrement dit, $\mathbf{C}^n$ possède une base de vecteurs propres pour H : dans cette base, toute matrice de H est diagonale. On effectue *illico* ce changement de base.

Fixons un élément $h\in H$, $h\neq 1$. Comme H est un sous-groupe distingué, pour tout $g\in G$ et tout $h\in H$, $g^{-1}hg$ appartient à H. Or, $g^{-1}hg$ est une matrice qui a mêmes valeurs propres que h et il n'y a qu'un nombre fini de telles matrices dans H. L'application $G\to H$ qui à g associe $g^{-1}hg$ est une application continue du groupe connexe G dans un ensemble fini. Elle est nécessairement constante. Puisque l'élément neutre de G a pour image h, on en déduit que $g^{-1}hg=h$ pour tout élément $g\in G$. En d'autre termes, $gh=hg$ pour tout $g\in G$. Par suite, H est contenu dans le centre de G.

Soit W un espace propre de h (comme $h\neq 1$, $0<\dim H<n$). Pour tout $g\in G$, g laisse stable W, car g et h commutent, donc G laisse stable le sous-espace vectoriel W. Par la première réduction, cela entraîne que $W=\mathbf{C}^n$, donc qu'il existe $\lambda_h\in\mathbf{C}^*$ tel que $h=\lambda_h\,\mathrm{id}$.

Le déterminant d'un commutateur est égal à 1. Comme $m-1 \geqslant 1$, on a donc $H \subset \mathrm{SL}(n,\mathbf{C})$ et $\lambda_h^n = 1$ pour tout $h \in H$. Par conséquent, H est un groupe fini. D'après le lemme ci-dessous, H est connexe, donc $H = \{1\}$, contradiction. □

LEMME 4.7.4. — *Le sous-groupe dérivé d'un sous-groupe connexe de* $\mathrm{GL}(n,\mathbf{C})$ *est connexe.*

Démonstration. — L'ensemble S de tous les commutateurs de G est l'image de $G \times G$ par l'application continue $(g_1, g_2) \mapsto g_1 g_2 g_1^{-1} g_2^{-1}$. Par suite, S est connexe.

Soit S_m l'ensemble des produits $s_1 \dots s_m$, avec $s_i \in S$ et $m \geqslant 1$. C'est l'image de S^m par l'application continue $(g_1, \dots, g_m) \mapsto g_1 \dots g_m$. Puisque S est connexe, S^m et S_m le sont aussi.

Puisque l'inverse d'un commutateur en est encore un, on a $D(G) = \{e\} \cup \bigcup_{m \geqslant 1} S_m$. Comme les S_m ont la matrice identique en commun, $D(G)$ est connexe, ainsi qu'il fallait démontrer. □

Exercices

Exercice 4.1. — **a)** Si m et n sont deux entiers premiers entre eux, montrer que $(\mathbf{Z}/mn\mathbf{Z})^*$ est isomorphe à $(\mathbf{Z}/m\mathbf{Z})^* \times (\mathbf{Z}/n\mathbf{Z})^*$.

b) En déduire que si $(\mathbf{Z}/n\mathbf{Z})^*$ est cyclique, il existe un nombre premier p et un entier $m \geqslant 0$ tels que $n = p^m$, ou $n = 2p^m$, ou $n = 4$.

c) En utilisant l'exercice 3.14, montrer la réciproque.

Exercice 4.2. — Rappelons que $\mathbf{H}$ désigne le corps (non commutatif) des quaternions. Soit G le sous-groupe $\{\pm 1; \pm i; \pm j; \pm k\}$ de $\mathbf{H}^*$. Montrer que tout sous-groupe de G est distingué bien que G ne soit pas abélien.

Exercice 4.3. — Soit G un groupe et H un sous-groupe de G. Montrer que H est le noyau d'un homomorphisme de G dans un groupe abélien si et seulement si H contient le sous-groupe dérivé de G.

(Remarque : commencer par montrer *directement* qu'un sous-groupe contenant le sous-groupe dérivé est distingué.)

Exercice 4.4. — **a)** Soit G un groupe et soit A, B deux sous-groupes distingués de G tels que $A \cap B = \{e\}$. Si $a \in A$ et $b \in B$, montrer que $aba^{-1}b^{-1} = e$, et donc que a et b commutent. En déduire que le sous-groupe $AB \subset G$ engendré par A et B est isomorphe au produit direct $A \times B$.

b) Soit G un groupe fini et soit $(A_i)_{1\leqslant i\leqslant r}$ une famille de sous-groupes de G. Notons $n_i = \operatorname{card} A_i$; on suppose que les entiers n_i sont premiers deux à deux et que $\prod_{i=1}^{r} n_i = \operatorname{card} G$. Montrer que G est isomorphe au produit direct $\prod_{i=1}^{r} A_i$.

Exercice 4.5 (Produit semi-direct). — **a)** Soit A et B deux groupes, et soit $\varphi\colon B \to \operatorname{Aut}(A)$ un morphisme de groupes (en d'autres termes, φ définit une action de B sur A par des automorphismes de groupes).

Munissons l'ensemble produit $G = A \times B$ de la loi de composition donnée par

$$(a,b)\cdot(a',b') = (a\varphi(b)(a'), bb').$$

Montrer que c'est une loi de groupe. Le groupe G, muni de cette loi, est appelé le produit semi-direct de A et B (pour l'action φ) et est en général noté $A \rtimes_\varphi B$.

b) Montrer que l'application $G \to B$ donnée par $(a,b) \mapsto b$ est un morphisme de groupes surjectif. Montrer que son noyau est isomorphe à A. Montrer que l'application $B \to G$ donnée par $b \mapsto (\varphi(b)(e), b)$ est un morphisme de groupes.

c) Pour tout $g = (a,b) \in G$, on définit $\sigma(g)\colon A \to A$ par $\sigma(g)(x) = a\varphi(b)(x)$. Montrer que $\sigma(g)$ est une permutation de A et que l'application $\sigma\colon G \to \mathfrak{S}(A)$ est un morphisme de groupe injectif.

d) Soit G un groupe, A un sous-groupe distingué de G, $B = G/A$ et soit $\pi\colon G \to B$ l'homomorphisme canonique. Soit f un morphisme de groupes $f\colon B \to G$ tel que $\pi(f(b)) = b$ pour tout $b \in B$ (on dit que f est une *section* de π). Montrer qu'il y a un unique morphisme de groupes $\varphi\colon B \to \operatorname{Aut}(A)$ tel que $\varphi(b)(a) = f(b)af(b^{-1})$ pour tout $a \in A$ et tout $b \in B$. Montrer alors que G est isomorphe à $A \rtimes_\varphi B$.

Exercice 4.6. — Soit n un entier $\geqslant 2$ et posons $\zeta = \exp(2i\pi/n)$. Considérons le polygone régulier à n côtés Γ dans le plan $\mathbf{R}^2$ dont les sommets sont les points A_k de coordonnées $(\cos(2k\pi/n), \sin(2k\pi/n))$, $1 \leqslant k \leqslant n$. Soit O l'origine du plan.

On note D_n le groupe des transformations affines du plan qui préservent (dans leur ensemble) les sommets de Γ.

a) Montrer que D_n contient le groupe cyclique d'ordre n engendré par la rotation r de centre O et d'angle $2\pi/n$. Montre qu'il contient aussi la symétrie orthogonale s par rapport à l'axe Ox.

b) Soit $g \in D_n$. Montrer que $g(O) = O$ et que $\det(g) \in \{\pm 1\}$. Si de plus $\det(g) = 1$ et si g fixe un sommet de Γ, montrer que $g = \mathrm{id}$. En conclure que D_n est engendré par r et s.

c) Montrer que $srs = r^{-1}$ et que D_n est isomorphe au produit semi-direct $(\mathbf{Z}/n\mathbf{Z}) \rtimes_\varphi \{\pm 1\}$, où $\varphi\colon \{\pm 1\} \to \operatorname{Aut}(\mathbf{Z}/n\mathbf{Z})$ est l'application donnée par $\varphi(\varepsilon)(m) = \varepsilon m$.

Exercice 4.7. — Soit G un groupe dont l'ordre est une puissance d'un nombre premier p.

a) Soit X un ensemble fini sur lequel G agit. Soit X^G l'ensemble des points fixes de G c'est-à-dire l'ensemble des $x \in X$ tels que $g\cdot x = x$ pour tout $g \in G$. Montrer que

$$\operatorname{card}(X) \equiv \operatorname{card}(X^G) \pmod{p}.$$

b) Si $g \in G$, soit $\varphi_g : G \to G$ défini par $h \mapsto ghg^{-1}$. Montrer que $g \mapsto \varphi_g$ définit une action de G sur lui-même (*action par conjugaison*).

c) Soit Z le centre de G. Montrer que $Z \neq \{1\}$.

Exercice 4.8 (Premier théorème de Sylow). — Soit G un groupe fini, p un nombre premier. Soit p^r la plus grande puissance de p qui divise l'ordre de G.

a) Soit X l'ensemble des parties de G de cardinal p^r. Montrer que le cardinal de X n'est pas multiple de p.

b) On considère l'action de G sur X par translation à gauche : si $A \subset G$, $g \cdot A = \{ga\,;\, a \in A\}$. Si $A \in X$, montrer que son stabilisateur $H = \{g \in G\,;\, gA = A\}$ est un sous-groupe de G de cardinal $\leqslant p^r$.

c) Montrer qu'il existe une partie $A \in X$ dont l'orbite sous G est de cardinal non multiple de p. (Utiliser la question a) de l'exercice 4.7.) En déduire que le stabilisateur de A est est un sous-groupe de G de cardinal p^r (*p-sous-groupe de Sylow*).

Exercice 4.9 (Deuxième théorème de Sylow). — Soit G un groupe fini, p un nombre premier, p^r la plus grande puissance de p qui divise $\operatorname{card} G$.

Soit P un p-sous-groupe de Sylow de G, c'est-à-dire un sous-groupe de G d'ordre p^r.

a) Soit H un sous-groupe de G d'ordre une puissance de p. Considérer l'action de H par translation à gauche sur l'ensemble G/P des classes à droites modulo P (autrement dit l'action définie par $h \cdot gP = (hg)P$). En déduire qu'il existe $g \in G$ tel que pour tout $h \in H$, $hgP = gP$, puis que $H \subset gPg^{-1}$.

b) Montrer que deux p-sous-groupes de Sylow quelconques sont conjugués.

Exercice 4.10. — Soit G un groupe.

a) On pose $D^0 = G$ et pour tout i, on définit D^{i+1} comme le sous-groupe dérivé de D^i. Montrer que G est résoluble si et seulement s'il existe n tel que $D^n = \{1\}$.

b) On pose $C^0 = G$ et pour tout i, on définit C^{i+1} comme le sous-groupe engendré par les commutateurs $ghg^{-1}h^{-1}$ avec $g \in G$ et $h \in C^i$ (*suite centrale descendante*). Montrer que G est nilpotent si et seulement s'il existe n tel que $C^n = \{1\}$.

Exercice 4.11. — **a)** Montrer qu'un sous-groupe ou un quotient d'un groupe nilpotent est encore nilpotent.

b) Soit G un groupe, H un sous-groupe de G contenu dans le centre de G. Remarquer que H est distingué dans G. Si G/H est nilpotent, alors G est nilpotent.

c) Montrer qu'un groupe fini dont l'ordre est une puissance d'un nombre premier est nilpotent. (Utiliser l'exercice 4.7.)

Exercice 4.12. — **a)** Soit G un groupe fini, H un sous-groupe distingué de G et soit π le morphisme surjectif canonique $G \to G/H$. Soit p un nombre premier et soiut P un p-sous-groupe de Sylow de G. Montrer que $P \cap H$ est un p-sous-groupe de Sylow de H et que $\pi(P)$ est un p-sous-groupe de Sylow de G/H.

b) Soit G un groupe fini, $C \subset G$ un sous-groupe contenu dans le centre de G. Soit P, P' deux p-sous-groupe de Sylow de G tels que $P \cap C = P' \cap C$ et $PC = P'C$. Pour tout $g \in P$, montrer qu'il existe $\pi(g) \in P'$ et $c(g) \in C$ tels que $g = \pi(g)c(g)$. Montrer que l'application $g \mapsto c(p)(P' \cap C)$ de P dans $C/(P' \cap C)$ est bien définie et que c'est un morphisme de groupe. Montrer qu'elle envoie tout élément sur l'élément neutre. En conclure que $P = P'$.

c) Soit G un groupe fini nilpotent. Montrer par récurrence sur le cardinal de G que G a un unique p-sous-groupe de Sylow.

d) Soit G un groupe fini nilpotent. Montrer que G est isomorphe au produit de ses p-sous-groupes de Sylow, pour p divisant l'ordre de G. (*Utiliser l'exercice 4.4.*)

e) Inversement, montrer que tout groupe fini qui est de la forme $\prod_p P_p$, pour P_p un groupe d'ordre une puissance du nombre premier p, est un groupe nilpotent.

Exercice 4.13. — Cet exercice propose une démonstration du fameux théorème de Wedderburn : *tout corps fini est commutatif.* Soit donc F un corps fini, qu'on ne suppose pas commutatif.

a) Soit Z le *centre* de F c'est-à-dire l'ensemble des $a \in F$ tels que pour tout $x \in F$, $ax = xa$. Montrer que Z est un sous-corps commutatif de F. On note q son cardinal. Montrer qu'il existe un entier $n \geqslant 1$ tel que $\operatorname{card} F = q^n$.

b) Soit $x \in F$. Montrer que l'ensemble C_x des $a \in F$ tels que $ax = xa$ est un sous-corps de F. Montrer que son cardinal est de la forme q^{n_x}, où n_x est un entier qui divise n.

c) Si $x \in F^*$, calculer en fonction de n_x le cardinal de la classe de conjugaison $\mathcal{C}(x)$ de x dans F^* (l'ensemble des éléments de F^* qui sont de la forme axa^{-1}).

d) Si $x \notin Z$, en déduire que le cardinal de $\mathcal{C}(x)$ est un multiple de $\Phi_n(q)$. (Φ_n désigne le n-ième polynôme cyclotomique.)

e) Montrer à l'aide de l'équation aux classes que $q^n - q$ est multiple de $\Phi_n(q)$. En déduire que $n = 1$ et que F est commutatif.

Exercice 4.14. — Soit G un sous-groupe transitif de $\mathfrak{S}_n$. Pour $i \in \{1, \ldots, n\}$, notons G_i l'ensemble des $g \in G$ tels que $g(i) = i$.

a) Montrer que G_i est un sous-groupe de G et que $(G : G_i) = n$.

b) Montrer que $\bigcup_{i=1}^{n} G_i \neq G$. (Majorer le cardinal du membre de gauche.) En déduire qu'il existe un élément de G qui agit sans point fixe sur $\{1, \ldots, n\}$ (Jordan, 1872).

Exercice 4.15. — Soit G un groupe fini agissant sur un ensemble fini X. Pour tout $g \in G$, notons $f(g)$ le nombre de points fixes de g.

a) Montrer la formule de Burnside suivante : il y a exactement

$$\frac{1}{\operatorname{card} G} \sum_{g \in G} f(g)$$

orbites de G dans X. (Compter de deux manières le nombre d'éléments (g, x) de $G \times X$ tels que $g \cdot x = x$, en sommant d'abord sur $g \in G$, puis sur $x \in X$.)

b) Montrer que

$$\frac{1}{\operatorname{card} G}\sum_{g\in G} f(g)^2 \geqslant 2.$$

(Considérer l'action de G sur $X\times X$.)

c) Supposons que l'action de G sur X soit transitive. En sommant sur $g\in G$ l'expression $(f(g)-1)(\operatorname{card} X - f(g))$, montrer qu'il y a au moins $\operatorname{card} G/\operatorname{card} X$ elements de G qui n'ont pas de point fixe dans X. (Cette amélioration du résultat de l'exercice 4.14 est du à Cameron et Cohen.)

Exercice 4.16 (Simplicité de $\mathfrak{A}_n$ pour $n\geqslant 5$). — Le but de cet exercice est de démontrer que le groupe alterné $\mathfrak{A}_n$ est simple pour $n\geqslant 5$.

a) Soit N un sous-groupe distingué de $\mathfrak{A}_5$. Montrer de la façon suivante que N contient un 3-cycle.

1) On suppose que N contient une double transposition, disons $\sigma=(1,2)(3,4)$. Montrer que la permutation $\tau=(1,5)(3,4)$ est conjuguée à σ dans $\mathfrak{A}_n$. Remarquer que $\sigma\tau$ est un 3-cycle dans N.

2) On suppose que N contient une permutation d'ordre 5, disons $\sigma=(1,2,3,4,5)$. Montrer alors que $\tau=(2,3,1,4,5)$ est conjuguée à σ et conclure que N contient le 3-cycle $(4,1,2)$.

b) Montrer que $\mathfrak{A}_5$ est simple.

c) Soit $n\geqslant 6$ et supposons par récurrence que $\mathfrak{A}_{n-1}$ est simple. Soit N un sous-groupe distingué de $\mathfrak{A}_n$, tel que $N\neq\{1\}$ et $N\neq\mathfrak{A}_n$.

Soit $\sigma\in N$, $\sigma\neq\mathrm{id}$; montrer que $n\neq\sigma(n)$.

d) (*suite*) Soit $\sigma\in N\setminus\{\mathrm{id}\}$. On considère deux entiers $i\neq j$, distincts de n et $\sigma(n)$ et on introduit la permutation $\tau=(i,j)(n,\sigma(n))$. Montrer que $\sigma'=\sigma\tau\sigma\tau^{-1}\in N$ mais que $\sigma'(n)=n$. En déduire que $\sigma'=\mathrm{id}$.

e) (*suite*) En utilisant l'égalité $\tau\sigma\tau^{-1}=\sigma$, montrer que $\sigma^2(n)=n$ et que

$$\{\sigma(i),\sigma(j)\}=\{i,j\}.$$

En conclure que $\sigma=(n,\sigma(n))$, ce qui contredit l'hypothèse $\sigma\in\mathfrak{A}_n$. Par suite, N n'existe pas et $\mathfrak{A}_n$ est simple.

Exercice 4.17. — Soit n un entier, avec $n\geqslant 5$, et soit G un sous-groupe du groupe symétrique $\mathfrak{S}_n$. Notons $d=(\mathfrak{S}_n:G)$ l'indice de G dans $\mathfrak{S}_n$.

a) Si G est un sous-groupe distingué de $\mathfrak{S}_n$, montrer que $G=\mathfrak{A}_n$ ou $G=\mathfrak{S}_n$. (Utiliser que $\mathfrak{A}_n$ est simple, exercice 4.16.)

b) Montrer qu'il existe un morphisme de groupes $\mathfrak{S}_n\to\mathfrak{S}_d$ dont le noyau est contenu dans G.

c) Si $G\neq\mathfrak{A}_n$ et $G\neq\mathfrak{S}_n$, montrer que $d\geqslant n$.

5

Applications

Nous étudions dans ce chapitre comment utiliser la théorie de Galois pour obtenir une réponse « satisfaisante » au problème de la constructibilité à la règle et au compas. Par des méthodes analogues, nous discutons de la résolution par radicaux. Nous montrons enfin comment la théorie de Galois permet de comprendre les résolutions explicites des équations de degrés 3 *et* 4.

5.1. Constructibilité à la règle et au compas

Revenons au problème de la constructibilité à la règle et au compas. On s'intéressera ici des nombres complexes constructibles à partir de l'ensemble $\{0;1\}$. Rappelons que d'après le théorème de Wantzel (théorème 1.4.1), il s'agit des nombres complexes z pour lesquels il existe une suite d'extensions de $\mathbf{Q}$, $\mathbf{Q} = K_0 \subset K_1 \subset K_2 \subset \cdots \subset K_n$ telles $z \in K_n$ et telles que que pour tout i, $[K_i : K_{i-1}] = 2$.

THÉORÈME 5.1.1. — *Un nombre algébrique $z \in \mathbf{C}$ est constructible (à partir de $\{0;1\}$) si et seulement si l'extension de $\mathbf{C}$ engendrée par z et ses conjugués est de degré une puissance de* 2.

Pour comprendre un peu ce qui se passe, commençons par démontrer la proposition suivante.

PROPOSITION 5.1.2. — *Soit $z \in \mathbf{C}$ un nombre constructible. Alors, tout conjugué de z est constructible.*

Démonstration. — Soit $\mathbf{Q} = K_0 \subset K_1 \subset \cdots \subset K_n$ une suite d'extensions quadratiques telles que $z \in K_n$. Soit $\mathbf{Q} \subset K_n \subset L$ une extension galoisienne. Si z' est un conjugué de z, il existe un élément $\sigma \in \mathrm{Gal}(L/\mathbf{Q})$ tel que $\sigma(z) = z'$. (C'est essentiellement le contenu de la démonstration de la proposition 3.3.2. Voir l'exercice 3.5.) Posons $K'_j = \sigma(K_j)$ pour $0 \leqslant j \leqslant n$. C'est un sous-corps de L et pour tout j, $[K'_j : K'_{j-1}] = 2$. Puisque $z' \in K'_n$, cela montre que z' est constructible. □

Soit maintenant $z \in \mathbf{C}$ un nombre algébrique constructible et soit L l'extension de $\mathbf{Q}$ engendrée par les conjugués de z. D'après la proposition précédente, tout élément de L est constructible. Or, le théorème de l'élément primitif affirme qu'il existe $\alpha \in L$ tel que $L = \mathbf{Q}[\alpha]$. Cet élément α est ainsi constructible, ce qui implique qu'il est de degré une puissance de 2. Par suite, $[L : \mathbf{Q}]$ est une puissance de 2, ce qu'il fallait démontrer.

Réciproquement, supposons que $[L : \mathbf{Q}]$ soit une puissance de 2. Comme c'est une extension galoisienne, cela signifie que son groupe de Galois $G = \mathrm{Gal}(L/\mathbf{Q})$ est d'ordre une puissance de 2. D'après le lemme 5.1.3 suivant, il existe une suite de sous-groupes $\{1\} = G_0 \subset G_1 \subset \cdots \subset G_n = G$ chacun étant d'indice 2 dans le suivant. Il correspond à cette suite de sous-groupes une suite d'extensions quadratiques $\mathbf{Q} = L^G \subset L^{G_{n-1}} \subset \cdots \subset L^{G_0} = L$. Tout élément de L est donc constructible, et en particulier z, ce qu'il fallait démontrer.

LEMME 5.1.3. — *Soit G un groupe fini dont l'ordre est une puissance de 2. Il existe alors une suite de sous-groupes $\{1\} = G_0 \subset G_1 \subset \cdots \subset G_n = G$ tels que pour tout j, $(G_j : G_{j-1}) = 2$.*

Démonstration. — On raisonne par récurrence sur l'ordre de G. D'après l'exercice 4.7, le centre Z de G est distinct de $\{1\}$. Remarquons que Z et G/Z sont d'ordres des puissances de 2. Si $Z \neq G$, on obtient par récurrence une suite de sous-groupes dans Z, ainsi qu'une suite de sous-groupes de G/Z qu'on raboute pour obtenir la suite de sous-groupes voulue. Si $Z = G$, c'est-à-dire si G est commutatif, on introduit le sous-groupe $2G \subset G$. Si $2G$ était égal à G, on aurait $2^m G = G$ pour tout m, ce qui contredit le fait que tout élément de G soit annulé par l'ordre de G. Par récurrence, $2G$ contient une suite de sous-groupes, chacun d'indice 2 dans le suivant. De plus, $V = G/2G$ est un groupe abélien fini annulé par 2, donc est un $(\mathbf{Z}/2\mathbf{Z})$-espace vectoriel de dimension finie. Le choix d'une base $(e_1, \ldots, e_d)$ de V fournit les sous-groupes voulus, à savoir $\mathrm{vect}(e_1) \subset \mathrm{vect}(e_1, e_2) \subset \cdots \subset V$. □

5.2. Cyclotomie

Ce nom est la concaténation de deux racines grecques et signifie à peu près « couper le cercle ». Considérons un polygone régulier à n côtés inscrit dans le cercle unité. Ses sommets divisent le cercle unité en n arcs de même longueur. En identifiant points du plan et nombres complexes, et en supposant qu'un des sommets est 1, ces sommets correspondent aux racines n-ièmes de l'unité. C'est pourquoi le mot cyclotomie est attaché à tout domaine des mathématiques qui est relié aux racines de l'unité : les corps cyclotomiques sont engendrés par une racine de l'unité, les racines du n-ième polynôme cyclotomique sont les racines primitives n-ièmes de l'unité…

Obéissons donc au titre de ce paragraphe et étudions en termes de théorie de Galois l'équation $X^n = 1$.

THÉORÈME 5.2.1. — *Soit K un corps et soit n un entier strictement positif. Supposons que la caractéristique du corps K ne divise pas n. Soit $K \subset L$ une extension de décomposition du polynôme $X^n - 1$. C'est une extension galoisienne et son groupes de Galois est isomorphe à un sous-groupe du groupe $(\mathbf{Z}/n\mathbf{Z})^*$.*

Plus précisément, il existe un unique homomorphisme de groupes injectif

$$\varphi\colon \mathrm{Gal}(L/K) \to (\mathbf{Z}/n\mathbf{Z})^*$$

tel que pour toute racine n-ième de l'unité $\zeta \in L$ et tout $\sigma \in \mathrm{Gal}(L/K)$, on ait

$$\sigma(\zeta) = \zeta^{\varphi(\sigma)}.$$

Démonstration. — Fixons une racine primitive n-ième de l'unité, ζ. Puisque le polynôme $X^n - 1$ est séparable, l'extension $K \subset L$ est galoisienne. Les racines de $X^n - 1$ sont les ζ^m, pour $0 \leqslant m \leqslant n-1$, donc $L = K(\zeta)$.

Soit $\sigma \in \mathrm{Gal}(L/K)$; l'image $\sigma(\zeta)$ est une racine n-ième de l'unité, donc est de la forme ζ^m, pour un entier m dont la classe modulo n est bien définie. En outre, si $\sigma(\zeta)^k = 1$, on a $\zeta^k = 1$, donc $\sigma(\zeta)$ est encore une racine primitive, si bien que m est premier à n. Cela définit une application $\varphi\colon \mathrm{Gal}(K(\zeta)/K) \to (\mathbf{Z}/n\mathbf{Z})^*$.

Soit θ une racine n-ième de l'unité et soit a un entier tel que $\theta = \zeta^a$. On a

$$\sigma(\theta) = \sigma(\zeta^a) = \sigma(\zeta)^a = (\zeta^m)^a = \zeta^{ma} = \theta^m,$$

et $\sigma(\theta) = \theta^{\varphi(\sigma)}$. Cela montre en particulier que l'application φ ne dépend pas du choix de la racine primitive ζ. De plus, si σ et τ appartiennent à $\mathrm{Gal}(L/K)$, on a

$$\zeta^{\varphi(\sigma\circ\tau)} = \sigma\circ\tau(\zeta) = \sigma(\zeta^{\varphi(\tau)}) = (\zeta^{\varphi(\tau)})^{\varphi(\sigma)} = \zeta^{\varphi(\tau)\varphi(\sigma)},$$

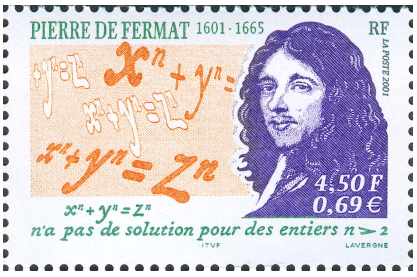
si bien que φ est un homomorphisme de groupes.

Enfin, si $\varphi(\sigma) = 1$, on a $\sigma(\zeta) = \zeta$; puisque $L = K(\zeta)$, $\sigma = \mathrm{id}$ et φ est injectif. □

Nous avons démontré au chapitre 1, exemple 1.4.7 qu'il n'est pas possible de construire à la règle et au compas un polyone régulier à 9 côtés. Cependant, C.-F. Gauss avait montré que l'on peut construire un polygone régulier à 17 côtés, ainsi qu'il l'a écrit dans son agenda mathématique, le 30 mars 1796. Il avait à peine 19 ans.

Plus généralement, le résultat suivant précise exactement les polygones réguliers que l'on peut construire à la règle et au compas.

THÉORÈME 5.2.2 (Construction des polygones réguliers). — *Un polygone régulier à n côtés est constructible à la règle et au compas si et seulement si n est produit d'une puissance de 2 et de nombres premiers de Fermat distincts.*



Rappelons qu'un *nombre premier de Fermat* est un nombre premier de la forme $F_m = 2^{2^m}+1$, où m est un nombre entier. Parmi ceux-ci, il y a 3, 5, 17, 257 et 65537, correspondant à $m = 0,\dots,4$. Fermat avait conjecturé qu'ils sont tous premiers mais Euler a montré que F_5 est divisible par 641. (*Exercice* : le faire ; montrer aussi que si n n'est pas une puissance de 2, 2^n+1 n'est pas un nombre premier.) En fait, les cinq nombres premiers de Fermat que nous avons cités sont les seuls que l'on connaît ! On sait aussi que $F_6,\dots,F_{16}$ ne sont pas premiers.

Démonstration. — Soit $\mathcal{P}$ l'ensemble des entiers $n \geqslant 3$ tels que l'on puisse construire, à la règle et au compas, un polygone régulier à n côtés. Dit autrement, un entier $n \geqslant 3$ appartient à $\mathcal{P}$ si et seulement si le nombre algébrique $\exp(2i\pi/n)$ est constructible. Ses conjugués sont des racines n-ièmes de l'unité.

Les trois remarques ci-dessous réduisent l'étude de ce problème au cas où n est un nombre premier, ou le carré d'un nombre premier.

a) *Si $n \in \mathcal{P}$, alors $2n \in \mathcal{P}$.*

Si un polygone régulier à n côtés est tracé, il suffit en effet, pour chaque arête AB, de tracer la perpendiculaire à AB passant par le centre O du polygone : elle coupe le secteur angulaire $\widehat{AOB}$ en deux parties égales.

b) *Si $n \in \mathcal{P}$, alors tout entier $m \geqslant 3$ qui divise n appartient à $\mathcal{P}$.*

Pour construire un polygone régulier à m côtés, il suffit de dessiner un polygone régulier à n côtés et de joindre un sommet sur (n/m).

c) *Si m et n sont deux entiers premiers entre eux qui appartiennent à $\mathcal{P}$, leur produit appartient à $\mathcal{P}$.*

Si m et n appartiennent à $\mathcal{P}$, les deux nombres complexes $\exp(2i\pi/m)$ et $\exp(2i\pi/n)$ sont constructibles. Puisque m et n sont supposés être premiers entre eux, il existe deux entiers u et v tels que $um+vn=1$. Alors,

$$\exp(2i\pi/mn) = \exp\big(2i\pi\big(\frac{u}{n}+\frac{v}{m}\big)\big) = \big(\exp(2i\pi/n)\big)^u\big(\exp(2i\pi/m)\big)^v$$

est constructible, ce qui entraîne que l'on a $mn \in \mathcal{P}$.

Pour démontrer le théorème, il nous reste maintenant à montrer que les nombres premiers dans $\mathcal{P}$ sont les nombres premiers de Fermat, et que $\mathcal{P}$ ne contient le carré d'aucun nombre impair. D'après le théorème 5.1.1, ces deux énoncés se ramènent aux deux suivants, où p désigne un nombre premier impair.

d) *Le nombre complexe* $\exp(2i\pi/p)$ *est un nombre algébrique de degré* $p-1$ *sur* $\mathbf{Q}$. *L'extension de* $\mathbf{Q}$ *engendrée par les racines* p*-ièmes de l'unité est de degré* $p-1$.

Soit P le polynôme minimal de $\exp(2i\pi/p)$. C'est un polynôme unitaire à coefficients entiers et il divise $(X^p-1)/(X-1) = 1+X+\cdots+X^{p-1}$, si bien qu'il existe $Q \in \mathbf{Z}[X]$ tel que

$$\frac{X^p-1}{X-1} = P(X)Q(X).$$

Posons $a = \deg P$, $b = \deg Q$; en particulier, on a $a+b = p-1$. Comme $\exp(2i\pi/p)$ n'est pas un nombre rationnel, on a $a \geqslant 2$.

Modulo p, on a $X^p - 1 \equiv (X-1)^p$. Par unicité de la décomposition en facteurs irréductibles sur $(\mathbf{Z}/p\mathbf{Z})$, il existe des polynômes A et $B \in \mathbf{Z}[X]$ tels que $P(X) = (X-1)^a + pA(X)$ et $Q(X) = (X-1)^p + pB(X)$. Par suite,

$$\frac{X^p-1}{X-1} = P(X)Q(X) = (X-1)^{a+b} + p\big(A(X)(X-1)^b + B(X)(X-1)^a\big) + p^2A(X)B(X).$$

Évaluons maintenant en $X=1$ les deux membres de cette égalité. Supposons que l'on ait $b \geqslant 1$; il vient la relation $p = p^2AB(1)$, ce qui est une contradiction manifeste, étant donné que $AB(1)$ est un entier. Par suite, $b=0$ et $a = p-1$.

La dernière assertion résulte de ce que $\mathbf{Q}(\exp(2i\pi/p))$ est l'extension de $\mathbf{Q}$ engendrée par les racines p-ièmes de l'unité.

e) *Le nombre complexe* $\exp(2i\pi/p^2)$ *est un nombre algébrique de degré* $p(p-1)$ *sur* $\mathbf{Q}$.

La démonstration est analogue. Le polynôme $(X^{p^2}-1)/(X^p-1)$ ne s'annule pas en $\exp(2i\pi/p^2)$. Si P est le polynôme minimal de $\exp(2i\pi/p^2)$, il existe un polynôme $Q \in \mathbf{Z}[X]$ tel que

$$\frac{X^{p^2}-1}{X^p-1} = P(X)Q(X).$$

Puisque $X^{p^2}-1 = (X-1)^{p^2}$ modulo p, il existe des polynômes A and $B \in \mathbf{Z}[X]$ vérifiant $P = (X-1)^a + pA$ et $Q = (X-1)^b + pB$, avec $a = \deg P \geqslant 2$ et $b = \deg Q$. En évaluant en $X=1$ l'égalité

$$\frac{X^{p^2}-1}{X^p-1} = (X-1)^{p^2-p} + p\big((X-1)^aB(X) + (X-1)^bA(X)\big) + p^2A(X)B(X),$$

on obtient comme ci-dessus que $b=0$, si bien que le degré de $\exp(2i\pi/p^2)$ sur $\mathbf{Q}$ vaut $a = p^2-p$. □

Remarque 5.2.3. — Ces deux derniers énoncés *d*) et *e*) sont des cas particuliers d'un théorème général de Gauss selon lequel le degré de $\exp(2i\pi/n)$ est égal à l'indicatrice d'Euler $\varphi(n)$ (exercice 2.5). Joint au théorème 5.2.1, il en résulte que le groupe de Galois de l'extension $\mathbf{Q} \subset \mathbf{Q}(\exp(2i\pi/n))$ est isomorphe à $(\mathbf{Z}/n\mathbf{Z})^*$.

Le cas particulier où $n = p^r$ est une puissance d'un nombre premier p est en général démontré à l'aide du critère d'Eisenstein (exercice 1.10). Appliqué au polynôme

$\Phi_{p^r}(Y+1)$ et au nombre premier p, ce critère permet en effet de montrer que Φ_{p^r} est irréductible.

COROLLAIRE 5.2.4 (Gauss, 1801). — *Le polygone régulier à 17 côtés est constructible à la règle et au compas.*

Expliquons maintenant comment C.-F. Gauss résolvait explicitement l'équation $X^{17}=1$. Soit ζ une racine primitive 17-ième de l'unité dans $\mathbf{C}$. L'extension $\mathbf{Q}\subset\mathbf{Q}(\zeta)$ est galoisienne et son groupe de Galois est isomorphe au groupe $(\mathbf{Z}/17\mathbf{Z})^*$. La remarque fondamentale de Gauss est que ce groupe est cyclique, engendrée par exemple par la classe de 3, dont les puissances modulo 17 sont successivement

$$1,3,9,10,13,5,15,11,16,14,8,7,4,12,2,6,1\ldots$$

Soit $\sigma\in\mathrm{Gal}(\mathbf{Q}(\zeta)/\mathbf{Q})$ le générateur correspondant et posons

$$a_0=\sum_{k=0}^{7}\sigma^{2k}(\zeta)=\zeta+\zeta^9+\zeta^{13}+\zeta^{15}+\zeta^{16}+\zeta^8+\zeta^4+\zeta^2,$$
$$a_1=\sum_{k=0}^{7}\sigma^{2k+1}(\zeta)=\zeta^3+\zeta^{10}+\zeta^5+\zeta^{11}+\zeta^{14}+\zeta^7+\zeta^{12}+\zeta^6.$$

On a $\sigma(a_0)=a_1$ et $\sigma(a_1)=a_0$. Par suite, a_0 et a_1 sont les deux racines d'une équation de degré 2 dans $\mathbf{Q}[X]$. Précisément, on a $a_0+a_1=-1$ et $a_0a_1=-4$ si bien que

$$a_0,\ a_1=\frac{-1\pm\sqrt{17}}{2}.$$

Le choix des signes dépend du choix de ζ. Si $\zeta=\exp(2i\pi/17)$, un calcul numérique montre que $a_0=(-1+\sqrt{17})/2$.

Posons ensuite $K_1=\mathbf{Q}(\sqrt{17})$. Le groupe de Galois de l'extension $K_1\subset\mathbf{Q}(\zeta)$ est engendré par σ^2. On définit, pour $0\leqslant i\leqslant 3$,

$$b_i=\sum_{k=0}^{3}\sigma^{4k+i}(\zeta),$$

si bien que $\sigma(b_i)=b_{i+1}$ si $i=0,1,2$ et $\sigma(b_3)=b_1$. En particulier, b_0 et b_2 sont permutées par σ^2, donc sont les deux racines d'une équation de degré 2 à coefficients dans K_1. On a $b_0+b_2=a_0$ et $b_0b_2=-1$ d'où l'on déduit que

$$b_0,\ b_2=\frac{1}{2}\big(a_0\pm\sqrt{a_0^2+4}\big)=-\frac{1}{4}+\frac{1}{4}\sqrt{17}\pm\sqrt{34-2\sqrt{17}}.$$

Un calcul numérique montre que b_0 est obtenu avec le signe $+$. De même,

$$b_1,\ b_2=-\frac{1}{4}-\frac{1}{4}\sqrt{17}\pm\sqrt{34+2\sqrt{17}}.$$

Posons alors $K_2 = \mathbf{Q}(\sqrt{34-2\sqrt{17}})$. L'extension $K_2 \subset \mathbf{Q}(\zeta)$ est galoisienne, de groupe de Galois engendré par σ^4. Définissons, pour $0 \leqslant i \leqslant 7$,

$$c_i = \sigma^i(\zeta) + \sigma^{i+8}(\zeta).$$

Les expressions c_0 et c_4 sont permutées par σ^4, donc sont les deux racines d'une équation de degré 2 à coefficients dans K_2. Concrètement, $c_0 + c_4 = a_0$ et $c_0 c_4 = b_1$ d'où l'on déduit les relations

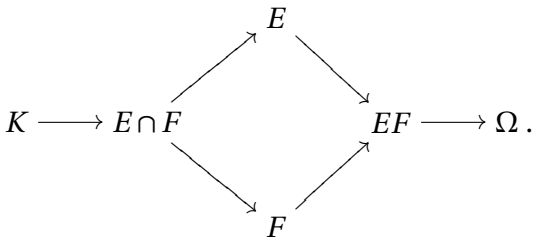
$$c_0,\ c_4 = \frac{1}{2}\big(a_0 \pm \sqrt{a_0^2 - 4b_1}\big).$$

Le calcul numérique, avec $\zeta = \exp(2i\pi/17)$, montre que $c_0 = 2\cos(2\pi/17)$ est obtenu avec le signe $+$, d'où la formule étonnante :

$$\begin{aligned} 2\cos(2\pi/17) = &-\frac{1}{8} + \frac{1}{8}\sqrt{17} + \frac{1}{8}\sqrt{34-2\sqrt{17}} \\ &+ \frac{1}{8}\sqrt{68+12\sqrt{17}-2\sqrt{34-2\sqrt{17}}+2\sqrt{34-2\sqrt{17}}\sqrt{17}-16\sqrt{34+2\sqrt{17}}}. \end{aligned}$$

5.3. Extensions composées

Dans ce paragraphe, on s'intéresse à la situation suivante. Soit K un corps ; soit Ω une clôture algébrique de K et soit E, F deux extension de K contenues dans Ω. On note EF le sous-corps de Ω engendré par E et F. C'est par définition *l'extension composée* de E et F. On s'intéresse aussi à l'intersection $E \cap F$, ce que l'on peut représenter par le diagramme :



LEMME 5.3.1. — *Si l'extension $K \subset E$ est galoisienne, l'extension $F \subset EF$ est galoisienne. Si de plus l'extension $K \subset F$ est galoisienne, les extensions $K \subset EF$ et $K \subset E \cap F$ sont galoisiennes.*

Démonstration. — Supposons que $K \subset E$ est une extension de décomposition d'un polynôme séparable $P \in K[X]$ (en l'occurrence, cela signifie que E est engendrée par les racines de P dans Ω). Alors, $F \subset EF$ est une extension de décomposition de P sur

le corps F, donc est galoisienne. Si $K \subset F$ est elle-même une extension de décomposition d'un polynôme séparable $Q \in K[X]$, $K \subset EF$ est alors une extension de décomposition du polynôme PQ ou, mieux, du polynôme séparable $\mathrm{ppcm}(P,Q)$. En particulier, l'extension $K \subset EF$ est galoisienne. Nous venons de démontrer les deux premières assertions.

Pour démontrer la dernière, il suffit de vérifier d'après la proposition 3.2.7 que tout K-homomorphisme $\sigma : E \cap F \to \Omega$ vérifie $\sigma(E \cap F) = E \cap F$. Un tel K-homomorphisme σ s'étend d'après le théorème 3.1.6 en un K-homomorphisme $\tau : EF \to \Omega$. Comme l'extension $K \subset E$ est galoisienne, $\tau(E) = E$. De même, $\tau(F) = F$. Ainsi, $\tau(E \cap F) \subset E \cap F$. Comme τ est un isomorphisme de K-espaces vectoriels, $\tau(E \cap F)$ a même degré sur K que $E \cap F$, d'où l'égalité $\tau(E \cap F) = E \cap F$. Par définition de τ, on a donc $\sigma(E \cap F) = E \cap F$, ainsi qu'il fallait démontrer. □

Supposons que $K \subset E$ est une extension galoisienne et montrons comment identifier $\mathrm{Gal}(EF/F)$ à un sous-groupe de $\mathrm{Gal}(E/K)$. Un élément $\sigma \in \mathrm{Gal}(EF/F)$ est un automorphisme de EF qui est l'identité sur F. En particulier, $\sigma|_K = \mathrm{id}_K$ et $\sigma \in \mathrm{Gal}(EF/K)$. Comme $K \subset E$ est galoisienne, $\sigma(E) = E$, si bien que σ définit un élément de $\mathrm{Gal}(E/K)$, noté $i(\sigma)$. L'homomorphisme i ainsi construit est le composé des deux homomorphismes naturels

$$\mathrm{Gal}(EF/F) \hookrightarrow \mathrm{Gal}(EF/K) \twoheadrightarrow \mathrm{Gal}(E/K).$$

PROPOSITION 5.3.2. — *Cet homomorphisme i est injectif, d'image* $\mathrm{Gal}(E/E \cap F)$.

Démonstration. — Si $\sigma \in \mathrm{Gal}(EF/F)$ définit l'identité sur E, $\sigma(x) = x$ pour tout x dans F et pour tout x dans E, donc $\sigma(x) = x$ pour tout x dans le corps engendré qui est EF. Ainsi, $\sigma = \mathrm{id}$, ce qui prouve l'injectivité de l'homomorphisme i.

Son image $i(\mathrm{Gal}(EF/F))$ est un sous-groupe H de $\mathrm{Gal}(E/K)$ et correspond à un sous-corps E^H de E de sorte que $H = \mathrm{Gal}(E/E^H)$. Par définition, E^H est l'ensemble des $x \in E$ tels que pour tout $\sigma \in \mathrm{Gal}(EF/F)$, $\sigma(x) = x$. Comme l'extension $F \subset EF$ est galoisienne, un tel x appartient à F. Ainsi, $E^H = E \cap F$ et $H = \mathrm{Gal}(E/E \cap F)$. □

On en déduit immédiatement un corollaire sur les degrés des diverses extensions :

COROLLAIRE 5.3.3. — *Supposons que l'extension $K \subset E$ soit galoisienne. Alors,*

$$[EF : F] = [E : E \cap F].$$

En particulier, $[EF : K] = [E : F]\,[F : E]$ *si et seulement si* $K = E \cap F$.

Démonstration. — En effet, $[EF : F]$ est le cardinal de $\mathrm{Gal}(EF/F)$, qui est celui de $i(\mathrm{Gal}(EF/F)) = \mathrm{Gal}(E/E \cap F)$, lequel vaut $[E : E \cap F]$. □

Dans le cas où les deux extensions $K \subset E$ et $K \subset F$ sont galoisiennes, nous allons déterminer le groupe de Galois de EF sur K en termes des groupes $\mathrm{Gal}(E/K)$ et

$\mathrm{Gal}(F/K)$. On considère tout d'abord l'homomorphisme

$$j\colon \mathrm{Gal}(EF/K) \to \mathrm{Gal}(E/K) \times \mathrm{Gal}(F/K)$$

déduit des deux homomorphismes surjectifs $\mathrm{Gal}(EF/K) \to \mathrm{Gal}(E/K)$ et $\mathrm{Gal}(EF/K) \to \mathrm{Gal}(F/K)$. (Ils existent bien car les extensions $K \subset E$ et $K \subset F$ sont galoisiennes.) Si $\sigma \in \mathrm{Gal}(EF/K)$ induit l'identité sur E et sur F, il induit l'identité sur le corps engendré par E et F dans Ω, donc $\sigma = \mathrm{id}$ et j est injectif.

Dans le cas où $K = E \cap F$, le corollaire 5.3.3 affirme que $[EF : K] = [E : K][F : K]$, si bien que j, étant injectif, est nécessairement surjectif.

Dans le cas général, rappelons que l'extension $K \subset E \cap F$ est galoisienne. Composons j avec les homomorphismes surjectifs

$$\pi_1\colon \mathrm{Gal}(E/K) \times \mathrm{Gal}(F/K) \to \mathrm{Gal}(E/K) \to \mathrm{Gal}(E \cap F/K)$$

et

$$\pi_2\colon \mathrm{Gal}(E/K) \times \mathrm{Gal}(F/K) \to \mathrm{Gal}(F/K) \to \mathrm{Gal}(E \cap F/K).$$

Par construction, $\pi_1 \circ j$ et $\pi_2 \circ j$ sont tous deux égaux à l'homomorphisme naturel

$$\mathrm{Gal}(EF/K) \to \mathrm{Gal}(E \cap F/K)$$

attaché à la sous-extension galoisienne $K \subset E \cap F$ de $K \subset EF$. Il en résulte que l'image de j est contenue dans le sous-groupe G de $\mathrm{Gal}(E/K) \times \mathrm{Gal}(F/K)$ formé des (σ_1, σ_2) tels que $\pi_1(\sigma_1) = \pi_2(\sigma_2)$.

Si l'on montre que $\mathrm{card}\, G = \mathrm{card}\, \mathrm{Gal}(EF/K)$, il en résultera que j est un isomorphisme de $\mathrm{Gal}(EF/K)$ sur G. Soit Δ le sous-groupe de $\mathrm{Gal}(E \cap F/K) \times \mathrm{Gal}(E \cap F/K)$ formé des couples (σ, σ), pour $\sigma \in \mathrm{Gal}(E \cap F/K)$ (sous-groupe diagonal). Par définition, G est l'image réciproque de Δ dans $\mathrm{Gal}(E/K) \times \mathrm{Gal}(F/K)$ par l'homomorphisme surjectif

$$(\pi_1, \pi_2)\colon \mathrm{Gal}(E/K) \times \mathrm{Gal}(F/K) \to \mathrm{Gal}(E \cap F/K) \times \mathrm{Gal}(E \cap F/K).$$

On a alors

$$\begin{aligned}
\mathrm{card}\, G &= \mathrm{card}\, \mathrm{Gal}(E \cap F/K) \times \mathrm{card}\, \mathrm{Ker}(\pi_1, \pi_2) \\
&= [E \cap F : K] \times \mathrm{card}\, \mathrm{Ker}\, \pi_1 \times \mathrm{card}\, \mathrm{Ker}\, \pi_2 \\
&= [E \cap F : K] \times [E : E \cap F] \times [F : E \cap F] \\
&= [F : K] \times [E : E \cap F] = [EF : K] \\
&= \mathrm{card}\, j(\mathrm{Gal}(EF/K)).
\end{aligned}$$

Nous avons ainsi démontré le théorème :

THÉORÈME 5.3.4. — *Considérons l'extension composée $K \subset EF$ de deux extensions galoisiennes $K \subset E$ et $K \subset F$ contenues dans une clôture algébrique de K.*

L'extension $K \subset EF$ est alors galoisienne, de groupe de Galois isomorphe au sous-groupe de $\mathrm{Gal}(E/K) \times \mathrm{Gal}(F/K)$ *formé des couples (σ, τ) tels que σ et τ aient même image dans* $\mathrm{Gal}(E \cap F/K)$. *Dans le cas particulier où $E \cap F = K$, le groupe* $\mathrm{Gal}(EF/K)$ *s'identifie ainsi au produit* $\mathrm{Gal}(E/K) \times \mathrm{Gal}(F/K)$.

5.4. Extensions cycliques

Par définition, une *extension cyclique* est une extension galoisienne dont le groupe de Galois est cyclique, isomorphe à $\mathbf{Z}/n\mathbf{Z}$ si n est le degré de l'extension.

Si K est un corps, notons $\mu_n(K)$, ou μ_n pour abréger, le groupe des racines n-ièmes de l'unité dans K. Dans ce paragraphe, nous supposerons généralement que μ_n est d'ordre n. Alors, il est cyclique, engendré par une racine primitive. Si K est de caractéristique p, cela implique aussi que n n'est pas un multiple de p. Dans ce paragraphe, on détermine les extensions cycliques de degré n d'un tel corps.

Commençons par un exemple (en fait *l'*exemple...).

THÉORÈME 5.4.1. — *Soit K un corps, n un entier supérieur ou égal à 2. On suppose que* $\mathrm{card}\,\mu_n(K) = n$.

Soit $a \in K^*$ et soit $K \subset L$ une extension de décomposition du polynôme $X^n - a$. Soit x une racine de P dans L.

L'extension $K \subset L$ est galoisienne. L'application $i : \sigma \mapsto i(\sigma) = \sigma(x)/x$ définit un morphisme de groupe injectif de $\mathrm{Gal}(L/K)$ *dans $\mu_n(K)$. Soit d le plus petit entier $\geqslant 1$ tel que $x^d \in K$; alors d divise n et l'image du morphisme i est égal à $\mu_d(K)$.*

En particulier, les assertions suivantes sont équivalentes :

(i) *si $m > 1$ est un diviseur de n, a n'est pas une puissance m-ième dans K ;*
(ii) *le polynôme $X^n - a$ est irréductible dans $K[X]$;*
(iii) $\mathrm{Gal}(L/K) \simeq \mathbf{Z}/n\mathbf{Z}$.

Démonstration. — Les racines de $P = X^n - a$ dans L sont de la forme ζx, avec $\zeta \in \mu_n(K)$. Puisque $\mathrm{card}\,\mu_n(K) = n$, la caractéristique de K ne divise pas n, si bien que $P'(\zeta x) = n(\zeta x)^{n-1} = na/(\zeta x) \neq 0$. Les racines de P sont toutes simples, le polynôme P est séparable et se factorise dans $L[X]$ en

$$P = X^n - a = \prod_{\zeta \in \mu_n} (X - \zeta x).$$

L'extension $K \subset L$ est en outre galoisienne. Remarquons aussi que $L = K(x)$.

Tout K-automorphisme σ de L est déterminé par l'image $\sigma(x)$ de x, qui est une racine de P. Par suite, $\sigma(x)/x$ est une racine n-ième de l'unité. En posant $i(\sigma) = \sigma(x)/x$, on définit ainsi une application $i : \mathrm{Gal}(L/K) \to \mu_n$.

Remarquons que i est un homomorphisme de groupes : si $\sigma(x) = ux$ et $\tau(x) = vx$ où $u,\ v \in \mu_n$, alors

$$(\sigma \circ \tau)(x) = \sigma(vx) = v\sigma(x) = uvx,$$

puisque $v \in K$, d'où $i(\sigma\circ\tau) = i(\sigma)i(\tau)$. l'image de i dans μ_n est un sous-groupe, nécessairement de la forme μ_d pour un entier d qui divise n. On a $[L:K] = \operatorname{card}\mathrm{Gal}(L/K) = d$, et d est le degré du polynôme minimal de x sur K (rappelons que $L = K[x]$). Remarquons aussi que $\mathrm{Gal}(L/K) \simeq \mu_d(K) \simeq \mathbf{Z}/d\mathbf{Z}$.

Soit m un entier. On a $x^m \in K$ si et seulement si $\sigma(x^m) = x^m$ pour tout $\sigma \in \mathrm{Gal}(L/K)$. Puisque $\sigma(x) = i(\sigma)x$, cela est vérifié si et seulement si $i(\sigma)^m = 1$ pour tout $\sigma \in \mathrm{Gal}(L/K)$, donc si et seulement si $\zeta^m = 1$ pour tout $\zeta \in i(\mathrm{Gal}(L/K))$. Comme $i(\mathrm{Gal}(L/K)) = \mu_d(K)$, on a donc démontré que $x^m \in K$ si et seulement si d divise m. En particulier, $x^d \in K$ et $a = x^n = (x^d)^{n/d}$ est une puissance (n/d)-ième dans K. Inversement, si l'on suppose que a n'est une puissance m-ième dans K pour aucun entier $m > 1$ divisant n, alors $d = n$ et $P = X^n - a$ est irréductible dans $K[X]$. En revanche, si $a = b^e$ pour un certain $b \in K$ et un diviseur $e > 1$ de n, l'égalité

$$P = X^n - a = X^{me} - b^e = (X^m - b)(X^{m(e-1)} + X^{m(e-2)}b + \cdots + b^{e-1})$$

montre que P n'est pas irréductible dans $K[X]$. □

Réciproquement, soit $K \to L$ une extension finie, galoisienne de groupe de Galois $\mathbf{Z}/n\mathbf{Z}$. Notons σ un générateur de $\mathrm{Gal}(L/K)$. Au vu de la démonstration précédente, on cherche un élément $x \in L$ tel que $L = K[x]$ et tel que $\sigma(x)/x$ soit une racine n-ième de l'unité. Soit $\zeta \in \mu_n$ une racine primitive n-ième de l'unité et définissons, pour $t \in L$, la *résolvante de Lagrange*

$$x = t + \zeta^{-1}\sigma(t) + \cdots + \zeta^{1-n}\sigma^{n-1}(t).$$

D'après l'exercice 3.11, les éléments de $\mathrm{Gal}(L/K)$ sont linéairement indépendants sur K. Par suite, on peut choisir t tel que $x \neq 0$. Alors,

$$\sigma(x) = \sigma(t) + \zeta^{-1}\sigma^2(t) + \cdots + \zeta^{1-n}\sigma^n(t) = \zeta x$$

puisque $\sigma^n = \mathrm{id}$. Par récurrence, pour tout $k \in \{0;1;\ldots;n-1\}$,

$$\sigma^k(x) = \zeta^k x.$$

Il en résulte que pour tout k, $\sigma^k(x^n) = x^n$. Comme $\mathrm{Gal}(L/K) = \{\mathrm{id};\sigma;\sigma^2;\ldots;\sigma^{n-1}\}$, $a = x^n$ appartient à K.

Les $\sigma^k(x) = \zeta^k x$, pour $0 \leqslant k \leqslant n-1$ sont les n racines, distinctes, du polynôme $X^n - a$ et l'extension $K \subset K(x)$ en est une extension de décomposition. Le groupe $\mathrm{Gal}(L/K)$ opère transitivement sur ses racines ; cela entraîne que ce polynôme est irréductible. Par suite, $[K(x):K] = n$ et comme $[L:K] = n$, on a nécessairement $L = K(x)$. Autrement dit, $K \subset L$ est une extension de décomposition du polynôme irréductible $X^n - a$ et x est un élément primitif de cette extension. (Voir aussi l'exercice 3.7).

Nous avons ainsi démontré le théorème suivant :

THÉORÈME 5.4.2. — *Soit K un corps, n un entier supérieur ou égal à 2 tel que* $\operatorname{card}\mu_n(K) = n$.

Soit $K \subset L$ une extension galoisienne de groupe de Galois isomorphe à $\mathbf{Z}/n\mathbf{Z}$. Alors, il existe $a \in K$ tel que $K \subset L$ soit une extension de décomposition du polynôme irréductible $X^n - a$.

5.5. Les équations de degrés inférieur à 4

Nous allons maintenant analyser les équations de degré $\leqslant 4$ à la lumière de la théorie de Galois. Le principe est que les 3 groupes $\mathfrak{S}_2$, $\mathfrak{S}_3$ et $\mathfrak{S}_4$ possèdent une suite de sous-groupes distingués dont les quotients successifs sont cycliques d'ordres 2 ou 3. On a en effet, le symbole d'inclusion signifiant ici que chaque groupe est distingué dans le suivant, et écrivant au-dessus l'ordre du quotient,

$$\{1\} = \mathfrak{A}_2 \overset{2}{\lhd} \mathfrak{S}_2 = \mathbf{Z}/2\mathbf{Z}\,;$$

$$\{1\} \overset{3}{\lhd} \langle(1\,2\,3)\rangle \overset{2}{\lhd} \mathfrak{A}_3 \overset{2}{\lhd} \mathfrak{S}_3\,;$$

$$\{1\} \overset{2}{\lhd} \{1;(1\,2)(3\,4)\} \overset{2}{\lhd} V_4 \overset{3}{\lhd} \mathfrak{A}_4 \overset{2}{\lhd} \mathfrak{S}_4\,,$$

Felix Klein (1849–1925)

où l'on a désigné par V_4 le *groupe de Klein*; c'est le sous-groupe de $\mathfrak{A}_4$ constitué des quatre permutations

$$\mathrm{id}, \quad (1\,2)(3\,4), \quad (1\,3)(2\,4), \quad (1\,4)(2\,3)$$

(produits de deux transpositions de supports disjoints et l'identité). C'est un groupe isomorphe à $(\mathbf{Z}/2\mathbf{Z})^2$.

Dans ce paragraphe, nous ne considérerons que des corps dont la caractéristique n'est ni 2, ni 3.

Considérons un tel corps K et soit P un polynôme unitaire dans $K[X]$ de degré $n \leqslant 4$. Soit $K \subset L$ l'extension de décomposition de P contenue dans une clôture algébrique Ω fixée de K. (Toutes les extensions que nous considérerons dans ce paragraphe seront contenues dans Ω.) On note $x_1, x_2, \ldots, x_n$ les racines de P dans L et $G = \mathrm{Gal}(L/K)$. C'est naturellement un sous-groupe de $\mathfrak{S}_n$.

Les intersections avec G des sous-groupes de $\mathfrak{S}_n$ que nous venons d'écrire définissent une suite de sous-groupe distingués de G dont les quotients successifs sont

cycliques d'ordre $\leqslant 3$, voire triviaux. Il leur correspond une suite d'extensions galoisiennes. On a déjà expliqué comment il correspond au sous-groupe $\mathfrak{A}_n \subset \mathfrak{S}_n$ l'extension engendrée par une racine carrée du discriminant de P.

Commençons par le degré 2, alors $P = X^2 + aX + b$ pour $a,\ b \in K$. Le discriminant de P vaut $\Delta = b^2 - 4ac$. Si c'est un carré dans K, $G = \{1\}$: P a ses deux racines dans K. Sinon, $L = K(\sqrt{\Delta})$ est de degré 2 sur K. On peut ordonner les racines de sorte que $x_1 - x_2 = \sqrt{\Delta}$. La relation $x_1 + x_2 = a$ permet d'en déduire $x_1 = (a + \sqrt{\Delta})/2$ et $x_2 = (a - \sqrt{\Delta})/2$.

Supposons maintenant que P soit un polynôme séparable de degré 3 dans $K[X]$:

$$P = X^3 + a_1X^2 + a_2X + a_3.$$

Le changement de variables $Y = X + a_1/3$ nous permet de supposer que la somme de ses racines est nulle, c'est-à-dire que P est de la forme $P = X^3 + pX + q$. Son discriminant est alors $D = -4p^3 - 27q^2$. Considérons alors la suite d'extensions

$$K \overset{2}{\subset} K(\sqrt{\Delta}) \overset{3}{\subset} L$$

où chaque extension est soit triviale, soit galoisienne de groupe de Galois le groupe cyclique dont le cardinal est indiqué au-dessus du symbole d'inclusion. Si le polynôme P est irréductible, on peut déjà en déduire le groupe de Galois de L sur K. En effet, le degré de l'extension $K \subset L$ est alors un multiple de 3. Par suite, $\mathrm{Gal}(L/K)$ vaut $\mathfrak{S}_3$ si Δ n'est pas un carré et $\mathfrak{A}_3$ si Δ est un carré.

Pour déterminer les racines de P, il nous faut commencer par adjoindre $\sqrt{\Delta}$. L'extension qui reste, $K(\sqrt{\Delta}) \overset{3}{\subset} L$ est ou triviale si le corps $K(\sqrt{\Delta})$ contient les trois racines de P, ou cyclique de groupe de Galois $\mathbf{Z}/3\mathbf{Z}$.

Pour pouvoir procéder comme au paragraphe 5.4 (qui concernait la théorie générale des extensions de groupe de Galois cyclique), adjoignons à $K(\sqrt{\Delta})$ les racines cubiques de l'unité ρ et ρ^2. Ce sont les racines du polynôme $X^2 + X + 1$. Rappelons qu'on peut supposer

$$\rho = -\frac{1}{2} + \frac{1}{2}\sqrt{-3}, \quad \rho^2 = -\frac{1}{2} - \frac{1}{2}\sqrt{-3}$$

où $\sqrt{-3}$ désigne une racine carrée de -3 dans $K(\sqrt{\Delta}, \rho)$. En particulier, $\rho - \rho^2 = \sqrt{-3}$. On note $K' = K(\rho)$ et $L' = L(\rho)$.

L'extension obtenue $K'(\sqrt{\Delta}) \subset L'$ est ou bien triviale, ou bien cyclique d'ordre 3. On peut écrire deux *résolvantes de Lagrange* correspondant à la permutation circulaire $(1, 2, 3)$:

$$\alpha = x_1 + \rho x_2 + \rho^2 x_3 \quad \text{et} \quad \beta = x_1 + \rho x_3 + \rho^2 x_2.$$

Calculons explicitement α^3 et β^3 :

$$\alpha^3 = x_1^3 + x_2^3 + x_3^3 + 6x_1x_2x_3 + 3\rho(x_1^2x_2 + x_2^2x_3 + x_3^2x_1) + 3\rho^2(x_1x_2^2 + x_2x_3^2 + x_3x_1^2)$$

et β^3 est donné par la formule obtenue en échangeant ρ et ρ^2. Le premier terme de ces expressions est une fonction symétrique des racines et s'exprime ainsi en fonction de p et q : on a de fait

$$\begin{aligned} x_1^3+x_2^3+x_3^3+6x_1x_2x_3 &= (x_1+x_2+x_3)^3-3(x_1^2x_2+\dots)\\ &= -3\big(x_1x_2(x_1+x_2)+\dots\big)\\ &= -3x_1x_2(-x_3)-\dots\\ &= 9x_1x_2x_3=-9q. \end{aligned}$$

Les deux autres termes ne sont pas des fonctions symétriques des trois racines, et ne peuvent pas l'être puisque sinon, α^3 et β^3 seraient (toujours) des éléments de K'. On *sait* cependant qu'ils appartiennent à $K'(\sqrt{\Delta})$ et il s'agit d'en donner une formule ! Comme Δ a deux racines carrées, on pose

$$\sqrt{\Delta}=(x_1-x_2)(x_1-x_3)(x_2-x_3)=(x_1^2x_2+x_2^2x_3+x_3^2x_1)-(x_1x_2^2+x_2x_3^2+x_3x_1^2).$$

Si l'on note

$$A=x_1^2x_2+x_2^2x_3+x_3^2x_1 \quad \text{et} \quad B=x_1x_2^2+x_2x_3^2+x_3x_1^2,$$

on a ainsi les relations

$$A+B=3q \quad \text{et} \quad A-B=\sqrt{\Delta},$$

d'où

$$A=\frac{3}{2}q+\frac{1}{2}\sqrt{\Delta} \quad \text{et} \quad B=\frac{3}{2}q-\frac{1}{2}\sqrt{\Delta}.$$

On reporte ceci dans les formules pour α^3 et β^3, ce qui donne

$$\begin{aligned} \alpha^3 &= -9q+3\rho A+3\rho^2B\\ &= -9q+\frac{3}{2}q(3\rho+3\rho^2)+\frac{1}{2}\sqrt{\Delta}(3\rho-3\rho^2)\\ &= -\frac{27}{2}q+\frac{3}{2}\sqrt{-3}\sqrt{\Delta} \end{aligned}$$

et

$$\beta^3=-\frac{27}{2}q-\frac{3}{2}\sqrt{-3}\sqrt{\Delta}.$$

De plus, $\sigma(\alpha)=\rho^{-1}\alpha$ et $\sigma(\beta)=\rho^{-2}\beta$, si bien que $\sigma(\alpha\beta)=\alpha\beta$ et $\alpha\beta$ est un élément de K'. Explicitement, on a

$$\begin{aligned} \alpha\beta &= (x_1+\rho x_2+\rho^2x_3)(x_1+\rho^2x_2+\rho x_3)\\ &= x_1^2+x_2^2+x_3^2+(\rho+\rho^2)(x_1x_2+x_2x_3+x_3x_1)\\ &= (x_1+x_2+x_3)^2+(\rho+\rho^2-2)(x_1x_2+x_2x_3+x_3x_1)\\ &= -3p. \end{aligned}$$

Pour en déduire des formules explicites pour x_1, x_2 et x_3, il reste à remarquer que l'on dispose d'un système de Cramer de trois équations à trois inconnues :

$$\begin{cases} x_1 + x_2 + x_3 = 0 \\ x_1 + \rho x_2 + \rho^2 x_3 = \alpha \\ x_1 + \rho^2 x_2 + \rho x_3 = \beta. \end{cases}$$

On a alors :

$$\begin{cases} x_1 = \dfrac{1}{3}\alpha + \dfrac{1}{3}\beta \\ x_2 = \dfrac{1}{3}\rho^2\alpha + \dfrac{1}{3}\rho\beta \\ x_3 = \dfrac{1}{3}\rho\alpha + \dfrac{1}{3}\rho^2\beta. \end{cases}$$

Jérôme Cardan (1501–1576)

Ce sont les « *formules de Cardan* » (1545). (Pour la petite histoire, Jérôme Cardan les avait achetées à Tartaglia moyennant la promesse de ne pas les diffuser, promesse rompue avec la parution en 1545 de l'*Ars magna sive de regulis algebraicis liber unus*. Auparavant, Scipione del Ferro, italien comme Cardan, avait découvert comment résoudre les équations de degré 3, mais ne divulgua sa méthode que sur son lit de mort, et encore, partiellement !)

Si l'on veut résoudre *en pratique* une équation du troisième degré, on peut ignorer tout ceci et ne retenir que la chose suivante : une des racines s'écrit $x = u + v$ avec $uv = -p/3$. Il reste à développer

$$0 = (u+v)^3 + p(u+v) + q = u^3 + v^3 + 3uv(u+v) + p(u+v) + q = u^3 + v^3 + q,$$

si bien que u^3 et v^3 sont solutions de l'équation du second degré

$$X^2 + qX - \frac{p^3}{27} = 0.$$

On en déduit u^3 moyennant une racine carrée du $q^2 + \dfrac{4}{27}p^3 = -\Delta/27$ puis u grâce à une extraction de racine cubique, d'où $x = u - p/3u$. (Ceci marche bien si $p \neq 0$, mais le cas $p = 0$ n'est pas sorcier.)

Remarquez aussi que si x_1, x_2 et x_3 sont des nombres réels, Δ est un réel strictement positif, donc les formules de Cardan nécessitent le passage par les nombres complexes. C'est ce qu'on appelle le *casus irreductibilis* et il n'y a pas de moyen d'y échapper (voir l'exercice 7.2).

Expliquons enfin la résolution des équations de degré 4. Soit $P = X^4 + pX^2 + qX + r$ un tel polynôme. (Un changement de variables affine permet effectivement de supposer

que le coefficient de X^3 est nul.) Rappelons la chaîne de sous-groupes distingués dans $\mathfrak{S}_4$:

$$\{1\} \overset{2}{\lhd} \{1; (1\,2)(3\,4)\} \overset{2}{\lhd} V_4 \overset{3}{\lhd} \mathfrak{A}_4 \overset{2}{\lhd} \mathfrak{S}_4,$$

d'où une chaîne d'extensions galoisiennes

$$K \overset{2}{\subset} K(\sqrt{\Delta}) \overset{3}{\subset} K_1 \overset{2}{\subset} K_2 \overset{2}{\subset} L,$$

les chiffres au-dessus du symbole d'inclusion signifiant que l'extension est ou bien cyclique du degré correspondant, ou bien triviale. Une approche analogue à celle menée pour les polynômes de degré 3 est donc possible.

On introduit d'emblée les *résolvantes* correspondant à l'extension $K \subset K_1$. En effet, les trois expressions

$$\theta_1 = (x_1 + x_2)(x_3 + x_4), \quad \theta_2 = (x_1 + x_3)(x_2 + x_4) \quad \text{et} \quad \theta_3 = (x_1 + x_4)(x_2 + x_3)$$

étant invariantes dans leur ensemble par permutations des indices, ce sont les trois racines d'un polynôme $Q \in K[X]$.

Exercice 5.5.1. — Montrer que $Q(X) = X^3 - 2pX^2 + (p^2 - 4r)X + q^2$.

Supposons que θ_1, θ_2 et θ_3 soient connues, par exemple à l'aide des formules de Cardan. Alors, les relations $(x_1 + x_2)(x_3 + x_4) = \theta_1$ et $(x_1 + x_2) + (x_3 + x_4) = 0$ montrent que $x_1 + x_2$ est une racine carrée de $-\theta_1$, soit $\sqrt{-\theta_1}$. De même, $x_1 + x_3$ et $x_1 + x_4$ sont des racines de $-\theta_2$ et $-\theta_3$. Il faut prendre garde au fait que les trois racines carrées $\sqrt{-\theta_j}$ ne peuvent pas être prises arbitrairement (le degré de l'extension $K_1 \subset L$ divise 4). On a en effet

$$\begin{aligned}\sqrt{-\theta_1}\sqrt{-\theta_2}\sqrt{-\theta_3} &= (x_1 + x_2)(x_1 + x_3)(x_1 + x_4) \\ &= x_1^3 + x_1^2(x_2 + x_3 + x_4) + x_1x_2x_3 + x_1x_2x_4 + x_1x_3x_4 + x_2x_3x_4 = -q.\end{aligned}$$

Si $q = 0$, l'équation quartique est « biquadratique » et se résout facilement. Si au contraire $q \neq 0$, les θ_i sont non-nuls et cette formule montre que $\sqrt{-\theta_3} = -q/\sqrt{-\theta_1}\sqrt{-\theta_2}$. Alors,

$$2x_1 = 3x_1 + x_2 + x_3 + x_4 = \sqrt{-\theta_1} + \sqrt{-\theta_2} + \sqrt{-\theta_3}$$

et des formules analogues pour x_2, x_3 et x_4.

Supposant que P est irréductible dans $K[X]$, déterminons maintenant les divers groupes de Galois possibles.

Remarquons d'abord que le degré de l'extension $K(\sqrt{\Delta}) \subset K_1$ est ou 1 ou 3, car elle est galoisienne et son groupe de Galois est un sous-quotient de $\mathfrak{A}_4/V_4 \simeq \mathbf{Z}/3\mathbf{Z}$. Cela montre que le polynôme Q ne peut avoir de facteur irréductible de degré 2 sur $K(\sqrt{\Delta})$. Il est donc, ou scindé, ou irréductible dans $K(\sqrt{\Delta})$.

Dans ce dernier cas, le degré $[L : K]$ est multiple de 3 et d'après le lemme de Cauchy (proposition 4.2.3, mais il est possible de le montrer directement dans ce cas), $\mathrm{Gal}(L/K)$

contient un élément d'ordre 3, donc un sous-groupe d'ordre 3. Mais il y a exactement quatre sous-groupes d'ordre 3, notés $H_1, \dots, H_4$, où H_i est le sous-groupe engendré par un 3-cycle qui fixe i. (Par exemple, H_1 est engendré par la permutation $(2,3,4)$.) Si $g \in \mathfrak{S}_4$ envoie i sur j, on a $gH_jg^{-1} = H_i$; puisque $\mathrm{Gal}(L/K)$ agit transitivement sur $\{1,2,3,4\}$, $\mathrm{Gal}(L/K)$ contient tous les H_i dès qu'il en contient un, donc il contient tous les 3-cycles, donc tout $\mathfrak{A}_4$. Autrement dit, si Q est irréductible sur $K(\sqrt{\Delta})$, alors $\mathrm{Gal}(L/K)$ contient $\mathfrak{A}_4$.

Si de plus Δ est un carré dans K, on a $\mathrm{Gal}(L/K) \subset \mathfrak{A}_4$, d'où l'égalité. Si Δ n'est pas un carré dans K, on a $\mathrm{Gal}(L/K) = \mathfrak{S}_4$.

Supposons maintenant que la résolvante Q soit scindée dans $K(\sqrt{\Delta})$, c'est-à-dire que $K_1 = K(\sqrt{\Delta})$. Puisque P est irréductible, $[L:K]$ est multiple de 4. De plus, $[L:K]$ divise 8, d'où $[L:K] = 4$ ou 8.

Si Δ est un carré dans K, on a $K_1 = K$ et $\mathrm{Gal}(L/K) \subset V_4$. Puisqu'aucun sous-groupe strict de V_4 n'agit transitivement sur $\{1,2,3,4\}$, on a nécessairement $\mathrm{Gal}(L/K) = V_4$ dans ce cas.

Si Δ n'est pas un carré dans K, on a $[K_1 : K] = 2$, d'où $[L:K] = 4$ si L est engendré par l'une des racines carrées des $-\theta_i$, et $[L:K] = 8$ sinon. Dans le premier cas, $\mathrm{Gal}(L/K)$ est un sous-groupe transitif d'ordre 4 de $\mathfrak{S}_4$ qui n'est pas contenu dans $\mathfrak{A}_4$. Seul le groupe cyclique engendré par une permutation circulaire est possible. Dans l'autre cas, $\mathrm{Gal}(L/K)$ est d'ordre 8 et est isomorphe au groupe dihédral D_4. (Remarque : c'est l'un des 2-sous-groupes de Sylow de $\mathfrak{S}_4$, il est engendré par un 4-cycle (a,b,c,d) et la transposition (a,c).)

5.6. Résolubilité par radicaux

Ce paragraphe explique le lien, découvert par Galois, entre résolubilité par radicaux d'une équation et le fait que son groupe de Galois est résoluble. Cela généralise plusieurs résultats :

– le théorème 5.1.1 concernant la constructibilité à la règle et au compas (d'un côté, un groupe d'ordre une puissance de 2 est résoluble ; de l'autre, les nombres constructibles sont contenus dans une extension quadratique itérée) ;

– la résolution explicite des équations de degrés 2, 3 ou 4 que nous avons exposés au paragraphe précédent (les groupes $\mathfrak{S}_2$, $\mathfrak{S}_3$ et $\mathfrak{S}_4$ sont résolubles) ;

– le théorème d'Abel (voir le corollaire 5.6.5 ci-dessous) selon lequel l'équation générale de degré $n \geqslant 5$ n'est pas résoluble par radicaux.

Pour simplifier, *nous ne considérerons dans ce paragraphe que des corps de caractéristique zéro.*

DÉFINITION 5.6.1. — *Soit E un corps de caractéristique nulle et soit $E \subset F$ une extension finie.*

On dit que l'extension $E \subset F$ est radicale élémentaire *d'exposant n s'il existe un élément $x \in F$ tel que $F = E[x]$ tel que $x^n \in E$.*

On dit que l'extensio $E \subset F$ est radicale *s'il existe une suite de sous-corps $E = E_0 \subset E_1 \subset \cdots \subset E_n = F$ telle que pour tout $i \in \{1; \ldots; n\}$, l'extension $E_{i-1} \subset E_i$ soit radicale élémentaire.*

On dit enfin que l'extension $E \subset F$ est résoluble par radicaux*, ou simplement* résoluble*, s'il existe une extension finie $F \subset F'$ telle que l'extension $E \subset F'$ soit radicale.*

PROPOSITION 5.6.2. — a) *Soit $E \subset F$ une extension finie et soit K un corps tel que $E \subset K \subset F$. Si l'extension $E \subset F$ est radicale, l'extension $K \subset F$ l'est aussi. Si l'extension $E \subset F$ est résoluble, les extensions $E \subset K$ et $K \subset F$ sont résolubles.*

b) *Soit $E \subset F_1$ et $E \subset F_2$ deux extensions finies isomorphes. Si $E \subset F_1$ est une extension radicale (*resp. *résoluble), alors $E \subset F_2$ l'est aussi.*

c) *Soit Ω un corps contenant E et soit $E \subset F$ et $E \subset F'$ deux extensions radicales (*resp. *résolubles) contenues dans Ω. Alors, l'extension composée $E \subset FF'$ est radicale (*resp. *résoluble).*

d) *Soit $E \subset F$ une extension finie radicale (*resp. *réosluble). Sa clôture galoisienne (dans toute clôture algébrique) $E \subset F^{\mathrm{g}}$ est encore radicale (*resp. *résoluble).*

Démonstration. — *a*) est évident sur la définition.

b) Supposons l'extension $E \subset F_1$ radicale. Soit $E = E_0 \subset E_1 \subset \cdots \subset E_n = F_1$ une suite d'extensions telles que $E_{i-1} \subset E_i$ soit radicale élémentaire. Soit $\sigma\colon F_1 \to F_2$ un E-isomorphisme. Pour tout i, l'extension $\sigma(E_{i-1}) \subset \sigma(E_i)$ est radicale élémentaire : si $E_i = E_{i-1}(x_i)$, avec $x_i^{n_i} \in E_{i-1}$, on a $\sigma(E_i) = \sigma(E_{i-1})(\sigma(x_i))$ et $\sigma(x_i)^{n_i} \in \sigma(E_{i-1})$. Par suite, l'extension $\sigma(E) \subset \sigma(F_1)$ est radicale, ce qu'il fallait démontrer.

Supposons l'extension $E \subset F_1$ résoluble et soit F_1' une extension de F_1 telle que l'extension $E \subset F_1'$ soit radicale. Si Ω désigne une clôture algébrique de F_2, il existe d'après le théorème 3.1.6 un homomorphisme $\sigma'\colon F_1' \to \Omega$ tel que $\sigma'|_{F_1} = \sigma$. Par suite, l'extension $E \subset \sigma'(F_1')$ est radicale et l'extension $E \subset F_2$ est résoluble.

c) Soit $E = E_0 \subset E_1 \subset \cdots \subset E_n = F$ et $E = E_0' \subset E_1' \subset \cdots \subset E_{n'}' = F'$ deux suites de corps telles que les extensions $E_{i-1} \subset E_i$ et $E_{i-1}' \subset E_i'$ soient radicales élémentaires. Si y_i est un élément de E_i' tel que $E_i' = E_{i-1}'(y_i)$ et dont une puissance appartient à E_{i-1}', on a $FE_i' = FE_{i-1}'(y_i)$ si bien que l'extension $FE_{i-1}' \subset FE_i'$ est radicale élémentaire. Ainsi, on a la suite d'extensions radicales élémentaires

$$E = E_0 \subset E_1 \subset \cdots \subset E_n = F \subset FE_1' \subset FE_2' \subset \cdots \subset FE_n' = FF'$$

et l'extension $E \subset FF'$ est radicale.

Supposons les deux extensions $E \subset F$ et $E \subset F'$ résolubles, et soit $F \subset L$ et $F' \subset L'$ des extensions telles que $E \subset L$ et $E \subset L'$ soient radicales. Les corps F et F' sont contenus

dans un même surcorps Ω de E, qu'on peut remplacer par sa clôture algébrique et donc supposer algébriquement clos. Il existe un F-homomorphisme $\sigma\colon L \to \Omega$ et un F'-homomorphisme $\sigma'\colon L' \to \Omega$. D'après *b*), les extensions $E \subset \sigma(L)$ et $E \subset \sigma'(L')$ sont radicales, donc l'extnesion $E \subset \sigma(L)\sigma'(L')$ l'est aussi. Puisque $E \subset FF' \subset \sigma(L)\sigma'(L')$, l'extension $E \subset FF'$ est résoluble.

d) Soit Ω une clôture algébrique de F. La clôture galoisienne de l'extension $E \subset F$ est le sous-corps de Ω engendré par les $\sigma(F)$, σ décrivant l'ensemble des E-homomorphismes de F dans Ω. D'après *b*), chacune des extensions $E \subset \sigma(F)$ est radicale (resp. résoluble). D'après le *c*) et une récurrence immédiate, l'extension $E \subset \prod_{\sigma} \sigma(F)$ est radicale (resp. résoluble). □

THÉORÈME 5.6.3. — *Soit E un corps de caractéristique zéro. Une extension galoisienne $E \subset F$ est résoluble si et seulement si son groupe de Galois* $\mathrm{Gal}(F/E)$ *est résoluble.*

Avant de passer à la démonstration, rappelons la théorie de Galois des extensions radicales élémentaires (théorème 5.4.1) et sa réciproque, le théorème 5.4.2, qui entraîne que les extensions galoisiennes de E de groupe de Galois $\mathbf{Z}/n\mathbf{Z}$ sont radicales élémentaires (rappelons que l'on a supposé que $\mathrm{card}\,\mu_n(E) = n$.)

PROPOSITION 5.6.4. — *Soit E un corps tel que* $\mathrm{card}\,\mu_n(E) = n$.

Si $E \subset F$ est une extension radicale élémentaire d'exposant n, elle est galoisienne et $\mathrm{Gal}(F/E)$ *est un sous-groupe de $\mathbf{Z}/n\mathbf{Z}$. (Il existe donc un entier d divisant n tel que* $\mathrm{Gal}(F/E) \simeq \mathbf{Z}/d\mathbf{Z}$.*)*

Réciproquement, si $E \subset F$ est une extension galoisienne de groupe de Galois $\mathbf{Z}/n\mathbf{Z}$, elle est radicale élémentaire d'exposant n.

La *démonstration du théorème 5.6.3* requiert quatre étapes.

a) *Soit $E \subset F$ une extension galoisienne, radicale, et supposons que E contienne une racine de l'unité d'ordre $[F : E]$, alors* $\mathrm{Gal}(F/E)$ *est un groupe résoluble.*

On démontre ceci par récurrence sur le degré $[F : E]$. Soit $E \subset E_1 \subset \cdots \subset F$ une suite d'extensions radicales élémentaires (non triviales). Notons $G = \mathrm{Gal}(F/E)$ et $H = \mathrm{Gal}(F/E_1)$. L'extension $E_1 \subset F$ est radicale et galoisienne. Comme $[F : E_1]$ et $[E_1 : E]$ divisent $[F : E]$, E contient une racine de l'unité d'ordre $[F : E_1]$ et d'ordre $[E_1 : E]$. Par récurrence, le groupe $H = \mathrm{Gal}(F/E_1)$ est résoluble. D'après la proposition précédente, l'extension $E \subset E_1$ est galoisienne, de groupe de Galois cyclique. Autrement dit, H est un sous-groupe distingué de G et $G/H \simeq \mathrm{Gal}(E/E_1)$ est un groupe fini cyclique. D'après la proposition 4.5.2, c), le groupe G est résoluble.

b) *Soit $E \subset F$ une extension galoisienne, résoluble, alors* $\mathrm{Gal}(F/E)$ *est résoluble.*

Soit $F \subset F_1$ une extension finie telle que l'extension $E \subset F_1$ soit radicale. Soit Ω une clôture algébrique de F_1 et soit $E \subset L$ la clôture galoisienne de l'extension $E \subset F_1$

dans Ω, de sorte que l'extension $E \subset L$ est radicale et galoisienne. Soit aussi K l'extension de E engendrée par une racine primitive de l'unité d'ordre $[L:E]$ dans Ω.

D'après la proposition 5.6.2, *c*), l'extension $K \subset KL$ est radicale et galoisienne. Puisque son degré $[KL:K]$ divise $[L:E]$, le *a*) implique que $\mathrm{Gal}(KL/K)$ est un groupe résoluble. D'autre part, l'extension $E \subset K$ est galoisienne et son groupe de Galois est un sous-groupe de $(\mathbf{Z}/N\mathbf{Z})^*$, où $N = [L:E]$ (voir le paragraphe 5.2). Ainsi, $\mathrm{Gal}(KL/K)$ est un sous-groupe distingué de $\mathrm{Gal}(KL/E)$ et le quotient $\mathrm{Gal}(KL/E)/\mathrm{Gal}(KL/K)$, isomorphe à $\mathrm{Gal}(K/E)$, est cyclique. Puisque le groupe $\mathrm{Gal}(KL/K)$ est résoluble, il résulte de la prop. 4.5.2, c), que le groupe $\mathrm{Gal}(KL/E)$ est résoluble. Comme $E \subset F$ est une extension galoisienne, avec $F \subset KL$, $\mathrm{Gal}(F/E)$ est un quotient de $\mathrm{Gal}(KL/E)$, donc est un groupe résoluble.

c) *Supposons que* $\mathrm{Gal}(F/E)$ *soit un groupe résoluble et que* E *contienne une racine de l'unité d'ordre* $[F:E]$. *Alors l'extension* $E \subset F$ *est radicale.*

On démontre ceci par récurrence sur $[F:E]$. Le groupe $G = \mathrm{Gal}(F/E)$ est résoluble. D'après la propositino 4.5.3, il possède un sous-groupe distingué H tel que G/H soit cyclique. Il existe ainsi un entier $d > 1$ divisant $[F:E]$ tel que G/H soit isomorphe à $\mathbf{Z}/d\mathbf{Z}$. Ainsi, l'extension $E \subset F^H$ est galoisienne, de groupe de Galosi $\mathbf{Z}/d\mathbf{Z}$; d'après la proposition 5.6.4, cette extension est radicale élémentaire. (Remarquer que E contient une racine primitive d-ième de l'unité.) L'extension $F^H \subset F$ est galoisienne et son groupe de Galois est égal à H, donc est résoluble (proposition 4.5.2, a). Puisque $[F:F^H]$ divise $[F:E]$, F^H contient une racine primitive de l'unité d'ordre $[F:F^H]$. Par récurrence, l'extension $F^H \subset F$ est radicale. Cela implique que l'extension $E \subset F$ est radicale.

d) *Si le groupe* $\mathrm{Gal}(F/E)$ *est résoluble, l'extension* $E \subset F$ *est résoluble.*

Soit Ω une clôture algébrique de F et soit K le corps engendré dans Ω par une racine primitive de l'unité d'ordre $[F:E]$. L'extension $E \subset K$ est radicale, galoisienne et son groupe de Galois est abélien. L'extension $K \subset KF$ est galoisienne et son groupe de Galois, isomorphe à un sous-groupe de $\mathrm{Gal}(F/E)$, est résoluble. Comme $[KF:K]$ divise $[F:E]$, K contient une racine de l'unité d'ordre $[KF:K]$ et le *c*) entraîne que l'extension $K \subset KF$ est radicale. Ainsi, l'extension $E \subset KF$ est radicale et l'extension $E \subset F$ est résoluble. □

Résoudre l'« équation générale de degré n » sur un corps K signifie donner des formules qui résolvent toute équation de degré n. De manière plus précise, on veut résoudre l'équation $X^n + a_1X^{n-1} + \cdots + a_n$ dans laquelle $a_1, \ldots, a_n$ sont des indéterminées. C'est une équation polynomiale sur le corps $K(a_1, \ldots, a_n)$ des fractions rationnelles en n indéterminées. D'après l'exercice 3.10, le groupe de Galois d'une extension de décomposition est le groupe symétrique $\mathfrak{S}_n$. Puisque ce groupe n'est pas résoluble si $n \geqslant 5$ (corollaire 4.6.8), le théorème 5.6.3 entraîne que l'équation générale de degré n n'est pas résoluble par radicaux, un résultat qu'avait pressenti le mathématicien italien P. Ruffini in 1799 et qu'a prouvé N. Abel en 1826.

COROLLAIRE 5.6.5 (Abel). — *Soit K un corps.*
Si $n \geqslant 5$, l'équation générale de degré n,

$$X^n + a_1 X^{n-1} + \cdots + a_n = 0,$$

vue comme équation polynomiale sur le corps $K(a_1, \ldots, a_n)$ des fractions rationnelles à coefficients dans K en n indéterminées, n'est pas résoluble par radicaux.

Dans la suite, et dans certains exercices, vous verrez des exemples explicites d'équations polynomiales (sur le corps des nombres rationnels) qui ne sont pas résolubles par radicaux.

5.7. Comment (ne pas) calculer des groupes de Galois

Les groupes de Galois qu'on veut étudier dans la pratique sont définis par un polynôme séparable P, irréductible ou non, à coefficients dans un corps K, et l'extension L à laquelle on s'intéresse est l'extension de décomposition de P, engendrée sur K par les racines $x_1, \ldots, x_n$ de P dans une clôture algébrique de K. Comme on l'a vu au paragraphe 3.3, le groupe de Galois $G = \mathrm{Gal}(L/K)$ est de manière naturelle un sous-groupe du groupe des permutations des racines $\{x_1, \ldots, x_n\}$, donc s'identifie à un sous-groupe du groupe symétrique $\mathfrak{S}_n$.

Le premier théorème de ce paragraphe montre que si l'on sait factoriser les polynômes à plusieurs indéterminées à coefficients dans K, on peut déterminer explicitement le groupe G.

Le groupe $G = \mathrm{Gal}(L/K)$ agit sur l'anneau $L[Y_1, \ldots, Y_n]$ coefficient par coefficient, donc aussi sur le corps des fractions rationnelles $L(Y_1, \ldots, Y_n)$ qui est son corps des fractions. Il agit aussi sur l'anneau des polynômes $L[X, Y_1, \ldots, Y_n]$. Pour simplifier les notations, nous écrirons Y comme abréviation de $Y_1, \ldots, Y_n$. Par exemple, nous écrirons $L[Y]$ pour $L[Y_1, \ldots, Y_n]$ et $L(Y)$ pour $L(Y_1, \ldots, Y_n)$.

Pour tout $\sigma \in \mathfrak{S}_n$, posons

$$\xi_\sigma = x_1 Y_{\sigma(1)} + \cdots + x_n Y_{\sigma(n)} \in L[Y].$$

LEMME 5.7.1. — a) *Pour tout élement τ du groupe de Galois $\mathrm{Gal}(L/K)$, on a*

$$\tau(\xi_\sigma) = \xi_{\sigma\tau^{-1}}.$$

b) *L'extension $K(Y) \subset L(Y)$ est galoisienne, de groupe de Galois G.*
c) *De plus, $\xi = x_1 Y_1 + \cdots + x_n Y_n$ en est un élément primitif.*

Démonstration. — Soit $\tau \in G$; on a

$$\tau(\xi_\sigma) = \sum_{i=1}^{n} \tau(x_i)\, Y_{\sigma(i)} = \sum_{i=1}^{n} x_{\tau(i)}\, Y_{\sigma(i)} = \sum_{j=1}^{n} x_j\, Y_{\sigma(\tau^{-1}(j))} = \xi_{\sigma\tau^{-1}},$$

ce qui démontre *a*).

b) Si $R = P/Q \in L(Y)$, on peut écrire

$$R = \frac{P}{Q} \prod_{\tau \in G\setminus\{1\}} \frac{\tau(Q)}{\tau(Q)} = \frac{P \prod\limits_{\tau \neq 1} \tau(Q)}{\prod\limits_{\tau} \tau(Q)}.$$

Le dénominateur D de cette dernière fraction appartient à $K[Y]$ puisqu'il est invariant par tout $\tau \in G$. Soit $N = RD$ son numérateur, alors R est invariant sous G si et seulement N l'est. Par suite, $L(Y)^G = K(Y)$, et il résulte du lemme d'Artin (Prop. 3.2.8) que l'extension $K(Y) \subset L(Y)$ est galoisienne de groupe de Galois G.

c) Posons $\xi = \xi_{\mathrm{id}} = x_1 Y_1 + \cdots + x_n Y_n$. Pour tout $\tau \in G$, $\tau(\xi) = \xi_{\tau^{-1}}$, si bien que $\tau = \mathrm{id}$ est le seul élément de G tel que $\tau(\xi) = \xi$. Cela montre que l'extension $K(Y) \subset L(Y)$ est engendrée par ξ. □

Il résulte du lemme que le polynôme minimal de ξ sur $K(Y)$ est égal à

$$M_\xi(T) = \prod_{\tau \in G} (T - \tau(\xi)) = \prod_{\tau \in G} (T - \xi_\tau).$$

Il appartient à $K[Y, T]$, est unitaire en T et est irréductible dans $K(Y)[T]$, donc est irréductible dans $K[Y, T]$ car l'anneau $K[Y]$ est factoriel.

THÉORÈME 5.7.2. — *Définissons un polynôme en des indéterminées $X, Y_1, \ldots, Y_n$ par la formule*

$$\mathcal{R}_P = \prod_{\sigma \in \mathfrak{S}_n} (T - \xi_\sigma) = \prod_{\sigma \in \mathfrak{S}_n} (T - (x_1 Y_{\sigma(1)} + \cdots + x_n Y_{\sigma(n)})).$$

C'est un polynôme séparable à coefficients dans K.

Soit M l'unique facteur irréductible de $\mathcal{R}_P$ dans $K(Y)[T]$ qui est unitaire en T et divisible par $T - \xi$ dans $L(Y)[T]$. Alors, $M = M_\xi$ et une permutation $\sigma \in \mathfrak{S}_n$ appartient à G si et seulement si

$$M(T, Y_1, \ldots, Y_n) = M(T, Y_{\sigma(1)}, \ldots, Y_{\sigma(n)}).$$

Démonstration. — Tout $\tau \in G$ définit une permutation des racines de $\mathcal{R}_P$, puisque $\tau(\xi_\sigma) = \xi_{\sigma\tau^{-1}}$, d'où $\tau(\mathcal{R}_P) = \mathcal{R}_P$ pour tout $\tau \in \mathrm{Gal}(L/K)$ et les coefficients de $\mathcal{R}_P$ appartiennent à K.

Puisque M et M_ξ ont un facteur commun $X - \xi$ dans $L(Y)[T]$, il résulte du corollaire 2.4.3 qu'ils ont un facteur commun dans $K(Y)[T]$. Étant tous deux unitaires et irréductibles, ils sont égaux et

$$M(T, Y_1, \ldots, Y_n) = \prod_{\tau \in G} (T - (x_1 Y_{\tau(1)} + \cdots + x_n Y_{\tau(n)})).$$

Enfin, si $\sigma \in \mathfrak{S}_n$, on a

$$\begin{aligned} M(T, Y_{\sigma(1)}, \dots, Y_{\sigma(n)}) &= \prod_{\tau \in G} \big(X - x_1 Y_{\tau(\sigma(1))} - \cdots - x_n Y_{\tau(\sigma(n))}\big) \\ &= \prod_{\tau \in G\sigma} \big(X - x_1 Y_{\tau(1)} - \cdots - x_n Y_{\tau(n)}\big). \end{aligned}$$

si bien que

$$M(X, Y_{\sigma(1)}, \dots, Y_{\sigma(n)}) = M(X, Y_1, \dots, Y_n)$$

si et seulement si $G\sigma = G$, c'est-à-dire $\sigma \in G$. □

Malheureusement, l'utilisation concrète de ce théorème est quasiment impossible. Par exemple, même si $K = \mathbf{Q}$ est le corps des nombres rationnels, factoriser des polynômes en plusieurs variables de degré élevé ($\deg \mathcal{R}_P = n!$) est d'une complexité phénoménale et cette approche échoue, même sur les systèmes de calculs les plus rapides qui soient disponibles. En revanche, nous en déduirons au paragraphe suivant une conséquence théorique fondamentale sur le comportement du groupe de Galois d'un polynôme par *spécialisation* de ses coefficients.

Remarquez que le polynôme $\mathcal{R}_P$ défini dans le théorème est symétrique en $Y_1, \dots, Y_n$ et qu'il est indépendant de la numérotation des racines. En revanche, son facteur irréductible M dépend de cette numérotation, ainsi que le groupe de Galois vu comme sous-groupe du groupe symétrique. Explicitons cette dépendance.

Soit $P \in K[X]$ un polynôme séparable de degré n et soit $K \to L$ une extension de décomposition de P. Soit R l'ensemble des racines de P dans L. Une numérotation de R est une bijection $\nu\colon \{1, \dots, n\} \xrightarrow{\sim} R$; elle définit un homomorphisme injectif $\lambda_\nu\colon \mathrm{Gal}(L/K) \hookrightarrow \mathfrak{S}_n$ tel que

$$\nu(\lambda_\nu(g)(i)) = g(\nu(i)), \quad g \in \mathrm{Gal}(L/K), \quad i \in \{1, \dots, n\}.$$

Notons $G_\nu = \lambda_\nu(\mathrm{Gal}(L/K))$ son image. Remarquons aussi que le polynôme $\mathcal{R}_P$ vérifie

$$\begin{aligned} \mathcal{R}_P(T) &= \prod_{\sigma \in \mathfrak{S}_n} \big(T - (x_{\sigma^{-1}(1)} Y_1 + \cdots + x_{\sigma^{-1}(n)} Y_n)\big) \\ &= \prod_{\text{numérotations } \nu} \big(T - (\nu(1) Y_1 + \cdots + \nu(n) Y_n)\big), \end{aligned}$$

où le dernier produit est sur l'ensemble de toutes les numérotations des racines de P. Notons aussi $\mathcal{R}_{P,\nu}$ le polynôme minimal de $\xi = \nu(1) Y_1 + \cdots + \nu(n) Y_n$ introduit plus haut, de sorte que

$$\begin{aligned} \mathcal{R}_{P,\nu}(T, Y_1, \dots, Y_n) &= \prod_{\tau \in G} \big(T - (\tau(\nu(1)) Y_1 + \cdots + \tau(\nu(n)) Y_n)\big) \\ &= \prod_{\sigma \in G_\nu} \big(T - (\nu(\sigma(1)) Y_1 + \cdots + \nu(\sigma(n)) Y_n)\big). \end{aligned}$$

Si μ est une autre numérotation, il existe une permutation $\sigma \in \mathfrak{S}_n$ telle que $\mu(i) = \nu(\sigma(i))$ pour tout $i \in \{1, \dots, n\}$. Alors, ou bien $\mathcal{R}_{P,\mu}$ et $\mathcal{R}_{P,\nu}$ sont premiers entre eux, ou

bien ils ont un facteur commun auquel cas ils sont nécessairement égaux, puisqu'ils sont tous deux irréductibles et unitaires. Ce cas se produit lorsque $\sigma \in G_v$. Ainsi, $\mathcal{R}_P$ est le produit des polynômes $\mathcal{R}_{P,v\circ\sigma}$, où σ parcourt les représentants dans $\mathfrak{S}_n$ des classes à gauche de G_v. Les plongements du groupe de Galois dans $\mathfrak{S}_n$ définis par les numérotations μ et ν satisfont la relations

$$\lambda_\mu(g) = \sigma^{-1}\lambda_\nu(g)\sigma.$$

En particulier, $G_\mu = \sigma^{-1}G_\nu\sigma$ est conjugué à G_ν dans $\mathfrak{S}_n$.

5.8. Spécialisation des groupes de Galois

Avant de donner une définition générale, explicitons deux exemples importants.

a) Soit P un polynôme unitaire à coefficients entiers et soit G le groupe de Galois d'une extension de décomposition de P sur $\mathbf{Q}$. Pour tout nombre premier, on peut réduire le polynôme P modulo p, d'où un nouveau groupe de Galois G_p correspondant à une extension finie de $\mathbf{Z}/p\mathbf{Z}$.

b) Soit $P \in \mathbf{Q}(t)[X]$ un polynôme à coefficients dans le corps $\mathbf{Q}(t)$ des fractions rationnelles. Pour tout nombre rationnel α qui n'est pas un pôle des coefficients de P, on peut évaluer le polynôme P en $t = \alpha$, d'où un polynôme $P_\alpha \in \mathbf{Q}[X]$ et un groupe de Galois G_α.

Nous allons voir que les groupes de Galois de ces équations spécialisées sont, de manière assez naturelle, des *sous-groupes* du groupe G.

DÉFINITION 5.8.1. — *Une* place *du corps K est une application $\varphi\colon K \to k \cup \{\infty\}$, où k est un corps, qui vérifie les propriétés suivantes :*

– *si $\varphi(x)$ et $\varphi(y)$ ne sont pas tous deux ∞, $\varphi(x+y) = \varphi(x)+\varphi(y)$, avec la convention $a+\infty = \infty$ pour $a \in k$;*

– *si $\{\varphi(x),\varphi(y)\} \neq \{0,\infty\}$, $\varphi(xy) = \varphi(x)\varphi(y)$, avec la convention $a\infty = \infty$ pour $a \neq 0$.*

Exemple 5.8.2. — Reprenons les deux exemples précédents.

a) Soit p un nombre premier. Soit $x = a/b$ un nombre rationnel, mis sous forme d'une fraction irréductible. Si p divise b, posons $\varphi_p(x) = \infty$. Si p ne divise pas b, soit $\varphi_p(x)$ le quotient dans $\mathbf{Z}/p\mathbf{Z}$ des classes de a et b. L'application $\varphi_p\colon \mathbf{Q} \to (\mathbf{Z}/p\mathbf{Z}) \cup \{\infty\}$ est une place.

b) Soit $\alpha \in \mathbf{Q}$. Une fraction rationnelle a une « valeur » en α, éventuellement ∞ si α est un pôle. L'application $\varphi_\alpha\colon \mathbf{Q}(t) \to \mathbf{Q} \cup \{\infty\}$ ainsi définie est une place.

Si $\varphi\colon K \to k\cup\{\infty\}$ est une place, soit $A = \varphi^{-1}(K)$ l'ensemble des $x \in K$ tels que $\varphi(x) \neq \infty$, et $\mathfrak{m} = \varphi^{-1}(0)$. La définition d'une place implique que A est un sous-anneau de K, appelé *anneau de valuation de φ*. (*Exercice* : le vérifier ! Voir aussi l'exercice 5.15.) Dans

les deux exemples ci-dessus, tout idéal de A est engendré par une puissance de p, ou de $X-\alpha$. En particulier, *dans ces deux cas, l'anneau A est un anneau principal.*

FIxons une place $\varphi\colon K \to k\cup\{\infty\}$ du corps K. Notons A l'anneau de valuation de φ. Soit $P\in K[X]$ un polynôme unitaire de degré n. Supposons que $P\in A[X]$ et que son discriminant $\Delta\in A$ vérifie $\varphi(\Delta)\neq 0$, de sorte que le polynôme $\varphi(P)\in k[X]$ est séparable.

Soit G le groupe de Galois d'une extension de décomposition L de P sur K, et soit H le groupe de Galois d'une extension de décomposition $k\subset\ell$ du polynôme $\varphi(P)$.

LEMME 5.8.3. — *Le polynôme $\mathcal{R}_P$ appartient à $A[T,Y]$ et $\mathcal{R}_{\varphi(P)}=\varphi(\mathcal{R}_P)$.*

Démonstration. — Considérons d'abord le polynôme

$$R=\prod_{\sigma\in\mathfrak{S}_n}(T-(\sum_{i=1}^{n}X_{\sigma(i)}Y_i))$$

vu comme polynôme en $T,Y_1,\dots,Y_n$ à coefficients dans $\mathbf{Z}[X_1,\dots,X_n]$. On écrit ainsi

$$R=\sum_{I=(i_0,\dots,i_n)}R_I(X_1,\dots,X_n)\,Y^{i_0}Y_1^{i_1}\dots Y_n^{i_n}.$$

Le polynôme R est symétrique en $X_1,\dots,X_n$, donc chacun de ses coefficients R_I est symétrique. Il existe donc pour tout I un polynôme $\tilde{R}_I\in\mathbf{Z}[S_1,\dots,S_n]$ tel que

$$R_I(X_1,\dots,X_n)=\tilde{R}_I(S_1(X),\dots,S_n(X)).$$

Écrivons $P=X^n+a_1X^{n-1}+\dots+a_n$ et notons $x_1,\dots,x_n$ les racines de P dans L, de sorte que $a_j=(-1)^jS_j(x_1,\dots,x_n)$. On a alors

$$\mathcal{R}_P=\sum_I\tilde{R}_I(-a_1,\dots,(-1)^na_n)\,T^{i_0}Y_1^{i_1}\dots Y_n^{i_n}.$$

Puisque les coefficients a_j appartiennent au sous-anneau A, $\mathcal{R}_P\in A[T,Y]$.

De plus, on a $\varphi(P)=X^n+\varphi(a_1)X^{n-1}+\dots+\varphi(a_n)$, et le même argument montre que

$$\tilde{R}_{\varphi(P)}=\sum_I\tilde{R}_I(-\varphi(a_1),\dots,(-1)^n\varphi(a_n))\,T^{i_0}Y_1^{i_1}\dots Y_n^{i_n}.$$

Par suite,

$$\varphi(R_P)=\sum_I\varphi(\tilde{R}_I(-a_1,\dots,(-1)^na_n))\,T^{i_0}Y_1^{i_1}\dots Y_n^{i_n}=\tilde{R}_{\varphi(P)}$$

est le polynôme attaché à $\varphi(P)$, ce qu'il fallait démontrer. □

LEMME 5.8.4. — *Pour toute numérotation ν des racines de P dans L, le polynôme $\mathcal{R}_{P,\nu}$ appartient à $A[T,Y]$.*

Démonstration. — Si l'anneau A est un anneau factoriel, par exemple dans les deux exemples ci-dessus, cela résulte du théorème 2.4.7. C'est vrai dans le cas général, car « un anneau de valuation est intégralement clos », mais nous ne le démontrerons pas ici, voir l'exercice 5.16. □

Nous avons vu que les facteurs irréductibles dans $k[T, Y]$ du polynôme $\mathcal{R}_{\varphi(P)}$ sont de la forme $\mathcal{R}_{\varphi(P),\mu}$ où μ est une numérotation des racines de $\varphi(P)$ dans ℓ. Puisque $\mathcal{R}_{P,\nu}$ divise $\mathcal{R}_P$, les lemmes précédents montrent que $\varphi(\mathcal{R}_{P,\nu})$ divise $\mathcal{R}_{\varphi(P)}$ dans $k[T, Y]$. Nous dirons qu'une numérotation ν des racines de P et une numérotation μ des racines de $\varphi(P)$ sont *compatibles* si $\mathcal{R}_{\varphi(P),\mu}$ divise $\varphi(\mathcal{R}_{P,\nu})$.

THÉORÈME 5.8.5. — *Fixons une numérotation ν des racines de P, d'où un homomorphisme injectif $\lambda_\nu\colon \mathrm{Gal}(L/K) \to \mathfrak{S}_n$ d'image G_ν.*

a) *Il existe une numérotation μ des racines de $\varphi(P)$ qui est compatible avec ν. Elle définit un plongement du groupe de Galois H dans $\mathfrak{S}_n$; son image H_μ est un sous-groupe de G_ν.*

b) *Soit μ' une numérotation des racines de $\varphi(P)$ et soit σ l'unique permutation $\in \mathfrak{S}_n$ telle que $\mu'(i) = \mu(\sigma(i))$ pour $i \in \{1, \dots, n\}$. Alors, μ' est compatible avec ν si et seulement si $\sigma \in G_\nu$. Dans ce cas, $H_{\mu'} = \sigma^{-1} H_\mu \sigma$ est conjugué à H_μ dans G_ν.*

Cela montre que « le » groupe de Galois H de l'équation spécialisée $\varphi(P)$ est, de façon presque naturelle, un *sous-groupe* du groupe de Galois G de l'équation P. De plus, si le groupe G est abélien, ou s'il s'avère que le groupe H est normal dans G, alors le groupe de Galois de l'équation spécialisée est un sous-groupe *canonique* du groupe de Galois de l'équation originale.

Démonstration. — Les facteurs irréductibles du polynôme $\varphi(\mathcal{R}_{P,\nu}) \in k[T, Y]$ divisent $\mathcal{R}_{\varphi(P)}$, donc sont de la forme $\mathcal{R}_{\varphi(P),\mu}$ pour certaines numérotations μ des racines de $\varphi(P)$ in ℓ. Ces numérotations sont précisément celles qui sont compatibles avec ν.

Plus précisément, si l'on désigne par N l'ensemble des numérotations des racines de $\varphi(P)$ qui sont compatibles avec ν, on a la formule

$$\varphi(\mathcal{R}_{P,\nu}) = \prod_{\mu \in N} (T - (\mu(1) Y_1 + \cdots + \mu(n) Y_n))$$

dans $\ell[T, Y]$. Soit $\sigma \in G_\nu$; alors,

$$\mathcal{R}_{P,\nu}(T, Y_{\sigma(1)}, \dots, Y_{\sigma(n)}) = \mathcal{R}_{P,\nu}(T, Y_1, \dots, Y_n),$$

d'où, appliquant φ aux deux membres,

$$\prod_{\mu \in N} (T - (\mu(1) Y_{\sigma(1)} + \cdots + \mu(n) Y_{\sigma(n)})) = \prod_{\mu \in N} (T - (\mu(1) Y_1 + \cdots + \mu(n) Y_n)).$$

En écrivant $\mu(i) = \mu \circ \sigma^{-1}(\sigma(i))$, on obtient la relation $N\sigma^{-1} = N$; en d'autres termes, $N = NG_\nu$ est une classe à droite modulo G_ν. Puisque le cardinal de N est celui de G_ν, on a $N = \mu G_\nu$ pour tout $\mu \in N$.

Fixons une telle numérotation μ. Le polynôme $\mathcal{R}_{\varphi(P),\mu}$ divise $\varphi(R_{P,\nu})$. En regardant les factorisations de ces polynômes dans $\ell[T, Y]$, on voit que $\mu H_\mu \subset N = \mu G_\nu$. Par suite, $H_\mu \subset G_\nu$.

Soit μ' une autre numérotation et soit $\sigma \in \mathfrak{S}_n$ telle que $\mu' = \mu \circ \sigma$. La numérotation μ' est compatible avec ν si et seulement si l'on a $\mu' \in N$, donc si et seulement si $\sigma \in G_\nu$. On a vu qu'alors, $H_{\mu'} = \sigma^{-1} H_\mu \sigma$. Les sous-groupes $H_{\mu'}$ et H_μ sont ainsi conjugués dans G_ν. □

Montrons maintenant comment, sur deux exemples, utiliser ce théorème pour obtenir des renseignements sur le groupe de Galois d'un polynôme à coefficients rationnels. Rappelons une remarque faite à la fin du paragraphe 3.5 sur les corps finis. Nous appelons *type* d'une permutation de $\{1,\dots,n\}$ la partition de n qu'elle définit (voir p. 85).

LEMME 5.8.6. — *Soit P un polynôme unitaire séparable à coefficients dans un corps fini k. Notons $n_1,\dots,n_r$ les degrés des facteurs irréductibles de P dans $k[X]$. Soit $k \to \ell$ une extension de décomposition de P ; l'automorphisme de Frobenius $F \in \mathrm{Gal}(\ell/k)$ induit une permutation des racines de P dans ℓ dont le type est précisément $(n_1,\dots,n_r)$.*

Rappelons aussi (prop. 4.6.1) que la classe de conjugaison de cette permutation est caractérisée par ces entiers $(n_1,\dots,n_r)$. Ainsi, ce lemme et le théorème 5.8.5 permettent d'exhiber des *classes de conjugaison* d'éléments du groupe de Galois. Dans certains cas, cela peut suffire à déterminer le groupe de Galois !

Exemple 5.8.7. — Commençons par le polynôme $P = X^5 - X - 1$. Notons G son groupe de Galois sur $\mathbf{Q}$, considéré comme sous-groupe du groupe des permutations des 5 racines, identifié à $\mathfrak{S}_5$.

Étudions la réduction modulo 2 du polynôme P. Il n'a pas de racine dans $\mathbf{F}_2$, mais il en a deux dans $\mathbf{F}_4$. En effet, le pgcd de $X^5 - X - 1$ et $X^4 - X$ vaut $X^2 - X - 1$, si bien que P a un facteur de degré 2, et l'autre facteur est de degré 3. En particulier, $P \mod 2$ est séparable sur $\mathbf{F}_2$ et son groupe de Galois sur $\mathbf{F}_2$ est engendré par un élément de $\mathfrak{S}_5$ de type $(2,3)$. D'après le théorème 5.8.5, G contient une permutation de ce type, donc aussi son cube qui est une transposition.

Regardons maintenant modulo 3. En calculant les pgcd de P et $X^3 - X$, *resp.* $X^9 - X$ (les systèmes de calcul formels sont bien utiles dans ce genre de situations...), on constate que $P \mod 3$ n'a pas de racine dans $\mathbf{F}_3$, ni dans $\mathbf{F}_9$. (*Exercice* : le faire à la main, en utilisant par exemple que l'on a $x^4 \in \{0, \pm 1\}$ pour tout $x \in \mathbf{F}_9$.) Par suite, le polynôme $P \mod 3$ est irréductible sur $\mathbf{F}_3$. D'après le théorème 5.8.5, G contient un 5-cycle. Incidemment, cela montre que le polynôme P est irréductible.

Il résulte maintenant de la proposition 4.6.2 que G est égal au groupe symétrique $\mathfrak{S}_5$. Au passage, cela fournit un exemple explicite d'une équation polynomiale à coefficients entiers qui n'est pas résoluble par radicaux, puisque son groupe de Galois, $\mathfrak{S}_5$, n'est pas résoluble.

Exemple 5.8.8. — Montrons de même que le groupe de Galois, noté G, du polynôme $P = X^5 + 20X - 16$ sur $\mathbf{Q}$ est égal au groupe alterné $\mathfrak{A}_5$. Modulo 2 on a $P \equiv X^5$ qui n'est pas séparable. Regardons ce qui se passe modulo 3. On a $P \equiv X^5 - X - 1$ modulo 3, et ainsi que nous l'avons vu dans l'exemple précédent, $P \mod 3$ est irréductible. De même, le groupe G contient un 5-cycle.

Modulo 7, $P = X^5 - X - 2$ et ses racines dans $\mathbf{F}_7$ sont 2 et 3. De plus, on a

$$P \equiv (X-2)(X-3)(X^3 - 2X^2 - 2X + 2) \pmod 7.$$

Le polynôme $X^3 - 2X^2 - 2X + 2$ n'a pas de racine dans $\mathbf{F}_7$ (le vérifier !), donc est irréductible puisqu'il est de degré 3. Cela implique que G contient un 3-cycle.

Modulo 23, on obtient une factorisation en un polynôme de degré 1 et le produit de deux polynômes de degré 2, d'où une permutation de la forme $(1)(2,3)(4,5)$ — une double transposition — dans G.

La considération d'autres nombres premiers ne semble pas apporter de renseignement supplémentaire sur G. Nous savons déjà que l'ordre du groupe est multiple de 2, 3 et 5, donc de leur ppcm 60. Puisque c'est un sous-groupe de $\mathfrak{S}_5$, son ordre divise $5! = 120$.

Nous devons alors utiliser une information d'un autre type. Remarquons que le discriminant de P est égal à

$$5^5 \times (-16)^4 + 4^4 \times 20^5 = 1024000000 = 2^1 6 5^6 = (2^8 5^3)^2$$

(voir l'exercice 3.21), donc est un carré dans $\mathbf{Q}$. D'après la proposition 3.4.2, cela implique que G est un sous-groupe de $\mathfrak{A}_5$. Comme $\operatorname{card} \mathfrak{A}_5 = 60$, on a donc $G = \mathfrak{A}_5$.

Dans des cas plus compliqués, réduction modulo des nombres premiers et considération du discriminant ne suffisent plus et on doit introduire des résolvantes plus générales (voir le paragraphe 3.4).

Exemple 5.8.9. — Les systèmes de calcul formel, tels MAGMA, PARI/GP ou MAPLE peuvent calculer des groupes de Galois, au moins si le degré de l'équation n'est pas trop grand. Voici par exemple la sortie d'une session (verbeuse) de MAPLE qui calcule le groupe de Galois du polynôme $t^5 - 5t + 12$ sur le corps des nombres rationnels.

```
> infolevel[galois]:=2;
> galois(t^5-5*t+12);
galois:   Computing the Galois group of    t^5-5*t+12
galois/absres:   64000000 = ‘‘(8000)^2
galois/absres:   Possible groups:   {"5T2", "5T1", "5T4"}
galois/absres:   p = 3    gives shape   2, 2, 1
galois/absres:   Removing   {"5T1"}
galois/absres:   Possible groups left:   {"5T2", "5T4"}
galois/absres:   p = 7    gives shape   5
galois/absres:   p = 11   gives shape   5
```

```
galois/absres:   p = 13   gives shape   5
galois/absres:   p = 17   gives shape   2, 2, 1
galois/absres:   p = 19   gives shape   5
galois/absres:   p = 23   gives shape   5
galois/absres:   p = 29   gives shape   2, 2, 1
galois/absres:   p = 31   gives shape   2, 2, 1
galois/absres:   p = 37   gives shape   5
galois/absres:   p = 41   gives shape   5
galois/absres:   The Galois group is probably one of   {"5T2"}
galois/respol:   Using the orbit-length partition of 2-sets.
galois/respol:   Calculating a resolvent polynomial...
galois/respol:   Factoring the resolvent polynomial...
galois/respol:   Orbit-length partition is   5, 5
galois/respol:   Removing   {"5T4"}
galois/respol:   Possible groups left:   {"5T2"}
        "5T2", {"5:2", "D(5)"}, "+", 10, {"(1 4)(2 3)", "(1 2 3 4 5)"}
```

Pour pouvoir comprendre ces lignes, il faut savoir qu'à conjugaison près, il y a cinq sous-groupes transitifs dans $\mathfrak{S}_5$. Ce sont

a) le groupe cyclique C_5, engendré par le 5-cycle $(1,2,3,4,5)$, isomorphe à $\mathbf{Z}/5\mathbf{Z}$ et noté dans ce contexte `5T1` ;

b) le groupe diédral D_5, engendré par $(1,2,3,4,5)$ et $(2,5)(3,4)$, désigné par `5T2` ;

c) le groupe métacyclique M_{20}, défini comme le normalisateur `5T3` de C_5 dans $\mathfrak{S}_5$,. De cardinal 20, il est isomorphe au groupe des applications $\mathbf{F}_5 \to \mathbf{F}_5$ de la forme $x \mapsto ax+b$ pour $a \in \mathbf{F}_5^*$ et $b \in \mathbf{F}_5$;

d) le groupe alterné $\mathfrak{A}_5$, de cardinal 60 et noté `5T4` ;

e) le groupe symétrique tout entier, $\mathfrak{S}_5$, noté `5T5`.

(En fait, tous les algorithmes utilisables pour calculer des groupes de Galois requièrent la liste des sous-groupes transitifs de $\mathfrak{S}_n$. Cete liste est connue jusqu'à $n = 31$. Les notations `5T1`, etc. viennent de cette classification.)

On calcule d'abord le discriminant. C'est un carré ($64\,000\,000 = (8000)^2$), donc le groupe est un sous-groupe du groupe alterné, ce qui exclut les groupes M_{20} et $\mathfrak{S}_5$ (respectivement `5T3` et `5T5`). Alors, le program réduit notre polynôme modulo de petits nombres premiers et calcule à chaque fois sa factorisation sur le corps fini correspondant, donc le type d'une permutation du groupe de Galois. Il vérifie simplement dans la liste des sous-groupes qui n'ont pas encore été exclus ceux qui contiennent une telle permutation. En fait, tous les éléments non-triviaux du groupe engendré par un 5-cycle sont eux-mêmes des 5-cycles, si bien que le groupe C_5 (`5T1`) est éliminé d'emblée en réduisant modulo $p = 3$. Cependant, on n'obtient aucune information nouvelle en réduisant modulo les nombres premiers jusqu'à 41.

MAPLE indique alors que le groupe est vraisemblablement égal au groupe D_5 (5T2). En effet, le théorème de densité de Čebotarev, un énoncé profond et difficile en théorie algébrique des nombres, affirme que toutes les classes de conjugaison d'éléments du groupe de Galois vont apparaître si l'on réduit modulo des nombres premiers de plus en plus grands, et qu'elles vont apparaître « proportionnellement » à leur cardinal. En fait, le type d'une permutation détecte seulement sa classe de conjugaison dans le groupe symétrique, si bien qu'un résultat antérieur dû à Frobenius est suffisant. La table 1 indique le nombre de permutations d'un type donné dans chacun des cinq groupes transitifs de $\mathfrak{S}_5$. Dans notre cas, les types qui apparaissons sont $(2,2)$, 4 fois, et (5), 7 fois. Si le groupe avait été $\mathfrak{A}_5$ (5T4), le type $(3,1,1)$ serait probablement apparu, si bien que MAPLE suggère que le groupe est D_5.

	C_5 (5T1)	D_5 (5T2)	M_{20} (5T3)	$\mathfrak{A}_5$ (5T4)	$\mathfrak{S}_5$ (5T5)
1,1,1,1,1	1	1	1	1	1
2,1,1,1					10
3,1,1				20	20
2,2,1		5	5	15	15
4,1			10		30
3,2					20
5	4	4	4	24	24
total	5	10	20	60	120

TABLE 1. Nombre de permutations de type donné dans les sous-groupes de $\mathfrak{S}_5$

Comme D_5 est un sous-groupe de $\mathfrak{A}_5$, il reste à vérifier si G est, à conjugaison près, un sous-groupe de D_5. Cela nécessite l'utilisation d'une résolvante telle que le polynôme

$$X_1X_2 + X_2X_3 + X_3X_4 + X_4X_5 + X_5X_1$$

dont le stabilisateur est exactement D_5. (Voyez-vous pourquoi ? Rappelez-vous que D_5 est le groupe de symétrie du pentagone régulier.) En calculant les racines complexes du polynôme $t^5 - 5t + 12$ avec une assez grande précision, on peut évaluer la résolvante précédente à toutes les permutations des racines. Certaines de ces évaluations sont des entiers et la proposition 3.4.5 entraîne que le groupe de Galois est D_5. En fait, un calcul en virgule flottante ne *démontre* pas réellement que les nombres obtenus sont des entiers, seulement qu'ils le sont à la précision du calcul. Cependant, des résultats tels que le théorème de Liouville (exercice 1.2) permettent de montrer que ce sont effectivement des entiers.

5.9. L'équation générique et le théorème d'irréductibilité de Hilbert

Dans ce paragraphe, j'explique quelques faits concernant la variation du groupe de Galois d'une équation polynomiale dépendant d'un paramètre Les trois théorèmes ci-dessous constituent ce qu'on appelle en général le « théorème d'irréductibilité de Hilbert ».

Soit P un polynôme unitaire à coefficients dans le corps $\mathbf{Q}(T)$ des fractions rationnelles. Supposons que P soit irréductible en tant que polynôme de $\mathbf{Q}(T)[X]$. Nous allons commencer par montrer que pour « beaucoup » de valeurs $t \in \mathbf{Z}$, le polynôme $P(t,X)$ n'a pas de racine dans $\mathbf{Q}$. Nous montrerons ensuite qu'en fait, pour « beaucoup » d'entiers t, $P(t,X)$ est irréductible. Rappelons (théorème 5.8.5) qu'essentiellement, le groupe de Galois sur $\mathbf{Q}$ du polynôme $P(t,X)$ est un sous-groupe du groupe de Galois sur $\mathbf{Q}(T)$ du polynôme $P(T,X)$. Le théorème 5.9.7 affirme que pour « beaucoup » d'entier t, ces groupes sont en fait *égaux*!

C'est un théorème *d'arithmétique*, et non d'algèbre, qui repose sur des propriétés du corps $\mathbf{Q}$. Il est évidemment faux si l'on remplace $\mathbf{Q}(T)$ par $\mathbf{C}(T)$: il existe des polynômes irréductibles $P \in \mathbf{C}(T)[X]$ de degré > 1. Cependant, comme $\mathbf{C}$ est algébriquement clos, pour tout t, le groupe de Galois du polynôme $P(t,X)$ est réduit à $\{1\}$. Le cœur des arguments arithmétiques se situe dans la démonstration de la proposition 5.9.1, au moment précis où la valeur absolue d'un entier non nul est minorée par 1. Notez qu'une telle minoration était aussi le point crucial dans la démonstration de la transcendance de e et π (théorèmes 1.6.3 et 1.6.6). Cependant, les arguments qui permettent de déduire de cette proposition les théorèmes 5.9.4, 5.9.6 et 5.9.7 sont de nature algébrique.

PROPOSITION 5.9.1. — *Soit e un entier $\geqslant 1$ et soit $\varphi = \sum_{n \geqslant -n_0} a_n u^{-n/e}$ une série de Laurent en $u^{-1/e}$ qui n'est pas un polynôme en u. (En d'autres termes, cette série a un coefficient $a_n \neq 0$, avec ou bien $n > 0$, ou bien n non multiple de e.) On suppose que $\varphi(u)$ converge pour $|u| \geqslant B_0$. Notons $N(B)$ le nombre des entiers $u \in [B_0, B]$ tels que $\varphi(u) \in \mathbf{Z}$. Alors, il existe $\alpha < 1$ tel que $N(B)/B^\alpha$ reste borné lorsque $B \to \infty$.*

Dans la suite, nous utiliserons la notation grand-O et écrirons $N(B) = \mathrm{O}(B^\alpha)$ pour dire que $N(B)/B^\alpha$ est borné lorsque B tend vers l'infini.

Démonstration. — Il suffit de traiter séparément les parties réelle et imaginaire de φ : l'une au moins n'est pas un polynôme. On suppose ainsi que φ est à coefficients réels. Remarquons que φ définit une fonction $\mathcal{C}^\infty$ sur l'intervalle $]B_0, +\infty[$, ses dérivées étant obtenues par dérivation terme à terme. On voit ainsi que pour $m > n_0/e$, $\varphi^{(\mu)}$ décroît vers 0 au voisinage de l'infini. Comme φ n'est pas un polynôme, $\varphi^{(m)}$ n'est pas identiquement nulle. Lorsque $u \to \infty$, $\varphi^{(m)}(u)$ est alors équivalent à son terme

de plus haut degré, qui est de la forme $cu^{-\mu}$ pour $c \neq 0$ et $\mu > 0$. Pour u assez grand, disons $u \geqslant B_1$, on a ainsi $c_1 u^{-\mu} \leqslant \left|\varphi^{(m)}(u)\right| \leqslant c_2 u^{-\mu}$.

Soit S l'ensemble des entiers $\geqslant B_0$ tels que $\varphi(u) \in \mathbf{Z}$. Considérons $m+1$ éléménts de S, $u_0 < \cdots < u_m$, avec $u_0 > B_1$, et introduisons le déterminant

$$D = \begin{vmatrix} 1 & \dots & 1 \\ u_0 & \dots & u_m \\ \vdots & & \vdots \\ u_0^{m-1} & \dots & u_m^m \\ \varphi(u_0) & \dots & \varphi(u_m) \end{vmatrix}.$$

C'est le déterminant d'une matrice à coefficients entiers, donc D est entier. D'après le lemme 5.9.3 ci-dessous, il existe un réel $\xi \in]u_0, u_m[$ tel que

$$D = \frac{1}{m!}\varphi^{(m)}(\xi) \prod_{i>j}(u_i - u_j).$$

Comme $u_0 \geqslant B_1$, $\varphi^{(m)}(\xi) \neq 0$, donc $D \neq 0$. Comme D est entier, $|D| \geqslant 1$, d'où la minoration

$$\prod_{i>j}(u_i - u_j) \geqslant \frac{m!}{\left|\varphi^{(m)}(\xi)\right|} \geqslant \frac{m!}{c_2}\xi^{\mu},$$

et, *a fortiori*,

$$(u_m - u_0)^{m(m+1)/2} \geqslant \frac{m!}{c_2} u_0^{\mu}.$$

Il existe ainsi des réels $b > 0$ et $\beta > 0$ tels que chaque fois que $u_0 < \cdots < u_m$ sont des éléments de S avec $u_0 > B_1$, on ait

$$u_m \geqslant u_0 + b u_0^{\beta}. \tag{5.9.2}$$

Posons maintenant $\alpha = 1/(1+\beta)$ et découpons l'intervalle $[B_0, B]$ en $[B_0, B^{\alpha}] \cup [B^{\alpha}, B]$. L'intervalle $[B_0, B^{\alpha}]$ contient au plus B^{α} éléments de S. Pour B assez grand, $B^{\alpha} \geqslant B_1$ et la minoration (5.9.2) implique que l'intervalle $[B^{\alpha}, B]$ contient au plus $(m/b)B^{1-\alpha\beta} = (m/b)B^{\alpha}$ éléments de S. En définitive, pour $B \geqslant B_1^{1/\alpha}$, $N(B) \leqslant (1 + m/b)B^{\alpha}$, ainsi qu'il fallait démontrer. □

LEMME 5.9.3. — *Soit I un intervalle de $\mathbf{R}$, $f : I \to \mathbf{R}$ une fonction de classe $\mathcal{C}^n$ et $x_0, \dots, x_n$ des éléments de I. Alors, il existe $\xi \in I$ tel que*

$$\begin{vmatrix} 1 & \dots & 1 \\ x_0 & \dots & x_n \\ \vdots & & \vdots \\ x_0^{n-1} & \dots & x_n^{n-1} \\ f(x_0) & \dots & f(x_n) \end{vmatrix} = \frac{f^{(n)}(\xi)}{n!} \prod_{i>j}(x_i - x_j).$$

Démonstration. — Il suffit de traiter le cas où les x_i sont tous distincts. Considérons x_0 comme un paramètre et notons $D(x_0)$ le déterminant ci-dessus. Si $A \in \mathbf{R}$, soit $F_A\colon I \to \mathbf{R}$ la fonction définie par $F_A(x) = D(x) - A\prod_{i=1}^{n}(x - x_i)$. La fonction F_A s'annule en $x_1, \ldots, x_n$; choisissons A pour qu'elle s'annule aussi en x_0.

D'après le lemme de Rolle, sa dérivée s'annule alors n fois sur I, puis sa dérivée seconde $n-1$ fois, etc. Enfin, il existe au moins un réel $\xi \in I$ tel que $F_A^{(n)}(\xi) = 0$. De plus,

$$F_A^{(n)}(\xi) = D^{(n)}(\xi) - An! = \begin{vmatrix} 0 & 1 & \ldots & 1 \\ x_0 & \ldots & x_n & \\ \vdots & \vdots & & \vdots \\ 0 & x_1^{n-1} & \ldots & x_n^{n-1} \\ f^{(n)}(\xi) & f(x_1) & \ldots & f(x_n) \end{vmatrix} - An!$$

$$= (-1)^n f^{(n)}(\xi) \begin{vmatrix} 1 & \ldots & 1 \\ x_0 & \ldots & x_n \\ \vdots & & \vdots \\ x_1^{n-1} & \ldots & x_n^{n-1} \end{vmatrix} - An!,$$

d'où $A = (-1)^n \dfrac{f^{(n)}(\xi)}{n!} \prod_{i>j\geqslant 1}(x_i - x_j)$ et

$$D(x_0) = A\prod_{i=1}^{n}(x_0 - x_i) = \frac{f^{(n)}(\xi)}{n!}\prod_{i>j}(x_i - x_j).$$

Le lemme est donc démontré. □

THÉORÈME 5.9.4. — *Soit P un polynôme unitaire de $\mathbf{Q}(T)[X]$. Soit $N(B)$ le cardinal de l'ensemble des entiers $t \in [0, B]$ tel que $P(t, X)$ a une racine dans $\mathbf{Q}$. Si P n'a pas de racine dans $\mathbf{Q}(T)$, il existe $\alpha < 1$ tel que, lorsque B tend vers l'infini, $N(B) = \mathrm{O}(B^\alpha)$.*

LEMME 5.9.5. — *Soit n le degré de P. Il existe un entier $e \geqslant 1$ et n séries de Laurent $x_1, \ldots, x_n$ à coefficients complexes, de rayon de convergence non nul, tels que pour tout nombre complexe t de module assez grand, les n racines complexes de $P(t^e, X)$ soient les $x_j(1/t)$, pour $1 \leqslant j \leqslant n$.*

Démonstration. — Puisque nous cherchons les racines de $P(t, X)$ pour t grand, faisons d'abord le changement de variable $t = 1/u$. Soit R un dénominateur commun des coefficients du polynôme $P(1/U, X) \in \mathbf{Q}(U)[X]$, de sorte que $R(U)P(1/U, X) \in \mathbf{Q}[U, X]$. En multipliant ce polynôme par $R(U)^{n-1}$, on boit qu'il existe un polynôme $\mathbf{Q} \in [U, Y]$, unitaire et de degré n par rapport à la variable Y, tel que $P(1/U, X)R(U)^n = Q(U, R(U)X)$. D'après le théorème de Puiseux (théorème 2.6.1), il existe un entier $e \geqslant 1$ et des séries entières $y_1, \ldots, y_n$ de rayon de convergence non

nul telles que, pour $|u|$ petit, les racines du polynôme $Q(u^e, Y)$ soient les $y_j(u)$, pour $1 \leqslant j \leqslant n$. Posons $x_j(u) = R(u)^{-e} y_j(u)$. En développant $R(u)^{-e}$ en série de Laurent au voisinage de $u = 0$, on voit que les x_j sont des séries de Laurent qui convergent pour $|u|$ petit, mais $u \neq 0$. Effectuons de nouveau le changement de variabless $t = 1/u$; les $x_j(1/t)$ sont les racines de $P(t^e, X)$, pourvu que $|t|$ soit assez grand. □

Démonstration du théoreme 5.9.4. — Soit $D \in \mathbf{Z}[T]$ un dénominateur commun des coefficients de P, de sorte que $P(T,X)D(T) \in \mathbf{Z}[T,X]$. Il existe un polynôme $\mathbf{Q} \in \mathbf{Z}[T,X]$, unitaire et de degré n en X tel que $P(T,X)D(T)^n = Q(T, D(T)X)$. Le polynôme Q n'a pas de racine dans $\mathbf{Q}(T)$ (si $R(T)$ était une telle racine, alors $R(T)/D(T)$ serait une racine de P dans $\mathbf{Q}(T)$). De même, si $D(t) \neq 0$, le polynôme $P(t,X) \in \mathbf{Z}[X]$ a une racine dans $\mathbf{Q}$ si et seulement si le polynôme $Q(t,X)$ a une racine dans $\mathbf{Q}$. Il suffit donc de démontrer le théorème pout le polynôme Q ce qui nous permet de suposer que $P \in \mathbf{Z}[T,X]$. Alors, pour tout $t \in \mathbf{Z}$, le polynôme $P(t,X)$ est unitaire et à coefficients entiers. D'après l'exercice 1.5, ses racines dans $\mathbf{Q}$ ne peuvent être que des entiers.

Notons $x_1, \ldots, x_n$ les séries fournies par le lemme 5.9.5. Comme P n'a pas de racine dans $\mathbf{Q}(T)$, aucune de ces séries n'est un polynôme. Il suffit maintenant d'appliquer à chacune d'entre elles la proposition 5.9.1 et d'ajouter les majorations obtenues, d'où la majoration requise pour $N(B)$. □

THÉORÈME 5.9.6. — *Soit $P \in \mathbf{Q}(T)X]$ un polynôme unitaire à coefficients dans $\mathbf{Q}(X)$, irréductible. Soit $N(B)$ le cardinal de l'ensemble des $t \in [0,B] \cap \mathbf{Z}$ tels que t soit un pôle d'un coefficient de P, ou bien tels que $P(t,X)$ soit réductible dans $\mathbf{Q}[X]$. Alors, il existe $\alpha < 1$ tel que $N(B) = \mathrm{O}(B^\alpha)$.*

Démonstration. — Comme dans la démonstration du théorème précédent, on suppose que $P \in \mathbf{Z}[T,X]$. Soit $x_1, \ldots, x_n$ les séries données par le lemme 5.9.5. Si t est assez grand, tout facteur unitaire de $P(t,X)$ est de la forme

$$P_I(t) = \prod_{i \in I} (X - x_i(t^{-1/e})),$$

où I est une partie de $\{1, \ldots, n\}$. Il suffit ainsi de montrer que, si $I \neq \emptyset$ et $I \neq \{1, \ldots, n\}$, l'ensemble des $t \in [0,B] \cap \mathbf{Z}$ tels que $P_I(t)$ appartient à $\mathbf{Z}[X]$ est de cardinal $\mathrm{O}(B^\alpha)$. Or, le polynôme P_I peut-être considéré comme polynôme à coefficients dans le corps K des séries de Laurent convergentes en $T^{-1/e}$, et c'est un facteur de P dans ce corps. Comme P est irréductible dans $\mathbf{Q}[T,X]$, le polynôme P_I n'appartient pas à $Q(T)[X]$ et au moins un de ses coefficients, disons φ_I, n'est pas un polynôme en T. La proposition 5.9.1 implique alors que l'ensemble des $t \in [0,B] \cap \mathbf{Z}$ tels que $\varphi_I(t)$ est entier est de cardinal $\mathrm{O}(B^\alpha)$ pour un certain $\alpha < 1$. Le théorème est donc démontré. □

Plus généralement, le théorème suivant affirme que le groupe de Galois sur $\mathbf{Q}$ du polynôme $P(t,X)$, avec $t \in \mathbf{Z}$, coïncide très souvent avec le groupe de Galois sur $\mathbf{Q}(T)$ du du polynôme $P(T,X)$.

THÉORÈME 5.9.7. — *Soit $P \in \mathbf{Q}(T)[X]$ un polynôme unitaire à coefficients dans $\mathbf{Q}(T)$. Soit G son groupe de Galois sur $\mathbf{Q}(T)$. Soit $N(B)$ le cardinal de l'ensemble des $t \in [0,B] \cap \mathbf{Z}$ tels que, ou bien t est un pôle de $P(T,X)$, ou bien le groupe de Galois du polynôme $P(t,X)$ sur $\mathbf{Q}$ soit un sous-groupe strict de G. Alors, il existe $\alpha < 1$ tel que $N(B) = \mathrm{O}(B^\alpha)$.*

Démonstration. — Comme dans la démonstration du théorème 5.9.6, on suppose que les coefficients de P sont des polynômes en T. Notons n le degré de P en la variable X. Soit $\mathbf{Q}(T) \to K$ une extension de décomposition du polynôme P et soit $\kappa \in K$ un élément primitif. Si $N = \operatorname{card} G$, alors $N = [K : \mathbf{Q}(T)]$ et N est aussi le degré du polynôme minimal Q de κ sur $\mathbf{Q}(T)$. *A priori,* Q est un polynôme de $\mathbf{Q}(T)[X]$. Cependant, si $D \in \mathbf{Q}[T]$ est un dénominateur commun des coefficients de Q, le polynôme minimal de $D\kappa$ est égal au polynôme $D(T)^N Q(T, D(T)^{-1}X)$ donc appartient à $\mathbf{Q}[T,X]$. Cela nous permet de supposer que $Q \in \mathbf{Q}[T,X]$.

Sur $\mathbf{Q}(T)$, les polynômes P et Q ont la même extension de décomposition, donc one le même groupe de Galois, même si en tant que groupes de permutations, ils ont l'air distincts (ils n'agissent pas sur le même ensemble).

D'après le lemme suivant, il existe une partie finie $S \subset \mathbf{Q}$ tel que pour tout $t \notin S$, les polynômes $Q(t,X)$ et $P(t,X)$ sont séparables ont une extension de décomposition commune K_t. D'après le théorème 5.8.5, le groupe de Galois $\mathrm{Gal}(K_t/\mathbf{Q})$ peut être considéré comme un sous-groupe de $\mathrm{Gal}(K/\mathbf{Q}(T))$, donc $[K_t : \mathbf{Q}] \leqslant [K : \mathbf{Q}(T)] = N$. D'après le théorème 5.9.6 appliqué au polynôme Q, il existe $\alpha < 1$ tel que le nombre des $t \in [0,B] \cap \mathbf{Z}$ tels que $t \notin S$ et $Q(t,X)$ soit irréductible est un $\mathrm{O}(B^\alpha)$. Pour de tels t, $[K_t : \mathbf{Q}] \geqslant N$, donc on a l'égalité $[K_t : \mathbf{Q}] = N$ et $\mathrm{Gal}(K_t/\mathbf{Q})$ est isomorphe à $\mathrm{Gal}(K/\mathbf{Q}(T))$. □

LEMME 5.9.8. — *Soit $P \in \mathbf{Q}(T)[X]$ un polynôme unitaire en X, soit $\mathbf{Q}(T) \to K$ une extension de décomposition de P. Soit $y \in K$ un élément primitif de polynôme minimal $Q \in \mathbf{Q}(T)[X]$. Il existe une partie finie $\Sigma \subset \mathbf{Q}$ tel que pour tout $t \notin \Sigma$, les polynômes $Q(t,X)$ et $P(t,X)$ sont séparables ont une extension de décomposition commune.*

Démonstration. — Notons $x_1, \ldots, x_n$ les racines de P dans K. Il existe des polynômes $A_i \in \mathbf{Q}(T)[Y]$ tels que pour tout i, $x_i = A_i(y)$, soit encore

$$P(T,X) = \prod_{i=1}^{n} (X - A_i(T,y)).$$

Remplaçant y par une indéterminée Y, cela implique que $Q(T,Y)$ divise les coefficients du polynôme

$$P(T,X) - \prod_{i=1}^{n} (X - A_i(T,Y))$$

car ces coefficients s'annulent en $Y = y$ et Q est le polynôme minimal de y. Il existe ainsi un polynôme $R \in \mathbf{Q}(T)[X,Y]$ tel que

$$P(T,X) = \prod_{i=1}^{n}(X - A_i(T,Y)) + R(T,Y)Q(T,Y). \tag{5.9.9}$$

De même, il existe un polynôme $B \in \mathbf{Q}(T)[X_1,\dots,X_n]$ tel que $y = Q(T,x_1,\dots,x_n)$. Pour la même raison, $Q(T,Y)$ divise les coefficients du polynôme $Y - B(T,A_1(Y),\dots,A_n(Y))$, si bien qu'il existe un polynôme $S \in \mathbf{Q}(T)[Y]$ tel que

$$Y = B(T,A_1(T,Y),\dots,A_n(T,Y)) + S(T,Y)Q(T,Y). \tag{5.9.10}$$

Enfin, le polynôme Q est scindé dans K, donc il existe des polynômes $C_i \in \mathbf{Q}(T)[Y]$ tels que l'on ait

$$Q(T,X) = \prod_{i=1}^{N}(X - C_i(T,y)).$$

Comme précédemment, il en résulte l'existence d'un polynôme $U \in \mathbf{Q}(T)[X,Y]$ tel que

$$Q(T,X) = \prod_{i=1}^{N}(X - C_i(T,Y)) + U(T,X,Y)Q(T,Y). \tag{5.9.11}$$

Les coefficients des polynômes $P,Q,A_1,\dots,A_n,B,C_1,\dots,C_N,R,S$ appartiennent à $\mathbf{Q}(T)$. Soit Σ l'ensemble des $t \in \mathbf{Q}$ tels que ou bien t soit un pôle de l'un de ces coefficients, ou bien le discriminant de P s'annule en t, ou bien celui de Q s'annule en t. Par définition, pour tout $t \notin \Sigma$, les polynômes $P(t,X)$ et $Q(t,X)$ sont séparables et les relations précédentes restent vraies une fois évaluées en $T = t$.

Soit $t \in \mathbf{Q} \setminus \Sigma$. Pour démontrer le lemme, il suffit maintenant de montrer que le polynôme $P(t,X)$ est scindé dans toute extension où $Q(t,X)$ l'est, et réciproquement.

Soit ainsi L une extension de $\mathbf{Q}$ dans laquelle $Q(t,X)$ ait une racine η. Pour $i \in \{1,\dots,n\}$, posons $\xi_i = A_i(t,\eta)$. La relation (5.9.9) montre que $P(t,X) = \prod_{i=1}^{n}(X - \xi_i)$, donc $P(t,X)$ est scindé dans L.

Réciproquement, soit L une extension de $\mathbf{Q}$ dans laquelle le polynôme $P(t,X)$ est scindé. Notons ses racines $\xi_1,\dots,\xi_n$. Soit η une racine de $Q(t,X)$ dans une extension L' de L. Les racines de P dans L' sont données par les $A_i(t,\eta)$, pour $1 \leqslant i \leqslant n$, donc il existe une permutation $\sigma \in \mathfrak{S}_n$ tells que $A_i(t,\eta) = \xi_{\sigma(i)}$ pour tout i. La relation (5.9.10) entraîne que

$$\eta = B(t,\xi_{\sigma(1)},\dots,\xi_{\sigma(n)}).$$

Par suite, $\eta \in L$ et $\mathbf{Q}(t,X)$ a une racine dans L. Alors, la relation (5.9.11) entraîne que $Q(t,X) = \prod_{i=1}^{N}(X - C_i(t,\eta))$ est scindé dans L. □

Exercices

Exercice 5.1. — **a)** Soit G un groupe fini et soit H un sous-groupe de G tel que $(G:H)=2$. Montrer que H est distingué dans G.

b) Quel lien y a-t-il avec le lemme 5.1.3 ?

c) Plus généralement, si $(G:H)$ est égal au plus petit facteur premier de G, montrer que H est distingué dans G.

Exercice 5.2. — Soit $K \subset E$ et $K \subset F$ deux extensions finies de degrés premiers entre eux, contenues dans une extension Ω de K. Montrer que $E \cap F = K$ et que $[EF:K] = [E:K][F:K]$.

Exercice 5.3. — Soit α et β deux racines distinctes dans $\mathbf{C}$ du polynôme X^3-2. Soit $E=\mathbf{Q}(\alpha)$, $F=\mathbf{Q}(\beta)$.

a) Montrer que l'extension composée EF est l'extension de décomposition du polynôme X^3-2 sur $\mathbf{Q}$.

b) Montrer que $E \cap F = \mathbf{Q}$, bien que $[EF:\mathbf{Q}] \neq [F:\mathbf{Q}]\,[E:\mathbf{Q}]$. (Cela montre que l'hypothèse du corollaire 5.3.3 imposant que l'une des extensions est galoisienne ne peut pas être supprimée.)

Exercice 5.4. — Cet exercice est la suite de l'exercice 1.13. On y avait montré que les deux racines réelles du polynôme $P=X^4-X-1$ ne sont pas toutes deux constructibles à la règle et au compas.

a) Montrer qu'en fait aucune racine de P n'est constructible à la règle et au compas.

b) Quel est le groupe de Galois de l'extension engendrée par les racines de P ?

Exercice 5.5. — Soit p un nombre premier, $P \in \mathbf{Q}[X]$ un polynôme irréductible de degré p ayant 2 racines complexes conjuguées, x_1, x_2 et $p-2$ racines réelles, $x_3, \ldots, x_p$. On note $K = \mathbf{Q}(x_1,\ldots,x_p)$ le corps engendré par les racines de P dans $\mathbf{C}$ et on identifie $\mathrm{Gal}(K/\mathbf{Q})$ à un sous-groupe de $\mathfrak{S}_p$.

a) Montrer que la permutation $\tau=(1\,2)$ appartient à $\mathrm{Gal}(K/\mathbf{Q})$. (Penser à la conjugaison complexe.)

b) Montrer que $\mathrm{Gal}(K/\mathbf{Q})$ contient un p-cycle σ.

c) Montrer que σ et τ engendrent $\mathfrak{S}_p$. En déduire que $\mathrm{Gal}(K/\mathbf{Q}) = \mathfrak{S}_p$.

d) *Application* : $P=X^5-6X+3$. (Pour l'irréductibilité de P, utiliser l'exercice 1.10.)

Exercice 5.6 (Extensions d'Artin-Schreier). — Soit p un nombre premier. Soit K un corps de caractéristique p et a un élément de K. On suppose que le polynôme $P=X^p-X-a$ n'a pas de racine dans K. Soit $K \subset L$ une extension de décomposition de P.

a) Si x est une racine de P dans L, montrer que les autres racines de P sont $x=x+1$, $x+2$, $\ldots$, $x+p-1$.

b) Montrer que P est irréductible dans $K[X]$. (Si Q est un diviseur de P de degré d, considérer le terme de degré $d-1$ de Q.)

c) (Autre démonstration de l'irréductibilité de P.) Si $x+u$ (pour $1 \leqslant u < p$) est une autre racine du polynôme minimal de x sur K, montrer qu'il existe $\sigma \in \mathrm{Gal}(L/K)$ tel que $\sigma(x)=x+u$.

En déduire qu'il existe $\sigma \in \mathrm{Gal}(L/K)$ tel que $\sigma(x) = x+1$ et que toutes les racines de P sont des conguguées de x. Conclure.

d) Montrer que $L = K[x]$ et que le groupe de Galois de L/K est isomorphe à $\mathbf{Z}/p\mathbf{Z}$.

Exercice 5.7 (Extensions cycliques de degré p en caractéristique p)

Soit K un corps de caractéristique $p > 0$ et soit L une extension finie de K, galoisienne de groupe de Galois $\mathbf{Z}/p\mathbf{Z}$. Soit σ un générateur de $\mathrm{Gal}(L/K)$.

a) Montrer qu'il existe $x \in L$ tel que $\sum_{i=0}^{p-1} \sigma^i(x) = 1$.

On pose alors $\alpha = \sum_{i=0}^{p-1} i\sigma^i(x)$.

b) Calculer $\sigma(\alpha)$. En déduire que $\alpha \notin K$ mais que $a = \alpha^p - \alpha$ appartient à K.

c) Montrer alors que $L = K[\alpha]$ et que $X^p - X - a$ est le polynôme minimal de α sur K.

Exercice 5.8. — Dans cet exercice, nous allons déterminer à l'aide de la réduction modulo des nombres premiers le groupe de Galois sur $\mathbf{Q}$ du polynôme $P = X^7 - X - 1$.

a) Montrer que P n'a pas de racine dans le corps fini $\mathbf{F}_8$. En déduire qu'il est irréductible en tant que polynôme de $\mathbf{F}_2[X]$.

b) Montrer que les seules racines de P dans $\mathbf{F}_9$ sont les racines du polynôme $X^2 + X - 1$ et qu'elles sont simples. En conclure que sur $\mathbf{F}_3$, P se scinde en le produit de deux polynômes irréductibles de degrés 2 et 5.

c) Montrer que le groupe de Galois de P sur le corps des nombres rationnels contient un 7-cycle et une transposition. En déduire que c'est le groupe symétrique $\mathfrak{S}_7$.

Remarque. —

En fait, pour tout entier n, le groupe de Galois sur $\mathbf{Q}$ du polynôme $X^n - X - 1$ est égal à $\mathfrak{S}_n$. Pour de petites valeurs de n, vous pouvez tenter de le prouver par des méthodes analogues. Si les calculs sont trop difficiles, n'hésitez pas à utiliser des programmes de calcul formel, ils savent factoriser des polynômes modulo des nombres premiers. Par exemple, la réponse à la première question est obtenue en moins d'une milliseconde en entrant `factormod(x^7-x-1,2)` dans PARI/GP, ou `Factor(x^7-x-1) mod 2` dans MAPLE.

Exercice 5.9 (Une autre démonstration du théorème 5.4.2). — Soit $K \subset L$ une extension finie de degré $n \geqslant 2$. Supposons qu'elle soit galoisienne et que son groupe de Galois est engendré par un élément $\sigma \in \mathrm{Gal}(L/K)$. Supposons de plus que $\mathrm{card}\,\mu_n(K) = n$.

a) Montrer que $\sigma : L \to L$ est un morphisme de K-espaces vectoriels et que ses valeurs propres sont des racines n-ièmes de l'unité.

b) Montrer que L est la somme directe des espaces propres $L_\zeta = \{x \in L ; \sigma(x) = \zeta x\}$, pour $\zeta \in \mu_n(K)$.

c) Si $y \in L_\zeta \setminus \{0\}$, montrer que l'application $x \mapsto x/y$ est une application K-linéaire injective $L_\zeta \to L_1$.

d) Montrer que $L_1 = K$ et en déduire que $\dim L_\zeta = 1$ pour tout $\zeta \in \mu_n(K)$. En particulier, si ζ est une racine primitive n-ième de l'unité, il existe $x \in L^*$ tel que $\sigma(x) = \zeta x$.

Exercice 5.10. — Soit $K \subset E$ une extension cyclique, extension de décomposition d'un polynôme irréductible de degré n. On suppose que $\operatorname{card} \mu_n(K) = n$; on fixe une racine primitive n-ième de l'unité dans K. Soit aussi σ un générateur de $\mathrm{Gal}(E/K)$. On note $x_1, x_2, \ldots, x_n$ les racines de P dans E.

Si $0 \leqslant j < n$, on pose

$$\alpha_j = x_1 + \zeta^j \sigma(x_1) + \cdots + \zeta^{j(n-1)} \sigma^{(n-1)}(x_1).$$

a) Montrer que $\alpha_0 \in K$. Montrer que pour tout $j \in \{1; \ldots; n-1\}$, α_j^n appartient à K.

b) Montrer que E est engendrée par les α_j.

c) Si n est premier, en déduire qu'il existe $j \in \{1; \ldots; n-1\}$ tel que $E = K(\sqrt[n]{\alpha_j^n})$.

Exercice 5.11. — Soit K un corps et considérons le polynôme $P = X^n - a$, où $a \in K^*$. Supposons de plus que n ne soit pas multiple de la caractéristique de K, de sorte que P est séparable.

a) Soit L une extension de décomposition de K. Montrer que L contient une racine primitive n-ième de l'unité, ζ. Posons $K_1 = K(\zeta)$ et $\mu_n = \mu_n(K_1)$.

b) Si $m \in \mathbf{Z}$ est premier à n, montrer que l'application $u \mapsto u^m$ est un automorphisme de μ_n. Inversement, montrer que tout automorphisme de μ_n est de cette forme. En déduire un isomorphisme de groupes $(\mathbf{Z}/n\mathbf{Z})^* \simeq \mathrm{Aut}(\mu_n)$.

c) Montrer que les extensions $K \subset K_1$ et $K_1 \subset L$ sont galoisiennes et identifier leurs groupes de Galois à des sous-groupes A de $(\mathbf{Z}/n\mathbf{Z})^*$ et B de μ_n. (Fixer $x \in L$ tel que $x^n = a$ et considérer l'action de $\mathrm{Gal}(L/K)$ sur x et ζ.)

d) Montrer que l'isomorphisme de la question b) se restreint en un morphisme de groupes $\varphi\colon A \to \mathrm{Aut}(B)$ et démontrer que $\mathrm{Gal}(L/K)$ est isomorphe au produit semi-direct $A \rtimes_\varphi B$.

e) On suppose de plus que $[K_1 : K]$ est premier à n et que P est irréductible dans $K[X]$. Montrer que P est encore irréductible dans $K_1[X]$ et que $B = \mu_n$.

f) *Application numérique*: $K = \mathbf{Q}$ and $P = X^7 - 2$. Montrer que $\mathrm{Gal}(L/K)$ est d'ordre 42 et qu'il est isomorphe au groupe des permutations de $\mathbf{Z}/7\mathbf{Z}$ de la forme $n \mapsto an + b$ pour $a \in (\mathbf{Z}/7\mathbf{Z})^*$ et $b \in \mathbf{Z}/7\mathbf{Z}$.

Exercice 5.12. — Cet exercice propose une démonstration via la théorie de Galois du théorème fondamental de l'algèbre.

Soit $\mathbf{R} \subset K$ une extension galoisienne du corps des nombres réels qui contient le corps des nombres complexes $\mathbf{C}$. Soit $G = \mathrm{Gal}(K/\mathbf{R})$ soit P un 2-sous-groupe de Sylow de G. On pose $\operatorname{card} P = 2^n$.

a) En utilisant le fait que $\mathbf{R}$ n'a pas d'extension finie de degré impair, montrer que $G = P$.

b) Soit $P_1 = \mathrm{Gal}(K/\mathbf{C})$. D'après le lemme 5.1.3, il existe une suite de sous-groupes

$$\{1\} = P_n \subset \cdots \subset P_2 \subset P_1 \subset P$$

telle que $(P_{j+1} : P_j) = 2$ pour tout j. On pose $K_j = K^{P_j}$. Montrer que l'extension $K_j \subset K_{j+1}$ est une extension quadratique. En utilisant que tout nombre complexe est un carré, montrer que $n = 1$, donc que $K = \mathbf{C}$.

Exercice 5.13. — Dans cet exercice, on va démontrer le théorème 5.1.1 sans aucune théorie des groupes, en utilisant à la place des idées utilisées dans la deuxième démonstration du théorème fondamental de l'algèbre.

Soit z un nombre algébrique, et supposons que le degré de l'extension de $\mathbf{Q}$ engendré par ses conjugués $z_1, \dots, z_d$ soit une puissance de 2.

Remarquer que d est une puissance de 2. Par récurrence sur d, montrer comme suit que z est constructible.

a) Fixons $c \in \mathbf{Q}$ et posons $z_{i,j,c} = z_i + z_j + c z_i z_j$ et $Q_c = \prod_{i<j} (X - z_{i,j,c})$. Montrer que Q_c est un polynôme à coefficients rationnels et que les degrés de ses facteurs irréductibles dans $\mathbf{Q}[X]$ sont des puissances de 2. Montrer que l'un au moins de ces degrés divise $d/2$. En déduire qu'il existe $i < j$ tels que $z_i + z_j + c z_i z_j$ soit constructible.

b) Montrer qu'il existe i et j tels que $z_i + z_j$ et $z_i z_j$ soient constructible. En déduire que z_i et z_j sont constructibles.

c) Montrer que z est constructible.

Exercice 5.14. — Soit n un entier, $n \geqslant 5$. Soit $K \subset L$ une extension galoisienne finie de groupes de Galois $\mathfrak{S}_n$.

a) Montrer qu'il existe une seule extension quadratique $K \subset K_1$, avec $K_1 \subset L$. Quel est le groupe de Galois de l'extension $K_1 \subset L$? (Utiliser l'exercice 4.17.)

b) Montrer que le degré de tout élément de $L \setminus K_1$ est au moins n.

Exercice 5.15. — Soit K un corps et soit $\varphi \colon K \to k \cup \{\infty\}$ une place de K. Rappelons que l'anneau de valuation de φ est défini comme l'ensemble $A = \{x \in K ; \varphi(x) \neq \infty\}$.

a) Montrer que pour tout $x \in K^*$, ou bien x, ou bien $1/x$ appartient à A (c'est la définition générale d'un anneau de valuation).

b) Soit $\mathfrak{m} = \varphi^{-1}(0)$. Montrer que $\mathfrak{m}$ est un idéal de A et qu'un élément $a \in A$ est inversible dans A si et seulement si $a \notin \mathfrak{m}$.

c) En déduire que $\mathfrak{m}$ est l'unique idéal maximal de A, que $A/\mathfrak{m}$ est un corps et que φ induit un homomorphisme de corps $A/\mathfrak{m} \to k$.

d) Dans les deux exemples du texte (exemple 5.8.2), montrer que l'idéal $\mathfrak{m}$ est engendré par un élément π. Montrer de plus que tout idéal de A est engendré par une puissance de π. (In fait, on peut poser $\pi = p$ dans le cas *a*) et $\pi = X - \alpha$ dans le cas *b*).) En particulier, dans ces deux cas, l'anneau A est un anneau principal.

Exercice 5.16. — Soit K un corps et soit A un sous-anneau de K Fixons une clôture algébrique Ω de K. On dit qu'un élément $x \in \Omega$ est *entier* sur A s'il existe un polynôme unitaire $P \in A[X]$ tel que $P(x) = 0$.

a) Soit x et y des éléments de Ω qui sont entiers sur A. Soit P et $Q \in A[X]$ des polynômes unitaires tels que $P(x) = Q(y) = 0$. On écrit

$$P = \prod_{i=1}^{n} (X - x_i) \quad \text{et} \quad Q = \prod_{j=1}^{m} (X - y_j)$$

où les x_i et les y_j sont des éléments de Ω. Montrer que les coefficients du polynôme $R = \prod_{i,j}(X - x_i - y_j)$ appartiennent à A. (Écrire $R = \prod_i Q(X - x_i)$ et utiliser le théorème sur les polynômes symétriques.) En déduire que $x+y$ est entier sur A. Prouver de même que xy est entier sur A.

b) Montrer que l'ensemble des éléments de Ω qui sont entiers sur A est un sous-anneau de Ω.

c) On suppose que A est un anneau de valuation. Montrer qu'un élément de K est entier sur A si et seulement s'il appartient à A. ("Un anneau de valuation est intégralement clos.")

d) Soit P et Q deux polynômes unitaires de $K[X]$. On suppose que $P \in A[X]$ et que Q divise P dans $K[X]$. Montrer que les coefficients de Q sont entiers sur A.

e) (*suite*) Si A est un anneau de valuation, en déduire que $Q \in A[X]$. ("Lemme de Gauss pour les anneaux de valuation.")

6

Équations différentielles

Dans ce chapitre, je montre comment certains aspects de la théorie des équations différentielles linéaires à coefficients, disons polynomiaux, peuvent être algébrisés. Il y a même une « théorie de Galois des équations différentielles » dont j'expliquerai quelques idées. Je termine par un théorème dû à J. Liouville qui contient le fait que la primitive de la fonction e^{x^2} n'a pas d'expression algébrique élémentaire.

6.1. Corps différentiels

DÉFINITION 6.1.1. — *Soit A un anneau. Une* dérivation *sur A est un homomorphisme de groupes abéliens $D\colon A \to A$ qui vérifie la* formule de Leibniz *: pour tous a et b dans A,*

$$D(ab) = aD(b) + bD(a).$$

Un anneau différentiel *est la donnée d'un anneau A et d'une dérivation de A. Quand l'anneau est un corps, on parle plutôt de* corps différentiel. *On note souvent $D(a) = a'$, $D(D(a)) = a''$, et si $n \geqslant 0$ est entier, $D^n(a) = a^{(n)}$.*

Exemples 6.1.2 **(Exemples d'anneaux différentiels)**. — *a*) L'anneau des fonctions $\mathcal{C}^\infty$ sur un intervalle I de $\mathbf{R}$ à valeurs, disons complexes, muni de la dérivation usuelle des fonctions : $D(f)$ est la dérivée de f.

b) Si X est une variété différentielle, une dérivation sur l'anneau des fonctions $\mathcal{C}^\infty$ sur X est aussi appelée un *champ de vecteurs* sur X.

c) L'anneau des fonctions analytiques réelles sur un intervalle ouvert de $\mathbf{R}$, muni de la dérivation usuelle.

d) L'anneau des fonctions holomorphes sur un ouvert Ω de $\mathbf{C}$, muni de la dérivation $f \mapsto f'$.

e) L'anneau $k[T]$ des polynômes en une indéterminée sur un corps k muni de la dérivation formelle $P \mapsto P'$.

f) (exemple idiot) N'importe quel anneau A avec la dérivation nulle $D = 0$.

Exemples 6.1.3 **(Exemples de corps différentiels)**. — *a*) Le corps $k(T)$ des fractions rationnelles en une indéterminée sur un corps k, muni de la dérivation formelle des fractions rationnelles $P \mapsto P'$.

b) Le corps des fonctions méromorphes sur un ouvert connexe de $\mathbf{C}$, muni de la dérivation usuelle.

Dans un anneau (ou un corps) différentiel, on a les relations familières suivantes :

LEMME 6.1.4. — *Soit* (A, D) *est un anneau différentiel, soit* a, b *des éléments de* A.

a) $D(1) = 0$;

b) *pour tout entier* $n \geqslant 1$, $D(a^n) = na^{n-1}D(a)$;

c) *pour tout entier* $n \geqslant 1$, $D^n(ab) = \sum_{k=0}^{n} \binom{n}{k} D^k(a)D^{n-k}(b)$;

d) *si* b *est inversible,* $D(a/b) = (bD(a) - aD(b))/b^2$. *En particulier,* $D(1/b) = -D(b)/b^2$.

Démonstration. — *a*) Appliquons la dérivation D aux deux membres de l'égalité $1 \times 1 = 1$. On obtient $1D(1) + D(1)1 = D(1)$, d'où $D(1) = 0$. Plus généralement, $D(n \cdot 1) = 0$ pour tout $n \in \mathbf{Z}$.

b) Montrons cette relation par récurrence sur n. Elle est vraie pour $n = 1$. Si elle vaut pour n, alors

$$\begin{aligned} D(a^{n+1}) = D(a \times a^n) &= aD(a^n) + a^n D(a) \\ &= a(na^{n-1}D(a)) + a^n D(a) = (n+1)a^n D(a) \end{aligned}$$

d'où la formule pour $n+1$.

c) Montrons cette formule par récurrence sur n. Elle vaut pour $n = 1$, et si elle vaut pour n, alors

$$\begin{aligned} D^{n+1}(ab) = D\big(D^n(ab)\big) &= D\left(\sum_{k=0}^{n} \binom{n}{k} D^k(a)D^{n-k}(b)\right) \\ &= \sum_{k=0}^{n} \binom{n}{k} D\Big(D^k(a)D^{n-k}(b)\Big) \\ &= \sum_{k=0}^{n} \binom{n}{k} \Big(D^{k+1}(a)D^{n-k}(b) + D^k(a)D^{n+1-k}(b)\Big) \\ &= \sum_{k=1}^{n+1} \binom{n}{k-1} D^k(a)D^{n+1-k}(b) + \sum_{k=0}^{n} \binom{n}{k} D^k(a)D^{n+1-k}(b) \\ &= \sum_{k=0}^{n+1} \binom{n+1}{k} D^k(a)D^{n+1-k}(b) \end{aligned}$$

d'après la formule classique

$$\binom{n+1}{k} = \binom{n}{k-1} + \binom{n}{k},$$

vraie pour $n \geqslant 1$ et $k \geqslant 1$.

d) Il suffit de dériver la relation $b(a/b) = a$; on obtient

$$D(b)\frac{a}{b} + bD(a/b) = D(a),$$

d'où

$$D(a/b) = \frac{D(a)}{b} - D(b)\frac{a}{b^2} = \frac{bD(a) - aD(b)}{b^2},$$

ainsi qu'il fallait démontrer. La dernière relation découle du fait que $D(1) = 0$. □

Un élément d'un anneau différentiel est dit *constant* si sa dérivée est nulle.

PROPOSITION 6.1.5. — *Soit (A, D) un anneau différentiel. L'ensemble des $a \in A$ tels que $D(a) = 0$ est un sous-anneau de A. Si (K, D) est un corps différentiel, l'ensemble des $a \in K$ tels que $D(a) = 0$ est un sous-corps de K ; on l'appelle* corps des constantes.

Démonstration. — Si a et b vérifient $D(a) = D(b) = 0$, on a $D(a+b) = D(a) + D(b) = 0$ et $D(ab) = aD(b) + bD(a) = 0$. On a vu que $D(1) = 0$. Ainsi, l'ensemble des $a \in A$ tels que $D(a) = 0$ est un sous-anneau de A. Si $a \in A$ est inversible et vérifie $D(a) = 0$, le lemme précédent montre que $D(1/a) = 0$, donc $1/a$ est constant. En particulier, si (K, D) l'ensemble des éléments $x \in K$ tels que $D(x) = 0$ est un sous-corps de K. □

On note souvent A^D, *resp.* K^D, l'ensemble des constantes d'un anneau différentiel (A, D), *resp.* d'un corps différentiel (K, D). Dans tous les exemples d'anneaux de fonctions donnés plus haut, les constantes sont les fonctions (localement) constantes. Pour les polynômes en caractéristique p, il se passe quelque chose d'amusant.

PROPOSITION 6.1.6. — *Soit k un corps. On pose $A = k[T]$ et $K = k(T)$ et on les munit de la dérivation usuelle. Si k est de caractéristique 0, $A^D = K^D = k$. Si k est de caractéristique p, $A^D = k[T^p]$ et $K^D = k(T^p)$.*

Démonstration. — Si $P = \sum_{n=0}^{N} a_n T^n$, $P' = \sum_{n=0}^{N} n a_n T^{n-1}$. Supposons $P' = 0$, c'est-à-dire $n a_n = 0$ pour tout n. Si k est de caractéristique nulle, cela entraîne $P = a_0$. Si k est de caractéristique p, cela implique seulement que $a_n = 0$ si n n'est pas multiple de p, d'où $P \in k[T^p]$. L'autre inclusion est évidente.

Passons aux fractions rationnelles et soit R une fraction rationnelle telle que $R' = 0$. Écrivons $R = A/B$ où A et B sont deux polynômes, B étant non nul et de degré minimal. On a alors $BR = A$, d'où, en dérivant, $B'R = A'$. Le degré de B' est strictement inférieur à celui de B, donc l'hypothèse de minimalité entraîne que $B' = 0$, d'où $A' = B'R = 0$. Si k est de caractéristique 0, A et B sont des polynômes constants. Si k

est de caractéristique p, A et B sont des polynômes en T^p, donc $R \in k(T^p)$. Réciproquement, une telle fraction rationnelle est de dérivée nulle, cqfd. □

6.2. Extensions différentielles. Construction de dérivations

DÉFINITION 6.2.1. — *Un homomorphisme d'anneaux différentiels* $f\colon (A, D_A) \to (B, D_B)$ *est un homomorphisme d'anneaux* $f\colon A \to B$ *tel que pour tout* $a \in A$, $f(D_A(a)) = D_B(f(a))$.

*Si A et B sont des corps, on parle d'*extension de corps différentiels *ou d'*extension différentielle.

Quand il ne peut y avoir de confusion sur l'homomorphisme d'anneaux $f\colon A \to B$, on dit aussi que D_B *étend* D_A.

LEMME 6.2.2. — *Soit* $f\colon (A, D_A) \to (B, D_B)$ *un homomorphisme d'anneaux différentiels. Le noyau de* f *est stable par* D_A.

En effet, si $a \in A$ est tel que $f(a) = 0$, on a $f(D_A(a)) = D_B(f(a)) = D_B(0) = 0$. On dit que $\operatorname{Ker} f$ est un *idéal différentiel*.

Inversement, soit I un idéal différentiel d'un anneau différentiel (A, D_A) et montrons comment munir l'anneau quotient $B = A/I$ d'une structure d'anneau différentiel telle que l'homomorphisme canonique $\pi\colon A \to B$ soit un homomorphisme d'anneaux différentiels. Par définition, l'homomorphisme de groupes abéliens

$$\pi \circ D_A\colon A \to B$$

est nul sur I. Comme I est un sous-groupe de A et que A est abélien, il existe un unique homomorphisme de groupes abéliens $D_B\colon B \to B$ tel que $D_B(\pi(x)) = \pi(D_A(x))$ pour tout $x \in A$. Montrons que D_B est une dérivation. Soit a et b deux éléments de B. Soit x et y dans A tels que $a = \pi(x)$ et $b = \pi(y)$. Alors,

$$\begin{aligned}
D_B(ab) &= D_B(\pi(x)\pi(y)) = D_B(\pi(xy)) \\
&= \pi(D_A(xy)) && \text{par définition de } D_B \\
&= \pi(yD_A(x) + xD_A(y)) && \text{car } D_A \text{ est une dérivation} \\
&= \pi(y)\pi(D_A(x)) + \pi(x)\pi(D_A(y)) \\
& && \text{car } \pi \text{ est un homomorphisme d'anneaux} \\
&= \pi(y)D_B(\pi(x)) + \pi(x)D_B(\pi(y)) \\
&= bD_B(a) + aD_B(b).
\end{aligned}$$

THÉORÈME 6.2.3. — *Soit (A, D_A) un anneau et soit I un idéal différentiel de A. Il existe alors une unique dérivation de A/I telle l'homomorphisme canonique $A \to A/I$ soit un homomorphisme d'anneaux différentiels.*

PROPOSITION 6.2.4. — *Soit (A, D) un anneau différentiel intègre et soit K son corps des fractions. Il existe une unique dérivation sur K qui coïncide avec D sur A.*

Ainsi, K a une structure de corps différentiel canonique.

Démonstration. — Vu les formules du paragraphe 6.1, on doit nécessairement poser, si $x \in K$ est le quotient a/b de deux éléments de A,

$$D(x) = \frac{D(a)b - aD(b)}{b^2}.$$

Il faut vérifier que cette formule ne dépend pas du choix de la fraction a/b et qu'elle définit une dérivation de K. Si $t \in A \setminus \{0\}$, on a

$$\begin{aligned}\frac{D(at)(bt) - (at)D(bt)}{(bt)^2} &= \frac{D(a)bt^2 + abtD(t) - at^2D(b) - atbD(t)}{b^2t^2} \\ &= \frac{D(a)b - D(b)a}{b^2}\end{aligned}$$

donc les formules pour $D(a/b)$ et $D(at/bt)$ fournissent le même résultat. Par suite, les formules pour $D(a/b)$ et $D(ad/bd)$ donnent le même résultat, de même que les formules pour $D(c/d)$ et $D(bc/bd)$. Comme $ad = bc$, les formules pour $D(a/b)$ et $D(c/d)$ sont égales et l'application $D\colon K \to K$ est bien définie.

De plus, si $x = a/b$ et $y = c/d$, on a

$$\begin{aligned}D(x+y) = D\Big(\frac{ad+bc}{bd}\Big) &= \frac{D(ad+bc)bd - (ad+bc)D(bd)}{b^2d^2} \\ &= \frac{D(ad)bd - adD(bd)}{b^2d^2} + \frac{D(bc)bd - bcD(bd)}{b^2d^2} \\ &= D\Big(\frac{ad}{bd}\Big) + D\Big(\frac{bc}{bd}\Big) = D(a/b) + D(c/d) = D(x) + D(y).\end{aligned}$$

Ainsi, D est un homomorphisme de groupes abéliens. D'autre part,

$$\begin{aligned}D(xy) = D\Big(\frac{ac}{bd}\Big) &= \frac{D(ac)bd - acD(bd)}{b^2d^2} \\ &= \frac{abdD(c) + bcdD(a) - acdD(b) - abcD(d)}{b^2d^2} \\ &= \frac{bcdD(a) - acdD(b)}{b^2d^2} + \frac{abdD(c) - abcD(d)}{b^2d^2} \\ &= \frac{bD(a) - aD(b)}{b^2}\frac{cd}{d^2} + \frac{dD(c) - cD(d)}{d^2}\frac{ab}{b^2} \\ &= D\Big(\frac{a}{b}\Big)\frac{c}{d} + D\Big(\frac{c}{d}\Big)\frac{a}{b} = D(x)y + D(y)x,\end{aligned}$$

ce qui prouve que D est une dérivation. □

Après les anneaux quotients et le corps des fractions, expliquons comment construire les dérivations d'un anneau de polynômes.

THÉORÈME 6.2.5. — *Soit (A,D) un anneau différentiel et soit $B = A[T]$ l'anneau des polynômes en une indéterminée sur A. Pour tout $b \in B$, il existe une unique dérivation D_b de B telle que $D_b(T) = b$ et telle que l'homomorphisme canonique $A \to A[T]$ soit un homomorphisme d'anneaux différentiels.*

Démonstration. — Soit $P = \sum_{k=0}^{n} a_k T^k$ un élément de B. Si D_B est une dérivation de B qui étend D, on a

$$\begin{aligned} D_B(P) &= \sum_{k=0}^{n} D_B(a_k T^k) = \sum_{k=0}^{n} \big(D(a_k)T^k + a_k D_B(T^k)\big) \\ &= \sum_{k=0}^{n} D(a_k)T^k + \big(\sum_{k=0}^{n} k a_k T^{k-1}\big) D_B(T) \\ &= P^D(T) + P'(T) D_B(T), \end{aligned}$$

où P^D désigne le polynôme de $A[T]$ obtenu en appliquant D aux coefficients de P. Cela montre qu'une telle dérivation est déterminée par l'image $D_B(T)$ de T. Réciproquement, soit $b \in B$ et montrons que la formule

$$D_B(P) = P^D(T) + bP'(T) \sum_{k=0}^{n} D(a_k)T^k + b\sum_{k=0}^{n} k a_k T^{k-1}$$

définit une dérivation de B qui étend la dérivation de A. L'application D_B est évidemment un morphisme de groupes abéliens.. Si $Q = \sum_{k=0}^{m} b_k T^k$ est un polynôme, on a

$$PQ = \sum_{k=0}^{m+n} c_k T^k, \qquad c_k = \sum_{i+j=k} a_i b_j$$

et

$$\begin{aligned} D_B(PQ) &= \sum_{k=0}^{m+n} D(c_k)T^k + b\sum_{k=0}^{n} k c_k T^{k-1} \\ &= \sum_{k=0}^{m+n} \sum_{i+j=k} \big(D(a_i)b_j + D(b_j)a_i\big)T^{i+j} + b\sum_{k=0}^{n} \sum_{i+j=k} (i+j) a_i b_j T^{i+j-1} \\ &= \sum_{i=0}^{n}\sum_{j=0}^{m} D(a_i) b_j T^{i+j} + b\sum_{i=0}^{n}\sum_{j=0}^{m} i\, a_i b_j T^{i+j-1} \\ &\qquad + \sum_{i=0}^{n}\sum_{j=0}^{m} D(b_j) a_i T^{i+j} + b\sum_{i=0}^{n}\sum_{j=0}^{n} j\, a_i b_j T^{i+j-1} \\ &= D_B(P)Q + D_B(Q)P, \end{aligned}$$

ce qu'on voulait démontrer. □

Un dernier cas, très important pour la suite, concerne les extensions algébriques (séparables).

THÉORÈME 6.2.6. — *Soit (K,D) un corps différentiel et soit L une extension algébrique finie, séparable, de K. Il existe alors une unique dérivation sur L qui étende D.*

Démonstration. — La démonstration est une version algébrique abstraite du calcul de la dérivée d'une fonction définie implicitement.

Soit $x \in L$ un élément primitif et notons $P = X^n + a_{n-1}X^{n-1} + \cdots + a_0$ son polynôme minimal, d'où un isomorphisme $L \simeq K[X]/(P)$. Si D_L est une dérivation de L qui étend celle de K, on obtient en dérivant la relation $P(x) = 0$ que

$$\begin{aligned} 0 = D_L(0) &= D_L(P(x)) \\ &= \sum_{k=0}^{n} D(a_k)x^k + \sum_{k=0}^{n} k a_k x^{k-1} D_L(x) \\ &= P^D(x) + P'(x)D_L(x). \end{aligned}$$

(On a noté P^D le polynôme obtenu en appliquant D aux coefficients de P.) Comme P est un polynôme séparable et $\deg P' < \deg P$, $P'(x) \neq 0$. Ainsi, on a nécessairement

$$D_L(x) = -P^D(x)/P'(x)$$

et il y a au plus une dérivation sur L qui étend celle de K.

Pour montrer l'existence d'une telle dérivation D_L, nous allons utiliser le théorème 6.2.3. Nous devons montrer qu'il existe une dérivation de $K[X]$ telle que l'idéal (P) en soit un idéal différentiel. Si $\tilde{D}$ est une dérivation de $K[X]$, on vient de voir que

$$\tilde{D}(P) = P^D + P'(X)\tilde{D}(X).$$

Comme P est séparable, P et P' sont premiers entre eux et il existe des polynômes U et $V \in K[X]$ tels que $UP + VP' = 1$. Alors, le choix $\tilde{D}(X) = -VP^D$ définit une dérivation $\tilde{D}$ sur $K[X]$ telle que

$$\tilde{D}(P) = P^D - VP^D P' = (1 - P'V)P^D = (UP^D)P.$$

C'est un multiple de P. Si l'anneau $K[X]$ est muni de cette dérivation $\tilde{D}$, l'idéal (P) est donc un idéal différentiel. L'anneau quotient $K[X]/(P)$ hérite alors d'une structure d'anneau différentiel, d'où une structure de corps différentiel sur L. □

6.3. Équations différentielles

Soit (K,D) un corps différentiel. Les équations différentielles qui nous intéressent sont de la forme

$$D^n(f) + a_{n-1}D^{n-1}(f) + \cdots + a_0 f = 0,$$

où $a_0,\dots,a_n \in K$, l'inconnue étant f. Autrement dit, on ne s'intéresse ici qu'aux équations différentielles *linéaires* et *homogènes*. Comme en analyse, nous dirons qu'une telle équation est d'ordre n. En fait, on considère plutôt des équations sous forme matricielle :

$$Y' = AY, \quad A \in M_n(K)$$

d'inconnue un vecteur colonne Y (la dérivée d'un vecteur colonne est définie en dérivant chaque coordonnée).

Le même procédé qu'en analyse permet de passer d'une équation du premier type à une équation du second : si l'on introduit le vecteur $Y = {}^{\mathrm{t}}(f, f', \dots, f^{(n-1)})$, on a

$$\begin{aligned} Y' &= {}^{\mathrm{t}}(f', f'', \dots, f^{(n)}) \\ &= {}^{\mathrm{t}}(f', f'', \dots, f^{(n-1)}, -a_{n-1}f^{(n-1)} - \cdots - a_0 f) \\ &= \begin{pmatrix} 0 & 1 & 0 & \\ & \ddots & \ddots & \\ & & 0 & 1 \\ -a_0 & -a_1 & \dots & -a_{n-1} \end{pmatrix} Y. \end{aligned}$$

On pourrait aussi considérer des équations différentielles matricielles d'ordre supérieur. Elles se ramènent au premier ordre par un procédé analogue.

THÉORÈME 6.3.1. — *Soit (K,D) un corps différentiel, de corps des constantes C. L'ensemble des solutions dans K^n d'une équation différentielle $Y' = AY$, où $A \in M_n(K)$, est un C-espace vectoriel de dimension inférieure ou égale à n.*

Démonstration. — Comme la dérivation $D\colon K \to K$ est C-linéaire, l'application φ de K^n dans lui-même qui à Y associe $\varphi(Y) = Y' - AY$ est C-linéaire. Son noyau est donc un C-espace vectoriel.

Montrons qu'il est de dimension inférieure ou égale à n. Il suffit ainsi de montrer que $n+1$ éléments de V sont linéairement dépendants sur C. Comme ils sont évidemment linéairement indépendants sur K, il suffit, pour terminer la démonstration, d'établir le lemme suivant. □

LEMME 6.3.2. — *Soit (K,D) un corps différentiel, de corps des constantes C. Soit $Y_1,\dots,Y_m$ des solutions d'une équation différentielle $Y' = AY$. Si elles sont linéairement indépendantes sur C, elles le sont sur K.*

Démonstration. — Démontrons ce lemme par récurrence sur m. Si $m = 1$, le résultat est évident (l'hypothèse et la conclusion signifient juste que $Y_1 \neq 0$). Supposons le vrai pour $(m-1)$. Par récurrence, on peut supposer que $Y_1, \ldots, Y_{m-1}$ sont linéairement indépendantes sur K. Considérons alors une relation de dépendance linéaire non triviale sur K, $a_1 Y_1 + \cdots + a_m Y_m = 0$. Nécessairement, $a_m \neq 0$, ce qui permet de diviser cette relation par a_m. Nous pouvons ainsi supposer $a_m = 1$. Dérivons cette relation de dépendance linéaire. On obtient ainsi

$$(a_1' Y_1 + a_1 Y_1') + \cdots + (a_{m-1}' Y_{m-1} + a_{m-1} Y_{m-1}') + Y_m' = 0,$$

soit encore

$$(a_1' Y_1 + \cdots + a_{m-1}' Y_{m-1}) + A(a_1 Y_1 + \cdots + a_{m-1} Y_{m-1} + Y_m) = 0$$

et donc

$$a_1' Y_1 + \cdots + a_{m-1}' Y_{m-1} = 0.$$

C'est une relation de dépendance linéaire sur K en $Y_1, \ldots, Y_{m-1}$. Par hypothèse, elle est triviale et $a_1' = \cdots = a_{m-1}' = 0$. Autrement dit, a_1, …, a_{m-1} sont dans C et $Y_1, \ldots, Y_m$ sont linéairement dépendantes sur C, contradiction. □

On dispose d'un outil très utile pour détecter l'indépendance linéaire sur C : le wronskien.

DÉFINITION 6.3.3. — *Soit (K, D) un corps différentiel. On appelle* wronskien *de n éléments $f_1, \ldots, f_n \in K$ le déterminant*

$$W(f_1, \ldots, f_n) = \det \begin{pmatrix} f_1 & f_2 & \cdots & f_n \\ f_1' & f_2' & \cdots & f_n' \\ \vdots & & & \vdots \\ f_1^{(n-1)} & f_2^{(n-1)} & \cdots & f_n^{(n-1)} \end{pmatrix}.$$

THÉORÈME 6.3.4. — *Soit (K, D) un corps différentiel de corps des constantes C. Des éléments $f_1, \ldots, f_n$ de K sont linéairement dépendants sur C si et seulement si leur wronskien est nul.*

Démonstration. — C'est une variante de la démonstration précédente. Si $f_1, \ldots, f_n$ sont linéairement dépendantes sur C, on voit immédiatement que les colonnes du wronskien sont liées. Par suite, $W(f_1, \ldots, f_n) = 0$. Montrons la réciproque par récurrence sur n. Si $n = 1$ le résultat est clair. Supposons alors que $W(f_1, \ldots, f_n) = 0$. Si $W(f_2, \ldots, f_n) = 0$, on conclut par récurrence que $f_2, \ldots, f_n$ sont linéairement dépendantes sur C. Supposons donc que $W(f_2, \ldots, f_n) \neq 0$. Puisque $W(f_1, \ldots, f_n) = 0$, les colonnes du wronskien sont liées par une relation de dépendance linéaire non triviale à coefficients dans K, soit

$$(*_j) \qquad a_1 f_1^{(j)} + a_2 f_2^{(j)} + \cdots + a_n f_n^{(j)} = 0, \qquad 0 \leqslant j \leqslant n-1.$$

Comme $W(f_2,\dots,f_n)\neq 0$, $a_1\neq 0$ et on peut supposer en divisant par a_1 que $a_1=1$. Dérivons alors les relations $(*_j)$ pour $0\leqslant j\leqslant n-2$, on obtient alors

$$f_1^{(j+1)}+(a_2f_2^{(j+1)}+a_2'f_2^{(j)})+\cdots+(a_nf_n^{(j+1)}+a_n'f_n^{(j)})=0,$$

et donc

$$a_2'f_2^{(j)}+\cdots+a_n'f_n^{(j)}=0,\qquad 0\leqslant j\leqslant n-2.$$

Si elles n'étaient pas triviales, ces relations impliqueraient que $W(f_2,\dots,f_n)=0$. Ainsi, $a_2'=\cdots=a_n'=0$ et les a_j sont tous constants. Nous avons ainsi démontré que $f_1,\dots,f_n$ sont linéairement dépendantes sur C. □

6.4. Extensions de Picard-Vessiot

De même que nous avons construit une extension de décomposition d'un polynôme qui est une extension minimale contenant les racines de ce polynôme, nous allons construire une extension minimale d'un corps différentiel dans laquelle une équation différentielle d'ordre n admet n solutions linéairement indépendantes.

Désormais, tous les corps que nous considérons sont de caractéristique 0.

DÉFINITION 6.4.1. — *Soit* (K,D) *un corps différentiel. On suppose que le corps* C *des constantes de* K *est algébriquement clos et de caractéristique* 0.

Soit (E) *:* $Y'=AY$ *une équation différentielle linéaire homogène à coefficients dans* K*, où* $A\in M_n(K)$*. On dit qu'une extension différentielle* (L,D) *de* K *est une* extension de Picard-Vessiot *pour cette équation si*

a) (E) *admet une base de solutions* $(Y_1,\dots,Y_n)$ *dans* L *;*
b) L *est engendré par les coefficients* Y_{ij} *de cette base ;*
c) *le corps des constantes de* L *est égal à* C.

THÉORÈME 6.4.2. — *Toute équation différentielle admet une extension de Picard-Vessiot. Deux telles extensions sont isomorphes (en tant que corps différentiels).*

La démonstration est assez compliquée et nous ne prouverons que l'existence d'une extension de Picard-Vessiot.

Démonstration de l'existence d'une extension de Picard-Vessiot

Comme une extension de Picard-Vessiot est engendrée par les coefficients des solutions, on commence par considérer l'anneau

$$R=K[Y_{11},\dots,Y_{nn}]$$

des polynômes en n^2 indéterminées. Si G désigne la matrice des Y_{ij}, munisons l'anneau A de la dérivation $D\colon A\to A$ définie par $D(G)=AG$. Nous avons ainsi *rajouté*

les solutions de l'équation différentielle (E). Il nous faut maintenant tenir compte de la condition que ces solutions sont linéairement indépendantes, condition qui s'écrit G inversible, donc $\det(G)$ inversible. On introduit ainsi l'anneau $S = R[T]/(1 - T\det(G))$ dans lequel T représente l'inverse de $\det(G)$. On veut étendre la dérivation D de R à S. Pour cela, il faut définir $D(T)$ de sorte que l'idéal $(1 - T\det(G))$ soit un idéal différentiel. Or, d'après l'exercice 6.2, la dérivée de $\det(G)$ vaut

$$D(\det G) = \mathrm{Tr}(\mathrm{Com}(G)G'),$$

où $\mathrm{Com}(G)$ désigne la comatrice de G (transposée de la matrice des cofacteurs). Comme $D(G) = AG$, on a ainsi

$$D(\det G) = \mathrm{Tr}(\mathrm{Com}(G)AG) = \mathrm{Tr}(AG\,\mathrm{Com}(G)) = \mathrm{Tr}(A\det(G)) = \mathrm{Tr}(A)\det(G).$$

Il vient alors

$$D(1 - T\det(G)) = -D(T)\det(G) + T\,\mathrm{Tr}(A)\det(G) = -\det(G)(D(T) - T\,\mathrm{Tr}(A)).$$

Autrement dit, l'idéal $(1 - T\det(G))$ est un idéal différentiel dès que $D(T) = T\,\mathrm{Tr}(A)$. Supposons cette relation vérifiée. On en déduit ainsi une structure d'anneau différentiel sur l'anneau quotient $S = K[Y_{11}, \ldots, Y_{nn}, T]/(1 - T\det(G))$ telle que $D(G) = AG$.

On n'est pas encore au bout de nos peines car en général, l'anneau différentiel S que nous avons construit a beaucoup trop d'éléments constants (voir l'exercice 6.4). Soit I un idéal différentiel de S, maximal parmi tous les idéaux différentiels de S distincts de S. (Une récurrence transfinie analogue à celle du théorème 2.5.3 montre qu'il en existe.) L'anneau différentiel S/I n'a pas d'idéal différentiel à part 0 et lui-même. D'après le lemme 6.4.3 ci-dessous il est intègre et le corps des constantes de son corps des fractions L est égal à C. Cela prouve que (L, D) est une extension de Picard-Vessiot pour l'équation différentielle $Y' = AY$. □

LEMME 6.4.3. — *Soit (K, D) un corps différentiel de caractéristique 0 ; notons C son corps des constantes. Soit (A, D) une extension différentielle de (K, D). On suppose que A n'a pas d'idéal différentiel autre que (0) et lui-même.*

a) *L'anneau A est intègre. Soit L son corps des fractions, muni de sa dérivation canonique.*

b) *Le corps des constantes de L est contenu dans A.*

c) *Si A est une K-algèbre de type fini et si C est algébriquement clos, le corps des constantes de L est égal à C.*

Démonstration. — *a*) Commençons par montrer que A ne contient pas d'élément nilpotent autre que 0. Pour cela, considérons l'ensemble I des $x \in A$ dont une puissance est nulle est réduit à $\{0\}$. C'est un idéal de A (voir l'exercice 2.10) et nous allons montrer que c'est même un idéal différentiel. Soit en effet $x \in I$ et soit n tel que $x^n = 0$. Dérivons cette relation. On trouve $nx^{n-1}x' = 0$, d'où en divisant par n, $x^{n-1}x' = 0$. Continuons

à dériver ; on obtient que $(n-1)x^{n-2}(x')^2 + x^{n-1}x'' = 0$, d'où en multipliant par x', que $(n-1)x^{n-2}(x')^3 = 0$. Montrons ainsi par récurrence que $x^{n-k}(x')^{2k} = 0$ si $0 \leqslant k \leqslant n$. C'est vrai pour $k = 0$ et $k = 1$. Si c'est vrai jusqu'au rang $k-1$, on dérive la relation $x^{n-k+1}(x')^{2k-2} = 0$ et on obtient

$$(n-k+1)x^{n-k}(x')^{2k-1} + 2(k-1)x^{n-k+1}(x')^{2k-3}x'' = 0.$$

On multiplie ceci par x', d'où la relation

$$(n-k+1)x^{n-k}(x')^{2k} = 0.$$

Comme $k \leqslant n$, $n-k+1 \neq 0$ est inversible dans A (c'est là qu'on utilise le fait que K est un corps de caractéristique 0), d'où $x^{n-k}(x')^{2k} = 0$. Arrivé au rang n, on a $(x')^{2n} = 0$, ce qui montre $x' \in I$. Ainsi, l'idéal I est stable par dérivation. Comme il n'est pas égal à A (1 n'appartient pas à I), il est réduit à 0.

Soit maintenant un élément non nul $a \in A$. Soit I l'ensemble des $b \in A$ tels que $ab = 0$. Si $b \in I$, on obtient en dérivant la relation $ab = 0$ que $ab' + a'b = 0$, d'où en multipliant par a que $a^2b' = 0$. Par suite, $(ab')^2 = 0$ et $ab' = 0$ puisque A n'a pas d'élément nilpotent non-nul. Ainsi, I est un idéal différentiel de A. Puisque $a \neq 0$, $I \neq A$, donc $I = 0$. Cela prouve que A est intègre.

b) Notons C' le corps des constantes de L ; c'est un sous-corps de L qui contient C. Considérons un élément $x \in C'$. Soit I l'ensemble des $a \in A$ tels que $ax \in A$. C'est un idéal de A. Montrons qu'il est stable par dérivation. Si en effet $ax = b \in A$, on a $ax' + a'x = b'$, et donc, puisque $x' = 0$, $a'x = 0$. Cela prouve que $a' \in I$. Comme x appartient au corps des fractions de A, $I \neq (0)$. Il en résulte que $I = A$. En particulier, $1 \in I$ et $x = 1x$ appartient à A.

c) D'après le *b*), $C' \subset A$. Considérons un idéal maximal $\mathfrak{m}$ de A. L'anneau $A/\mathfrak{m}$ est alors d'une part un corps, et d'autre part une K-algèbre de type fini. Par suite, c'est une extension algébrique de K. Comme tout homomorphisme de corps, l'homomorphisme $C' \to A/\mathfrak{m}$ est nécessairement injectif et on peut ainsi identifier C' à son image dans $A/\mathfrak{m}$. Par suite, tout élément de C' est algébrique sur K. Comme C' est formé de constantes, tout élément de C' est algébrique sur le corps C des constantes de K (voir le lemme 6.4.4 ci-dessous). Puisque C est algébriquement clos, $C' = C$. □

LEMME 6.4.4. — *Soit $(K, D) \to (L, D)$ une extension de corps différentiels ; on note C le corps des constantes de K. Soit $x \in L$. Les deux propriétés suivantes sont équivalentes :*

a) *x est algébrique sur C ;*
b) *x est constant et algébrique sur K.*

Démonstration. — Supposons que x soit algébrique sur C. Il est *a fortiori* algébrique sur K. Soit $P = X^n + a_{n-1}X^{n-1} + \cdots + a_0$ le polynôme minimal de x sur C. Dérivons la relation $P(x) = 0$. On obtient alors $P'(x)x' = 0$. Comme K est de caractéristique 0, P est séparable et $P'(x) \neq 0$. Par suite, $x' = 0$.

Supposons maintenant que $x' = 0$ et que x soit algébrique sur K. Soit $P = X^n + a_{n-1}X^{n-1} + \cdots + a_0$ son polynôme minimal sur K. Dérivons encore la relation $P(x) = 0$. Comme $x' = 0$, il vient $\sum_{k=0}^{n-1} a'_k x^k = 0$. Cette relation étant de degré strictement inférieur à n, cela implique $a'_k = 0$ pour tout k. Ainsi, P appartient à $C[X]$ et x est algébrique sur C. □

6.5. Le groupe de Galois différentiel. Exemples

Soit (K, D) un corps différentiel dont le corps des constantes C est algébriquement clos de caractéristique nulle. Soit (L, D) une extension de Picard-Vessiot de K pour une équation (E) : $Y' = AY$. Soit $(Y_1, \ldots, Y_n)$ une base du C-espace vectoriel V des solutions de (E) dans L^n.

DÉFINITION 6.5.1. — *On appelle* groupe de Galois différentiel *de L sur K le groupe des K-automorphismes différentiels de L, c'est-à-dire l'ensemble des automorphismes $\sigma : L \to L$ tels que*

a) *pour tout $x \in K$, $\sigma(x) = x$;*
b) *pour tout $y \in L$, $\sigma(y)' = \sigma(y')$.*

On le note $\mathrm{Gal}^D(L/K)$.

De même que les groupes de Galois classiques sont des sous-groupes du groupe symétrique, le groupe de Galois différentiel est un sous-groupe du groupe $\mathrm{GL}(V)$ des automorphismes C-linéaires de V. (Remarque : $\mathrm{GL}(V) \simeq \mathrm{GL}_n(C)$.)

PROPOSITION 6.5.2. — *Si $\sigma \in \mathrm{Gal}^D(L/K)$. Pour toute solution Y de l'équation différentielle* (E)*, $\sigma(Y)$ est une solution de* (E) *et l'application $\sigma : V \to V$ ainsi obtenue est un isomorphisme de C-espaces vectoriels.*

De plus, l'application $\rho : \mathrm{Gal}^D(L/K) \to \mathrm{GL}_n(C)$ définie par $\sigma \mapsto \sigma|_V$ est un homomorphisme de groupes, injectif.

Démonstration. — Soit $\sigma \in \mathrm{Gal}^D(L/K)$. Soit $Y = {}^t(y_1, \ldots, y_n)$ une solution de (E). Par définition, on a donc

$$\sigma(Y)' = \sigma(Y') = \sigma(AY) = A\sigma(Y)$$

car σ est K-linéaire. Ainsi, $\sigma(Y)$ est une solution de (E). Cela définit une application $\sigma|_V : V \to V$ qui est évidemment C-linéaire puisque $C \subset K$. L'isomorphisme réciproque est donné par σ^{-1}.

Il est évident que ρ est un homomorphisme de groupes de $\mathrm{Gal}^D(L/K)$ dans $\mathrm{GL}(V)$. Il reste à montrer qu'il est injectif. Or, si $\sigma \in \mathrm{Gal}^D(L/K)$ vérifie $\rho(\sigma) = \mathrm{id}$, on a $\sigma(Y_j) = Y_j$ pour tout j. Comme L est engendré sur K par les composantes des Y_j et comme $\sigma|_K = \mathrm{id}_K$, on a $\sigma(y) = y$ pour tout $y \in L$, ce qui prouve $\sigma = \mathrm{id}$. Ainsi, ρ est injectif. □

Donnons maintenant quelques exemples.

Exemple 6.5.3 **(Exponentielle)**. — Soit $K = \mathbf{C}(X)$, muni de sa dérivation usuelle et considérons l'équation $y' = y$. Nécessairement, une solution non nulle y dans une extension différentielle de $\mathbf{C}(X)$ est transcendante sur $\mathbf{C}(X)$. Sinon, y serait solution d'une équation de degré minimal

$$y^n + a_{n-1}y^{n-1} + \cdots + a_0 = 0, \quad a_0, \ldots, a_{n-1} \in \mathbf{C}(X).$$

Comme $y \neq 0$, $a_0 \neq 0$. Dérivons alors cette relation. On obtient

$$ny^{n-1}y' + ((n-1)a_{n-1}y^{n-2}y' + a'_{n-1}y^{n-1}) + \cdots + a'_0 = 0,$$

d'où puisque $y' = y$,

$$ny^n + ((n-1)a_{n-1} + a'_{n-1})y^{n-1} + \cdots + (a_1 + a'_1)y + a'_0 = 0,$$

ce qui est une autre équation algébrique de degré au plus n. Elles sont donc multiples l'une de l'autre et $a'_0 = na_0$.

Or, si $\lambda \in \mathbf{C}^*$, il n'existe pas de fraction rationnelle non nulle R telle que $R' = \lambda R$. Soit R une telle fraction rationnelle et notons $R = c\prod_{j=1}^{m} {P_j}^{n_j}$ sa factorisation comme produit de polynômes irréductibles unitaires P_j distincts, avec des exposants $n_j \in \mathbf{Z} \setminus \{0\}$, et $c \in \mathbf{C}^*$. On a alors

$$\frac{R'}{R} = \sum_{j=1}^{m} n_j \frac{P'_j}{P_j}.$$

C'est une décomposition en éléments simples de R'/R et ne peut être constant à moins que $m = 0$, ce qui entraîne $\lambda = 0$.

En particulier, aucune fraction rationnelle $R \neq 0$ ne vérifie $R' = nR$ et y est transcendant sur $\mathbf{C}(X)$.

Le corps des fractions rationnelles en deux indéterminées, $\mathbf{C}(X, Y)$, muni de la dérivation définie par $Y' = Y$, définit ainsi une extension de Picard-Vessiot. D'après l'exercice 6.1, on a, si $P \in \mathbf{C}(X, Y)$, la relation

$$P' = \frac{\partial P}{\partial X} + Y\frac{\partial P}{\partial Y}.$$

L'espace vectoriel des solutions est de dimension 1, $V = \mathbf{C}Y$. (C'est un corollaire de la construction.) Un automorphisme σ de L fixant $\mathbf{C}(X)$ est défini par l'image de Y qui doit être dans V. Il existe donc $\rho(\sigma) \in \mathbf{C}^*$ tel que $\sigma(Y) = \rho(\sigma)Y$. Inversement, si $c \in \mathbf{C}^*$, l'application $\sigma_c \colon P \mapsto P(X, cY)$ définit un automorphisme de $\mathbf{C}(X, Y)$ qui appartient

bien à $\mathrm{Gal}^D(L/K)$: si $P \in \mathbf{C}(X,Y)$,

$$\begin{aligned} P(X,cY)' &= \frac{\partial P}{\partial X}(X,cY) + (cY)'\frac{\partial P}{\partial Y}(X,cY) \\ &= \frac{\partial P}{\partial X}(X,cY) + cY\frac{\partial P}{\partial Y}(X,cY) \\ &= \Big(\frac{\partial P}{\partial X} + Y\frac{\partial P}{\partial Y}\Big)(X,cY), \end{aligned}$$

et σ_c est un automorphisme de corps différentiels.

En définitive, l'homomorphisme de groupes $\mathrm{Gal}^D(L/K) \to \mathrm{GL}_1(\mathbf{C}) = \mathbf{C}^*$, $\sigma \mapsto \rho(\sigma)$, est un isomorphisme.

Exemple 6.5.4 **(Logarithme)**. — Supposons encore $K = \mathbf{C}(X)$ et considérons l'équation $y' = 1/X$. Elle n'est pas homogène ; comme en analyse, ses solutions vérifient $(Xy')' = 0$ et on se ramène à l'équation homogène $y'' + (1/X)y' = 0$.

Déterminons une extension de Picard-Vessiot (L,D) pour cette équation. Il est évident que toute constante est solution, et en particulier $g = 1$ est solution. Soit f une solution non constante. Alors, (f,g) sont linéairement indépendantes sur $\mathbf{C}$ et forment une base de l'espace vectoriel des solutions. Comme $Xf'' + f' = (Xf')' = 0$, $c = Xf'$ est une constante non nulle, si bien qu'on peut supposer que $f' = 1/X$, quitte à remplacer f par f/c.

Montrons que f est transcendant sur $\mathbf{C}(X)$. Sinon, f satisferait une équation de degré minimal

$$0 = f^n + a_{n-1} + \cdots + a_0, \quad a_0, \ldots, a_{n-1} \in \mathbf{C}(X).$$

En dérivant, on obtient

$$0 = nf^{n-1}f' + ((n-1)a_{n-1}f^{n-2}f' + a'_{n-1}f^{n-1}) + \cdots + (a_1f' + a'_1f) + a'_0 = 0,$$

d'où

$$0 = (n/X + a'_{n-1})f^{n-1} + \cdots + (a_1/X + a'_0) = 0.$$

Cette relation est de degré strictement inférieur à n et est donc identiquement nulle. En particulier, $a'_{n-1} = -n/X$.

Or, si $\lambda \in \mathbf{C}^*$, aucune fraction rationnelle de $\mathbf{C}(X)$ ne vérifie $R' = \lambda/X$. Sa décomposition en éléments simples

$$R = P + \sum_{j=1}^{m} Q_j/P_j^{n_j},$$

où P est un polynôme, $m \geqslant 0$, les P_j sont des polynômes irréductibles distincts, Q_j est un polynôme premier à P_j dont le degré vérifie $\deg Q_j < n_j \deg P_j$. Alors,

$$R' = P' + \sum_{j=1}^{m} \frac{Q'_jP_j - n_jP'_jQ_j}{P_j^{n_j+1}},$$

ce qui est la décomposition en éléments simples de R', à ceci près que certains termes peuvent être nuls. Par unicité de la décomposition en éléments simples, on a

– $P' = 0$: P est constant :

– pour tout j tel que $P_j \neq X$, $Q_j' P_j - n_j P_j' Q_j = 0$. Comme P_j est irréductible et comme il ne divise pas P_j', il doit diviser Q_j, ce qui est absurde ;

– si $P_j = X$, posant $Q = Q_j'$ et $m = n_j$, on a alors $Q'X - mQ = -nX^m$. Puisque $m \geqslant 1$, X divise Q, ce qui est absurde.

Ainsi, $R' = 0$, ce qui contredit l'hypothèse $R = \lambda/X$. Par suite, f est transcendant sur $\mathbf{C}(X)$.

Alors, $L = \mathbf{C}(X, Y)$ muni de la dérivation donnée par $Y' = 1/X$ est une extension de Picard-Vessiot pour l'équation $xy'' + y' = 0$. De plus, si $P \in L$, sa dérivée est donnée par

$$P' = \frac{\partial P}{\partial X} + \frac{1}{X}\frac{\partial P}{\partial Y}$$

(voir l'exercice 6.1).

La base (f, g) de V nous permet d'identifier $\mathrm{GL}(V)$ et $\mathrm{GL}_2(C)$. Soit $\sigma \in \mathrm{Gal}^D(L/K)$ un automorphisme différentiel. Comme $g = 1 \in K$, on a $\sigma(g) = g$. De plus, il existe a et $b \in \mathbf{C}$ tels que $\sigma(f) = af + bg$. En dérivant, on obtient $\sigma(f)' = af' = a/X$, alors que $\sigma(f') = \sigma(1/X) = 1/X$. Nécessairement, $a = 1$ et l'image de l'homomorphisme $\mathrm{Gal}^D(L/K) \to \mathrm{GL}_2(\mathbf{C})$ est contenue dans le sous-groupe U des matrices de la forme $\left(\begin{smallmatrix} 1 & 0 \\ b & 1 \end{smallmatrix}\right)$.

Réciproquement, si $c \in \mathbf{C}$, l'application $\sigma_c \colon P \mapsto P(X, Y + c)$ définit un automorphisme différentiel : en effet, si $P \in \mathbf{C}(X, Y)$, on a

$$\begin{aligned}
\sigma(P)' &= P(X, Y + c)' \\
&= \frac{\partial P}{\partial X}(X, Y + c) + (Y + c)' \frac{\partial P}{\partial Y}(X, Y + c) \\
&= \Big(\frac{\partial P}{\partial X} + \frac{1}{X}\frac{\partial P}{\partial Y}\Big)(X, Y + c) \\
&= \sigma(P').
\end{aligned}$$

Ainsi, $\mathrm{Gal}^D(L/K) \simeq U$. On remarque aussi que l'application $b \mapsto \left(\begin{smallmatrix} 1 & 0 \\ b & 1 \end{smallmatrix}\right)$ définit un isomorphisme de groupes $\mathbf{C} \simeq U$.

Exemple 6.5.5 **(Extensions galoisiennes)**. — Soit (K, D) un corps différentiel. Supposons que le corps des constantes de K soit algébriquement clos et de caractéristique zéro. Soit $K \to L$ une extension galoisienne de K. D'après le théorème 6.2.6, L possède une unique dérivation D telle que l'homomorphisme $K \to L$ soit un homomorphisme de corps différentiels. Montrons que l'extension $K \to L$ est une extension de Picard-Vessiot associée à une certaine équation différentielle. Une constante de L, étant algébrique sur K, est d'après le lemme 6.4.4 algébrique sur le corps C des constantes de K. Comme on a supposé que C est algébriquement clos, C est le corps des constantes

de L. D'autre part, posons $n = [L:K]$ et soit f un élément de L. La dimension du K-espace vectoriel engendré par $f, f', f'', \ldots$ dans L est finie, inférieure ou égale à n. Cela implique que f satisfait des équations différentielles non triviales.

Soit σ un élément du groupe de Galois (usuel) $\mathrm{Gal}(L/K)$ et considérons l'application $\tilde{D}\colon L \to L$ définie par $\tilde{D}(x) = \sigma(D(\sigma^{-1}(x)))$. C'est une dérivation de L. C'est en effet évidemment un homomorphisme de groupes abéliens ; d'autre part, si $x,\ y \in L$, on a

$$\begin{aligned}\tilde{D}(xy) &= \sigma(D(\sigma^{-1}(xy))) = \sigma(D(\sigma^{-1}(x)\sigma^{-1}(y)))\\ &= \sigma\big(D(\sigma^{-1}(x))\,\sigma^{-1}(y) + D(\sigma^{-1}(x))\,\sigma^{-1}(y)\big)\\ &= \sigma(D(\sigma^{-1}(x)))\sigma(\sigma^{-1}(y)) + \sigma(D(\sigma^{-1}(y)))\sigma(\sigma^{-1}(x))\\ &= \tilde{D}(x)\,y + \tilde{D}(y)\,x.\end{aligned}$$

Comme D est l'unique dérivation de L qui étend la dérivation de K, on a $\tilde{D} = D$, ce qui signifie que pour tout $x \in L$, $\sigma(D(x)) = D(\sigma(x))$. De plus, toute équation différentielle satisfaite par f est aussi satisfaite par $\sigma(f)$.

Puisque l'extension $K \to L$ est galoisienne, il existe $f \in L$ tel que $L = K[f]$. Soit V le sous-C-espace vectoriel de L engendré par les conjugués de f et soit $(f_1, \ldots, f_d)$ une base de V formée de conjugués de f, avec $f_1 = f$. Construisons une équation différentielle d'ordre d dont V est l'espace des solutions. On utilise le wronskien. Comme $f_1, \ldots, f_d$ sont libres sur $\mathbf{C}$, $W(f_1, \ldots, f_d) \neq 0$. D'autre part, développons le déterminant

$$W(f_1, \ldots, f_d, Y) = \begin{vmatrix} f_1 & \cdots & f_d & Y \\ f_1' & \cdots & f_d' & Y' \\ \vdots & & \vdots & \vdots \\ f_1^{(d)} & \cdots & f_d^{(d)} & Y^{(d)} \end{vmatrix} = A_0 Y + A_1 Y' + \cdots + A_d Y^{(d)},$$

où Y désigne une « indéterminée différentielle ». On obtient ainsi une équation différentielle d'ordre d à coefficients dans L. Remarquez que $A_d = W(f_1, \ldots, f_d) \neq 0$.

Montrons qu'en fait $A_j/A_d \in K$ pour tout j, si bien que l'équation différentielle

$$\text{(E)} \qquad Y^{(d)} + \frac{A_{d-1}}{A_d} Y^{(d-1)} + \cdots + \frac{A_0}{A_d} Y = 0$$

est à coefficients dans K. Pour cela, nous devons montrer que pour tout j, $0 \leqslant j \leqslant d$, et tout σ dans $\mathrm{Gal}(L/K)$, $\sigma(A_j)/\sigma(A_d) = A_j/A_d$. Remarquons alors en manipulant les d premières colonnes du déterminant $W(f_1, \ldots, f_d, Y)$ qu'il ne dépend essentiellement que de l'espace vectoriel engendré sur $\mathbf{C}$ par $f_1, \ldots, f_d$. Plus précisément, si $P(\mathbf{f},g) \in \mathrm{GL}_d(\mathbf{C})$ désigne la matrice de passage de la base $\mathbf{g} = (g_1, \ldots, g_d)$ à la base $\mathbf{f} = (f_1, \ldots, f_d)$,

$$W(g_1, \ldots, g_d, Y) = \det P(\mathbf{f}, \mathbf{g})\, W(f_1, \ldots, f_d, Y).$$

Si σ est un élément de $\mathrm{Gal}(L/K)$, comme $\sigma(f_1), \ldots, \sigma(f_d)$ forment aussi une base de V, on a ainsi

$$W(\sigma(f_1), \ldots, \sigma(f_d), Y) = \det P(\sigma(\mathbf{f}), \mathbf{f})\, W(f_1, \ldots, f_d, Y),$$

ce qui entraîne en développant le déterminant que $\sigma(A_j) = \det P(\mathbf{f}, \sigma(\mathbf{f}))A_j$ pour tout $j \in \{0, \dots, d\}$. Alors, $\sigma(A_j/A_d) = A_j/A_d$, comme il fallait démontrer.

L'espace vectoriel des solutions de (E) dans L est de dimension d. De plus, L est engendrée comme corps, donc comme corps différentiel, par $f_1, \dots, f_d$. Il n'y a pas d'autres constantes que $\mathbf{C}$ dans L. Par suite, c'est une extension de Picard-Vessiot de (E). De plus, l'homomorphisme naturel $\mathrm{Gal}^D(L/K) \to \mathrm{Gal}(L/K)$ est un isomorphisme. Sa réciproque correspond essentiellement aux homomorphismes classiques du groupe symétrique $\mathfrak{S}_n$ dans le groupe linéaire $\mathrm{GL}_n(\mathbf{C})$ fourni par les matrices de permutations.

6.6. La correspondance de Galois différentielle

Dans la théorie algébrique des équations différentielles, il y a des groupes de Galois, ainsi qu'un analogue de la correspondance de Galois. Les démonstrations sont trop difficiles pour être présentées dans ce livre, mais j'aimerais vous donner quelques idées des *énoncés*.

Fixons une extension de Picard-Vessiot $K \subset L$, dont le corps des constantes C est supposé algébriquement clos et de caractéristique zéro, attachée à une équation différentielle $Y' = AY$, où $A \in M_n(K)$. Nous avons vu que son groupe de Galois différentiel $\mathrm{Gal}^D(L/K)$ peut être considéré comme un sous-groupe de $\mathrm{GL}_n(C)$.

Pour tout sous-groupe $H \subset \mathrm{Gal}^D(L/K)$, nous pouvons introduire le sous-corps $L^H \subset L$ formé des $x \in L$ tels que $\sigma(x) = x$ pour tout $\sigma \in H$. Il est facile de vérifier que la dérivation $D\colon L \to L$ envoie L^H dans lui-même, si bien que L^H est un corps différentiel. Les extensions $K \subset L^H$ et $L^H \subset L$ sont des extensions différentielles.

Il y a cependant un fait nouveau : les groupes de Galois différentiels ne sont pas des sous-groupes arbitraires de $\mathrm{GL}_n(C)$, ce sont automatiquement des *groupes algébriques,* ce qui signifie qu'il existe des polynômes $P_j \in C[a_{11}, \dots, a_{nn}]$ tels qu'une matrice $A = (a_{ij}) \in \mathrm{GL}_n(C)$ appartient au groupe de Galois différentiel si et seulement si $P_j(a_{11}, \dots, a_{nn}) = 0$ pour tout j.

Alors, les principaux énoncés de la correspondance de Galois différentielle sont les suivants.

– Pour tout sous-groupe $H \subset \mathrm{Gal}^D(L/K)$, l'extension $L^H \subset L$ est une extension de Picard-Vessiot (pour la même équation différentielle que l'équation $K \subset L$), et son groupe de Galois différentiel s'identifie à H.

– Inversement, toute sous-extension différentielle $K \subset E$ est de la forme L^H, pour un certain sous-groupe algébrique $H \subset \mathrm{Gal}^D(L/K)$.

– Si $H \subset \mathrm{Gal}^D(L/K)$ est un sous-groupe algébrique, l'extension différentielle $K \subset L^H$ est une extension de Picard-Vessiot (pour une certaine équation différentielle) si

et seulement si H est un sous-groupe distingué de $\mathrm{Gal}^D(L/K)$. Alors, $\mathrm{Gal}^D(L^H/K) \simeq \mathrm{Gal}^D(L/K)/H$.

Le problème analogue à la résolution par radicaux est la résolution des équations différentielles par *quadratures*, c'est-à-dire uniquement à l'aide de primitives. Pour que la théorie soit agréable, on autorise aussi des extensions algébriques. Alors, on démontre que pour qu'une équation différentielle soit résoluble par quadratures et extensions algébriques, il faut et il suffit que la composante neutre[(1)] du groupe de Galois différentiel $\mathrm{Gal}^D(L/K)$ est résoluble. C'est là qu'intervient le théorème de Lie-Kolchin 4.7.2 dans la théorie algébrique des équations différentielles.

6.7. Extensions élémentaires

Dans ce dernier paragraphe, je démontre un théorème de Liouville sur les fonctions dont une primitive peut s'exprimer de manière « élémentaire », par exemple en ne faisant intervenir que des logarithmes ou des exponentielles. Liouville a démontré de tels résultats dans une série d'articles publiés autour des années 1830, mais ce n'est qu'au milieu du XX$^{\mathrm{e}}$ siècle qu'Ostrowski a replacé le théorème de Liouville dans le cadre algébrique de la théorie des corps différentiels. La théorie a ensuite évolué vers un *algorithme* (Risch) pour calculer les primitives, au moins lorsque c'est possible. Il est implémentaé dans la plupart des systèmes de calcul formel.

Joseph Liouville (1809–1882)

Tous les corps que l'on considère sont de caractéristique nulle.

DÉFINITION 6.7.1. — *Soit (K,D) un corps différentiel et soit $a \in K$. On dit qu'un élément t d'une extension différentielle est un* logarithme *de a si $a \neq 0$ et si $t' = a'/a$. On dit que t est une* exponentielle *de a si $t'/t = a'$.*

DÉFINITION 6.7.2. — *Soit (K,D) un corps différentiel. Une extension différentielle (L,D) de (K,D) est dite* élémentaire *s'il existe $t_1,\dots,t_n$ dans L tels que*

a) *$L = K(t_1,\dots,t_n)$;*

b) *L n'a pas d'autres constantes que celles de K ;*

et tels que pour tout j, l'une des trois assertions est vérifiée :

(1) Si $C = \mathbf{C}$, c'est la composante connexe de l'identité dans le groupe de Galois différentiel, vu comme sous-groupe de $\mathrm{GL}_n(\mathbf{C})$. Pour un corps arbitraire C, on doit utiliser la topologie dite de Zariski.

3a) t_j *est algébrique sur* $K(t_1,\dots,t_{j-1})$ *;*
3b) t_j *est un logarithme d'un élément non nul de* $K(t_1,\dots,t_{j-1})$ *;*
3c) t_j *est une exponentielle d'un élément de* $K(t_1,\dots,t_{j-1})$.

Exercice 6.7.3. — Si $K \subset L$ est une extension élémentaire, vérifier que, avec les notations de la définition précédente, le corps $K(t_1,\dots,t_j)$ est, pour tout j, un sous-corps différentiel de L.

THÉORÈME 6.7.4 (Liouville, 1835 ; Ostrowski, 1946). — *Soit* (K,D) *un corps différentiel et soit* $f \in K$. *Si l'équation* $y' = f$ *a une solution dans une extension différentielle élémentaire de* K, *il existe un entier* $n \geqslant 0$, *des constantes* $c_1,\dots,c_n \in K$ *et des éléments* $u_1,\dots,u_n, v$ *dans* F *tels que*

$$f = v' + \sum_{i=1}^{n} c_i \frac{u_i'}{u_i}.$$

La démonstration se fait par récurrence sur le nombre d'étapes dans la définition d'une extension élémentaire. On a besoin pour cela d'un lemme concernant les extensions différentielles « en un cran », c'est-à-dire celles qui sont engendrées par un élément algébrique, une exponentielle ou un logarithme. Supposons pour l'instant avoir démontré la proposition ci-dessous, on démontre le théorème de Liouville comme suit. On commence avec $n = 0$ en prenant pour v la primitive de f. Grâce à la proposition suivante, on descend ensuite un à un tous les étages dans la définition d'une extension élémentaire, d'où le théorème.

PROPOSITION. — *Soit* $K \subset K(t)$ *une extension élémentaire « en un cran » et soit* f *un élément de* K *qui s'écrit sous la forme*

$$f = v' + \sum_{i=1}^{n} c_i \frac{u_i'}{u_i}$$

pour des constantes c_i *et des éléments* $u_1,\dots,u_n$ *et* v *dans* $K(t)$. *Alors,* f *admet une expression analogue dans* K.

Nous démontrons cette proposition en distinguant trois cas.

Premier cas : t ***est algébrique sur*** K**.** — Soit $K \subset L$ une clôture galoisienne de l'extension $K \subset K(t)$ et munissons L de l'unique dérivation pour laquelle l'homomomorphisme $K \to L$ est un homomorphisme de corps différentiels. Si $\sigma \in \mathrm{Gal}(L/K)$ et $x \in L$, $x \neq 0$, on a

$$\sigma\Big(\frac{x'}{x}\Big) = \frac{\sigma(x')}{\sigma(x)} = \frac{\sigma(x)'}{\sigma(x)}.$$

On calcule alors

$$[L:K]f = \sum_{\sigma\in\mathrm{Gal}(L/K)} \sigma(f) = \sum_{\sigma\in\mathrm{Gal}(L/K)} \sigma(v)' + \sum_{i=1}^{n} c_i \sum_{\sigma\in\mathrm{Gal}(L/K)} \sigma(u_i'/u_i).$$

Posons $\tilde{v} = (\sum_\sigma \sigma(v))/[L:K]$ et $\tilde{u}_i = \prod_\sigma \sigma(u_i)$. Comme ce sont des éléments de L invariants par $\mathrm{Gal}(L/K)$, ce sont des éléments de K. On a ainsi

$$f = \tilde{v}' + \sum_{i=1}^{n} \frac{1}{[L:K]} c_i \frac{\tilde{u}_i'}{\tilde{u}_i}.$$

Deuxième cas :** t **est transcendant sur** K **et est un logarithme. — Dans ce cas, on peut identifier le corps $K(t)$ au corps des fractions rationnelles en t, si bien qu'on écrit $u_i = U_i(t)$ et $v = V(t)$ (mais la dérivation est différente). Soit π un polynôme unitaire irréductible de $K[T]$. Pour tout $U \in K(T)^*$, notons $\mathrm{ord}_\pi(U)$ l'exposant de π lorsqu'on écrit U comme un produit de polynômes irréductibles unitaires de $K[T]$ (avec des exposants dans $\mathbf{Z}$), que multiplie un élément de K^*. Si $u = U(t) \in K(t)$, on écrit $\mathrm{ord}_\pi(u)$ pour $\mathrm{ord}_\pi(U)$. De même, si $u = U(t)$ avec $U \in K[T]$, nous écrirons $\deg u$ au lieu de $\deg U$.

LEMME 6.7.5. — (Supposant $t' \in K^*$.) *Soit $u \in K(t)^*$ et soit π un polynôme irréductible unitaire de $K[T]$.*

a) *Si* $\mathrm{ord}_\pi(u) = 0$, *alors* $\mathrm{ord}_\pi(u'/u) \geqslant 0$.
b) *Si* $\mathrm{ord}_\pi(u) \neq 0$, *on a* $\mathrm{ord}_\pi(u'/u) = -1$.
c) *Si* $u = U(t)$, *avec* $U \in K[T]$, *alros* $\deg u - 1 \leqslant \deg u' \leqslant \deg u$.

Démonstration du lemme. — Soit $U \in K(T)$ tel que $u = U(T)$ et écrivons $U = a\prod_j \pi_j(T)^{n_j}$, où $a \in K^*$, les n_j sont des entiers relatifs non-nuls et les π_j sont des polynômes irréductibles unitaires de $K[T]$, deux à deux distincts. Ainsi, $u = a\prod_j \pi_j(t)^{n_j}$ et

$$\frac{u'}{u} = \frac{a'}{a} + \sum_j n_j \frac{\pi_j(t)'}{\pi_j(t)} = \frac{a'}{a} + \sum_j n_j \frac{\pi_j^D(t) + t'\pi_j'(t)}{\pi_j(t)}.$$

Remarquons que pour tout j, $\pi_j^D + t'\pi_j'$ est un polynôme de $K[T]$ dont le degré est $< \deg(\pi_j)$, car π_j est unitaire. De plus, t est transcendant sur K, de sorte que $\pi_j(t) \notin K$ et donc $\pi_j(t)' \neq 0$ puisque $K(t)$ et K ont le même corps de constantes. Par suite, π_j ne divise pas le polynôme $\pi_j^D + t'\pi_j'$ et ord_{π_j} du j-ième terme dans la formule pour u'/u est égal à -1. Puisque ord_{π_j} des autres termes vaut 0, on a $\mathrm{ord}_{\pi_j}(u'/u) = -1$, d'où l'assertion *b*). La formule ci-dessus montre aussi que pour tout polynôme irréductible unitaire π, qui n'est pas l'un des π_j, on a $\mathrm{ord}_\pi(u'/u) \geqslant 0$, d'où *a*).

Montrons enfin *c*). Soit $u = U(t)$ où $U = u_0 + u_1 T + \cdots + u_n T^n \in K[T]$, avec $u_n \neq 0$ de sorte que $\deg u = n$. On a

$$u' = (u_0' + u_1 t') + (u_1' + 2u_2 t')t + \cdots + (u_{n-1}' + n u_n t')t^{n-1} + u_n' t^n.$$

Si $u'_n \neq 0$, alors $\deg(u') = n = \deg(u)$. Sinon, remarquons que l'annulation de

$$u'_{n-1} + nu_n t' = (u_{n-1} + nu_n t)'$$

entraîne que $u_{n-1} + nu_n t$ est constant, donc appartient à K, d'où $t \in K$, ce qui est absurde ! Par suite, $u'_{n-1} + nu_n t' \neq 0$ et $\deg(u') = \deg(u) - 1$. □

Reprenons la démonstration du second cas de la proposition et développons les dérivées logarithmiques dans la formule

$$f = v' + \sum_i c_i \frac{u'_i}{u_i}.$$

Elle se récrit ainsi

$$(*) \qquad f = v' + \sum_i c_i \frac{a'_i}{a_i} + \sum_\pi c_\pi \frac{\pi'}{\pi},$$

où les a_i appartiennent à K^*, π parcourt l'ensemble des polynômes irréductibles unitaires de $K[T]$, et c_i, c_π sont des constantes dans K.

Pour tout polynôme irréductible unitaire $\pi \in K[T]$ qui apparaît au dénominateur de v, on a $\mathrm{ord}_\pi(v') = \mathrm{ord}_\pi(v) - 1 \leqslant -2$. Cependant, ord_π de chacun des autres termes est au moins -1, si bien que la somme ne peut être égale à f, étant donné que $\mathrm{ord}_\pi(f) = 0$. Cela montre que $v = V(t)$ avec $V \in K[T]$.

Puisque $\deg \pi(t)' < \deg \pi(t)$, la formule $(*)$ est une décomposition en éléments simples de la fraction rationnelle « constante » f. L'unicité de cette décomposition entraîne que les termes polaires s'annulent, d'où

$$f = v' + \sum_i c_i \frac{a'_i}{a_i}.$$

En particulier, $v' = f - \sum_i c_i (a'_i / a_i)$ appartient à K et son degré est nul. Cela implique que $V(T) = cT + d$, avec c et $d \in K$, et $c' = 0$. Si t est un logarithme de $a \in K^*$, c'est-à-dire $t' = a'/a$, il s'ensuit

$$f = ct' + d' + \sum_i c_i \frac{a'_i}{a_i} = d' + \left(c\frac{a'}{a} + \sum_i c_i \frac{a'_i}{a_i} \right).$$

C'est une expression de la forme cherchée, d'où la proposition dans ce cas.

Troisième cas : t est transcendant sur K et est une exponentielle.

Nous identifions encore les éléments de $K(t)$ à des fractions rationnelles en une indéterminée T. La démonstration sera proche de celle du deuxième cas, le lemme 6.7.5 étant remplacé par le lemme suivant.

LEMME 6.7.6. — (Supposant $t'/t \in K^*$.) *Soit $\pi \in K[T]$ un polynôme irréductible unitaire et soit $u \in K(t)$.*

a) *Si* $\mathrm{ord}_\pi(u) = 0$, *alors* $\mathrm{ord}_\pi(u'/u) \geqslant 0$.

b) *Supposons* $\mathrm{ord}_\pi(u) \neq 0$. *Si* $\pi \neq T$, $\mathrm{ord}_\pi(u'/u) = -1$ *; si* $\pi = T$, $\mathrm{ord}_\pi(u'/u) \geqslant 0$.
c) *Si* $u = U(t)$ *avec* $U \in K[T]$, *alors* $\deg(u') = \deg(u)$.

Démonstration du lemme. — On commence comme dans la démonstration du lemme 6.7.5 : si $u = a\prod_j \pi_j(t)^{n_j}$, on a

$$\frac{u'}{u} = \frac{a'}{a} + \sum_j n_j \frac{\pi_j(t)'}{\pi_j(t)} = \frac{a'}{a} + \sum_j n_j \frac{\pi_j^D(t) + t'\pi_j'(t)}{\pi_j(t)}.$$

L'assertion *a*) en résulte immédiatement. Remarquons en outre que le degré du polynôme $\pi_j^D(T) + (t'/t)T\pi_j'(T)$ est inférieur ou égal à celui de π_j. Cela entraîne que soit ces polynômes sont premiers entre eux et $\mathrm{ord}_{\pi_j}(u'/u) = -1$, soit il existe $\lambda \in K$ tel que $\pi_j^D + (t'/t)T\pi_j' = \lambda\pi_j$, d'où $\mathrm{ord}_{\pi_j}(u'/u) \geqslant 0$.

Montrons que ce second cas ne se produit que pour $\pi_j = T$. Écrivons $\pi = T^n + p_{n-1}T^{n-1} + \cdots + p_0$, où $p_0, \ldots, p_{n-1} \in K$. Alors, si l'on note $a = t'/t$, la relation $\pi^D + aT\pi' = \lambda\pi$ peut être récrite en

$$anT^n + (p_{n-1}' + a(n-1)p_{n-1})T^{n-1} + \cdots + (p_1' + ap_1)T + p_0' = \lambda T^n + \lambda p_{n-1}T^{n-1} + \cdots + \lambda p_0.$$

Par suite, $\lambda = an$. De plus, pour tout entier j tel que $0 \leqslant j < n$ et $p_j \neq 0$, on a $p_j'/p_j = a(n-j) = (n-j)t'/t$. Cela entraîne que t^{n-j}/p_j est constant, donc appartient à K, ce qui contredit l'hypothèse que t est transcendant sur K. Ainsi, $\pi = T^n$, d'où $\pi = T$ puisque π est irréductible. Inversement, si $\pi = T$, on a $\pi(t)'/\pi(t) = t'/t \in K^*$, d'où $\mathrm{ord}_\pi(u'/u) \geqslant 0$.

Pour démontrer *c*), considérons un polynôme $U \in K[T]$ tel que $u = U(T)$. Si $a = t'/t \in K^*$ et $U = u_nT^n + \cdots + u_0$, avec $u_n \neq 0$, on a

$$u' = \sum_{k=0}^{n} (u_k' + aku_k)t^k,$$

si bien que $\deg(u') \leqslant \deg(u)$. Si l'on avait $u_n' + nau_n = 0$, alors

$$\frac{u_n'}{u_n} = -na = -n\frac{t'}{t},$$

et u_nt^n serait constant, donc dans K. Cela contredit l'hypothèse que t est transcendant sur K. Par suite, $u_n' + nau_n \neq 0$ et $\deg(u') = \deg(u)$. □

Terminons la démonstration de la proposition dans le cas où t est une exponentielle, c'est-à-dire $t' = a't$, avec $a \in K^*$. Comme avant, on développe les dérivées logarithmiques dans l'expression

$$f = v' + \sum c_i \frac{u_i'}{u_i},$$

d'où l'on déduit

$$(**) \qquad f = v' + \sum_i c_i \frac{a_i'}{a_i} + \sum_\pi c_\pi \frac{\pi'}{\pi},$$

où les a_i appartiennent à K^*, π parcourt les polynômes irréductibles unitaires de $K[T]$, c_i et c_π snt des constantes non-nulles dans K. Il en résulte que

$$f = v' + \sum_i c_i \frac{a_i'}{a_i} + \sum_\pi c_\pi a' + \sum_\pi c_\pi \frac{\pi^D(t) + a' t\pi'(t) - a'\pi(t)}{\pi(t)}.$$

Si $\pi \neq T$ et $\mathrm{ord}_\pi(v) < 0$, alors $\mathrm{ord}_\pi(v') \leqslant -2$, bien que ord_π du membre de droite soit au moins -1. Cela montre que $\mathrm{ord}_\pi(v) \geqslant 0$, sauf peut-être pour $\pi = T$. On peut ainsi écrire $v = \sum_{j\in\mathbf{Z}} v_j t^j$, avec $v_j \in K$. Remarquons maintenant que pour tout π, $\deg(\pi^D + a' T\pi' - a'\pi) < \deg(\pi)$. Comme $f \in K$ est une fraction rationnelle « constante », l'unicité de la décomposition en éléments simples entraîne que l'on peut omettre les termes avec π au dénominateur. Notant alors $c = \sum_\pi c_\pi$, la formule $(**)$ devient

$$f = \sum_j (v_j' + a' j v_j) t^j + ca' + \sum_i c_i \frac{a_i'}{a_i}.$$

En comparant les termes de degré 0, on obtient

$$f = (v_0 + ac)' + \sum_i c_i \frac{a_i'}{a_i},$$

c'est-à-dire une expression de la forme requise par la proposition.

La démonstration de ce dernier cas de la proposition conclut la démonstration du théorème de Liouville. Donnons-en maintenant quelques applications concrètes.

PROPOSITION 6.7.7. — *Soit f et g deux fractions rationnelles de $\mathbf{C}(X)$. On suppose que $f \neq 0$, que g n'est pas constante et que $f\exp(g)$ admette une primitive dans une extension différentielle élémentaire de $\mathbf{C}(X, \exp(g))$. Alors, il existe a dans $\mathbf{C}(X)$ telle que*

$$f = a' + ag'.$$

Démonstration. — Remarquons d'abord que si $f = a' + ag'$, on a $f\exp(g) = (a\exp(g))'$. Réciproquement, supposons que f a une primitive dans une extension élémentaire de $\mathbf{C}(X, \exp(g))$. D'après le théorème de Liouville, on peut écrire

$$f\exp(g) = v' + \sum_{i=1}^n c_i \frac{u_i'}{u_i},$$

où $v \in \mathbf{C}(X, \exp(g))$, $c_i \in \mathbf{C}$, $u_i \in \mathbf{C}(X, \exp(g))$. Posons $T = \exp(g)$; il est transcendant sur $\mathbf{C}(X)$ (voir l'exercice 1.3) et permet d'identifier u_i et v à des fractions rationnelles en T sur le corps $\mathbf{C}(X)$. Comme auparavant, on peut supposer que les u_i sont ou bien dans $\mathbf{C}(X)$, ou bien des polynômes irréductibles unitaires à coefficients dans $\mathbf{C}(X)$.

Comme dans la démonstration du théorème de Liouville, on voit que les seuls u_i qui peuvent intervenir sont $u_i = T$ ou bien des u_i dans $\mathbf{C}(X)$. De même, v n'a au plus qu'une puissance de T au dénominateur. On écrit donc $v = \sum_j v_j(X)T^j$ (les j sont des entiers relatifs) d'où

$$fT = \sum_j (v_j' + jg'v_j)T^j + cg' + \sum_i c_i \frac{u_i'(X)}{u_i(X)}.$$

Comparant les coefficients de T de chaque côté, on obtient

$$f = v_1' + g'v_1,$$

d'où la proposition avec $a = v_1$. □

Exemple 6.7.8. — La « fonction » $\exp(x^2)$ *n'a pas de primitive dans une extension élémentaire.* En effet, il existerait sinon une fraction rationnelle $a \in \mathbf{C}(x)$ telle que $1 = a' + 2xa$. Ceci est impossible : un pôle de a est pôle double de a' et pôle au plus simple de $1 - 2xa = a'$, donc a est un polynôme. Alors, $2xa = 1 - a'$ bien que ces deux polynômes n'aient pas le même degré.

L'exercice 6.6 propose d'autres exemples.

6.8. Appendice : théorème des zéros de Hilbert

Ce paragraphe est consacré à l'étude des idéaux maximaux des anneaux de polynômes $k[X_1, \ldots, X_n]$ sur un corps k. Le résultat principal est le théorème des zéros de Hilbert. Il possède plusieurs incarnations, toutes intéressantes. En voici trois. Lorsque le corps k n'est pas dénombrable (par exemple si $k = \mathbf{C}$, et c'est déjà un cas très important), on peut donner une démonstration très simple de ce théorème.

David Hilbert (1862–1943)

THÉORÈME 6.8.1 (Algèbres). — *Soit k un corps et soit A une k-algèbre de type fini. Si A est un corps, c'est une extension algébrique finie de k.*

THÉORÈME 6.8.2 (Idéaux). — *Soit k un corps algébriquement clos et soit I un idéal maximal de l'anneau de polynômes $k[X_1, \ldots, X_n]$. Alors, il existe $a_1, \ldots, a_n$ dans k tels que $I = (X_1 - a_1, \ldots, X_n - a_n)$.*

THÉORÈME 6.8.3 (Équations). — *Soit k un corps algébriquement clos et soit $P_1,\dots,P_m$ des polynômes de $k[X_1,\dots,X_n]$. Si le système d'équations*

$$P_1(x_1,\dots,x_n)=\cdots=P_m(x_1,\dots,x_n)=0$$

n'a pas de solution dans k^n, il existe des polynômes $Q_1,\dots,Q_m$ tels que

$$1=P_1Q_1+\cdots+P_mQ_m.$$

Cette dernière forme du théorème des zéros de Hilbert signifie qu'un système d'équations polynomiales qui n'a pas de solution dans un corps algébriquement clos est incompatible en un sens très fort car une relation telle que dans le théorème empêche le système $P_1=\cdots=P_m$ d'avoir une solution dans *tout* corps contenant k.

Démonstration du théorème 6.8.1 sous l'hypothèse que k n'est pas dénombrable

Soit $x_1,\dots,x_n$ dans A tels que $A=k[x_1,\dots,x_n]$. Tout élément de A peut s'exprimer (certes de manière non unique) comme un polynôme en $x_1,\dots,x_n$. Ainsi, la dimension de A comme k-espace vectoriel est inférieure ou égale au cardinal de l'ensemble des monômes. Elle est donc dénombrable.

Supposons maintenant que l'un des x_j, disons x_1, soit transcendant. Alors, l'anneau $k[x_1]$ est isomorphe à l'anneau de polynômes $k[X]$. Comme A est un corps, A contient le corps $k(x_1)$ qui est isomorphe au corps des fractions rationnelles $k(X)$. Or, la décomposition en éléments simples affirme (entre autres) que les éléments $1/(X-a)$ de $k(X)$ sont linéairement indépendants sur k. Comme k n'est pas dénombrable, la dimension de $k(X)$ comme k-espace vectoriel n'est pas dénombrable. Ceci contredit le fait que la dimension de A le soit. □

Démonstration du théorème 6.8.2. — Soit $(a_1,\dots,a_n)\in k^n$ et soit I l'idéal de $k[X_1,\dots,X_n]$ engendré par $X_1-a_1,\dots,X_n-a_n$. Montrons que I est un idéal maximal. Soit $P\in k[X_1,\dots,X_n]$ et effectuons la division euclidienne de P par X_1-a_1 (en la variable X_1). Il en résulte deux polynômes P_1 et $Q_1\in k[X_1,\dots,X_n]$ tels que

$$P(X_1,\dots,X_n)=(X_1-a_1)Q_1(X_1,\dots,X_n)+P_1(X_1,\dots,X_n),$$

le polynôme P_1 étant de degré $<\deg(X_1-a_1)$ en X_1. Ainsi, P_1 ne dépend pas de X_1 et est un polynôme de $k[X_2,\dots,X_n]$. On continue ainsi de suite, d'où une expression

$$P(X_1,\dots,X_n)=(X_1-a_1)Q_1+(X_2-a_2)Q_2+\cdots+(X_n-a_n)Q_n+P_n$$

où P_n est un polynôme constant, égal à $P(a_1,\dots,a_n)$. Par suite, $P(a_1,\dots,a_n)=0$ si et seulement si $P\in I$.

Montrons que I est maximal. Soit J un idéal contenant I, $J\neq I$ et soit $P\in J\setminus I$. Ainsi, $P(a_1,\dots,a_n)\neq 0$. Comme le polynôme

$$P(X_1,\dots,X_n)-P(a_1,\dots,a_n)$$

est nul en $(a_1,\dots,a_n)$, il appartient à I, donc à J. Il en résulte que $P(a_1,\dots,a_n)$ appartient à J. Comme c'est un élément non nul de k, son inverse appartient à J et $1 \in J$. Alors, $J = A$. On a donc prouvé que I est un idéal maximal de $k[X_1,\dots,X_n]$.

Soit I un idéal maximal de $k[X_1,\dots,X_n]$. Considérons l'anneau quotient A/I et l'homomorphisme canonique $k[X_1,\dots,X_n] \to A/I$. Si x_j désigne l'image de X_j dans A/I, il est évident que $A/I = k[x_1,\dots,x_n]$. Ainsi, A/I est une k-algèbre de type fini. D'autre part, comme I est un idéal maximal, A/I est un corps. D'après le théorème 6.8.1, l'extension $k \subset A/I$ est donc algébrique finie. Comme k est algébriquement clos, c'est un isomorphisme. Autrement dit, chaque x_j appartient à k, ce qui signifie qu'il existe $a_j \in k$ tel que $X_j - a_j \in I$. Alors, I contient l'idéal $(X_1 - a_1,\dots,X_n - a_n)$. Comme ce dernier idéal est maximal, on a l'égalité. □

Démonstration du théorème 6.8.3. — Soit I l'idéal engendré par $P_1,\dots,P_m$. Soit $\mathfrak{m}$ un idéal maximal de $k[X_1,\dots,X_n]$. Si on avait $I \subset \mathfrak{m}$, le n-uplet $(a_1,\dots,a_n)$ tel que $\mathfrak{m} = (X_1 - a_1,\dots,X_n - a_n)$ serait une solution du système $P_j(x_1,\dots,x_n) = 0$, $1 \leqslant j \leqslant m$. Ainsi, I n'est contenu dans aucun idéal maximal (théorème 2.5.3) et est donc l'idéal A. Ainsi, $1 \in I$ et il existe $Q_1,\dots,Q_m$ dans $k[X_1,\dots,X_n]$ tels que $1 = P_1Q_1 + \cdots + P_mQ_m$. □

Exercices

Exercice 6.1. — Soit (A,D) un anneau différentiel et soit $P \in A[X,Y]$ un polynôme en deux variables. On note P^D le polynôme obtenu en dérivant les coefficients de P, $\partial P/\partial X$ et $\partial P/\partial Y$ les dérivées partielles formelles de P par rapport à X et Y.

Si x, y sont des éléments de A, montrer que

$$P(x,y)' = P^D(x,y) + x'\frac{\partial P}{\partial X}(x,y) + y'\frac{\partial P}{\partial X}(x,y).$$

Exercice 6.2. — Soit (A,D) un anneau différentiel et soit $G \in M_n(A)$. On désigne par $\mathrm{Com}(G)$ la comatrice de G, c'est-à-dire la matrice transposée des cofacteurs. Montrer que

$$(\det G)' = \mathrm{Tr}(\mathrm{Com}(G)G').$$

Exercice 6.3. — Soit A un anneau. On note $A[\varepsilon]$ l'anneau $A[X]/(X^2)$, ε désignant la classe de X.

a) Montrer qu'il existe un unique homomorphisme d'anneaux $\pi\colon A[\varepsilon] \to A$ tel que $\pi(a) = a$ pour tout $A \in A$.

b) Soit D une dérivation de A. Montrer que l'application de A dans $A[\varepsilon]$ définie par $\varphi(a) = a + \varepsilon D(a)$ est un homomorphisme d'anneaux.

c) Réciproquement, si $\varphi\colon A \to A[\varepsilon]$ est un homomorphisme d'anneaux tel que $\pi \circ \varphi = \mathrm{id}_A$, montrer qu'il existe une dérivation D de A telle que $\varphi(a) = a + \varepsilon D(a)$.

Exercice 6.4. — On veut expliciter une extension de Picard-Vessiot de l'équation $y''+y=0$ sur le corps $\mathbf{C}(X)$ muni de la dérivation usuelle.

a) On a $R=\mathbf{C}[X,Y_1,Y_2,Y_1',Y_2']$ muni de l'unique dérivation telle que $(Y_j)'=Y_j'$ et $(Y_j')'=-Y_j$.

b) Montrer que l'anneau des constantes de R contient strictement $\mathbf{C}(X)$. (Penser à $\sin^2(x)+\cos^2(x)=1$.)

c) Montrer que le corps $\mathbf{C}(X,Y)$ muni de la dérivation définie par $Y'=iY$ est une extension de Picard-Vessiot de l'équation (E).

Exercice 6.5. — Soit (K,D) un corps différentiel de caractéristique 0 et de corps des constantes C. Soit (E) : $y^{(n)}+a_{n-1}y^{(n-1)}+\cdots+a_0y=0$ une équation différentielle d'ordre n. On note (L,D) une extension de Picard-Vessiot pour cette équation.

Soit $f_1,\dots,f_n$ n une C-base des solutions de (E) dans L.

a) Calculer la dérivée de $W(f_1,\dots,f_n)$.

b) Si $\sigma\in \mathrm{Gal}^D(L/K)$, calculer $\sigma(W(f_1,\dots,f_n))$ en termes de l'image de σ dans $\mathrm{GL}_n(C)$.

c) Généraliser au cas d'un système différentiel $Y'=AY$.

Exercice 6.6. — **a)** Montrer que les fonctions $\exp(x)/x$, $\exp(\exp(x))$ n'ont pas de primitive élémentaire.

b) Montrer que $1/(x^2+1)$ n'a pas de primitive dans une extension élémentaire de $\mathbf{R}(x)$ mais qu'elle en a une dans une extension élémentaire de $\mathbf{C}(x)$.

c) Montrer que $\sin(x)/x$ n'a pas de primitive élémentaire.

Problèmes d'examen

Je termine ce livre par des exercices et des problèmes d'examen. Certains sont substantiels.

L'exercice 7.1 démontre un théorème de Selmer selon lequel, pour tout entier $n \geqslant 2$, le polynôme $X^n - X - 1$ est irréductible sur $\mathbf{Q}$.

L'exercice 7.2 est une élaboration du casus irreductibilis. *Il explique et généralise le fait que, bien que les trois racines d'une équation polynomiale de degré 3 puissent être réelles, les formules de Cardan utilisent des nombres complexes.*

L'exercice 7.5 est un théorème de Galois sur la résolution par radicaux des équations de degré premier.

L'exercice 7.11 démontre un théorème de E. Artin et O. Schreier sur les sous-corps F d'un corps algébriquement clos Ω tel que $[\Omega : F]$ soit fini.

1. Problème de révision (2002)

Exercice 7.1. — Soit n un entier $\geqslant 2$ et S le polynôme $X^n - X - 1$. Le but du problème est de montrer que S est irréductible dans $\mathbf{Z}[X]$.

a) Montrer que S a n racines distinctes dans $\mathbf{C}$.

b) Si $P \in \mathbf{Q}[X]$, $P = a_m X^m + \cdots + a_0$, avec $a_0 a_m \neq 0$, de racines $z_1, \ldots, z_m$ dans $\mathbf{C}$, on pose

$$\varphi(P) = \sum_{j=1}^{m} \big(z_j - \frac{1}{z_j}\big).$$

Calculer $\varphi(P)$ en fonction de $a_0, \ldots, a_m$. Que vaut $\varphi(S)$?

Montrer aussi que si P et Q sont deux polynômes de $\mathbf{Q}[X]$ tels que $P(0)Q(0) \neq 0$, $\varphi(PQ) = \varphi(P) + \varphi(Q)$.

c) Si z est une racine de S, montrer l'inégalité

$$2\Re\big(z - \frac{1}{z}\big) > \frac{1}{|z|^2} - 1.$$

(Poser $z = re^{i\theta}$ et évaluer $\cos(\theta)$ en fonction de r.)

d) Si $x_1, \dots, x_m$ sont des réels strictement positifs tels que $\prod_{j=1}^{m} x_j = 1$. Montrer l'inégalité $\sum_{j=1}^{m} x_j \geqslant m$.

e) Soit P et Q deux polynômes de $\mathbf{Z}[X]$ de degrés non nuls tels que $S = PQ$. Montrer que $|P(0)| = 1$ puis que $\varphi(P)$ est un entier strictement positif. En déduire une contradiction et donc que S est un polynôme irréductible dans $\mathbf{Z}[X]$.

Exercice 7.2. — Si E est un sous-corps de $\mathbf{R}$, une *extension radicale réelle* est par définition une extension radicale de E contenue dans $\mathbf{R}$.

a) Soit $E \subset F$ une extension finie galoisienne, avec $F \subset \mathbf{R}$; soit $\alpha \in \mathbf{R}$ tel que α^N appartient à E, pour un certain entier $N \geqslant 2$, de sorte que l'extension $E \subset E(\alpha)$ est radicale réelle (d'exposant N).

(*i*) Soit $m = [E(\alpha) : F \cap E(\alpha)]$ et posons $\beta = \alpha^m$. Montrer que β appartient à $F \cap E(\alpha)$. En déduire que $F \cap E(\alpha) = E(\beta)$.

(*ii*) En remarquant qu'une puissance de β appartient à E, montrer que $[E(\beta) : E]$ est égal à 1 ou 2.

b) Soit $E \subset F$ une extension finie galoisienne, avec $F \subset \mathbf{R}$; soit $E \subset K$ une extension radicale réelle. Montrer que $[K \cap F : E]$ est une puissance de 2. (Raisonner par récurrence. Introduire $L \subset K$ telle que $E \subset L$ soit radicale élémentaire, appliquer l'hypothèse de récurrence à l'extension galoisienne $L \subset FL$ et à l'extension radicale $L \subset K$.)

c) Soit $P \in \mathbf{Q}[X]$ un polynôme irréductible de degré n dont toutes les racines sont réelles. On suppose qu'une des racines α de P appartient à une extension radicale réelle de $\mathbf{Q}$.

Montrer que n est une puissance de 2.

2. Contrôle classant (2002)

Exercice 7.3. — **a)** Montrer que les réels 1, $\sqrt{2}$ et $\sqrt{5}$ sont linéairement indépendants sur le corps $\mathbf{Q}$ des nombres rationnels.

b) Quel est le degré du corps $K = \mathbf{Q}(\sqrt{2}, \sqrt{5})$ sur $\mathbf{Q}$?

c) Montrer que l'extension $\mathbf{Q} \subset K$ est galoisienne et déterminer son groupe de Galois.

d) Trouver un élément $\alpha \in K$ tel que $K = \mathbf{Q}(\alpha)$.

e) Combien existe-t-il de sous-corps $E \subset K$? En donner la liste.

Exercice 7.4. — **a)** Soit K un corps (de caractéristique zéro), d un élément de K qui n'est pas un carré et $K \subset K(\sqrt{d})$ l'extension quadratique correspondante.

Soit $x \in K$. Montrer que x est un carré dans $K(\sqrt{d})$ si et seulement si, ou bien x est un carré dans K, ou bien dx est un carré dans K.

On considère dans la suite trois rationnels r, s, t. On suppose que t n'est pas un carré dans $\mathbf{Q}$; on note $\sqrt{t}$ l'une des deux racines complexes de t et on pose $E = \mathbf{Q}(\sqrt{t})$. On suppose aussi que $r + s\sqrt{t}$ n'est pas un carré dans $\mathbf{Q}(\sqrt{t})$, on note α l'une des deux racines complexes de $r + s\sqrt{t}$ et on pose $F = E(\alpha)$.

b) Montrer que $[F : E] = 4$. Quel est le polynôme minimal sur $\mathbf{Q}$ de l'élément α ? Quels sont ses conjugués dans $\mathbf{C}$?

c) Montrer les équivalences :

(i) l'extension $\mathbf{Q} \subset F$ est galoisienne ;
(ii) $r - s\sqrt{t}$ est un carré dans F ;
(iii) il existe $x \in \mathbf{Q}$ tel que $r^2 - s^2 t = x^2$ (premier cas) ou $r^2 - s^2 t = t x^2$ (second cas).

d) On suppose l'extension $\mathbf{Q} \subset F$ galoisienne. Dans le premier cas, montrer que $\mathrm{Gal}(F/\mathbf{Q}) \simeq (\mathbf{Z}/2\mathbf{Z})^2$. Dans le second cas, montrer que $\mathrm{Gal}(F/\mathbf{Q}) \simeq \mathbf{Z}/4\mathbf{Z}$. (Remarquer qu'un élément du groupe de Galois est déterminé par l'image de α, au moins si $s \neq 0$, et procéder avec méthode.)

e) (*Application numérique*) Écrire $\sqrt{5 + \sqrt{21}}$ sans radicaux emboîtés. Est-ce possible pour $\sqrt{7 + 2\sqrt{5}}$?

Exercice 7.5. — Le but de cet exercice est de démontrer la proposition VIII du mémoire de Galois : « *Pour qu'une équation irréductible de degré premier soit soluble par radicaux, il* faut *et il* suffit *que deux quelconques des racines étant connues, les autres s'en déduisent rationnellement.* »

Partie 1. Théorie des groupes

a) Soit X un ensemble fini, G un sous-groupe du groupe $\mathfrak{S}(X)$ des permutations de X. On suppose que G agit transitivement sur X. Soit H un sous-groupe distingué de G.

(*i*) Si x et y sont deux éléments de X, $\mathrm{Stab}_H(x)$ et $\mathrm{Stab}_H(y)$ leurs stabilisateurs dans H, montrer qu'il existe $g \in G$ tel que $g\,\mathrm{Stab}_H(y)\,g^{-1} = \mathrm{Stab}_H(x)$. En déduire que les orbites de x et de y sous l'action de H ont même cardinal.

(*ii*) On suppose de plus que X est de cardinal premier p. Si $H \neq \{1\}$, montrer que H agit transitivement sur X.

b) Soit p un nombre premier et soit B_p le sous-groupe des permutations de $\mathbf{Z}/p\mathbf{Z}$ qui sont de la forme $m \mapsto am + b$ avec a et b dans $\mathbf{Z}/p\mathbf{Z}$.

(*i*) Quel est le cardinal de B_p ?

(*ii*) Montrer que B_p agit transitivement sur $\mathbf{Z}/p\mathbf{Z}$. Soit h un élément de B_p qui stabilise deux éléments de $\mathbf{Z}/p\mathbf{Z}$. Montrer que $h = \mathrm{id}$.

(*iii*) Montrer que B_p est résoluble. (On pourra introduire le sous-groupe de B_p formé des permutations de la forme $m \mapsto m+b$ avec $b \in \mathbf{Z}/p\mathbf{Z}$.)

c) Soit p un nombre premier et G un sous-groupe fini du groupe symétrique $\mathfrak{S}_p$ qui est transitif et résoluble. Soit

$$\{1\} = G_0 \subsetneq G_1 \subsetneq \cdots \subsetneq G_m = G$$

une suite de sous-groupes, G_i étant distingué dans G_{i+1} et G_{i+1}/G_i cyclique d'ordre premier.

(*i*) Montrer que G_1 est engendré par une permutation circulaire d'ordre p.

(*ii*) Montrer qu'il existe $\sigma \in \mathfrak{S}_p$ tel que $\sigma^{-1}G_1\sigma$ soit engendré par la permutation circulaire $(1\,2\,\ldots\,p)$.

(*iii*) On identifie l'ensemble $\{1;\ldots;p\}$ à $\mathbf{Z}/p\mathbf{Z}$ par l'application qui à un entier associe sa classe modulo p. De la sorte, le groupe $\mathfrak{S}_p$ des permutations de $\{1;\ldots;p\}$ est identifié au groupe des permutations de $\mathbf{Z}/p\mathbf{Z}$. Cela permet en particulier de considérer le groupe B_p comme un sous-groupe de $\mathfrak{S}_p$.

Montrer que $\sigma^{-1}G\sigma$ est contenu dans le groupe B_p de la question 2.

Partie 2. Extensions de corps

a) Soit E un corps, $P \in E[X]$ un polynôme irréductible de degré premier p et $E \subset F$ une extension de décomposition de P.

(*i*) Rappeler comment le groupe de Galois $\mathrm{Gal}(F/E)$ s'identifie à un sous-groupe transitif de $\mathfrak{S}_p$.

(*ii*) Si $\mathrm{Gal}(F/E)$ est résoluble, montrer que si α et β sont deux racines distinctes de P dans F, on a $F = E(\alpha,\beta)$.

b) Soit E un corps, $P \in E[X]$ un polynôme irréductible de degré premier p. Soit $E \subset F$ une extension de décomposition de P. On identifie toujours $\mathrm{Gal}(F/E)$ à un sous-groupe de $\mathfrak{S}_p$.

(*i*) Montrer que $\mathrm{Gal}(F/E)$ contient une permutation circulaire (d'ordre p).

(*ii*) On suppose qu'il existe une racine α de P tel que $F = E(\alpha)$. Montrer que $\mathrm{Gal}(F/E) \simeq \mathbf{Z}/p\mathbf{Z}$.

On suppose dans la suite de cette question qu'il existe deux racines distinctes α et β de P telles que $F = E(\alpha,\beta)$.

(*iii*) Montrer que $[F:E] \leqslant p(p-1)$.

(*iv*) Montrer que $\mathrm{Gal}(F/E)$ contient une permutation circulaire d'ordre p.

(*v*) Soit σ et τ deux permutations circulaires d'ordre p de $\mathrm{Gal}(F/E)$. Montrer qu'elles engendrent le même sous-groupe cyclique d'ordre p. En déduire que ce sous-groupe cyclique est distingué dans G.

(*vi*) Montrer que $\mathrm{Gal}(F/E)$ est résoluble.

3. Session de rattrapage (2002)

Exercice 7.6. — **a)** Les nombres complexes suivants sont-ils algébriques ? Si oui, en donner un polynôme minimal.

$\sqrt{2}$, $\sqrt{1+\sqrt{2}}$, $(1+\pi^2)/(1-\pi)$.

b) Existe-t-il un élément $x \in \mathbf{Q}(\sqrt{3})$ dont le carré est 2 ?

c) Soit $K \subset E$ une extension quadratique. Soit $P \in K[X]$ un polynôme de degré 3 qui a une racine dans E. Montrer que P a une racine dans K. Est-il vrai que P est scindé dans K ? Dans E ?

Exercice 7.7. — **a)** Soit G le groupe fini $\mathfrak{S}_4$. Soit H l'ensemble des permutations $\sigma \in G$ telles que $\sigma(1) = 1$.

(*i*) Calculer $\operatorname{card} G$, $\operatorname{card} H$. Montrer que H est un sous-groupe de G et calculer $(G : H)$.

(*ii*) Montrer que H n'est pas distingué dans G.

(*iii*) Si $\tau \in G \setminus H$, montrer que le sous-groupe de G engendré par H et τ est égal à G.

b) Montrer qu'un groupe de cardinal 4 contient un élément d'ordre 2. De quel résultat du cours est-ce un cas (très) particulier ?

c) Soit G un groupe fini, soit H un sous-groupe distingué de G tel que $(G : H) = 4$. Montrer qu'il existe un sous-groupe K de G contenant H tel que $(G : K) = 2$.

d) Soit $K \subset E \subset F$ trois corps. On suppose que l'extension $K \subset F$ est galoisienne et que $[F : E] = 4$. Donner une condition suffisante sur l'extension $K \subset E$ pour qu'il existe un corps E' vérifiant $E \subsetneq E' \subsetneq F$.

4. Contrôle classant (2003)

Exercice 7.8. — **a)** Soit E un corps infini et soit $P \in E[X_1, \ldots, X_d]$ un polynôme non nul. Montrer par récurrence sur d qu'il existe $(x_1, \ldots, x_d) \in E^d$ tel que $P(x_1, \ldots, x_d) \neq 0$.

Soit A et B deux matrices de $M_n(E)$. On suppose qu'il existe une extension finie F de E telle que A et B soient semblables dans $M_n(F)$. Soit $(\alpha_1, \ldots, \alpha_d)$ une base de F comme E-espace vectoriel.

b) Montrer qu'il existe des matrices $P_1, \ldots, P_d \in M_n(E)$ telles que $P_i A = B P_i$ pour tout i et telles que $\det(\sum \alpha_i P_i) \neq 0$.

c) Montrer qu'il existe $x_1, \ldots, x_d \in E$ tels que la matrice $P = \sum_{i=1}^{d} x_i P_i$ soit inversible.

En déduire que A et B sont semblables dans $M_n(E)$.

Exercice 7.9. — **a)** Quels sont les conjugués de $\sqrt{2+\sqrt{5}}$ sur $\mathbf{Q}$?

b) Soit $K = \mathbf{Q}(\sqrt{2+\sqrt{5}})$. Quel est son degré sur $\mathbf{Q}$? Montrer que l'extension $\mathbf{Q} \subset K$ n'est pas galoisienne.

c) Soit $\mathbf{Q} \subset L$ sa clôture galoisienne dans $\mathbf{C}$. Calculer $[L : \mathbf{Q}]$.

Exercice 7.10. — Soit $p_1, \ldots, p_n$ des nombres premiers distincts. On note $K = \mathbf{Q}(\sqrt{p_1}, \ldots, \sqrt{p_n})$.

a) Montrer que l'extension $\mathbf{Q} \subset K$ est galoisienne.

b) Soit $\sigma \in \mathrm{Gal}(K/\mathbf{Q})$. Montrer qu'il existe pour tout i un élément $\varepsilon_i(\sigma) \in \{\pm 1\}$ tel que

$$\sigma(\sqrt{p_i}) = \varepsilon_i(\sigma)\sqrt{p_i}.$$

On note ε l'application $\mathrm{Gal}(K/Q) \to \{\pm 1\}^n$ telle que $\sigma \mapsto (\varepsilon_1(\sigma), \ldots, \varepsilon_n(\sigma))$. Montrer que c'est un homomorphisme de groupes.

c) Montrer que ε est injective.

d) Montrer que pour toute partie non vide $I \subset \{1; \ldots; n\}$, il existe $\sigma \in \mathrm{Gal}(K/\mathbf{Q})$ tel que $\prod_{i \in I} \varepsilon_i(\sigma) = -1$. En déduire que ε est surjective.

e) Que vaut $[K : \mathbf{Q}]$? Montrer en particulier que les réels $\sqrt{p_1}, \ldots, \sqrt{p_n}$ sont linéairement indépendants sur $\mathbf{Q}$.

Exercice 7.11. — Le but de cet exercice est de démontrer un théorème d'E. Artin et O. Schreier (1927) qui décrit les corps F dont une clôture algébrique Ω vérifie $[\Omega : F] < \infty$. En particulier, on va voir que nécessairement $[\Omega : F] = 2$.

Les parties 1 et 2 sont indépendantes. La partie 3 fait usage des résultats de la partie 2.

Partie 1. Corps réels clos

On dit qu'un corps K est réel clos s'il vérifie les trois propriétés :

a) -1 n'est pas un carré dans K ;
b) tout élément de K est ou un carré ou l'opposé d'un carré.
c) le corps $K(\sqrt{-1})$ est algébriquement clos.

a) Montrer que $\mathbf{R}$ est réel clos, ainsi que l'ensemble $\mathbf{R} \cap \overline{\mathbf{Q}}$ des nombres réels qui sont algébriques sur $\mathbf{Q}$.

b) Si K est un corps réel clos, montrer qu'un polynôme de degré impair a une racine dans K. Plus généralement, décrire les polynômes irréductibles à coefficients dans un corps réels clos.

c) Soit K un corps réel clos. Si a et b sont dans K, montrer que $a^2 + b^2$ est un carré dans K. En déduire que toute somme de carrés dans K est encore un carré.

d) Montrer qu'un corps réel clos est de caractéristique zéro. (Montrer que pour tout entier $n \geqslant 0$, $n1_K$ est un carré dans K.)

Partie 2. Préliminaires sur les extensions cycliques

Soit p un nombre premier. Soit $E \subset F$ une extension galoisienne de groupe $\mathbf{Z}/p\mathbf{Z}$. Soit σ un générateur de $\mathrm{Gal}(F/E)$.

a) Si $x \in F$, on pose

$$N(x) = x\sigma(x)\dots\sigma^{p-1}(x) \quad \text{et} \quad T(x) = x + \sigma(x) + \cdots + \sigma^{p-1}(x).$$

(*i*) Montrer que ce sont des éléments de E.

(*ii*) Montrer que pour $x,\ y \in F$, on a $N(xy) = N(x)N(y)$ et $T(x+y) = T(x) + T(y)$.

(*iii*) Montrer que pour $a \in E$ et $x \in F$, on a $N(ax) = a^n N(x)$ et $T(ax) = aT(x)$.

b) On suppose qu'il existe $\zeta \in E$, $\zeta \neq 1$, tel que $\zeta^p = 1$. Montrer qu'il existe $y \in F$ tel que $\sigma(y) = \zeta y$; en déduire que $y^p \in E$ et $F = E(y)$.

c) Justifier l'existence d'un élément $\theta \in F$ tel que $F = E[\theta]$. Montrer que le déterminant

$$\det \begin{pmatrix} 1 & \theta & \theta^2 & \dots & \theta^{p-1} \\ 1 & \sigma(\theta) & \sigma(\theta^2) & \dots & \sigma(\theta^{p-1}) \\ \vdots & & & \vdots & \\ 1 & \sigma^{n-1}(\theta) & \sigma^{p-1}(\theta^2) & \dots & \sigma^{p-1}(\theta^{p-1}) \end{pmatrix}$$

n'est pas nul.

d) Montrer que $T\colon F \to E$ est une application E-linéaire surjective. Montrer que pour $x \in F$, $T(x) = 0$ si et seulement s'il existe $y \in F$ tel que $x = \sigma(y) - y$.

e) On suppose que E est un corps de caractéristique p. Montrer qu'il existe $y \in F$ tel que $\sigma(y) = y + 1$. En déduire que $F = E(y)$ et que $y^p - y \in E$.

Partie 3. Théorème d'Artin–Schreier

Soit Ω un corps algébriquement clos et $F \subset \Omega$ un sous-corps, distinct de Ω, tel que $[\Omega : F] < \infty$. On notera i un élément de Ω de carré -1.

a) Montrer que l'extension $F \subset \Omega$ est galoisienne. (Si F est de caractéristique $p > 0$, on montrera d'abord que le corps F est parfait.)

Dans les questions 11 à 14 qui suivent, on suppose que $[\Omega : F]$ est un nombre premier p.

b) Quel est le groupe de Galois de l'extension $F \subset \Omega$?

c) (*i*) Si $z \in \Omega$, montrer que $T(z)^p - T(z) = T(z^p - z)$.

(*ii*) Montrer que tout élément de F est de la forme $x^p - x$ avec $x \in F$.

(*iii*) En déduire que F n'est pas de caractéristique p. (Utiliser la dernière question de la première partie.)

d) On suppose que p est impair. Montrer que F contient un élément $\zeta \neq 1$ tel que $\zeta^p = 1$. D'après la partie 1, question 2, il existe $y \in \Omega$ tel que $\Omega = F(y)$ et $y^p \in F$. Soit $z \in \Omega$ tel que $z^p = y$; montrer que $N(z)^p = y^p$ et obtenir une contradiction.

e) On a donc $p = 2$. Montrer que $\Omega = F(\mathrm{i})$ et que F est un corps réel clos.

f) (*Retour au cas général.*) Montrer que F est réel clos et que $[\Omega : F] = 2$.

Bibliographie

[1] E. ARTIN – *Galois theory*, second éd., Dover Publications Inc., 1998, Edited and with a supplemental chapter by Arthur N. Milgram.

[2] M. AUDIN – *Les systèmes hamiltoniens et leur intégrabilité*, Cours spécialisés, vol. 8, SMF, EDP Sciences, 2001.

[3] N. BOURBAKI – *Éléments d'histoire des mathématiques*, Masson, 1984.

[4] A. DAHAN & J. PEIFFER – *Une histoire des mathématiques. routes et dédales*, Points Seuil, 1985.

[5] N. HUNGERBÜHLER – « A short elementary proof of the Mohr-Mascheroni theorem », *Amer. Math. Monthly* **101** (1994), no. 8, p. 784–787.

[6] I. KAPLANSKY – *An introduction to differential algebra*, seconde éd., Publications de l'Institut de Mathématique de l'Université de Nancago, vol. 5, Hermann, Paris, 1976.

[7] S. LANG – *Algebra*, third éd., Graduate Texts in Mathematics, vol. 211, Springer-Verlag, New York, 2002.

[8] A. R. MAGID – *Lectures on differential Galois theory*, University Lecture Series, vol. 7, Amer. Math. Soc., 1994.

[9] PLATON – *La république*, GF, Flammarion, 1966, introduction, traduction et notes par R. Baccou.

[10] M. ROSENLICHT – « Integration in finite terms », *American Math. Monthly* **79** (1972), p. 963–972.

[11] W. RUDIN – *Real and complex analysis*, 3 éd., McGraw-Hill, 1987, Traduction française, Dunod, 1998.

[12] I. STEWART – *Galois theory*, seconde éd., Chapman and Hall Ltd., 1989.

[13] R. WILSON – *Stamping through mathematics*, Springer Verlag, 2001.

[14] ZACHARIE – *Traité du compas. Traité élémentaire de tous les traits servant aux Arts et Métiers et à la construction des Bâtiments*, 1833, disponible à l'adresse *http://melusine.eu.org/syracuse/metapost/compas.pdf*.

Index

Abel, Niels Hendryk, 75, 117
action, 78, 93, 96
  du groupe de Galois sur les racines d'un polynôme, 118, 135
  par conjugaison, 125
  transitive, 125
algèbre, **13**
  de type fini, **13**, 149, 150, 163
algorithme de Berlekamp, 72
algorithme de Risch, 157
anneau, **4**
  de valuation, 120
  des entiers de Gauß, **4**
  différentiel, **139**
  factoriel, **39**, 40, 49, 118, 121
  intègre, **5**
  noethérien, **48**
  principal, 37
  quotient, **40**
anneau de valuation, 136
Artin, Emil, 57
automorphisme de Frobenius, 123
bon ordre, **36**, 41
caractéristique, 99, 113, 115, 135, 141, 156
Cardan, Jérôme, 111
casus irreductibilis, 111, 167
Cauchy, Augustin-Louis, 77
centralisateur, **78**, 79
centre, **77**, **80**, 91, 95
classe de conjugaison, 123, 126
  d'une permutation, 85, 123
clôture galoisienne, 114, 115, 158
conjugué
  d'un élément dans un groupe, 85, 96, 123
  d'un nombre algébrique, 100, 136
  d'un sous-groupe, 120, 122, 123
conjugués, **11**
constante, **141**
contenu
  d'un polynôme, **40**
contenu d'un polynôme, 26
corps, **3**
  algébriquement clos, **33**, 46
  cyclotomique, 98
  des fractions, **5**
  des quaternions, **3**
  différentiel, **139**
  fini, 123
  homomorphisme de, **5**
  non-commutatif, **3**
  parfait, **53**
correspondance de Galois, 55
  différentielle, 156
critère d'Eisenstein, 26, 101
critère de Liouville, 24
cyclotomie, 98
décomposition en éléments simples, 160, 162
degré
  d'un élément, **11**
  d'un élément algébrique, 136
  d'une extension, **9**
  extensions de petit, 109, 113
dérivation, **139**
discriminant, 15, **20**, 63, 64, 109, 111
  d'un polynôme, 64, 74
division euclidienne, 7
élément
  algébrique, **10**
  inversible, **4**
  irréductible, **39**, 49
  primitif, 61, 62, 70, 117, 131, 155
  séparable, **52**
  transcendant, **10**, 159, 160
équation aux classes, 79
équation générale, 116
estimées de Cauchy, 42
exponentielle, 160
extension

algébrique, **10**
composée, 103, 114
cyclique, **106**, 115, 134
de corps, **8**
de décomposition, 46
de Picard-Vessiot, 148, 149, 151–154, 156
différentielle, **142**
élémentaire, **157**
finie, **9**
galoisienne, 55
homomorphisme, **31**
quadratique, **14**
radicale, **114**
radicale élémentaire, **114**
résoluble, **114**, 115
séparable, **52**
Fermat, Pierre de, 100
del Ferro, Scipione, 111
formule d'inversion de Möbius, 71
formule de Burnside, 95
formule de Leibniz, 139
formules de Cardan, 111, 112, 167
formules de Newton, 27
Galois, Évariste, 66
correspondance, 55
Gauss, 99, 102
et les polygones réguliers, 99, 102
groupe, **75**
commutatif, 75, 116, 122
cyclique, 102
nilpotent, **84**, 94
résoluble, **82**, 115
simple, **81**, 96
groupe abélien
cyclique, 27
fini, 27
groupe alterné, **87**
est simple, 96
groupe de Galois, 55, 98, 104, 106, 112, 155
différentiel, 151, 156
groupe de Klein, 108
groupe symétrique, **85**, 96
Hamilton, William Rowan, 3
Hermite, Charles, 21
Hilbert, David, 163, *voir* théorème des zéros
homomorphisme
d'anneaux, **4**
de corps, **5**
de groupes, **76**
idéal, **37**
différentiel, **142**, 150
premier, 49
principal, **37**
indicatrice d'Euler, 101
indice, 96
intégration, 157
isomorphisme, **5**
d'extensions, **31**
de groupes, **76**
Klein, Felix, 108
Lagrange, Joseph-Louis, 76
Leibniz, Gottfried Wilhelm von, 139
lemme d'Artin, 57, 118
lemme de Cauchy, 112
lemme de Gauss, 26, 39, 136
lemme de Rolle, 129
Liouville, Joseph, 157
logarithme, 159
morphisme, *voir* homomorphisme
nombre constructible à la règle et au compas, 97, 99, 102, 113, 136
nombre constructible à la règle et au compas, **1**, 14
nombre premier de Fermat, **100**
normalisateur, 58, 125
noyau, **76**
opération, 78
orbite, 78, 95
partition, 85
place d'un corps, **120**
point constructible à la règle et au compas, **1**
polynôme
cyclotomique, 98, 101
irréductible, **11**
minimal, **11**
séparable, **52**, 135, 150
polynôme symétrique, **18**, 27, 137
élémentaire, **18**, 27
produit semi-direct, 93
propriété universelle, 6, 7, 30
quaternions, 3, 4, 92
racine primitive de l'unité, 98, 99, 102, 107, 116, 134, 135
résoluble par radicaux, 123
résolvante, **65**, 112, 126
résolvante de Lagrange, 107, 109
résultant de deux polynômes, 74
Ruffini, Paolo, 116
signature d'une permutation, **86**
somme de Gauss, 71
sous-annea
engendré, **10**

sous-anneau, 4, 120, 136
  engendré, **10**
sous-corps, 156
  engendré, **4**, 10
sous-groupe, **76**
  de Sylow, 94, 113, 135
  dérivé, **80**
  distingué, **79**, 92
  engendré par une partie, **76**
sous-groupe de Sylow, 94
stabilisateur, 70, 78, 126
système de calcul formel, 66, 123, 124, 134, 157
théorème d'Abel sur l'équation générale, 116
théorème d'irréductibilité de Hilbert, 129, 130
théorème de Čebotarev, 126
théorème de Bézout, 38
théorème de Chevalley–Warning, 72
théorème de Dirichlet, 72
théorème de Frobenius, 126
théorème de Galois, 55, 58
théorème de Gauss
  sur l'irréductibilité des polynômes cyclotomiques, 101
théorème de Hilbert, 48
théorème de Krull, 149
théorème de Lagrange
  sur les polynômes symétriques, 70
théorème de Lie-Kolchin, 157
théorème de Liouville
  sur les fonctions entières bornées, 25
théorème de Liouville sur l'intégration, 157, 158
théorème de Mohr–Mascheroni, 2
théorème de Perron, 26
théorème de Pythagore, 2
théorème de Rouché, 25
théorème de Thalès, 2
théorème de Wantzel, 14, 15
théorème de Wedderburn, 95
théorème de Wilson, 46
théorème des zéros, 13, 27
théorème fondamental de l'algèbre, 135, 136
wronskien, **147**