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 *de quelques problèmes classiques. Nous verrons plus tard que la théorie de Galois fournit un critère définitif permettant de décider si une construction géométrique est réalisable à la règle et au compas, ou non.*

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 ;

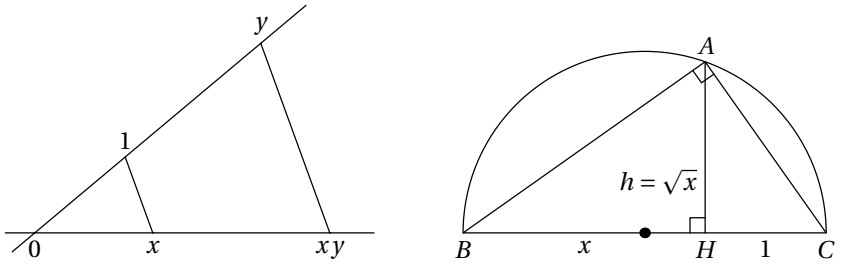
– il existe quatre points O, M, O' et $M' \in \Sigma_i$ tels que P_i soit l'un des (au plus) deux points d'intersection des cercles distincts respectivement de centre O et de rayon OM, et de centre O' et de rayon $O'M'$.

DÉFINITION 1.1.2. — *Considérons une partie* Σ *de* $\mathbf{R}$. *On dit qu'un nombre réel* x *est* 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. — La démonstration 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)

FIGURE 1. Constructions géométriques

Exercice 1.1.4. — Pour pouvoir utiliser effectivement ces constructions, on doit cependant être capable de construire des points hors de l'axe des abscisses. Vérifiez-le. Vérifiez aussi que vous savez construire la droite parallèle, ou perpendiculaire, à une droite donnée et passant par un point donné.

Dans la définition 1.1.1 d'un point constructible, les cercles sont de centre un point construit et passent par un autre point construit : la règle n'est pas graduée et le compas se referme dès qu'on l'enlève de la feuille. Expliquer comment construire le cercle de centre un point donné et de rayon la distance entre deux autres points.

Remarque 1.1.5. — 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 $\mathbf{Q}$.

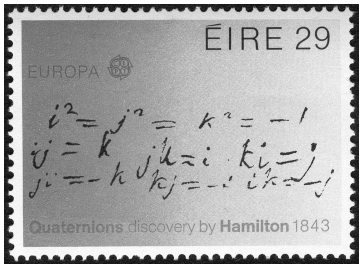
c) Si p est un nombre premier, l'ensemble $\mathbf{Z}/p\mathbf{Z}$ des entiers modulo p est un corps ; il est fini de cardinal p.

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 (non vide !) de $\mathbf{C}$, l'ensemble des fonctions méromorphes dans Ω est un 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.[(2)]

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, 1 est l'élément neutre pour la multiplication, les multiples réels de 1 commutent à tout élément, et telle que les relations : $\mathrm{i}^2 = \mathrm{j}^2 = \mathrm{k}^2 = -1$, $\mathrm{ij} = \mathrm{k}$ soient satisfaites. On en déduit facilement



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

(2) Un corps non commutatif peut très bien être commutatif ! La terminologie anglaise, *division algebra*, est meilleure ; on trouve aussi l'expression « corps gauche ».

d'autres identités. Par exemple, si l'on multiplie la relation $ij = k$ à gauche par i, on obtient $(-1)j = ik$, d'où $ik = -j$. C'est le corps des quaternions, découvert par Hamilton.

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.

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

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

où n est un entier, $P,Q \in \mathbf{Z}[X_1,\dots,X_n]$ 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 $x+iy$ 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*) Si A est un anneau dans lequel $0 = 1$, alors $A = \{0\}$ (anneau nul, d'intérêt limité).

b) Un corps est un anneau. Plus précisément, un corps est un anneau non nul dont tout élément autre que 0 soit inversible.

c) 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 nombres rationnels.

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. Nous verrons au paragraphe 2.4 quelques propriétés algébriques des anneaux de polynômes.

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 ; un *automorphisme* est un isomorphisme d'un anneau sur lui-même. L'image d'un homomorphisme d'anneaux $A\to B$ est un sous-anneau de B ; l'image d'un homomorphisme de corps $K\to L$ est un sous-corps de L.

DÉFINITION 1.2.9. — *Un anneau non nul A est dit* intègre *si pour tous a et $b\in A\setminus\{0\}$, $ab\neq 0$.*

Exercice 1.2.10. — 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 de cette construction est le même que celui qui permet d'obtenir le corps des nombres rationnels à partir de l'anneau des entiers relatifs. On définit l'ensemble K comme l'ensemble des classes d'équivalences dans 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 ; vous devrez utiliser l'hypothèse que A est intègre.) 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 $1 \times a = 0 \times 1$, d'où $a = 0$. Il n'y a donc pas de dommage à identifier un élément $a \in A$ et son image $i(a) \in K$. 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 $i(A)$.

Exemples 1.2.11. — *a*) 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.

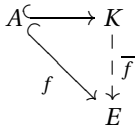
b) Si Ω est un ouvert connexe de $\mathbf{C}$, l'anneau des fonctions holomorphes sur Ω est intègre (cela résulte du principe des zéros isolés) et son corps des fractions est le corps des fonctions méromorphes sur cet ouvert. C'est un théorème d'analyse assez délicat qui repose sur la possibilité de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

Les corps des fractions possèdent une « propriété universelle » importante.

PROPOSITION 1.2.12. — *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 visuellement 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 ».

LEMME 1.2.13. — *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* $I = \{0\}$.

Démonstration. — Laissée au lecteur en exercice ! □

DÉFINITION 1.2.14. — *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* $\operatorname{Ker} f$.

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 *ne soit pas injectif. Si* A *est un anneau 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* $g : \mathbf{Q} \to A$.

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 à l'aide d'un raisonnement par récurrence analogue.

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 un anneau intègre et que f ne soit pas injective. Soit n le plus petit entier strictement positif tel que $f(n) = 0$. Puisque $f(1) = 1 \neq 0$, on a $n \geqslant 2$. 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. 1.2.12) en un homomorphisme de $\mathbf{Q}$ dans A. □

Remarque 1.2.16. — Soit K un corps de caractéristique p et $f : \mathbf{Z} \to K$ l'homomorphisme canonique introduit 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*.

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 $\varphi : A \to A$ définie par $\varphi(a) = a^p$ est un homomorphisme d'anneaux.

Démonstration. — La formule du binôme de Newton est valable dans tout anneau commutatif et s'écrit

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

Or, lorsque $1 \leqslant n \leqslant p - 1$, la formule $\binom{p}{n} = p!/n!(p - n)!$ entraîne que $n!(p - n)!\binom{p}{n} = p!$ est multiple de p. Comme p est un nombre premier et comme $1 \leqslant n \leqslant p - 1$, ni $n!$, ni $(p - n)!$ ne sont multiples de p. Par suite, $\binom{n}{p}$ est 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 $\varphi : K \to K$, $x \mapsto x^p$ est appelé* homomorphisme de Frobenius.

Lorsque l'homomorphisme de Frobenius est un automorphisme, on parle naturellement d'*automorphisme de Frobenius*

1.3. Extensions de corps

DÉFINITION 1.3.1. — *On appelle* extension de corps *un homomorphisme de corps* $j : E \to F$.

Remarquons qu'un tel homomorphisme j est toujours injectif : en effet, si $x \neq 0$, 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, on peut ainsi la plupart du temps penser à j comme à une inclusion.

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

On dit que l'extension $j : E \to F$ *est* 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 $j_1 : E \to F$ définie par $P(X) \mapsto P(Y)$ est de degré 1 (c'est un isomorphisme) alors que $j_2 : E \to F$ définie par $P(X) \mapsto P(Y^2)$ est de degré 2. Lorsque E est un sous-corps de F, ce qui est le cas le plus 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 s'ensuit 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 $x_1,\dots,x_m$ une base de F comme E-espace vectoriel et soit $y_1,\dots,y_n$ 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 $a_1,\dots,a_n \in F$. 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 $P(x) = 0$. Dans le cas contraire, on dit que x est* transcendant.

L'extension $E \to F$ est dite algébrique *si tout élément de F est algébrique sur E.*

L'usage veut qu'on dise qu'un nombre complexe est 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 $z = x + \mathrm{i}y$ 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 nombre réel $\sqrt{2}$ est algébrique sur $\mathbf{Q}$, ainsi que le nombre complexe $\sqrt{2} + \mathrm{i}\sqrt[3]{3} + \sqrt[5]{5}$. (*Exercice…*)

c) Le nombre 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. Comme l'ensemble des nombres réels n'est pas dénombrable, l'ensemble des nombres transcendants n'est pas dénombrable (Cantor, 1874).

e) Les nombres réels $e \approx 2{,}718\ldots$, $\pi \approx 3{,}14159$ sont transcendants (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 $E[X_1, \ldots, X_n]$. Le *sous-corps de F engendré par les x_i sur E*, noté $E(x_1, \ldots, x_n)$, en est 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 de corps et soit x un élément de F*

a) *Si x est transcendant sur E, φ_x est un injectif 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 $P(x) = 0$. De plus, P est irréductible,* $\dim_E E[x] = \deg P$ *et tout polynôme $Q \in E[X]$ tel que $Q(x) = 0$ est multiple de P.*

DÉFINITION 1.3.10. — *Ce polynôme P est appelé* polynôme minimal *de x sur E. Ses racines (y compris x) sont les* conjugués *de x. Son degré est appelé* degré *de x sur E.*

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. Un polynôme unitaire est un polynôme dont le coefficient du terme de plus haut degré est 1. Enfin, si $E \to F$ est une extension de corps, une *racine* dans F d'un polynôme $P \in E[X]$ est un élément $x \in F$ tel que $P(x) = 0$. Par division euclidienne, on peut alors écrire $P(X) = (X - x)Q(X)$, où Q est un polynôme dans $F[X]$. Par récurrence, on démontre ainsi qu'un polynôme n'a pas plus de racines dans F que son degré.

Démonstration. — a) Si x est transcendant, φ_x est injective par définition, donc définit un isomorphisme de $E[X]$ sur son image $E[x]$. 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 $P(x) = 0$, car deux polynômes unitaires qui se divisent l'un l'autre sont égaux.

Posons $d = \deg P$; l'argument que nous venons de faire montre que φ_x induit un homomorphisme injectif $\varphi_{x,d}$ de l'espace vectoriel $E[X]_{<d}$ (polynômes de degrés $< d$ à coefficients dans E) 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 encore.

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 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 $1,x,\dots,x^{m-1}$ et $1,y,\dots,y^{n-1}$ 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 $E[x,y]$. Ce sont par conséquent des E-espaces vectoriels de dimension finie et la proposition précédente permet 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 x est un élément non nul de F dont l'inverse 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 « empilée » $E \to E[x] \to F$. 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, l'extension « empilée » $E \to G$ 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 sur n, 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 $K[X_1, \ldots, X_n]$ en n variables $X_1, \ldots, X_n$ 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* (le terme allemand *Nullstellensatz* est souvent employé) 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 (dites aussi *extensions quadratiques*.) : elles sont obtenues par « adjonction d'une racine carrée ».

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 $\delta = 2ax + b$; alors, $\delta^2 = b^2 - 4ac \in E$ 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 une construction à la règle et au compas, ainsi que sur la résolution explicite des équations donnant les coordonnées de leurs points d'intersection.

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, si $M = (a, b)$, $M' = (a', b')$ et $O = (a'', b'')$ sont des points du plan dont les coordonnées sont dans K, le cercle de rayon MM' et de centre O 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 est un des points d'intersection d'une droite et d'un cercle, ses coordonnées (x, y) satisfont des 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. Son discriminant Δ appartient à K et x, puis y, appartiennent à l'extension $K(\sqrt{\Delta})$ qui est de degré au plus 2 sur K.

Si le point P est obtenu par une intersection cercle/cercle, on soustrait les deux équations de cercles, ce qui nous ramène au cas précédent cercle/droite. (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 nombre réel qui est constructible à la règle et au compas à partir de E. Alors, x est algébrique sur E et son degré est 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 $E \subset E[x] \subset E_n$, on voit que 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 (Duplication du cube). — *Le nombre 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 de montrer que $X^3 - 2$ est irréductible sur $\mathbf{Q}$, car cerla entraînera que le degré de α est

égal à 3. Si X^3-2 n'était pas irréductible, 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 qu'il l'est sur le corps $\mathbf{Q}(\cos(\alpha))$. En outre, si l'on suppose que $\cos(\alpha/3)$ est constructible sur le corps $\mathbf{Q}(\cos(\alpha))$, $\sin(\alpha/3)$ le sera aussi. Ainsi, *on peut trisecter l'angle α si et seulement si* $\cos(\alpha/3)$ *est constructible sur le 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 $\cos((\alpha+2\pi)/3)$ et $\cos((\alpha+4\pi)/3)$. 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 $\mathbf{Q}(\cos(\alpha))$; c'est alors le produit de deux polynômes de degrés 1 et 2 et toutes ses racines sont constructibles sur $\mathbf{Q}(\cos(\alpha))$. 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* $X^3-3X-2\cos(\alpha)$ *a une racine dans le corps* $\mathbf{Q}(\cos(\alpha))$.

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 $P=X^3-3X-1$ n'a pas de racine dans $\mathbf{Q}$. Considérons une éventuelle 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. Mais F. Lindemann a démontré en 1882 que π est transcendant (théorème 1.6.6). □

On a utilisé plusieurs fois le lemme suivant.

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 $a \in K$, on peut écrire $P = (X-a)Q$, où Q est un polynôme de degré 1 ou 2, donc P n'est pas irréductible.

Inversement, si P est réductible, écrivons $P = QR$, où Q et R sont des polynômes non constants à coefficients dans K. 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 $n! = n(n-1)\dots 2\cdot 1$.

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 $(T-X_1)\dots(T-X_n)$ (c'est un polynôme en T à coefficients dans l'anneau $A[X_1,\dots,X_n]$). Précisément, 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

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

Ils satisfont $N_1 = S_1$,

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

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

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

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

Démonstration. — Introduisons le polynôme $\Pi = (T - X_1)\ldots(T - X_n)$ et soit M sa matrice compagnon, c'est-à-dire la matrice carrée de taille n

$$\begin{pmatrix} 0 & & & (-1)^{n-1}S_n \\ 1 & 0 & & (-1)^{n-2}S_{n-1} \\ & \ddots & \ddots & \vdots \\ & & 0 & -S_2 \\ & & 1 & S_1 \end{pmatrix}$$

dont les coefficients appartiennent au sous-anneau $\mathbf{Z}[S_1, \ldots, S_n]$ de $\mathbf{Z}[X_1, \ldots, X_n]$. Le polynôme minimal et le polynôme caractéristique de M sont égaux à Π. Le polynôme Π est scindé dans le corps $\mathbf{Q}(X_1, \ldots, X_n)$, ses racines étant $X_1, \ldots, X_n$. Par suite, la matrice M est semblable à une matrice triangulaire supérieure dont les termes diagonaux sont $X_1, \ldots, X_n$. En particulier, N_p est la trace de M^p. Comme M est à coefficients dans l'anneau $\mathbf{Z}[S_1, \ldots, S_n]$, il en est de même de ses puissances, ainsi que de leurs traces. Cela montre l'existence du polynôme P_p. □

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

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

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

Démonstration. — On démontre l'existence de Q par récurrence sur le nombre de variables n, puis sur le degré de P. 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, ainsi qu'en degrés $< m$ si le nombre de variables est n. Soit P un polynôme symétrique de degré m en n variables. Le polynôme P_0 en $(n-1)$ variables défini par

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

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 $Q = Q_0 + Y_n Q_2$.

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, pour tout $\sigma \in \mathfrak{S}_n$,

$$\begin{aligned} D(X_{\sigma(1)},\dots,X_{\sigma(n)}) &= (-1)^{n(n-1)/2} \prod_{i\neq j} (X_{\sigma(i)} - X_{\sigma(j)}) \\ &= (-1)^{n(n-1)/2} \prod_{i\neq j} (X_i - X_j) \\ &= D(X_1,\dots,X_n), \end{aligned}$$

donc D est symétrique.

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*

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

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

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

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

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

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

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

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.*

Charles Hermite (1822–1901)

Démonstration. — Raisonnons par l'absurde. Si e n'est pas transcendant, il existe des entiers $a_0,\dots,a_n$ non tous nuls 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, mais nous le ferons tendre vers l'infini) et soit $f(x) = x^{p-1}(x-1)^p\dots(x-n)^p$. Posons

$$J_p = a_0 I(f;0) + a_1 I(f;1) + \cdots + a_n I(f;n).$$

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.

D'après le lemme 1.6.1, il existe un réel c tel que $\left|J_p\right| \leqslant c^p$ pour tout p.

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 vertu du lemme 1.6.2. 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 $j \geqslant p$; en outre,

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

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 $\left|J_p\right| \geqslant (p-1)!$.

Pour de tels nombres premiers, on obtient L l'inégalité $c^p \geqslant (p-1)!$, ce qui contredit 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 et soit c son coefficient dominant. Alors, pour tout $n \geqslant 0$,*

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

Démonstration. — Soit m le degré de f et notons A la matrice compagnon de polynôme minimal f/c. Les valeurs propres de A sont les racines de f, comptées avec multiplicités, donc celles de cA sont les $c\alpha$, où α parcourt les racines de f, avec multiplicités. Par suite, les valeurs propres de $c^n A^n$ sont les $c^n \alpha^n$, pour $f(\alpha) = 0$. Ainsi, $c^n \sum_{f(\alpha)=0} \alpha^n$ est la trace de $c^n A^n$. Par hypothèse, cA est une matrice à coefficients entiers, donc $c^n A^n$ aussi et sa trace est un nombre entier. Le lemme est donc démontré. □

PROPOSITION 1.6.5. — *Soit f un polynôme à coefficients entiers tel que $f(0) \neq 0$. Si la somme $\sum_{f(\alpha)=0} e^{\alpha}$ est un nombre entier, elle est égale à zéro.*

Démonstration. — Soit $N = \sum_{f(\alpha)=0} e^{\alpha}$ et supposons que N soit un entier distinct de 0. Notons c 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

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

La majoration de l'intégrale I dans le lemme 1.6.1 implique qu'il existe un réel $M > 0$ tel que l'on ait

$$|J_p| \leqslant M^p$$

De plus, toujours d'après le lemme 1.6.1, on a

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

Si $f(\alpha) = 0$, α est racine 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 il existe un nombre entier A_p tel que

$$c^{m-n} \sum_{f(\alpha)=0} g^{(n)}(\alpha) = p! A_p.$$

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 B_p tel que

$$\sum_n g^{(n)}(0) = (p-1)!f(0)^p + p!B_p.$$

Finalement,

$$J_p = (p-1)!f(0)^p N + p!(c^{p-m}A_p + NB_p)$$

et

$$\frac{c^{m-p}}{(p-1)!}J_p = c^{m-p}Nf(0)^p + p(A_p + c^{m-p}NB_p)$$

est un nombre entier. De plus, si le nombre premier p ne divise pas $cNf(0)$, il n'est pas multiple de p. Il est en particulier non nul, et par conséquent au moins égal à 1 en valeur absolue ! Cela entraîne la minoration

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

Puisque $cNf(0) \neq 0$, tout nombre premier assez grand vérifie cette dernière inégalité. Jointe à la majoration démontrée plus haut, cela implique

$$(p-1)!c^{1-p\deg f} \leqslant M^p,$$

ce qui contredit une nouvelle fois la formule de Stirling lorsque p tend vers l'infini. La proposition est donc démontrée. □

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

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

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

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 la multiplicité de la racine 0 dans F_0 et posons $F = NF_0/X^q$. Alors, F est un polynôme à coefficients entiers et $F(0) \neq 0$. De plus, on a

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

Comme 0 est racine de F_0, correspondant au choix $\varepsilon_j = 0$ pour tout j, on a $q \geqslant 1$, d'où une contradiction avec 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 algébrique et soit d son degré. Montrer qu'il existe un polynôme $P \in \mathbf{Z}[X]$ de degré d tel que $P(\alpha) = 0$ et $P'(\alpha) \neq 0$.

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

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

c) Montrer que le nombre réel

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

est transcendant (Liouville, 1844). Un nombre réel dont ont peut montrer de cette façon qu'il est transcendant est appelé *nombre de Liouville*. L'ensemble des nombres de Liouville est non dénombrable, mais est de mesure nulle dans $\mathbf{R}$. On sait aussi que e et π ne sont pas des nombres de Liouville.

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

a) Soit f et g des éléments de $\mathbf{C}(z)$ tels que $f' = fg'$. Montrer que f et g sont constants.

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

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

d) Si $f_1, \ldots, f_n$ sont des éléments non constants de $\mathbf{C}(z)$ dont les dérivées sont deux à deux distinctes. 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 les racines carrées $\sqrt{2}, \sqrt{3}, \sqrt{5}, \sqrt{7}, \ldots$ des nombres premiers sont linéairement indépendantes 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 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 dans $\mathbf{Q}[X]$ qui divise P dans $\mathbf{Q}[X]$. Montrer que Q est à coefficients entiers et que Q divise P dans $\mathbf{Z}[X]$.

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 est réductible dans $\mathbf{Q}[X]$.

a) Montrer à l'aide de la question a) de l'exercice précédent qu'il existe des 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 le plus petit sous-corps de $\mathbf{C}$ qui soit 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 que P est irréductible sur $\mathbf{Q}$. (Vous pouvez réduire modulo 2, ou bien observer que P a exactement une racine de valeur absolue strictement inférieure à 1.)

c) On cherche à écrire $P(X) = (X^2+aX+b)(X^2+cX+d)$, où a, b, c, d sont indéterminés. 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 x_1 et x_2 ne peuvent pas être tous deux constructibles à la règle et au compas. (Il résultera de l'exercice 5.4 qu'aucune des deux ne l'est.)

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

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

b) En déduire que tout polynôme symétrique de $\mathbf{Q}[X_1,\dots,X_n]$ s'écrit de manière unique comme un polynôme à coefficients rationnels en les sommes de Newton $N_1,\dots,N_n$.

c) Qu'en est-il dans un corps de caractéristique $p > 0$?

Exercice 1.15. — Soit $(G,+)$ un groupe abélien fini. On dit qu'un élément $g \in G$ est d'ordre d si d est le plus petit entier $\geqslant 1$ tel que $dg = 0$.

a) Soit g et h deux éléments de G d'ordres m et n. Si m et n sont premiers entre eux, montrer que $g+h$ 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 $h \in G$, $dh = 0$.

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 $j\colon K \to E$ une extension de corps et soit $x_1,\dots,x_n$ des éléments de E. Montrer l'équivalence des propriétés suivantes :

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

L'implication (c) ⇒ (d) nécessite le théorème des zéros de Hilbert (théorème 6.8.1).

Exercice 1.18. — On appelle degré, poids et degré partiel d'un monôme $X_1^{i_1}\dots X_n^{i_n}$ les expressions $i_1+\dots+i_n$, $i_1+2i_2+\dots+ni_n$ et $\max(i_1,\dots,i_n)$. 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 $S_1,\dots,S_n$.

b) Soit $P\in\mathbf{Z}[X_1,\dots,X_n]$ un polynôme symétrique. D'après le théorème 1.5.3, il existe un unique polynôme $Q\in\mathbf{Z}[Y_1,\dots,Y_n]$ tel que $P=Q(S_1,\dots,S_n)$. En revenant à la preuve par récurrence du théorème 1.5.3, démontrer que $\deg(P)=w(Q)$ et $\delta(P)=\deg(Q)$.