ALGÈBRE L3 S2

par

Laurent Berger

Table des matières

1. Anneaux

1.1. Anneaux. — Un anneau est un ensemble A, contenant 0 et 1, muni de deux lois $+$ et $\cdot$ telles que :

1. $(A, +)$ est un groupe abélien de neutre 0 ;
2. $a(bc) = (ab)c$ et $a \cdot 1 = 1 \cdot a = a$;
3. $a(b + c) = ab + ac$ et $(b + c)a = ba + ca$.

On a $0 \cdot x = 0$. En effet $0 \cdot x + x = (0 + 1) \cdot x = x$. Si $0 = 1$, alors $A = \{0\}$. Si $ab = ba$ pour tous a, $b \in A$, alors on dit que A est commutatif. À partir de maintenant, on ne considère (sauf mention explicite du contraire) que des anneaux commutatifs.

On dit que $x \in A$ est inversible (ou une unité) s'il existe $y \in A$ tel que $xy = 1$. On note $A^\times$ l'ensemble des unités de A. C'est un groupe pour la loi $\cdot$. Si $0 \neq 1$ et si tout $x \neq 0$ admet un inverse, alors on dit que A est un corps.

Un sous anneau B de A est un sous ensemble tel que B est un sous-groupe de A pour $+$ et tel que B contient 1 et est stable par $\cdot$. Un morphisme d'anneaux $f : A \to B$ est une application telle que f est un morphisme de groupes et $f(1_A) = 1_B$ et $f(xy) = f(x)f(y)$. Un morphisme bijectif d'anneaux est un isomorphisme d'anneaux.

On dit que a divise b s'il existe c tel que $b = ac$. On dit que $a \neq 0$ est un diviseur de zéro s'il existe $c \neq 0$ tel que $ac = 0$. Si $0 \neq 1$ et si $a \neq 0$ et $b \neq 0$ implique que $ab \neq 0$, alors on dit que A est un anneau intègre. On dit que $x \in A$ est irréductible si x n'est ni 0 ni une unité, et si dans toute écriture $x = ab$, a ou b est nécessairement une unité. On dit que $p \in A$ est premier si p n'est ni 0 ni une unité, et si quand p divise ab, p divise nécéssairement a ou b.

Proposition 1.1. — *Si A est intègre, alors un élément premier est irréductible.*

Démonstration. — Soit $p \in A$ premier. Si $p = ab$, alors p divise a ou b, disons a. On a donc $a = pc$ et $p = pbc$ ce qui fait que $p(1 - bc) = 0$. Comme A est intègre et que $p \neq 0$, $bc = 1$ et donc b est une unité. □

Dans $\mathbf{Z}$ ou dans $K[X]$ les éléments irréductibles coïncident avec les éléments premiers, mais en général, ce n'est pas le cas. Par exemple, dans $A = \mathbf{Z}[\sqrt{-5}]$, on a $2 \cdot 3 = (1 + \sqrt{-5}) \cdot (1 - \sqrt{-5})$ et les éléments 2, 3, $1 + \sqrt{-5}$ et $1 - \sqrt{-5}$ sont irréductibles mais pas premiers.

D'autres types d'éléments d'un anneau : nilpotents, idempotents...

1.2. Idéaux. — Rappelons qu'on ne travaille qu'avec des anneaux commutatifs. Un idéal de A est une partie I de A telle que $(I,+)$ est un sous-groupe de $(A,+)$ et $a \cdot i \in I$ pour tout $a \in A$ et $i \in I$. Par exemple, les sous-groupes de $\mathbf{Z}$ sont tous de la forme $n \cdot \mathbf{Z}$ et donc les idéaux de $\mathbf{Z}$ sont de la forme $n \cdot \mathbf{Z}$.

Si $f : A \to B$ est un morphisme d'anneaux, alors $\ker(f)$ est un idéal de A.

On dit qu'un idéal I de A est :

1. propre si $I \neq A$;
2. de type fini s'il existe $f_1, \ldots, f_r \in I$ tels que $I = \{\sum_{i=1}^r a_i f_i,\ a_i \in A\}$ (on écrit alors $I = (f_1, \ldots, f_r)$) ;
3. principal s'il existe $a \in I$ tel que $I = (a)$;
4. premier si I est propre et si $x \notin I$ et $y \notin I$ implique $xy \notin I$. Si $I = (a)$ avec $a \neq 0$, alors a est premier si et seulement si I est un idéal premier ;
5. maximal si I est un idéal propre et si $I \subset J \subset A$ implique que $J = I$ ou que $J = A$.

Si I et J sont deux idéaux de A, alors $I + J$, IJ et $I \cap J$ sont des idéaux de A.

Si I est un idéal de A, alors le quotient A/I est un anneau (on pose $\overline{a} + \overline{b} = \overline{a+b}$ et $\overline{a} \cdot \overline{b} = \overline{ab}$), et I est donc le noyau du morphisme d'anneaux surjectif $A \to A/I$. Par exemple, I est maximal si et seulement si A/I est un corps et I est premier si et seulement si A/I est intègre. En particulier, un idéal maximal est toujours premier. L'idéal nul est premier si et seulement si A est intègre, et il est maximal ssi A est un corps.

Dans un anneau intègre, deux éléments a et b engendrent le même idéal si et seulement s'il existe $u \in A^\times$ tel que $a = bu$.

Si A est un anneau, on a un morphisme $\mathbf{Z} \to A$ donné par $n \mapsto n \cdot 1_A$. Le noyau de ce morphisme est un idéal I de $\mathbf{Z}$ et donc de la forme $n \cdot \mathbf{Z}$. L'anneau A contient donc $\mathbf{Z}/n\mathbf{Z}$ comme sous-anneau, et $n \cdot a = 0$ pour tout $a \in A$. Si A est un anneau intègre, n est nécessairement nul ou un nombre premier p. On dit alors que A est de caractéristique nulle ou de caractéristique p. Si A est de caractéristique p, alors $x \mapsto x^p$ est un endomorphisme d'anneaux de A.

Si I et J sont deux idéaux de A, on dit que I et J sont premiers entre eux si $I + J = A$. Le résultat ci-dessous est connu sous le nom de lemme chinois (ou théorème des restes).

Théorème 1.2. — *Si $I_1, \ldots, I_n$ sont n idéaux de A qui sont premiers entre eux deux à deux, alors l'application $f : A/I_1 \cdots I_n \to A/I_1 \times \cdots \times A/I_n$ est un isomorphisme.*

Démonstration. — On montre par récurrence sur $1 \leq k \leq n-1$ que $I_n + I_1 \cdots I_k = A$ et donc que les idéaux I_n et $I_1 \cdots I_{n-1}$ sont premiers entre eux. Il suffit alors de montrer le

théorème pour $n = 2$, le cas général s'en déduisant par récurrence puisqu'alors :

$$A/I_1 \cdots I_n \simeq A/I_1 \cdots I_{n-1} \times A/I_n \simeq A/I_1 \times \cdots A/I_n.$$

Montrons donc que si I et J sont premiers entre eux, alors $f : A/IJ \to A/I \times A/J$ est un isomorphisme. Comme $I + J = A$, on peut écrire $1 = i + j$ avec $i \in I$ et $j \in J$. Si $x \in I \cap J$, alors $x = x(i + j) \in IJ$ et donc $I \cap J = IJ$, ce qui fait que f est injective. Enfin, on voit que si $x, y \in A$, alors $f(xj + yi) = (\overline{x}, \overline{y}) \in A/I \times A/J$ et donc f est surjective. □

1.3. Polynômes. — Si A est un anneau, on note $A[X]$ l'anneau des polynômes en X à coefficients dans A. On peut le définir comme l'anneau des suites presque nulles, muni du produit de convolution. Un polynôme a un degré ($\deg(0) = -\infty$ par convention), un coefficient dominant (polynômes unitaires), et un coefficient constant. Si $a \in A$, alors on a un morphisme d'évaluation $P(X) \mapsto P(a)$ de $A[X]$ dans A.

Remarque 1.3. — Si on n'impose plus la condition "presque nulle", on trouve l'anneau $A[[X]]$. On ne peut pas évaluer une série formelle en $a \in A$, sauf si a est nilpotent.

Proposition 1.4. — *Si A est un anneau intègre, alors $A[X]$ est intègre.*

Démonstration. — Si $P(X) = p_0 + p_1X + \cdots + p_mX^m$ et $Q(X) = q_0 + q_1X + \cdots + q_nX^n$ sont deux polynômes avec $p_m \neq 0$ et $q_n \neq 0$, alors le coefficient dominant de PQ est $p_mq_n \neq 0$ ce qui fait que $PQ \neq 0$. □

On dit que a est une racine de $P(X) \in A[X]$ si $P(a) = 0$. Dans ce cas, il existe $Q(X) \in A[X]$ tel que $P(X) = (X-a)Q(X)$. En effet, si l'on écrit $P(X) = P(a+(X-a)) = a_0 + a_1(X - a) + \cdots + a_d(X - a)^d$, alors $P(a) = 0$ ssi $a_0 = 0$ et la formule pour $Q(X)$ est alors évidente. On dit que P a une racine double en a si $(X - a)^2$ divise P.

Proposition 1.5. — *Le polynôme P a une racine double en a ssi $P(a) = P'(a) = 0$.*

Démonstration. — Si $P(X) = (X - a)^2Q(X)$, alors $P(a) = P'(a) = 0$. Réciproquement, on écrit $P(X) = a_0 + a_1(X - a) + \cdots + a_d(X - a)^d$ et $a_0 = P(a)$ et $a_1 = P'(a)$. □

Une racine a de P est de multiplicité m si $P(X) = (X - a)^mQ(X)$ avec $Q(a) \neq 0$.

Proposition 1.6. — *Si A est un anneau intègre et $P \in A[X]$, alors le nombre de racines de P (comptées avec multiplicités) est inférieur ou égal à* $\deg(P)$.

Démonstration. — Si a est une racine de multiplicité m, alors $P(X) = (X - a)^mQ(X)$ avec $\deg(Q) = \deg(P) - m$ et $Q(a) \neq 0$. Si $P(b) = 0$, alors $(b - a)^mQ(b) = 0$ ce qui

fait que, comme A est intègre, soit $a = b$ soit $Q(b) = 0$. Ceci permet de démontrer la proposition par récurrence sur le degré de P. □

Si A n'est pas intègre, alors la proposition 1.6 n'est pas nécessairement vraie. Par exemple, dans $A = \mathbf{Z}/8\mathbf{Z}$, le polynôme $P(X) = X^2 - 1$ a pour racines $X = 1$, 3, 5 et 7.

Proposition 1.7. — *Si A est un anneau intègre et si G est un sous-groupe fini de $A^\times$, alors G est cyclique.*

Démonstration. — Soit $m = \mathrm{card}(G)$, de sorte que $g^m = 1$ pour tout $g \in G$. Soit φ l'indicatrice d'Euler, définie par $\varphi(n) =$ le nombre d'éléments d'ordre n dans $\mathbf{Z}/n\mathbf{Z}$ et soit ψ définie par $\psi(n) =$ le nombre d'éléments d'ordre n dans G. Il suffit de montrer que $\psi(m) \neq 0$.

Si $n \geq 1$ est tel que $\psi(n) \neq 0$, c'est qu'il existe $g \in G$ d'ordre n. L'application $\overline{a} \mapsto g^a$ de $\mathbf{Z}/n\mathbf{Z} \to G$ est alors injective, et son image est composée d'éléments dont l'ordre divise n. Comme l'ordre d'un élément g divise n si et seulement si $g^n = 1$, il y a au plus n tels éléments (les racines de $X^n - 1$). Donc si $\psi(n) \neq 0$, alors ces éléments sont tous dans l'image de l'application ci-dessus et $\psi(d) = \varphi(d)$ pour tout $d \mid n$ ce qui fait que $\psi(n) = \varphi(n)$. Par suite, on a que pour tout n, on a soit $\psi(n) = 0$, soit $\psi(n) = \varphi(n)$. Enfin, $\sum_{d|m} \psi(d) = m = \sum_{d|m} \varphi(d)$ et on a donc forcément $\psi(d) = \varphi(d)$ pour tout d divisant m, et en particulier $\psi(m) = \varphi(m) \neq 0$. □

1.4. Corps des fractions. — Si K est un corps et si A est un sous-anneau de K, alors A est nécessairement intègre. Réciproquement, on a le résultat ci-dessous.

Théorème 1.8. — *Si A est un anneau intègre, alors il existe un corps K et un morphisme injectif $A \hookrightarrow K$.*

Démonstration. — Soit B l'ensemble $\{(x, y) \in A \times A \setminus \{0\}\}$ sur lequel on définit une relation d'équivalence par $(a, b) \sim (c, d)$ si et seulement si $ad - bc = 0$. On note K l'ensemble des classes d'équivalence et on munit K des lois $+$ et $\cdot$ définies par :

1. $\overline{(a, b)} + \overline{(c, d)} = \overline{(ad + bc, bd)}$;
2. $\overline{(a, b)} \cdot \overline{(c, d)} = \overline{(ac, bd)}$.

On vérifie que K est bien un anneau et comme $\overline{(a, b)} \cdot \overline{(b, a)} \sim \overline{(1, 1)}$, tout élément non nul est inversible et K est en fait un corps. Enfin, l'application $a \mapsto \overline{(a, 1)}$ de A dans K est injective puisque $(a, 1) \sim (0, 1)$ si et seulement si $a = 0$. □

Le corps construit ci-dessus s'appelle le corps des fractions de A, noté $\mathrm{Frac}(A)$. C'est le plus petit corps contenant A : si $x \in K$, alors il existe $b \in A \setminus \{0\}$ tel que $bx \in A$. On note a/b la classe de (a, b).

Si K est un corps, alors le corps des fractions de $K[X]$ est le corps $K(X)$ des fractions rationnelles à coefficients dans K.

1.5. Anneaux principaux et euclidiens. — On dit qu'un anneau A est principal s'il est intègre et si tout idéal I de A est principal. On dit que A est euclidien si A est intègre et s'il existe une application $N : A \setminus \{0\} \to \mathbf{N}$ (appelée stathme euclidien) telle que si $a \in A$ et $b \in A \setminus \{0\}$, alors il existe q, $r \in A$ vérifiant $a = qb + r$ avec soit $r = 0$, soit $N(r) < N(b)$.

Les exemples les plus importants sont $A = \mathbf{Z}$ avec $N(a) = |a|$ et $A = K[X]$ avec $N(P) = \deg(P)$.

Théorème 1.9. — *Si A est un anneau euclidien, alors A est principal.*

Démonstration. — Par définition, A est intègre. Si I est un idéal de A qui est différent de (0), alors $\{N(a),\ a \in I \setminus \{0\}\}$ est un sous-ensemble non vide de $\mathbf{N}$ et admet donc un plus petit élément, disons $N(b)$ avec $b \in I$.

Si $a \in I$, alors il existe q, $r \in A$ vérifiant $a = qb + r$ avec soit $r = 0$, soit $N(r) < N(b)$. Comme a, $b \in I$, on a $r \in I$ et donc $N(r) < N(b)$ n'est pas possible ce qui fait que $r = 0$ et donc que $a = bq$. On en déduit que $I = (b)$. □

Si A est un anneau principal, et si a, $b \in A$, alors l'idéal engendré par a et b est principal, engendré par un élément $d \in A$. On dit que d est « le » pgcd de a et b (bien sûr, d n'est bien défini qu'à une unité de A près). Le pgcd a la propriété suivante : $\mathrm{pgcd}(a, b)$ divise a et b, et si c divise a et b, alors c divise $\mathrm{pgcd}(a, b)$. Comme $d \in (a, b)$, il existe x et $y \in A$ tels que $ax + by = d$ (relation de Bezout).

Dans un anneau euclidien, on peut utiliser l'algorithme d'Euclide pour calculer le pgcd de deux éléments a et b. On pose $a_0 = a$ et $a_1 = b$ et pour $i \geq 1$, on définit a_{i+1} comme étant le reste d'une division euclidienne de a_{i-1} par a_i. Comme la suite des $N(a_i)$ est strictement décroissante, il existe i_0 tel que $a_{i_0} \neq 0$ et $a_{i_0+1} = 0$ et on a alors $a_{i_0} = \mathrm{pgcd}(a, b)$. En effet, si c divise a et b alors c divise a_i pour tout i et donc a_{i_0}. Si $d = a_{i_0}$, alors d divise a_{i_0} et a_{i_0-1} et donc d divise a_i pour tout i.

Rappelons que dans un anneau intègre, les éléments premiers sont irréductibles. Dans un anneau principal, les éléments irréductibles sont aussi premiers.

Proposition 1.10. — *Si A est principal et si $x \in A$ est irréductible, alors x est premier.*

Démonstration. — Supposons que $x \mid ab$, c'est-à-dire que $ab = xy$. On va montrer que $x \mid a$ ou que $x \mid b$. Considérons l'idéal (b, x) ; il est principal, engendré par un élément c. On a $x \in (c)$ et donc on peut écrire $x = cz$. Comme x est irréductible, soit c est une unité, soit z est une unité.

Si z est une unité, alors $(b, x) = (x)$ et donc il existe $d \in A$ tel que $b = xd$ et donc $x \mid b$.

Si c est une unité, alors $(b, x) = A$ et en particulier, il existe $d, e \in A$ tels que $bd+xe = 1$. On a alors $abd + axe = a$ et donc $xyd + xae = a$ ce qui fait que $x(yd + ae) = a$ et que $x \mid a$. □

1.6. Anneaux factoriels. — Dans $\mathbf{Z}$ ou dans $K[X]$, on a une décomposition en produit de nombres premiers ou en produit de polynômes irréductibles. Nous allons généraliser cette notion.

On dit qu'un anneau A est factoriel si A est intègre et si tout élément a une factorisation unique en produit d'irréductibles, ce qui veut dire que si $a \in A \setminus \{0\}$ n'est pas une unité, alors il existe $p_1, \ldots, p_r$ irréductibles tels que $a = p_1 \cdots p_r$ et que si l'on a aussi $a = q_1 \cdots q_s$ alors $r = s$ et quitte à permuter les q_i on a $p_i = q_i u_i$ avec u_i unité de A.

Théorème 1.11. — *Si A est un anneau principal, alors A est factoriel.*

Démonstration. — Commençons par montrer que tout élément admet une décomposition. Si ce n'est pas le cas, soit $a \in A$ un élément qui n'en admet pas. On peut alors écrire $a = a_1 b_1$ où ni a_1 ni b_1 ne sont des unités et où soit a_1 soit b_1 n'admet pas de décomposition, disons a_1. On peut alors itérer ce procédé : $a = a_1 b_1$, $a_1 = a_2 b_2$ …où chaque a_i divise a_{i-1} strictement et n'admet pas de décomposition. On a alors $(a_1) \subset (a_2) \subset \cdots$. L'idéal $I = \cup_{i \geq 1}(a_i)$ est principal, disons $I = (f)$ et il existe alors un indice i tel que $f \in (a_i)$ ce qui fait que $(a_i) = (a_{i+1}) = \cdots$, ce qui est une contradiction.

Montrons maintenant l'unicité de la décomposition. Si $a = p_1 \cdots p_r = q_1 \cdots q_s$, alors p_1 est irréductible et donc premier par la proposition 1.10 ce qui fait que (quitte à permuter les q_i) on a $p_1 \mid q_1$. Comme q_1 est irréductible, cela implique que $p_1 = u_1 q_1$ avec $u_1 \in A^\times$ et donc $u_1 p_2 \cdots p_r = q_2 \cdots q_s$. Ceci permet de montrer $r = s$ et l'unicité par récurrence. □

Proposition 1.12. — *Si A est factoriel et si $x \in A$ est irréductible, alors x est premier.*

Démonstration. — Si x divise ab, alors écrivons $ab = xc$ et $a = p_1 \cdots p_r$ et $b = q_1 \cdots q_s$ et $c = \ell_1 \cdots \ell_t$. On a $x\ell_1 \cdots \ell_t = p_1 \cdots p_r q_1 \cdots q_s$ et donc x est l'un des p_i ou q_j à une unité près, ce qui fait que x divise a ou b. □

Tout élément de A peut donc s'écrire sous la forme $a = p_1^{e_1} \cdots p_r^{e_r} u$ où les p_i sont premiers, $e_i \geq 1$, p_i ne divise pas p_j si $i \neq j$, et $u \in A^\times$.

Au §1.5, on a défini le pgcd de deux éléments d'un anneau principal. On peut étendre cette définition aux anneaux factoriels. Si a et $b \in A$, écrivons $a = p_1^{e_1} \cdots p_r^{e_r} u$ et $b = p_1^{f_1} \cdots p_r^{f_r} v$. On pose alors $\mathrm{pgcd}(a,b) = p_1^{\min(e_1,f_1)} \cdots p_r^{\min(e_r,f_r)}$. Le pgcd a la propriété suivante : $\mathrm{pgcd}(a,b)$ divise a et b, et si d divise a et b, alors d divise $\mathrm{pgcd}(a,b)$.

Si A est principal, la définition correspond à celle du §1.5. En général, on a $(a,b) \subset (\mathrm{pgcd}(a,b))$ mais on n'a pas toujours égalité. Si $A = K[X,Y]$ (dont on va voir qu'il est factoriel si K est un corps), alors $\mathrm{pgcd}(X,Y) = 1$ bien que $(X,Y) \neq A$.

On définit aussi le ppcm de a et b par $\mathrm{ppcm}(a,b) = p_1^{\max(e_1,f_1)} \cdots p_r^{\max(e_r,f_r)}$.

1.7. Polynômes à coefficients dans un anneau factoriel. — On suppose désormais que A est factoriel. Si $P(X) = a_0 + a_1 X + \cdots + a_d X^d \in A[X]$, alors on définit son contenu $\mathrm{cont}(P) = \mathrm{pgcd}(a_0, \ldots, a_d)$ (il est donc défini à une unité de A près). On dit que P est primitif si $\mathrm{cont}(P) = 1$. Le résultat ci-dessous est connu sous le nom de lemme de Gauss.

Théorème 1.13. — *Si P et $Q \in A[X]$, alors* $\mathrm{cont}(PQ) = \mathrm{cont}(P)\,\mathrm{cont}(Q)$.

Démonstration. — En divisant P par $\mathrm{cont}(P)$ et Q par $\mathrm{cont}(Q)$, on se ramène à montrer que si P et Q sont primitifs, alors PQ l'est aussi. Si p est un élément premier de A, alors l'anneau A/pA est intègre et $\overline{P}$, $\overline{Q} \in A/pA[X]$ sont $\neq 0$. Comme $A/pA[X]$ est lui-même intègre, on a $\overline{PQ} \neq 0$ et donc p ne divise pas $\mathrm{cont}(PQ)$. Ceci étant vrai pour tout p premier, on a bien $\mathrm{cont}(PQ) = 1$. □

Corollaire 1.14. — *Soit A un anneau factoriel et K son corps des fractions. Si P et $Q \in K[X]$ sont unitaires et $PQ \in A[X]$, alors $P, Q \in A[X]$.*

Démonstration. — Il existe a et $b \in A$ tels que aP et bQ sont à coefficients dans A, et primitifs (si $aP \in A[X]$ et si $d = \mathrm{cont}(aP)$, alors d divise a comme P est unitaire et on peut alors remplacer a par a/d). On a alors $\mathrm{cont}(ab \cdot PQ) = ab = \mathrm{cont}(aP)\,\mathrm{cont}(bQ) = 1$ et donc a et b sont des unités. □

Théorème 1.15. — *Si A est un anneau factoriel, et K son corps des fractions, alors $A[X]$ est factoriel et les irréductibles de $A[X]$ sont ceux de A ainsi que les polynômes primitifs de $A[X]$ qui sont irréductibles dans $K[X]$.*

Démonstration. — Les irréductibles de A le restent dans $A[X]$. Ensuite, si $P \in A[X]$ est un polynôme primitif qui est irréductible dans $K[X]$, et si on a $P = P_1 P_2$ dans $A[X]$, alors l'un des P_i appartient nécessairement à $K \cap A[X] = A$ et en regardant les contenus, on voit que ce P_i est forcément une unité de A ce qui fait que P est un irréductible de $A[X]$. Ces éléments sont donc des irréductibles de $A[X]$.

Montrons l'existence de la décomposition. L'anneau $K[X]$ est principal, et donc factoriel. Par ailleurs, tout polynôme de $K[X]$ peut être multiplié par un élément de $K^\times$ pour le rendre à coefficients dans A et primitif. Si $P(X) \in A[X]$, on peut donc le factoriser en $P(X) = (a/b) \cdot P_1(X) \cdots P_r(X)$ où a, $b \in A$ et $P_i(X) \in A[X]$ est irréductible dans $K[X]$ et primitif. En regardant les contenus, on voit que $b \cdot \mathrm{cont}(P) = a$ et donc que $P(X) = \mathrm{cont}(P) \cdot P_1(X) \cdots P_r(X)$. Ceci montre l'existence de la décomposition en produit d'irréductibles dans $A[X]$. On en déduit aussi qu'il n'y a pas d'autres irréductibles dans $A[X]$ que ceux de A et les polynômes primitifs qui sont irréductibles dans $K[X]$.

Enfin, il reste à vérifier l'unicité de la décomposition. Si $P(X) \in A[X]$ s'écrit $P(X) = a_1 \cdots a_r \cdot P_1(X) \cdots P_s(X)$, alors $a_1 \cdots a_r$ est une décomposition de $\mathrm{cont}(P)$ et est donc unique aux unités près. Enfin, $P_1(X) \cdots P_s(X)$ est une décomposition de $P/\mathrm{cont}(P)$ dans $K[X]$ et est donc unique à multiplication par des éléments de $K^\times$ près. L'hypothèse que $P_i(X)$ est primitif implique que $P_i(X)$ est bien déterminé à une unité de A près. □

En appliquant n fois le théorème 1.15, on trouve que si K est un corps, alors l'anneau $K[X_1, \ldots, X_n]$ est factoriel : tout polynôme à n variables s'écrit de manière unique comme produit de polynômes irréductibles.

Il n'est en général pas facile de déterminer les irréductibles de $K[X]$. On a par exemple le critère d'Eisenstein. Soit A un anneau factoriel et p un élément premier de A. On dit qu'un polynôme $Q(X) \in A[X]$ est d'Eisenstein si $Q(X) = X^d + q_{d-1}X^{d-1} + \cdots + q_0$ où les q_i sont tous divisibles par p et q_0 n'est pas divisible par p^2.

Proposition 1.16. — *Si A est factoriel, et $K = \mathrm{Frac}(A)$, et $Q(X) \in A[X]$ est d'Eisenstein, alors il est irréductible dans $K[X]$.*

Démonstration. — Comme Q est primitif, il suffit (par le théorème 1.15) de montrer que Q est irréductible dans $A[X]$. Supposons que $Q(X) = B(X)C(X)$.

On a un morphisme d'anneaux $A[X] \to A/pA[X]$ et A/pA est un anneau intègre. On a $\overline{B}(X)\overline{C}(X) = \overline{Q}(X) = X^d$ et donc $\overline{B}(X) = b_k X^k$ et $\overline{C}(X) = c_\ell X^\ell$ avec $k + \ell = d$. Si k, $\ell \geq 1$, alors p divise $B(0)$ et $C(0)$ et donc p^2 divise q_0. On en déduit que l'un de $\overline{B}$ et $\overline{C}$ est de degré d, et donc de même pour B ou C. □

1.8. Anneaux noethériens. — Rappelons qu'un idéal I est de type fini s'il existe $f_1, \ldots, f_r \in I$ tels que $I = \{\sum_{i=1}^r a_i f_i,\ a_i \in A\}$ (on écrit alors $I = (f_1, \ldots, f_r)$).

On dit qu'un anneau A est noethérien (d'après Emmy Noether) si tout idéal de A est de type fini. Par exemple, un anneau principal est noethérien (tout idéal étant engendré par un seul élément). En revanche, il existe des anneaux factoriels non noethériens.

Théorème 1.17. — *Un anneau A est noethérien si et seulement si toute suite croissante $I_1 \subset I_2 \subset \cdots$ d'idéaux de A est stationnaire (constante après un certain rang).*

Démonstration. — Si A est noethérien et si $I_1 \subset I_2 \subset \cdots$ est une telle suite, alors $I = \cup_{k \geq 1} I_k$ est un idéal de A, et donc de type fini, engendré par $f_1, \ldots, f_r \in I$. Il existe alors $n \gg 0$ tel que $f_i \in I_n$ pour tout i, ce qui fait que $I_n = I_{n+1} = \cdots = I$.

Réciproquement, montrons que la condition sur les suites implique que tout idéal de A est de type fini. Soit I un idéal de A dont on suppose qu'il n'est pas de type fini. On peut choisir $f_1 \in I$ et poser $I_1 = (f_1)$. On a $I \neq I_1$ car I n'est pas de type fini. Il existe donc $f_2 \in I \setminus I_1$ et on pose $I_2 = (I_1, f_2)$. Par récurrence, on construit une suite strictement croissante $I_1 \subset I_2 \subset \cdots$, contradiction. □

Si A est un anneau noethérien, alors A admet un idéal maximal (sinon, on trouverait une suite strictement croissante d'idéaux). Ce résultat reste vrai si l'on ne suppose plus A noethérien, mais il faut alors utiliser l'axiome du choix.

Nous verrons ci-dessous que les anneaux de polynômes $K[X_1, \ldots, X_n]$ sont noethériens. Soit $A = C^0(\mathbf{R}, \mathbf{R})$ et I l'idéal des fonctions qui s'annulent sur un voisinage de 0. Cet idéal n'est pas de type fini. Un autre exemple est l'anneau des polynômes en une infinité de variables (si A est un anneau et I est un ensemble, $A[X_i]_{i \in I}$ est l'anneau des suites presque nulles $a = (a_{\underline{n}})$ où $\underline{n} = (n_i)_{i \in I}$ avec $n_i \in \mathbf{Z}_{\geq 0}$. On pose $(a+b)_{\underline{n}} = a_{\underline{n}} + b_{\underline{n}}$ et $(ab)_{\underline{n}} = \sum_{\underline{j}+\underline{k}=\underline{n}} a_{\underline{j}} b_{\underline{k}}$. Cet anneau est factoriel si A l'est.).

Le résultat ci-dessous est connu sous le nom de théorème de la base de Hilbert.

Théorème 1.18. — *Si A est un anneau noethérien, alors $A[X]$ est noethérien.*

Démonstration. — Soit I un idéal de $A[X]$ et I_k l'ensemble des $a_k \in A$ tels qu'il existe $P(X) \in I$ de degré k de coefficient dominant a_k, auquel on rajoute 0. L'ensemble I_k est un idéal de A et de plus $I_0 \subset I_1 \subset \cdots$. Comme A est noethérien, il existe n tel que $I_n = I_{n+1} = \cdots$. Chaque I_j est de type fini, disons que I_j est engendré par des $a_{i,j} \in A$ avec $1 \leq i \leq n_j$. Soit $P_{i,j} \in I$ un polynôme de degré j et de coefficient dominant $a_{i,j}$.

Montrons que I est engendré par les $P_{i,j}$. Si $P \in I$ est un polynôme de degré d et si $d \geq n$, alors les $a_{i,n}$ engendrent $I_n = I_d$ et donc il existe des $\lambda_{i,n} \in A$ tels que $\mathrm{dom}(P) = \sum \lambda_{i,n} a_{i,n}$ ce qui fait que $P - \sum \lambda_{i,n} X^{d-n} P_{i,n}$ est de degré $\leq d-1$ et appartient à I. En itérant, on se ramène à montrer que si $P \in I$ est un polynôme de degré $d \leq n$, alors P est combinaison linéaire des $P_{i,j}$. Le coefficient dominant de P est combinaison A-linéaire des $a_{i,d}$ et donc il existe des $\lambda_{i,d} \in A$ tels que $P - \sum \lambda_{i,d} P_{i,d}$ est de degré $\leq d-1$ et appartient à I, ce qui permet de finir la démonstration. □

On peut aussi montrer que si A est noethérien, alors $A[[X]]$ est noethérien.

1.9. Le lemme de Zorn. — Dans la suite, nous avons besoin du lemme de Zorn. Commençons par quelques rappels sur l'axiome du choix. L'axiome du choix dit que si I est un ensemble et si $\{E_i\}_{i\in I}$ est une collection d'ensembles non vides, alors le produit $\prod_{i\in I} E_i$ est non-vide, c'est-à-dire que l'on peut choisir une suite $\{x_i\}_{i\in I}$ telle que $x_i \in E_i$. Cela a l'air évident, mais c'est un axiome, c'est-à-dire que c'est une proposition logiquement indépendante des autres axiomes de la théorie des ensembles, comme le postulat d'Euclide est un axiome de la géométrie.

Plutôt que l'axiome du choix, on utilise généralement un énoncé qui en résulte, le lemme de Zorn. Soit E un ensemble ordonné, c'est-à-dire un ensemble muni d'une relation $\leq$ telle que :

1. $x \leq x$ pour tout x ;
2. si $x \leq y$ et $y \leq z$, alors $x \leq z$;
3. si $x \leq y$ et $y \leq x$, alors $x = y$.

On ne demande pas de pouvoir comparer tous les éléments de E. On dit qu'une partie P de E est totalement ordonnée si pour tous x, $y \in P$ on a $x \leq y$ ou $y \leq x$. Si P est une partie de E, alors un majorant de P est un élément $y \in E$ tel que $p \leq y$ pour tout $p \in P$. On dit que l'ensemble ordonné E est inductif si toute partie non vide totalement ordonnée admet un majorant. Enfin, un élément maximal m de E est un élément de E tel que si $x \in E$ vérifie $x \geq m$, alors $x = m$.

Le lemme de Zorn est l'énoncé suivant : tout ensemble ordonné inductif non vide admet un élément maximal. L'axiome du choix implique le lemme de Zorn mais la démonstration n'est pas très éclairante (elle se trouve par exemple dans Lang). Voici deux exemples typiques d'application du lemme de Zorn.

Proposition 1.19. — *Tout espace vectoriel V non nul admet une base.*

Démonstration. — Soit E l'ensemble des familles libres d'éléments de V, ordonné par l'inclusion. C'est un ensemble ordonné inductif : si $\{F_i\}_{i\in I}$ est un ensemble totalement ordonné de familles libres de E, alors $\cup_{i\in I} F_i$ est libre et est donc un majorant des F_i.

Il existe donc une famille F maximale pour l'inclusion. Soit W le sous-espace de V engendré par F. Si $W \neq V$, alors on pourrait rajouter à F un élément de $V \setminus W$ ce qui contredirait la maximalité de F. □

Proposition 1.20. — *Tout anneau non nul A admet un idéal maximal.*

Démonstration. — Soit E l'ensemble des idéaux propres de A. C'est un ensemble ordonné par la relation $I \leq J$ si et seulement si $I \subset J$. Si P est une partie totalement ordonnée de E, alors $\cup_{I \in P} I$ est un idéal de A qui contient tous les idéaux de P, qui est propre (1 n'appartient à aucun des idéaux $I \in P$ et donc à leur union non plus) et qui est donc un majorant de P. L'ensemble des idéaux propres de A est donc un ensemble ordonné inductif, et par le lemme de Zorn, il admet un élément maximal qui est alors un idéal maximal de A. □

2. Corps

2.1. Éléments algébriques. — Soit K un corps et F un sous-corps de K. On dit que K est une extension de F. Le corps K est un F-espace vectoriel, et on dit que K/F est une extension finie ou infinie selon que $\dim_F K$ est finie ou infinie. On note $[K : F] = \dim_F K$, c'est le degré de l'extension K/F.

Proposition 2.1. — *Si $E \subset F \subset K$, alors $[K : E] = [K : F] \cdot [F : E]$. Si $\{f_i\}_{i \in I}$ est une base de F comme E-espace vectoriel, et si $\{k_j\}_{j \in J}$ est une base de K comme F-espace vectoriel, alors $\{f_i \cdot k_j\}_{i,j \in I \times J}$ est une base de K comme E-espace vectoriel.*

Démonstration. — La deuxième assertion implique la première. Montrons que $\{f_i \cdot k_j\}_{i,j \in I \times J}$ engendre K sur E. Si $x \in K$, on peut écrire $x = \sum_j y_j k_j$ avec $y_j \in F$ et $y_j = \sum_i z_{i,j} f_i$ avec $z_{i,j} \in E$, ce qui fait que $x = \sum_{i,j} z_{i,j} f_i k_j$. Montrons que $\{f_i \cdot k_j\}_{i,j \in I \times J}$ est linéairement indépendante sur E. Si $\sum_{i,j} x_{i,j} f_i k_j = 0$, alors $\sum_j (\sum_i x_{i,j} f_i) k_j = 0$ et donc (comme $\{k_j\}_{j \in J}$ est une base de K sur F) on a $\sum_i x_{i,j} f_i = 0$ pour tout j. Comme $\{f_i\}_{i \in I}$ est une base de F sur E, on trouve que $x_{i,j} = 0$ pour tous i, j. □

Soit K une extension de F. Si $\alpha \in K$, on a $F[\alpha]$ et $F(\alpha)$. On dit que $\alpha \in K$ est algébrique sur F s'il existe un polynôme non nul $P(X) \in F[X]$ tel que $P(\alpha) = 0$.

Proposition 2.2. — *Si $\alpha \in K$, alors les propriétés suivantes sont équivalentes :*

1. *α est algébrique sur F ;*
2. *$F[\alpha]$ est de dimension finie sur F ;*
3. *$F[\alpha] = F(\alpha)$.*

Démonstration. — Montrons que (1) implique (2) ; si α est annulé par $P(X)$, alors $F[\alpha]$ est un quotient de $F[X]/P(X)$ et est donc de dimension finie sur F.

Montrons que (2) implique (3) ; si $\beta \in F[\alpha]$ est non nul, alors la multiplication par β est un endomorphisme injectif de $F[\alpha]$ qui est alors surjectif comme on est en dimension finie, ce qui fait que tout élément non nul de $F[\alpha]$ a un inverse et que $F[\alpha]$ est un corps.

Montrons que (3) implique (1) ; on a $1/\alpha \in F[\alpha]$ et il existe donc $R(X)$ tel que $1/\alpha = R(\alpha)$ ce qui fait que α est annulé par le polynôme $P(X) = XR(X) - 1$. □

Si α est algébrique sur F, alors $I_\alpha = \{P(X) \in F[X] \text{ tels que } P(\alpha) = 0\}$ est un idéal de $F[X]$ dont on note $P_{\min,\alpha}$ le générateur unitaire, c'est le polynôme minimal de α. Ce polynôme est irréductible sur F (mais pas nécessairement à racines simples).

Lemme 2.3. — *On a* $\dim_F(F[\alpha]) = \deg(P_{\min,\alpha})$.

Le degré de α est alors défini par $\deg(\alpha) = \dim_F(F[\alpha]) = \deg(P_{\min,\alpha})$.

Proposition 2.4. — *L'ensemble des éléments de K qui sont algébriques sur F est un sous-corps de K.*

Démonstration. — Si $\alpha, \beta \in K$ sont algébriques sur F, alors $F[\alpha, \beta]$ est engendré par les $\alpha^i\beta^j$ avec $0 \leq i \leq \deg(\alpha) - 1$ et $0 \leq j \leq \deg(\beta) - 1$, et est donc un F-espace vectoriel de dimension finie. On déduit alors de la proposition 2.2 que $\alpha \pm \beta$ et $\alpha\beta$ sont algébriques. Enfin si $\beta \neq 0$, alors $1/\beta \in F[\beta]$. □

Remarque 2.5. — Si α n'est pas algébrique sur F, alors $F[X] \to K$ donné par $P(X) \mapsto P(\alpha)$ est injectif et se prolonge donc en $F(X) \to K$, dont l'image est $F(\alpha)$.

Si K/F est une extension de corps et si E_1 et E_2 sont deux sous-extensions de K/F, alors le compositum $E_1 \cdot E_2$ est le sous-corps de K engendré par E_1 et E_2.

Proposition 2.6. — *Si E_1 et E_2 sont deux sous-extensions finies de K/F, alors le compositum $E_1 \cdot E_2$ est une extension finie de F. On a* $[E_1E_2 : F] \leq [E_1 : F] \cdot [E_2 : F]$

Démonstration. — Soit A l'anneau engendré par E_1 et E_2. La proposition 2.4 montre que tout $\alpha \neq 0 \in A$ est algébrique sur F, et donc inversible dans $F[\alpha] \subset A$. On en déduit que $A = E_1 \cdot E_2$. Si $E_1 = \oplus_i F \cdot b_i$ et $E_2 = \oplus_j F \cdot c_j$, alors A est engendré par les $b_i \cdot c_j$ et est donc un F-espace vectoriel de dimension inférieure ou égale à $[E_1 : F] \cdot [E_2 : F]$. □

Notons que l'on a une tour $F \subset E_i \subset E_1E_2$ et donc que $[E_i : F]$ divise $[E_1E_2 : F]$. Si $[E_1 : F]$ et $[E_2 : F]$ sont premiers entre eux, on a donc $[E_1E_2 : F] = [E_1 : F] \cdot [E_2 : F]$.

2.2. Clôture algébrique. — Revenons à une extension de corps K/F. On dit que l'extension K/F est algébrique si tout $\alpha \in K$ est algébrique sur F. La proposition 2.2 implique que si K/F est finie, alors elle est algébrique. On dit que K est algébriquement clos si tout polynôme non constant $P \in K[X]$ a une racine dans K. Si K est algébriquement clos et si L/K est une extension algébrique, alors $L = K$. Nous allons montrer que tout corps admet une clôture algébrique, c'est à dire une extension algébrique et algébriquement close, et que deux clôtures algébriques d'un corps sont isomorphes. Remarquons que si L/F est une extension, avec L algébriquement clos, alors l'ensemble des éléments de L qui sont algébriques sur F est une clôture algébrique de F.

Lemme 2.7. — *Si $P(X) \in K[X]$ est irréductible, alors $K[X]/P(X)$ est un corps.*

Démonstration. — Plus généralement, soit A un anneau principal et $p \in A$ irréductible. Montrons que (p) est un idéal maximal. Si $x \in A$, alors (p, x) est principal, $(p, x) = (a)$. L'élément a divise p et donc soit $(a) = (p)$ soit $(a) = A$. □

Proposition 2.8. — *Si K est un corps et $Q(X) \in K[X]$ est non constant, alors il existe une extension finie L de K dans laquelle Q a une racine.*

Démonstration. — Soit P un facteur irréductible de Q et soit $L = K[X]/P(X)$ et α l'image de X dans L. On a $P(\alpha) = 0$ et donc $Q(\alpha) = 0$. □

Corollaire 2.9. — *Si K est un corps et $Q(X) \in K[X]$ est non constant, alors il existe une extension finie M de K dans laquelle Q est scindé.*

Démonstration. — Soit $d = \deg(Q)$. Si $d = 1$, on peut prendre $M = K$. Sinon, la proposition 2.8 nous donne une extension finie L de K qui contient une racine α de Q. Le polynôme $Q(X)/(X - \alpha)$ appartient à $L[X]$ et par récurrence sur d, il existe une extension finie M de L dans laquelle $Q(X)/(X - \alpha)$, et donc $Q(X)$, est scindé. □

Étant donné un corps et un polynôme, on peut donc rajouter une ou plusieurs racines de ce polynôme au corps. Pour construire une clôture algébrique d'un corps, on rajoute toutes les racines de tous les polynômes.

Théorème 2.10. — *Tout corps K admet une clôture algébrique.*

Démonstration. — On pourrait être tenté d'appliquer le lemme de Zorn à l'ensemble des extensions algébriques de K, mais il n'y a pas d'objet global contenant toutes ces extensions. On va donc s'y prendre autrement.

Soit Pol l'ensemble des polynômes non constants à coefficients dans K et $A = K[X_P]_{P \in \mathrm{Pol}}$ et I l'idéal de A engendré par les $P(X_P)$ où P parcourt Pol. Si on avait

$I = A$, alors on pourrait écrire $1 = \sum_{P\in H} g_P P(X_P)$ où H est un sous ensemble fini de Pol. Par le corollaire 2.9, il existe une extension finie L de K dans laquelle chaque $P \in H$ a une racine α_P et en évaluant $1 = \sum_{P\in H} g_P P(X_P)$ en $X_P = \alpha_P$ on aurait $1 = 0$. On en déduit que I est un idéal propre de A.

Par le lemme de Zorn, I est contenu dans un idéal maximal M de A. Le corps $K_1 = A/M$ est alors une extension de K dans laquelle tout polynôme non constant $P(X) \in K[X]$ admet une racine. En itérant cette construction, on trouve une suite de corps $K_0 = K \subset K_1 \subset K_2 \subset \cdots$ telle que tout polynôme non constant à coeffcients dans K_n a une racine dans K_{n+1}. Le corps $L = \cup_{n\geq 1} K_n$ est algébriquement clos. Le sous-corps des éléments algébriques de L est alors une clôture algébrique de K. □

Ceci montre l'existence d'une clôture algébrique. Montrons à présent que deux clôtures algébriques d'un corps sont isomorphes.

Proposition 2.11. — *Soit K/F une extension algébrique de corps et L un corps. Soit $\sigma : F \to L$ un morphisme de corps. Si $\alpha \in K$, alors il y a une bijection entre l'ensemble des prolongements de σ à $F(\alpha)$ et l'ensemble des racines de $P^{\sigma}_{\min,\alpha}(X)$ dans L.*

Démonstration. — Un tel $\sigma : F(\alpha) \to L$ est déterminé par $\sigma(\alpha)$, et $\sigma(\alpha)$ doit être une racine de $P^{\sigma}_{\min,\alpha}(X)$ dans L. Réciproquement, si $\beta \in L$, alors on a un morphisme $F[X] \to L$ donné par $Q(X) \mapsto Q^{\sigma}(\beta)$ et si β est une racine de $P^{\sigma}_{\min,\alpha}(X)$, alors ce morphisme est nul sur $(P_{\min,\alpha})$ et donne un morphisme $F(\alpha) = F[X]/P_{\min,\alpha}(X) \to L$ qui étend σ. □

Théorème 2.12. — *Soit K/F une extension algébrique de corps, et L un corps algébriquement clos. Tout morphisme de corps $\sigma : F \to L$ s'étend à K.*

Démonstration. — Soit S l'ensemble des paires (E, τ) où $F \subset E \subset K$ et où $\tau : E \to L$ prolonge σ. On dit que $(E, \tau) \leq (E', \tau')$ si $E \subset E'$ et si $\tau' = \tau$ sur E. Ceci fait de S un ensemble ordonné, qui contient (F, σ). Si P est une partie totalement ordonnée de S, alors posons $E = \cup_{p\in P} E_p$ avec le τ commun. C'est un majorant de P. L'ensemble S est donc ordonné inductif, et admet un élément maximal (E, τ). Si $E \neq K$, alors la proposition 2.11 permet d'étendre τ à une extension $E(\alpha)$ de E. On a donc $E = K$ et σ se prolonge à K. □

Corollaire 2.13. — *Deux clôtures algébriques d'un corps F sont isomorphes en tant qu'extensions de F.*

Démonstration. — Soient K et L deux clôtures algébriques d'un corps F. Notons σ l'inclusion de F dans L. Par le théorème 2.12, σ se prolonge à $\tau : K \to L$. Comme K est algébriquement clos, $\tau(K)$ est algébriquement clos. Le corps L est une extension algébrique de $\tau(K)$ ce qui fait que $L = \tau(K)$. L'application $\tau : K \to L$ est donc un isomorphisme F-linéaire. □

En pratique, on parle souvent de la clôture algébrique d'un corps. Cette terminologie est incorrecte : deux clôtures algébriques d'un corps sont isomorphes, mais pas égales. Notons tout de même que $\mathbf{Q}$ a une clôture algébrique privilégiée, l'ensemble des nombres algébriques dans $\mathbf{C}$ (mais $\mathbf{C}$ n'est bien défini qu'à conjugaison complexe près).

2.3. Nombres réels et complexes. — On a le résultat (bien connu) ci-dessous.

Théorème 2.14. — *Le corps* $\mathbf{C}$ *des nombres complexes est algébriquement clos.*

Démonstration. — Soit $P(X) = a_0 + a_1X + \cdots + a_dX^d \in \mathbf{C}[X]$ un polynôme de degré $d \geq 1$. Comme $|P(z)| = |z|^d \cdot |a_d + a_{d-1}/z + \cdots + a_0/z^d|$, avec $a_d \neq 0$, on a $|P(z)| \to +\infty$ quand $|z| \to +\infty$ et il existe donc un point $z_0 \in \mathbf{C}$ où $|P(z)|$ admet un minimum global. Si $P(z_0) = 0$, alors on a terminé ; sinon, on écrit :

$$P(z) = P(z_0) \cdot (1 + b_m(z - z_0)^m + \mathrm{O}((z - z_0)^{m+1})),$$

avec $b_m \neq 0$ et si l'on écrit $b_m = |b_m|e^{i\theta_m}$, et que l'on prend $z = z_0 + \varepsilon \cdot e^{i(-\theta_m+\pi)/m}$, alors on a :

$$P(z) = P(z_0) \cdot (1 - |b_m|\varepsilon^m + \mathrm{O}(\varepsilon^{m+1})),$$

ce qui permet de trouver z tel que $|P(z)| < |P(z_0)|$, absurde. □

On dit que $\alpha \in \mathbf{C}$ est un nombre algébrique s'il l'est sur $\mathbf{Q}$. L'ensemble des nombres algébriques de $\mathbf{C}$ est dénombrable, et c'est une clôture algébrique de $\mathbf{Q}$. Le résultat suivant permet de construire des exemples d'éléments de $\mathbf{R}$ qui ne sont pas algébriques.

Théorème 2.15. — *Si* $\alpha \in \mathbf{R}$ *est irrationel et algébrique de degré* d*, alors il existe* $c > 0$ *telle que*

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

pour tous $p, q \in \mathbf{Z}$ *(*$q \neq 0$*).*

Démonstration. — Soit $P = m \cdot P_{\min,\alpha}$ où $m \in \mathbf{Z}_{\geq 1}$ est tel que $P(X) \in \mathbf{Z}[X]$. Si $\alpha \in \mathbf{R}$ et $p, q \in \mathbf{Z}$ $(q \neq 0)$, il existe $y \in [\alpha; p/q]$ tel que $P(\alpha) - P(p/q) = (\alpha - p/q) \cdot P'(y)$. On a $P(\alpha) = 0$ et $P(p/q) \in 1/q^d \cdot \mathbf{Z} \setminus \{0\}$ ce qui fait que $|\alpha - p/q| \geq 1/q^d \cdot 1/|P'(y)|$. Il suffit alors de prendre $c = \min(1, \min_{y\in[\alpha-1;\alpha+1]} 1/|P'(y)|)$. □

Par exemple, on en déduit que $\sum_{k\geq 0} 1/2^{k!}$ n'est pas algébrique.

2.4. Corps finis. — Si p est un nombre premier, alors $\mathbf{Z}/p\mathbf{Z}$ est un corps de cardinal p que l'on note $\mathbf{F}_p$. Il existe d'autres corps finis que les $\mathbf{F}_p$. Si K est un corps fini, alors le morphisme naturel $\mathbf{Z} \to K$ n'est pas injectif et il existe donc $n \geq 2$ tel que $\mathbf{Z}/n\mathbf{Z}$ est un sous-anneau de K. Comme $\mathbf{Z}/n\mathbf{Z}$ n'est intègre que si n est premier, il existe un nombre premier p tel que $\mathbf{F}_p \subset K$. On a alors $p = 0$ dans K, et K est de caractéristique p.

Proposition 2.16. — *Si K est un corps fini de caractéristique p, alors son cardinal est p^n pour un entier $n \geq 1$.*

Démonstration. — Comme K est fini et contient $\mathbf{F}_p$, c'est un espace vectoriel de dimension finie sur $\mathbf{F}_p$. Si on note n sa dimension, on a $K \simeq \mathbf{F}_p^n$ et donc $\mathrm{card}(K) = p^n$. □

Si K est un corps fini de cardinal $q = p^n$, alors $K^\times$ est un groupe abélien (pour la multiplication) de cardinal $q-1$ et on a donc $x^{q-1} = 1$ pour tout $x \in K^\times$, ce qui fait que tout élément de K est racine du polynôme $X^q - X$. En particulier, le polynôme $X^q - X - 1$ n'a pas de racines dans K et donc un corps fini n'est jamais algébriquement clos. On note $\overline{\mathbf{F}}_p$ une clôture algébrique de $\mathbf{F}_p$.

Si K est de caractéristique p, alors l'application $\mathrm{Fr}_p : K \to K$ donnée par $x \mapsto x^p$ est un morphisme d'anneaux qui est $\mathbf{F}_p$-linéaire, puisque $a^p = a$ si $a \in \mathbf{F}_p$ et que $(a+b)^p = a^p + b^p$ dans un anneau où $p = 0$. Cette application s'appelle le morphisme de Frobenius.

Théorème 2.17. — *Si $q = p^h$, alors l'ensemble $\mathbf{F}_q = \{x \in \overline{\mathbf{F}}_p \mid x^q = x\}$ est un sous-corps de $\overline{\mathbf{F}}_p$ qui est une extension de $\mathbf{F}_p$ de degré h, et c'est le seul sous-corps de $\overline{\mathbf{F}}_p$ qui ait cette propriété.*

Démonstration. — Comme l'application $x \mapsto x^q$ est un morphisme d'anneaux (c'est Fr_p^h), $\mathbf{F}_q$ est bien un sous-anneau de $\overline{\mathbf{F}}_p$. Si $x \in \mathbf{F}_q \setminus \{0\}$, alors $(x^{-1})^q = (x^q)^{-1} = x^{-1}$ et donc $x^{-1} \in \mathbf{F}_q$ ce qui fait que $\mathbf{F}_q$ est bien un corps. Comme $\overline{\mathbf{F}}_p$ est algébriquement clos, le polynôme $P(X) = X^q - X$ a $\deg(P) = q$ solutions (distinctes) dans $\overline{\mathbf{F}}_p$ et donc $\mathbf{F}_q$ est de cardinal $q = p^h$ ce qui fait que c'est une extension de $\mathbf{F}_p$ de degré h. Enfin, si K est un sous-corps de $\overline{\mathbf{F}}_p$ de cardinal q, alors on a vu que le polynôme $X^q - X$ est nul sur K et donc on a forcément $K = \mathbf{F}_q$. □

La situation est donc radicalement différente de ce qui se passe sur $\mathbf{Q}$, qui a une infinité d'extensions de degré n pour tout $n \geq 2$.

Si $m, n \geq 1$, alors $\mathbf{F}_{q^m}$ et $\mathbf{F}_{q^n}$ sont deux sous-corps de $\overline{\mathbf{F}}_p$ et $\mathbf{F}_{q^m} \subset \mathbf{F}_{q^n}$ si et seulement si m divise n. En effet, si $\mathbf{F}_{q^m} \subset \mathbf{F}_{q^n}$ alors $\mathbf{F}_{q^n}$ est un $\mathbf{F}_{q^m}$ espace vectoriel de dimension d

et alors $q^n = (q^m)^d$ et donc $n = dm$. Réciproquement, si $n = dm$, alors $x^{q^m} = x$ implique $x^{q^{md}} = x$ et donc $\mathbf{F}_{q^m} \subset \mathbf{F}_{q^n}$.

Enfin, une partie importante de la théorie des nombres a été motivée par l'étude des carrés dans $\mathbf{F}_p$. Supposons que $p \geq 3$. L'application $x \mapsto x^2$ est un morphisme de groupes de $\mathbf{F}_p^\times$ dans $\mathbf{F}_p^\times$. Son noyau est $\{\pm 1\}$ et son image est donc constituée de $(p-1)/2$ éléments. Si $a \in \mathbf{Z}$, on dit que a est un carré modulo p, ou encore un résidu quadratique modulo p, si l'image de a dans $\mathbf{F}_p$ est un carré. On définit une fonction, le symbole de Legendre $\left(\frac{\cdot}{p}\right) \to \{0, \pm 1\}$ par $\left(\frac{a}{p}\right) = 0$ si p divise a, $\left(\frac{a}{p}\right) = 1$ si a est un carré non nul modulo p et $\left(\frac{a}{p}\right) = -1$ si a n'est pas un carré modulo p.

Lemme 2.18. — *On a* $\left(\frac{a}{p}\right) \equiv a^{(p-1)/2} \bmod p$.

Démonstration. — On a manifestement $\left(\frac{a}{p}\right) \equiv a^{(p-1)/2} \bmod p$ si a est un carré modulo p. Le polynôme $X^{p-1} - 1$ est le produit de $X^{(p-1)/2} - 1$ par $X^{(p-1)/2} + 1$ et est scindé dans $\mathbf{F}_p[X]$. Les racines de $X^{(p-1)/2} - 1$ sont les carrés non nuls et les racines de $X^{(p-1)/2} + 1$ sont donc les non-carrés. □

Ceci implique que $\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right) \times \left(\frac{b}{p}\right)$.

Exemple 2.19. — On a $\left(\frac{-1}{p}\right) = 1$ si $p = 1 \bmod 4$ et $\left(\frac{-1}{p}\right) = -1$ si $p = 3 \bmod 4$.

Démonstration. — On a $\left(\frac{-1}{p}\right) \equiv (-1)^{(p-1)/2} \bmod p$. □

Le théorème suivant est la célèbre loi de réciprocité quadratique, conjecturée par Euler et Legendre, et démontrée (six fois !) par Gauss (1801).

Théorème 2.20. — *Si $p \neq \ell$ sont deux nombres premiers impairs, alors :*

$$\left(\frac{p}{\ell}\right) = \left(\frac{\ell}{p}\right) \cdot (-1)^{\frac{(p-1)(\ell-1)}{4}}, \quad \text{et} \quad \left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}.$$

Démonstration. — Commençons par remarquer que dans $\overline{\mathbf{F}}_p$, il existe un élément $\zeta_\ell \neq 1$ tel que $\zeta_\ell^\ell = 1$. On définit dans $\overline{\mathbf{F}}_p$ les sommes de Gauss par $G(a) = \sum_{k=0}^{\ell-1} \left(\frac{k}{\ell}\right) \zeta_\ell^{ak}$. On voit que $G(a) = \left(\frac{a}{\ell}\right) G(1)$. On a donc $\sum_{a=0}^{\ell-1} G(a)G(-a) = (\ell-1)\left(\frac{-1}{\ell}\right) G(1)^2$ et par ailleurs

$$\sum_{a=0}^{\ell-1} G(a)G(-a) = \sum_{a=0}^{\ell-1} \sum_{k,j=0}^{\ell-1} \left(\frac{k}{\ell}\right)\left(\frac{j}{\ell}\right) \zeta_\ell^{ak-aj} = \sum_{k,j=0}^{\ell-1} \left(\frac{k}{\ell}\right)\left(\frac{j}{\ell}\right) \sum_{a=0}^{\ell-1} \zeta_\ell^{ak-aj} = \ell(\ell-1).$$

On a donc $(\ell-1)\left(\frac{-1}{\ell}\right) G(1)^2 = \ell(\ell-1)$ et on peut simplifier par $\ell - 1$ quitte à supposer $p > \ell$ de telle sorte que $\ell - 1 \neq 0$. En particulier, si on pose $\ell^* = \left(\frac{-1}{\ell}\right)\ell$, alors $G(1)^2 = \ell^*$ et donc $(\ell^*)^{(p-1)/2} = G(1)^{p-1}$. On a $G(1)^p = \left(\frac{p}{\ell}\right) \cdot G(1)$ et donc $G(1) \cdot (\ell^*)^{(p-1)/2} = \left(\frac{p}{\ell}\right) \cdot G(1)$.

En multipliant par $G(1)$ et comme ℓ^* est inversible dans $\overline{\mathbf{F}}_p$, on trouve que $\left(\frac{\ell^*}{p}\right) = \left(\frac{p}{\ell}\right)$, ce qui implique la première formule puisque $\left(\frac{-1}{\ell}\right) = (-1)^{(\ell-1)/2}$.

La deuxième se démontre de manière similaire. On choisit $\zeta_8 \in \overline{\mathbf{F}}_p$ et on pose $G = \zeta_8 + \zeta_8^7$ de sorte que $G^2 = 2$ et $2^{(p-1)/2} = G^{p-1}$. On a donc $G \cdot 2^{(p-1)/2} = \zeta_8^p + \zeta_8^{7p}$ et il sufit alors d'examiner les quatre possibilités pour p mod 8. □

Le théorème permet de calculer $\left(\frac{a}{p}\right)$ en écrivant $a = q_1 \cdots q_r$ et $\left(\frac{a}{p}\right) = \prod_{i=1}^r \left(\frac{q_i}{p}\right)$. Par exemple,

$$\left(\frac{57}{73}\right) = \left(\frac{3}{73}\right) \cdot \left(\frac{19}{73}\right) = \left(\frac{73}{3}\right) \cdot \left(\frac{73}{19}\right) = 1 \cdot \left(\frac{16}{19}\right) = 1.$$

Ce théorème implique aussi que la valeur de $\left(\frac{a}{p}\right)$, quand p varie, p ne divisant pas a, ne dépend que de p modulo a ou $4a$. Par exemple, $\left(\frac{5}{p}\right) = 1$ si $p = 1, 4$ mod 5 et $\left(\frac{5}{p}\right) = -1$ si $p = 2, 3$ mod 5. De même, $\left(\frac{3}{p}\right) = 1$ si $p = 1, 11$ mod 12 et $\left(\frac{3}{p}\right) = -1$ si $p = 5, 7$ mod 12.

2.5. Extensions normales. — Rappelons le théorème 2.12 : soit F/K une extension algébrique de corps, et L un corps algébriquement clos. Tout morphisme de corps $\sigma : K \to L$ s'étend à F.

Soit K un corps et $P(X) \in K[X]$ de degré ≥ 1. Un corps de décomposition de P est une extension E de K telle que $P(X)$ est scindé dans E et telle que E est engendré au-dessus de K par les racines de P. Un polynôme P a toujours un corps de décomposition, le corps engendré par ses racines dans une clôture algébrique de K. Un corps de décomposition est une extension finie de K.

Théorème 2.21. — *Soit L une clôture algébrique de K et F le corps engendré par les racines de P dans L. Si E est un corps de décomposition de P, alors il existe un plongement K-linéaire de E dans L, et tout plongement K-linéaire de E dans L est un isomorphisme de E vers F.*

Démonstration. — L'existence d'un plongement K-linéaire $\sigma : E \to L$ suit du théorème 2.12. Dans E, on a une factorisation $P(X) = c(X - \alpha_1) \cdots (X - \alpha_d)$ et donc dans $\sigma(E)$ on a $P(X) = c(X - \sigma(\alpha_1)) \cdots (X - \sigma(\alpha_d))$. Le corps $\sigma(E)$ est engendré par les $\sigma(\alpha_i)$, qui sont les racines de P dans L, et donc $\sigma(E) = F$. □

On en déduit que deux corps de décomposition de P sont toujours isomorphes.

Proposition 2.22. — *Si $P(X) \in K[X]$ est de degré n, et si F est un corps de décomposition de P, alors $[F : K]$ divise $n!$.*

Démonstration. — La démonstration se fait par récurrence sur n. On se place dans une clôture algébrique de K.

Si P est irréductible, et si α est une racine de P, alors $[K(\alpha) : K] = n$ et F est un corps de décomposition de $P(X)/(X - \alpha) \in K(\alpha)[X]$. Par récurrence, $[F : K(\alpha)]$ divise $(n-1)!$ et donc $[F : K]$ divise $n!$.

Si $P = P_1P_2$ avec $\deg(P_i) = n_i$, alors le corps E engendré par les racines de P_1 est un corps de décomposition pour P_1 et F est un corps de décomposition pour $P_2 \in E[X]$. On en déduit que $[F : K]$ divise $n_1!n_2!$, qui divise $n!$. □

Soit $\{P_i\}_{i\in I}$ une famille de polynômes de degrés ≥ 1 à coefficients dans K. Un corps de décomposition de $\{P_i\}_{i\in I}$ est une extension E de K telle que pour tout i, P_i a toutes ses racines dans E, et E est engendré par les racines des $\{P_i\}_{i\in I}$. Un tel corps est algébrique sur K. Si L est une clôture algébrique de K et si F_i est le corps de décomposition de P_i dans L, alors le compositum F des F_i est un corps de décomposition de $\{P_i\}_{i\in I}$ dans L. Le théorème 2.21 s'étend à cette situation.

Proposition 2.23. — *Si E est un corps de décomposition de la famille $\{P_i\}_{i\in I}$, alors il existe un plongement K-linéaire de E dans L, et tout plongement K-linéaire de E dans L est un isomorphisme de E vers F.*

Démonstration. — L'existence d'un plongement K-linéaire $\sigma : E \to L$ suit du théorème 2.12. Si $\sigma : E \to L$ est un plongement K-linéaire, alors pour tout i, $\sigma(E_i) = F_i$ par le théorème 2.21 et donc $\sigma(E)$ est le compositum des F_i, c'est à dire F. □

Soit L une clôture algébrique de K et F/K une extension contenue dans L. Si $\sigma : F \to L$ est un plongement K-linéaire, alors son image n'est pas nécessairement F. On dit que l'extension F/K est normale si $\sigma(F) = F$ pour tout plongement K-linéaire $\sigma : F \to L$.

Théorème 2.24. — *Soit L une clôture algébrique de K et F/K une extension contenue dans L. Les conditions suivantes sont équivalentes.*

1. *L'extension F/K est normale ;*
2. *Tout polynôme irréductible $P(X) \in K[X]$ qui a une racine dans F a toutes ses racines dans F ;*
3. *F est le corps de décomposition d'une famille $\{P_i\}_{i\in I}$ d'éléments de $K[X]$.*

Démonstration. — Montrons que (1) implique (2). Soit α une racine de P dans F et β une racine de P dans L. Par la proposition 2.11, il existe un plongement K-linéaire de $K(\alpha)$ dans L, qui envoie α sur β. Par le théorème 2.12, on peut le prolonger en $\sigma : F \to L$. Si F/K est normale, on a $\sigma(F) = F$ et donc $\beta \in F$.

Montrons que (2) implique (3). Si $\alpha \in F$, le polynôme $P_{\min,\alpha}(X) \in K[X]$ admet α comme racine dans F, et donc F contient toutes les racines de $P_{\min,\alpha}$. Le corps F est donc le corps de décomposition de $\{P_{\min,\alpha}\}_{\alpha\in F}$.

Le fait que (3) implique (1) suit immédiatement de la proposition 2.23. □

Si E et F sont deux extensions normales de K, incluses dans L, alors $E \cap F$ et EF sont aussi des extensions normales de K. Si F/K est normale et $E/K \subset F$, alors F/E est normale, mais E/K ne l'est pas nécessairement.

Si F/K est une extension algébrique, alors un corps de décomposition de $\{P_{\min,\alpha}\}_{\alpha\in F}$ est une extension normale de K qui contient F, et c'est la plus petite possible. C'est la clôture normale de F, et elle est unique à isomorphisme près.

2.6. Extensions séparables. — Soit F/K une extension finie de corps et L une extension algébriquement close de K (par exemple une clôture algébrique de K). On s'intéresse aux plongements K-linéaires de F dans L. Cet ensemble est noté $\mathrm{Hom}_K(F, L)$.

On dit que $\alpha \in F$ est séparable sur K si les racines de $P_{\min,\alpha}(X)$ sont simples. Ceci est équivalent à ce que $P_{\min,\alpha}$ est premier avec $P'_{\min,\alpha}$. En particulier si K est de caractéristique 0, alors tout $\alpha \in F$ est séparable sur K. On dit que F/K est séparable si tout $\alpha \in F$ est séparable sur K. Remarquons que si $F/E/K$ est une tour d'extensions, et si F/K est séparable, alors E/K est séparable (immédiat) et F/E est séparable (si $\alpha \in F$, alors $P^E_{\min,\alpha}(X)$ divise $P^K_{\min,\alpha}(X)$).

On dit qu'un corps K est parfait si toute extension finie de K est séparable.

Théorème 2.25. — *Un corps de caractéristique nulle est parfait. Un corps de caractéristique $p > 0$ est parfait si et seulement si le morphisme $x \mapsto x^p$ de K dans K est surjectif.*

Lemme 2.26. — *Si K est de caractéristique p et si $P(X) \in K[X]$ est tel que $P'(X) = 0$, alors $P(X) \in K[X^p]$.*

Démonstration du théorème 2.25. — Si K est de caractéristique nulle, et si $\alpha \in F$ avec F/K finie, alors $P'_{\min,\alpha} \neq 0$, et $P_{\min,\alpha}$ et $P'_{\min,\alpha}$ sont premiers entre eux. Les racines de $P_{\min,\alpha}$ sont donc simples.

Supposons que K est de caractéristique p et parfait. Soit $\alpha \in K$ et F une extension de K contenant y tel que $y^p = \alpha$. Le polynôme $P_{\min,y}(X)$ divise $X^p - \alpha$, qui a pour racine y avec multiplicité p. Si $P_{\min,y}(X)$ est à racines simples, alors $P_{\min,y}(X) = X - y$ et donc $y \in K$. On en déduit que si K est parfait, alors $x \mapsto x^p$ est surjectif.

Supposons que K est de caractéristique p et que $x \mapsto x^p$ est surjectif. Soit F une extension de K et $\alpha \in F$. Si $P'_{\min,\alpha} \neq 0$, alors $P_{\min,\alpha}$ et $P'_{\min,\alpha}$ sont premiers entre eux et donc les racines de $P_{\min,\alpha}$ sont simples. Sinon il existe $Q(X) \in K[X]$ tel que $P_{\min,\alpha}(X) = Q(X^p)$. Si $x \mapsto x^p$ est surjectif dans K, il existe $R(X) \in K[X]$ tel que $P_{\min,\alpha}(X) = R(X)^p$ et alors $P_{\min,\alpha}(X)$ n'est pas irréductible, contradiction. □

Théorème 2.27. — *Si F/K est une extension finie et si L est un corps algébriquement clos et si $\sigma : K \to L$ est un plongement de K dans L, alors σ s'étend en au plus $[F : K]$ plongements de F dans L, avec égalité si et seulement si F/K est séparable.*

Démonstration. — Par la proposition 2.11, on a le résultat suivant : si $\alpha \in F$, alors il y a une bijection entre l'ensemble des prolongements de σ à $K(\alpha)$ et l'ensemble des racines de $P^{\sigma}_{\min,\alpha}(X)$ dans L.

Par ailleurs, on a $[K(\alpha) : K] = \deg P_{\min,\alpha}$. Ceci montre le résultat quand $F = K(\alpha)$.

Écrivons $F = K(\alpha_1, \ldots, \alpha_n)$. Le raisonnement ci-dessus montre qu'un plongement $\sigma : K(\alpha_1, \ldots, \alpha_i) \to L$ s'étend à $K(\alpha_1, \ldots, \alpha_{i+1})$ d'au plus $[K(\alpha_1, \ldots, \alpha_{i+1}) : K(\alpha_1, \ldots, \alpha_i)]$ avec égalité si et seulement si cette extension est séparable. Ceci montre l'inégalité du théorème, et l'égalité si F/K est séparable.

Enfin si F/K n'est pas séparable, il existe $\alpha \in F$ qui n'est pas séparable sur K et alors $\sigma : K \to L$ se prolonge en strictement moins que $[K(\alpha) : K]$ plongements à $K(\alpha)$. Comme chaque plongement $K(\alpha) \to L$ se prolonge en au plus $[F : K(\alpha)]$ plongements de F, ceci montre que l'inégalité est stricte si F/K n'est pas séparable. □

Corollaire 2.28. — *Si L est une extension algébriquement close de K, et F/K est une extension finie, alors* $\operatorname{card} \operatorname{Hom}_K(F, L) \leq [F : K]$*, avec égalité si et seulement si F/K est séparable.*

Corollaire 2.29. — *Si F/K est une extension finie et si $F/E/K$ est telle que F/E et E/K sont séparables, alors F/K est séparable.*

Démonstration. — Soit L une extension algébriquement close de K. Si E/K est séparable, alors $\operatorname{card} \operatorname{Hom}_K(E, L) = [E : K]$. Par ailleurs, comme F/E est séparable, tout plongement de E dans L s'étend en $[F : E]$ plongements de F dans L. On en déduit que $\operatorname{card} \operatorname{Hom}_K(F, L) = [F : K]$ et donc que F/K est séparable. □

Corollaire 2.30. — *Soit F/K une extension finie. Si $x \in F$, alors x est séparable si et seulement si $K(x)/K$ est séparable. L'ensemble des éléments séparables de F est un sous-corps de F.*

Démonstration. — Soit L une extension algébriquement close de K. La première assertion suit de ce que $\operatorname{card}\operatorname{Hom}_K(K(x), L)$ est le nombre de racines de $P_{\min,x}$ dans L. Si x et y sont séparables sur K, alors $K(x)/K$ et $K(x,y)/K(x)$ sont séparables. Par le corollaire 2.29, l'extension $K(x,y)/K$ est alors séparable et donc $x \pm y$, xy et x/y le sont. □

Corollaire 2.31. — *Soit L une extension algébriquement close de K, et $F \subset L$ une extension finie séparable de K.*

On a $K = \{x \in F$ tels que $\sigma(x) = x$ pour tout $\sigma \in \operatorname{Hom}_K(F, L)\}$.

Démonstration. — Si $x \in F$, alors x est séparable, et il y a $[K(x) : K]$ plongements distincts de $K(x)$ dans L, qui s'étendent tous à F. Si $\sigma(x) = x$ pour chacun d'eux, alors $[K(x) : K] = 1$ et donc $x \in K$. □

Théorème 2.32. — *Si F/K est une extension finie séparable, alors il existe $\alpha \in F$ tel que $F = K(\alpha)$.*

Démonstration. — Si K est un corps fini, alors $F^\times$ est cyclique et si α engendre $F^\times$ alors $F = K(\alpha)$. On suppose dans la suite que F est infini.

Comme F/K est finie, il existe $\alpha_1, \ldots, \alpha_k \in F$ tels que $F = K(\alpha_1, \ldots, \alpha_k)$. Pour montrer le théorème, il suffit donc de montrer que si $F = K(x,y)$, alors il existe $z \in F$ tel que $F = K(z)$. Pour cela, plaçons nous dans une extension de F qui contient les racines $x_1 = x, x_2, \ldots, x_r$ de $P_{\min,x}(X)$ et les racines $y_1 = y, y_2, \ldots, y_s$ de $P_{\min,y}(X)$. Comme K est infini, il existe $t \neq 0 \in K$ tel que $x_i + ty_j \neq x + ty$ pour tout $(i,j) \neq (1,1)$ et on pose $z = x + ty$. Si on pose $Q(X) = (X - z + ty_1) \cdots (X - z + ty_s)$, alors $Q(X) = (-t)^s P_{\min,y}((X-z)/(-t))$ est à coefficients dans $K(z)$ et l'hypothèse faite sur t, ainsi que la séparabilité de $P_{\min,y}$ et $P_{\min,x}$, implique que le pgcd de $Q(X)$ avec $P_{\min,x}(X)$ est $X - x$ ce qui fait que $x \in K(z)$. On a de même $y \in K(z)$ et donc on a bien $K(x,y) = K(z)$. □

3. Théorie de Galois

3.1. Extensions galoisiennes. — Soit K un corps et $\overline{K}$ une clôture algébrique de K. Soit F/K, avec $F \subset \overline{K}$, une extension finie de corps. On note $\operatorname{Aut}_K(F)$ l'ensemble des automorphismes K-linéaires de F. On a $\operatorname{Aut}_K(F) \subset \operatorname{Hom}_K(F, \overline{K})$, et si $\sigma \in \operatorname{Hom}_K(F, \overline{K})$, alors $\sigma \in \operatorname{Aut}_K(F)$ si et seulement si $\sigma(F) = F$. On dit que F/K est galoisienne si elle est normale et séparable. Dans ce cas, $\operatorname{card}\operatorname{Hom}_K(F, \overline{K}) = [F : K]$ (séparabilité) et pour tout $\sigma \in \operatorname{Hom}_K(F, \overline{K})$, on a $\sigma(F) = F$ (normalité). On en déduit que si F/K est galoisienne, alors $\operatorname{card}\operatorname{Aut}_K(F) = [F : K]$. On note alors $\operatorname{Gal}(F/K)$ le groupe $\operatorname{Aut}_K(F)$. Le corollaire 2.31 montre que si F/K est galoisienne, alors $K = F^{\operatorname{Gal}(F/K)}$.

On dit qu'un polynôme $P(X) \in K[X]$ est séparable s'il est à racines simples.

Proposition 3.1. — *Une extension finie F/K est galoisienne si et seulement si F est le corps de décomposition d'un polynôme séparable $P(X) \in K[X]$.*

Démonstration. — Si F/K est séparable, alors par le théorème 2.32, on peut écrire $F = K(\alpha)$. Si de plus F/K est normale, alors F est le corps de décomposition de $P_{\min,\alpha}(X)$.

Si F est le corps de décomposition d'un polynôme séparable $P(X) \in K[X]$, alors F est engendré par les racines α_i de P. Comme P est séparable, les α_i sont séparables sur K. Le résultat suit alors du corollaire 2.30. □

Proposition 3.2. — *Soit $P(X) \in K[X]$ un polynôme séparable de degré n et F le corps de décomposition de P. Le groupe* $\mathrm{Gal}(F/K)$ *est isomorphe à un sous-groupe de $\mathfrak{S}_n$.*

Démonstration. — Le groupe $\mathrm{Gal}(F/K)$ permute les racines de P, d'où un morphisme $\mathrm{Gal}(F/K) \to \mathfrak{S}_n$. Si $g(\alpha) = \alpha$ pour toute racine α de P, alors $g = \mathrm{Id}$ et le morphisme ci-dessus est donc injectif. □

Proposition 3.3. — *Si P est de plus irréductible, alors* $\mathrm{Gal}(F/K)$ *agit transitivement sur les racines de P.*

Démonstration. — Si α est une racine de P, alors les plongements de $K(\alpha)$ dans $\overline{K}$ sont en bijection avec les racines de P, et pour toute racine β, il existe donc $\sigma : K(\alpha) \to \overline{K}$ tel que $\sigma(\alpha) = \beta$. Le plongement σ se prolonge à $\tau : F \to \overline{K}$ et $\tau \in \mathrm{Gal}(F/K)$ vérifie alors $\tau(\alpha) = \beta$. Le groupe $\mathrm{Gal}(F/K)$ est donc un sous-groupe transitif de $\mathfrak{S}_n$. □

Soit F/K une extension finie séparable. Par le théorème de l'élément primitif, il existe $\alpha \in F$ tel que $F = K(\alpha)$. Le corps de décomposition F^{Gal} de $P_{\min,\alpha}(X)$ est alors une extension galoisienne de K, et toute extension galoisienne de K qui contient F contient F^{Gal}. Le corps F^{Gal} est la clôture galoisienne de F.

3.2. Cyclotomie. — Soit K un corps et $\zeta_n \in \overline{K}$ une racine de l'unité d'ordre $n \geq 2$. L'entier n est premier avec la caractéristique de K (si $n = mp$, alors $\zeta_n^{mp} - 1 = 0$ et donc $\zeta_n^m - 1 = 0$). Le polynôme $X^n - 1$ est donc séparable sur K. Ses racines sont les racines de l'unité d'ordre divisant n, et celles-ci forment un sous-groupe de $\overline{K}^\times$, qui est engendré par ζ_n. On en déduit que $K(\zeta_n)$ est le corps de décomposition de $X^n - 1$, et donc que $K(\zeta_n)/K$ est galoisienne. Si $g \in \mathrm{Gal}(K(\zeta_n)/K)$, alors $g(\zeta_n)$ est une racine de l'unité d'ordre n et est donc de la forme $\zeta_n^{\chi(g)}$ avec $\chi(g) \in (\mathbf{Z}/n\mathbf{Z})^\times$. Ceci donne un morphisme injectif $\chi : \mathrm{Gal}(K(\zeta_n)/K) \to (\mathbf{Z}/n\mathbf{Z})^\times$. On trouve donc que $[K(\zeta_n) : K]$ divise $\varphi(n)$.

Rappelons que si $n = p_1^{e_1} \cdots p_r^{e_r}$, alors $\varphi(n) = \prod_{i=1}^r p_i^{e_i-1}(p_i - 1)$. L'extension $K(\zeta_n)/K$ est un exemple d'extension abélienne.

Les corps cyclotomiques sont les corps $\mathbf{Q}(\zeta_n)$ où $n \geq 1$ et $\zeta_n = \exp(2i\pi/n)$. Le n-ième polynôme cyclotomique est $\Phi_n(X) = \prod_{k\in(\mathbf{Z}/n\mathbf{Z})^\times}(X - \zeta_n^k)$.

Lemme 3.4. — *Le polynôme $\Phi_n(X)$ appartient à $\mathbf{Z}[X]$.*

Démonstration. — Si $k \in \mathbf{Z}/n\mathbf{Z}$, alors ζ_n^k est d'ordre n si et seulement si $k \in (\mathbf{Z}/n\mathbf{Z})^\times$. On a donc $X^n - 1 = \prod_{d|n} \Phi_d(X)$. Ceci implique par récurrence sur n que $X^n - 1 = \Phi_n(X)Q_n(X)$ avec $Q_n(X) \in \mathbf{Z}[X]$ unitaire.

Le polynôme $\Phi_n(X)$ est le quotient de la division euclidienne de $X^n - 1$ par $Q_n(X)$ dans $\mathbf{Q}[X]$ et donc $\Phi_n(X) \in \mathbf{Q}[X]$ puis $\Phi_n(X) \in \mathbf{Z}[X]$ par le lemme de Gauss. □

Proposition 3.5. — *Le polynôme $\Phi_n(X)$ est irréductible dans $\mathbf{Q}[X]$.*

Démonstration. — Soit $P(X)$ le polynôme minimal de ζ_n de telle sorte qu'on peut écrire $X^n - 1 = P(X)Q(X)$. Par le lemme de Gauss, $P, Q \in \mathbf{Z}[X]$. Si p est un nombre premier qui ne divise pas n, et si $P(z) = 0$, montrons que $P(z^p) = 0$. Si ce n'est pas le cas, alors c'est que $Q(z^p) = 0$ et donc, comme $P = P_{\min,z}$, que $P(X)$ divise $Q(X^p)$ (dans $\mathbf{Q}[X]$ et donc dans $\mathbf{Z}[X]$ par Gauss). Dans $\mathbf{F}_p[X]$, le polynôme $P(X)$ diviserait alors $Q(X)^p$ et donc $X^n - 1$ admettrait des racines multiples. Ceci n'est pas possible car $X^n - 1$ est premier avec sa dérivée nX^{n-1} si p ne divise pas n. On en déduit que $P(\zeta_n^p) = 0$ pour tout p premier ne divisant pas n, puis que $P(\zeta_n^k) = 0$ pour tout k premier à n ce qui fait que $P(X) = \Phi_n(X)$ qui est donc irréductible. □

Le polynôme $\Phi_n(X)$ est donc le polynôme minimal de ζ_n et $[\mathbf{Q}(\zeta_n) : \mathbf{Q}] = \varphi(n)$. Le morphisme injectif $\chi : \mathrm{Gal}(\mathbf{Q}(\zeta_n)/\mathbf{Q}) \to (\mathbf{Z}/n\mathbf{Z})^\times$ est donc bijectif.

3.3. Extensions de Kummer. — Si $n \geq 2$, si le corps K contient une racine ζ_n de l'unité d'ordre n et si $y \in K^\times$, alors $K(\sqrt[n]{y})/K$ est galoisienne. En effet, les racines de $X^n - y$ sont de la forme $\zeta_n^j \sqrt[n]{y} \in K(\sqrt[n]{y})$ et donc $K(\sqrt[n]{y})/K$ est le corps de décomposition de $X^n - y$ (qui est séparable).

Si $g \in \mathrm{Gal}(K(\sqrt[n]{y})/K)$, alors il existe $c(g) \in \mathbf{Z}/n\mathbf{Z}$ tel que $g(\sqrt[n]{y}) = \zeta_n^{c(g)} \sqrt[n]{y}$ et on en déduit un morphisme injectif $c : \mathrm{Gal}(K(\sqrt[n]{y})/K) \to \mathbf{Z}/n\mathbf{Z}$. Les extensions de K qui sont de cette forme sont les extensions de Kummer.

Si $n \geq 2$ est premier à la caractéristique de K et si $y \in K$, choisissons ζ_n et $\sqrt[n]{y} \in \overline{K}$. Soit $F = K(\zeta_n, \sqrt[n]{y})$. C'est une extension galoisienne de K (c'est le corps de décomposition de $X^n - y$). On peut écrire $g(\sqrt[n]{y}) = \zeta_n^{c(g)} \sqrt[n]{y}$ et $g(\zeta_n) = \zeta_n^{\chi(g)}$, et le morphisme $g \mapsto \left(\begin{smallmatrix} \chi(g) & c(g) \\ 0 & 1 \end{smallmatrix}\right)$ est un morphisme injectif de $\mathrm{Gal}(F/K) \to \mathrm{GL}_2(\mathbf{Z}/n\mathbf{Z})$.

Le résultat suivant dit d'indépendance linéaire des caractères est dû à Dedekind.

Proposition 3.6. — *Si F est un corps et si G est un ensemble fini d'automorphismes de F, alors les éléments de G sont linéairement indépendants sur F, c'est-à-dire que si les $\lambda_g \in F$ sont tels que $\sum_{g\in G} \lambda_g g(x) = 0$ pour tout $x \in F$, alors $\lambda_g = 0$ quel que soit g.*

Démonstration. — On considère une relation de longueur r minimale $\sum_{i=1}^r \lambda_i g_i = 0$. Si $r = 1$, alors $\lambda_1 g_1(x) = 0$ pour tout $x \in F$ et donc $\lambda_1 = 0$. Sinon, soit $y \in F$ tel que $g_1(y) \neq g_2(y)$. On a $\sum_{i=1}^r \lambda_i g_i(xy) = 0$ d'une part et $g_1(y)\sum_{i=1}^r \lambda_i g_i(x) = 0$ d'autre part pour tout $x \in F$. En soustrayant ces deux relations, on trouve une relation non triviale de longueur plus petite, contradiction. □

On a alors la proposition suivante.

Proposition 3.7. — *Si $\zeta_n \in K$ et si F/K est une extension galoisienne de groupe de Galois $\mathbf{Z}/n\mathbf{Z}$, alors il existe $y \in K$ tel que $F = K(\sqrt[n]{y})$.*

Démonstration. — Soit g un élément qui engendre $\mathrm{Gal}(F/K)$. Si $t \in F$, posons $z(t) = t + \zeta_n g(t) + \cdots + \zeta_n^{n-1} g^{n-1}(t)$. Par le lemme d'indépendance linéaire des caractères, il existe $t \in F$ tel que $z = z(t)$ est non nul. On voit alors que $g(z) = \zeta_n^{-1} z$ ce qui fait que $[K(z) : K] \geq n$ et $z^n \in K$. On a donc bien $F = K(\sqrt[n]{y})$ avec $y = z^n$. □

3.4. Correspondance de Galois. — Le résultat suivant est le lemme d'Artin.

Théorème 3.8. — *Si F est un corps et si G est un groupe fini d'automorphismes de F, alors F/F^G est galoisienne de groupe de Galois G.*

Commençons par ce corollaire du théorème de l'élément primitif.

Corollaire 3.9. — *Si $d \geq 1$ et si F/K est une extension séparable, telle que $[K(x) : K] \leq d$ pour tout $x \in F$, alors F/K est finie et $[F : K] \leq d$.*

Démonstration. — On peut supposer qu'il existe $x \in F$ tel que $[K(x) : K] = d$. Si $y \in F$, alors $K(x, y)/K$ est de la forme $K(z)$ par le théorème de l'élément primitif et donc $[K(x, y) : K] \leq d$. On en déduit que $y \in K(x)$ pour tout $y \in F$, et donc que $F = K(x)$ ce qui fait que F/K est finie et que $[F : K] \leq d$. □

Démonstration du lemme d'Artin. — Soit $d = \mathrm{card}\, G$. Soit $\alpha \in F$, et soit A l'orbite de α sous G. Le polynôme $P(X) = \prod_{y\in A}(X - y)$ est à coefficients dans F^G et annule α ce qui fait que α est séparable sur F^G et que $[F^G(\alpha) : F^G] \leq d$. Le corollaire 3.9 implique que F/F^G est finie de degré $\leq d$. Comme F/F^G admet au moins d automorphismes, on en déduit que F/F^G est galoisienne de groupe de Galois G. □

Le théorème principal de la théorie de Galois est le suivant.

Théorème 3.10. — *Si F/K est une extension galoisienne de groupe de Galois $G = \mathrm{Gal}(F/K)$, alors on a une bijection entre l'ensemble des sous-extensions $K \subset E \subset F$ et l'ensemble des sous-groupes H de G, donnée par $E \mapsto \mathrm{Gal}(F/E)$ et $H \mapsto F^H$, ces deux constructions étant réciproques l'une de l'autre.*

De plus, l'extension F^H/K est galoisienne si et seulement si H est un sous-groupe distingué de G. Dans ce cas, $\mathrm{Gal}(F^H/K) = G/H$.

Démonstration. — Il faut vérifier que $E = F^{\mathrm{Gal}(F/E)}$, ce qui suit du corollaire 2.31, et que $H = \mathrm{Gal}(F/F^H)$, ce qui suit du lemme d'Artin.

Ensuite, si $K \subset E \subset F$, alors E/K est galoisienne si et seulement si $g(E) = E$ pour tout $g \in \mathrm{Gal}(F/K)$. Si $H \subset G$ et si $g \in G$, alors $g(F^H) = F^{gHg^{-1}}$ et donc $g(F^H) = F^H$ pour tout $g \in G$ si et seulement si $H = gHg^{-1}$ pour tout $g \in G$ (par la première partie du théorème). Si F^H/K est galoisienne, alors les éléments de $\mathrm{Gal}(F^H/K)$ se relèvent à F, et l'application $G \to \mathrm{Gal}(F^H/K)$ est surjective. Son noyau est alors $H = \mathrm{Gal}(F/F^H)$. □

On se place dans un corps algébriquement clos contenant K (par exemple $\overline{K}$). Si E et F sont deux extensions de K, on a leur compositum EF.

Proposition 3.11. — *Soit F/K une extension galoisienne et E/K une extension. L'extension EF/E est galoisienne, $\mathrm{Gal}(EF/E)$ s'injecte dans $\mathrm{Gal}(F/K)$, et son image est $\mathrm{Gal}(F/F \cap E)$.*

Démonstration. — Si F est le corps de décomposition d'un polynôme séparable $P(X) \in K[X]$, alors EF est le corps de décomposition de P sur E, et est donc galoisienne sur E. Ensuite $g \mapsto g|_F$ donne un morphisme de $\mathrm{Gal}(EF/E) \to \mathrm{Gal}(F/K)$, et si $g|_F = \mathrm{Id}$ alors $g = \mathrm{Id}$ sur E et F et donc sur EF. Enfin, $F^{\mathrm{Gal}(EF/E)} \subset F \cap (EF)^{\mathrm{Gal}(EF/E)} = F \cap E$, ce qui implique la dernière assertion par correspondance de Galois. □

Notons que E/K n'a pas à être finie (ni même algébrique).

Corollaire 3.12. — *On a $[EF : E] = [F : F \cap E]$.*

Proposition 3.13. — *Soient F/K et E/K deux extensions galoisiennes.*

On a $\mathrm{Gal}(EF/K) = \{(g_F, g_E) \in \mathrm{Gal}(F/K) \times \mathrm{Gal}(E/K)$ tels que $g_F = g_E$ sur $F \cap E\}$.

Démonstration. — Si $g \in \mathrm{Gal}(EF/K)$, on peut le restreindre à F et à E. On en déduit un morphisme injectif $g \mapsto (g|_F, g|_E)$ entre les deux groupes. Le cardinal de $\mathrm{Gal}(EF/K)$ est $[EF : K] = [EF : E][E : K] = [F : K][E : K]/[F \cap E : K]$ (par le corollaire 3.12) qui est aussi le cardinal du groupe de droite par le lemme 3.14. □

Lemme 3.14. — *Soient G_1 et G_2 deux groupes finis, et $p_i : G_i \to H$ deux morphismes surjectifs. L'ensemble $\{(g_1, g_2) \in G_1 \times G_2$ tels que $p_1(g_1) = p_2(g_2)\}$ est alors un groupe de cardinal* $\mathrm{card}(G_1)\,\mathrm{card}(G_2)/\,\mathrm{card}(H)$.

Démonstration. — Si g_1 est fixé, alors il y a $\mathrm{card}(G_2)/\,\mathrm{card}(H)$ choix pour g_2. □

Terminons avec le discriminant d'un polynôme. Soit K un corps de caractéristique $\neq 2$. Si $P(X) \in K[X]$ est séparable de degré n et si F est son corps de décomposition, alors $\mathrm{Gal}(F/K)$ s'injecte dans $\mathfrak{S}_n$. Quand est-ce que l'image de $\mathrm{Gal}(F/K)$ est contenue dans $\mathfrak{A}_n$? Soient $x_1, \ldots, x_n$ les racines de P et soit $\Delta = \prod_{i<j}(x_i - x_j) \in F^\times$. Si $g \in \mathfrak{S}_n$, alors $g(\Delta) = \varepsilon(g) \cdot \Delta$ et donc $\mathrm{Gal}(F/K) \subset \mathfrak{A}_n$ si et seulement si $\Delta \in K$. Si P est unitaire, on a $\Delta^2 = \mathrm{Disc}(P) = \prod_{i<j}(x_i - x_j)^2 = (-1)^{n(n-1)/2} \prod_{i=1}^n P'(x_i)$. On en déduit que $\mathrm{Gal}(F/K) \subset \mathfrak{A}_n$ si et seulement si $\mathrm{Disc}(P)$ est un carré dans K.

On a $\mathrm{Disc}(X^2 + aX + b) = a^2 - 4b$ et $\mathrm{Disc}(X^3 + aX + b) = -4a^3 - 27b^2$.

3.5. Extensions résolubles par radicaux. — Soit K un corps de caractéristique $\neq 2$. Le polynôme $X^2 + aX + b$ a pour racines $(-a \pm \sqrt{a^2 - 4b})/2$. On peut aussi donner des formules pour les racines d'un polynôme de degré 3, en se laissant guider par la théorie de Galois. Soit K un corps de caractéristique $\neq 2, 3$ et $P(X) = X^3 + aX + b \in K[X]$ et F le corps engendré par ses racines x_1, x_2, x_3. Le groupe $\mathrm{Gal}(F/K)$ est un sous-groupe de $\mathfrak{S}_3$. De plus $K(\Delta)/K$ est triviale ou quadratique, et $\mathrm{Gal}(F/K(\Delta))$ est un sous-groupe de $\mathfrak{A}_3 \simeq \mathbf{Z}/3\mathbf{Z}$. Si on suppose que K contient j, on peut donc appliquer ce qu'on a vu sur les extensions de Kummer. Posons $u = x_1 + jx_2 + j^2x_3$ et $v = x_1 + j^2x_2 + jx_3$. On a $u^3, v^3 \in K(\Delta)$. Un calcul montre que $u^3, v^3 = (-27/2) \cdot b \pm 3/2 \cdot \sqrt{-3} \cdot \Delta$. Comme $x_1 + x_2 + x_3 = 0$, on a $x_1 = (u + v)/3$, et de même pour x_2 et x_3. Notons que $uv = -3a$ (le choix d'une racine cubique de u^3 détermine une racine cubique de v^3). On retrouve ainsi la formule de Cardan (1545).

$$x = \sqrt[3]{-\frac{b}{2} + \sqrt{\frac{a^3}{27} + \frac{b^2}{4}}} + \sqrt[3]{-\frac{b}{2} - \sqrt{\frac{a^3}{27} + \frac{b^2}{4}}}.$$

L'analyse du groupe $\mathfrak{S}_4$ permet de même de trouver des formules pour les racines d'un polynôme de degré 4 (Cardan, Ferrari). En revanche, personne n'a pu trouver de formule pour les racines d'un polynôme de degré 5. Nous allons voir pourquoi.

On suppose maintenant que K est de caractéristique 0. Une extension F/K est dite radicale élémentaire s'il existe $y \in F$ et $n \geq 1$ tels que $F = K(y)$ et $y^n \in K$. Une extension F/K est dite radicale s'il existe une tour de sous-extensions $K = F_1 \subset F_2 \subset \cdots \subset F_d = F$ avec F_{i+1}/F_i radicale élémentaire pour tout i. Enfin F/K est dite résoluble par radicaux

s'il existe E/F finie telle que E/K est radicale. Si $P(X) \in K[X]$, on dit que P est résoluble par radicaux si son corps de décomposition est résoluble par radicaux.

Lemme 3.15. — *Si E/K et F/K sont radicales, alors EF/K est radicale.*

Démonstration. — Si $K = F_1 \subset F_2 \subset \cdots \subset F_d = F$ et $K = E_1 \subset E_2 \subset \cdots \subset E_n = E$, alors $K = F_1 \subset F_2 \subset \cdots \subset F_d = E_1F_d \subset E_2F_d \subset E_3F_d \subset \cdots \subset E_nF_d = EF$ montre que EF/K est radicale. □

Si G est un groupe fini, on dit que G est résoluble s'il existe une suite de sous-groupes $\{1\} = G_d \subset G_{d-1} \subset \cdots \subset G_1 = G$ avec G_{i+1} distingué dans G_i et G_i/G_{i+1} cyclique pour tout i.

Lemme 3.16. — *Si G est résoluble et si H est un sous-groupe de G, alors H est résoluble. Si de plus H est distingué, alors G/H est résoluble. Si G est un groupe et H est un sous-groupe distingué tel que H et G/H sont résolubles, alors G est résoluble.*

Démonstration. — Commençons par rappeler qu'un sous-groupe et qu'un quotient d'un groupe cyclique sont cycliques.

Soit $\{1\} = G_d \subset G_{d-1} \subset \cdots \subset G_1 = G$ une suite telle que G_{i+1} est distingué dans G_i et G_i/G_{i+1} cyclique. Si on pose $H_i = H \cap G_i$, alors H_{i+1} est distingué dans H_i et $H_i/H_{i+1} \to G_i/G_{i+1}$ est injectif, ce qui fait que H est résoluble. Si H est distingué, alors $G_i/G_{i+1} \to G_iH/G_{i+1}H$ est surjectif. On peut alors poser $(G/H)_i = G_iH$ ce qui montre que G/H est résoluble. Enfin si H et G/H sont résolubles, soit $\pi : G \to G/H$ la projection et $G_i = \pi^{-1}(G/H)_i$. L'application $G_i/G_{i+1} \to (G/H)_i/(G/H)_{i+1}$ est injective. Le groupe G est résoluble via la suite $\{1\} = H_e \subset \cdots \subset H_1 = H = G_d \subset G_{d-1} \subset \cdots \subset G_1 = G$. □

On en déduit que les groupes abéliens finis sont résolubles. Les groupes $\mathfrak{S}_3$, $\mathfrak{A}_4$ et $\mathfrak{S}_4$ le sont (on a $\{\mathrm{Id}\} \subset \{\mathrm{Id}, [12][34]\} \subset V_4 \subset \mathfrak{A}_4 \subset \mathfrak{S}_4$ où $V_4 = \{\mathrm{Id}, [12][34], [13][24], [14][23]\}$), mais pas $\mathfrak{A}_n$ pour $n \geq 5$ (comme $\mathfrak{A}_n$ est simple) ni $\mathfrak{S}_n$ pour $n \geq 5$ (comme $\mathfrak{A}_n$ est un sous-groupe de $\mathfrak{S}_n$). Tout groupe de cardinal < 60 est résoluble.

Le théorème principal (dû à Galois) sur la résolubilité par radicaux est alors le suivant.

Théorème 3.17. — *Une extension F/K est résoluble par radicaux si et seulement si* $\mathrm{Gal}(F^{\mathrm{Gal}}/K)$ *est résoluble.*

Démonstration. — Commençons par montrer que si $G = \mathrm{Gal}(F^{\mathrm{Gal}}/K)$ est résoluble, alors F/K est résoluble par radicaux. Il existe une suite de sous-groupes $\{1\} = G_d \subset G_{d-1} \subset \cdots \subset G_1 = G$ avec G_{i+1} distingué dans G_i et G_i/G_{i+1} cyclique pour tout i. Soit $F_i = (F^{\mathrm{Gal}})^{G_i}$. L'extension F_{i+1}/F_i est galoisienne de groupe de Galois $\mathbf{Z}/n_i\mathbf{Z}$.

Soit n le ppcm de $n_1, \dots, n_d$ et ζ_n une racine de 1 d'ordre n. Par la proposition 3.11, l'extension $F_{i+1}(\zeta_n)/F_i(\zeta_n)$ est galoisienne, de groupe de Galois un sous-groupe de $\mathbf{Z}/n_i\mathbf{Z}$. On peut alors appliquer la proposition 3.7, qui implique que $F_{i+1}(\zeta_n)/F_i(\zeta_n)$ est radicale élémentaire. Ceci montre que $F^{\mathrm{Gal}}(\zeta_n)/K$ est radicale, et donc que F/K est résoluble par radicaux.

Montrons à présent que si F/K est résoluble par radicaux, alors $\mathrm{Gal}(F^{\mathrm{Gal}}/K)$ est résoluble. Soit E/K une extension radicale qui contient F. Le lemme 3.15 implique que l'on peut supposer que E/K est galoisienne. Écrivons $K = E_1 \subset E_2 \subset \cdots \subset E_d = E$, et prenons pour n le ppcm des n_i tels que $E_{i+1} = E_i(y_{i+1})$ avec $y_{i+1}^{n_i} \in E_i$. On a $K \subset K(\zeta_n) = E_1(\zeta_n) \subset E_2(\zeta_n) \subset \cdots \subset E_d(\zeta_n) = E(\zeta_n)$. Pour tout i, l'extension $E_{i+1}(\zeta_n)/E_i(\zeta_n)$ est galoisienne de groupe de Galois un sous-groupe de $\mathbf{Z}/n_i\mathbf{Z}$. L'extension $K(\zeta_n)/K$ est abélienne. On en déduit que $\mathrm{Gal}(E(\zeta_n)/K)$ est un groupe résoluble. Comme $\mathrm{Gal}(F^{\mathrm{Gal}}/K)$ est un quotient de $\mathrm{Gal}(E(\zeta_n)/K)$, il est lui-même résoluble. □

Si on applique la démonstration du théorème au corps de décomposition d'un polynôme de degré 3, on retrouve la méthode qui permet d'établir la formule de Cardan. Voyons ce qui se passe pour un polynôme général de degré ≥ 5.

Soit K un corps de caractéristique nulle et $n \geq 2$ et $K_X = K(X_1, \dots, X_n)$ le corps des fractions rationnelles en n variables. Pour $1 \leq k \leq n$, soit $S_k = \sum_{i_1 < \cdots < i_k} X_{i_1} \cdots X_{i_k}$ les fonctions symétriques élémentaires et $K_S = K(S_1, \dots, S_n)$. Soit

$$P(T) = \prod_{i=1}^{n} (T - X_i) = T^n - S_1 T^{n-1} + \cdots \pm S_n \in K_S[T].$$

Le corps K_X est le corps de décomposition du polynôme séparable $P(T) \in K_S[T]$, et il est donc galoisien sur K_S de degré $\leq n!$. Par ailleurs, $\mathfrak{S}_n$ agit sur K_X par $\sigma(X_i) = X_{\sigma(i)}$ et cette action laisse K_S invariant. On en déduit que $\mathrm{card}\,\mathrm{Gal}(K_X/K_S) \geq n!$. Ceci implique $[K_X : K_S] = n!$ et $\mathrm{Gal}(K_X/K_S) = \mathfrak{S}_n$.

Par le théorème 3.17, il n'existe pas de formule générale avec des radicaux, à coefficients dans K, pour exprimer les X_i en termes des S_j si $n \geq 5$.

3.6. Extensions constructibles. — Soit K un corps de caractéristique $\neq 2$. On dit qu'une extension F/K est constructible s'il existe une chaîne de corps $K = K_1 \subset K_2 \subset \cdots \subset K_n$ telle que $F \subset K_n$ et K_{i+1}/K_i est de degré 2. Remarquons que le degré d'une extension constructible est une puissance de 2, et qu'une extension constructible est résoluble par radicaux, puisque si K_{i+1}/K_i est de degré 2, alors il existe $y_i \in K_i$ tel que $K_{i+1} = K_i(\sqrt{y_i})$.

Rappelons que les points de $\mathbf{R}^2$ que l'on peut construire à la règle et au compas à partir des points $(0,0)$ et $(1,0)$ sont ceux dont les coordonnées appartiennent à une extension constructible de $\mathbf{Q}$. Avant de caractériser les extensions constructibles, donnons ce résultat de théorie des groupes.

Proposition 3.18. — *Si G est un p-groupe avec p premier, alors il existe une chaîne de sous-groupes $\{1\} = G_d \subset G_{d-1} \subset \cdots \subset G_1 = G$ telle que G_{i+1} est distingué dans G_i et $G_i/G_{i+1} = \mathbf{Z}/p\mathbf{Z}$.*

Démonstration. — Commençons par montrer que si G est un p-groupe, alors son centre $Z(G)$ est non trivial. Si on fait agir G sur lui-même par conjugaison, alors les orbites sont de deux types : $\{z\}$ si $z \in Z(G)$ et sinon les orbites de $x \in G \setminus Z(G)$ qui sont de cardinal $\operatorname{card}(G)/\operatorname{card}(\operatorname{Stab}(x))$, divisible par p. On en déduit que $\operatorname{card}(Z(G))$ est divisible par p.

Le lemme 3.16 implique alors, par récurrence sur $\operatorname{card}(G)$, que G est résoluble. On a $G_i/G_{i+1} = \mathbf{Z}/p^{n_i}\mathbf{Z}$ et la proposition suit quitte à rajouter des sous-groupes. □

Théorème 3.19. — *Une extension F/K est constructible si et seulement si $[F^{\mathrm{Gal}} : K]$ est une puissance de 2.*

Démonstration. — La même démonstration que celle du lemme 3.15 montre que si E/K et F/K sont constructibles, alors EF/K est constructible. Si F/K est constructible, alors F^{Gal}/K est aussi constructible, et $[F^{\mathrm{Gal}} : K]$ est une puissance de 2.

Montrons à présent la réciproque. Par la proposition 3.18 appliquée à $p = 2$, il existe une chaîne de sous-groupes $\{1\} = G_d \subset G_{d-1} \subset \cdots \subset G_1 = G$ telle que G_{i+1} est distingué dans G_i et $G_i/G_{i+1} = \mathbf{Z}/2\mathbf{Z}$. On pose alors $K_i = (F^{\mathrm{Gal}})^{G_i}$. □

Ceci permet par exemple de déterminer quels polygones réguliers à n côtés on peut construire à la règle et au compas à partir des points $(0,0)$ et $(1,0)$. Il faut pouvoir construire le point $(\cos(2\pi/n), \sin(2\pi/n))$. Ce point est constructible si et seulement si $\exp(2i\pi/n)$ est dans une extension constructible de $\mathbf{Q}$. L'extension $\mathbf{Q}(\exp(2i\pi/n))/\mathbf{Q}$ est galoisienne de degré $\varphi(n)$. Le théorème 3.19 implique le résultat suivant.

Théorème 3.20. — *Le polygone régulier à n côtés est constructible à la règle et au compas si et seulement si $\varphi(n)$ est une puissance de 2.*

C'est donc possible pour $n = 3, 4, 5, 6$ mais pas $n = 7$. Si $n = p_1^{e_1} \cdots p_r^{e_r}$, alors $\varphi(n) = \prod_{i=1}^r p_i^{e_i - 1}(p_i - 1)$. Il faut et il suffit donc que les facteurs premiers de n soient 2 et (avec multiplicité 1) des nombres premiers p tels que $p - 1$ est une puissance de 2 (nombres

premiers de Fermat). Le polygone régulier à 17 côtés est donc constructible, ainsi que ceux à 257 et 65 537 côtés.

On peut donner des formules explicites pour $2\cos(2\pi/n)$. Par exemple si $n=5$, posons $\omega_5=\exp(2i\pi/5)$ de sorte que $c=2\cos(2\pi/5)=\omega_5+\omega_5^4$. Le groupe de Galois $\mathrm{Gal}(\mathbf{Q}(c)/\mathbf{Q})$ est engendré par l'image de $2\in(\mathbf{Z}/5\mathbf{Z})^\times$ et $[2](c)+c=\omega_5+\omega_5^4+\omega_5^2+\omega_5^3=-1$. De même $c\cdot[2](c)=-1$ et donc $(X-c)(X-[2](c))=X^2+X-1$ d'où $c=(-1\pm\sqrt{5})/2$.

Faisons à présent le calcul de $c=2\cos(2\pi/17)$. Soit $\omega=\exp(2i\pi/17)$ de sorte que $c=\omega+\omega^{16}$. On a $\mathrm{Gal}(\mathbf{Q}(\omega)/\mathbf{Q})=(\mathbf{Z}/17\mathbf{Z})^\times$ qui est cyclique, engendré par 3. La suite de corps $\mathbf{Q}=K_1\subset K_2\subset K_3\subset K_4\subset K_5=\mathbf{Q}(\omega)$ est donc donnée par $K_1=\mathbf{Q}(\omega)^{\langle 3\rangle}$, $K_2=\mathbf{Q}(\omega)^{\langle 9\rangle}$, $K_3=\mathbf{Q}(\omega)^{\langle 13\rangle}$ et $K_4=\mathbf{Q}(\omega)^{\langle -1\rangle}$. On a $c\in K_4$ et donc $s_3=c+[13](c)\in K_3$ et $p_3=c\cdot[13](c)\in K_3$. On trouve que $s_3=\omega+\omega^{-1}+\omega^4+\omega^{-4}$ et $p_3=\omega^3+\omega^{-3}+\omega^5+\omega^{-5}$. Ensuite $s_2=s_3+[9](s_3)\in K_2$ et $p_2=s_3\cdot[9](s_3)\in K_2$. On a $s_2=\omega+\omega^{-1}+\omega^2+\omega^{-2}+\omega^4+\omega^{-4}+\omega^8+\omega^{-8}$ et $p_2=-1$. De même $s_2+[3](s_2)=-1$ et $s_2\cdot[3](s_2)=-4$. Enfin $p_3+[9](p_3)=-1-s_2$ et $p_3\cdot[9](p_3)=-1$. On trouve donc les équations suivantes :

$$\begin{aligned} s_2 &: X^2+X-4=0\\ s_3 &: X^2-s_2X+1=0\\ p_3 &: X^2+(1+s_2)X+1=0\\ c &: X^2-s_3X+p_3=0 \end{aligned}$$

Ceci permet de montrer (en choisissant bien les signes) que

$$2\cos\left(\frac{2\pi}{17}\right)=-\frac{1}{8}+\frac{1}{8}\sqrt{17}+\frac{1}{8}\sqrt{34-2\sqrt{17}}+\frac{1}{4}\sqrt{17+3\sqrt{17}-\sqrt{34-2\sqrt{17}}-2\sqrt{34+2\sqrt{17}}}$$

3.7. Le théorème de la base normale. — Le but de cette section est de montrer le théorème suivant.

Théorème 3.21. — *Si F/K est une extension galoisienne, alors il existe $x\in F$ tel que $\{g(x)\}_{g\in\mathrm{Gal}(F/K)}$ est une base de F sur K.*

Démonstration du théorème 3.21 pour K corps fini. — On a $\mathrm{Gal}(\mathbf{F}_{q^n}/\mathbf{F}_q)=\mathbf{Z}/n\mathbf{Z}=\langle\varphi_q\rangle$ où $\varphi_q(y)=y^q$. On a $\varphi_q^n=\mathrm{Id}$ et par l'indépendance linéaire des caractères, le polynôme minimal de φ_q est X^n-1. Comme ce polynôme est de degré maximal, il existe un vecteur cyclique $x\in\mathbf{F}_{q^n}$ pour φ_q. En d'autres termes, $\mathbf{F}_{q^n}=\oplus_{i=0}^{n-1}\varphi_q^i(x)\cdot\mathbf{F}_q$. □

On suppose à présent que K est infini.

Lemme 3.22. — *Soit E un corps et $P(X_1, \dots, X_n) \in E[X_1, \dots, X_n]$ un polynôme en n variables. Si $A_1, \dots, A_n$ sont des parties infinies de E telles que $P(x_1, \dots, x_n) = 0$ pour tout $(x_1, \dots, x_n) \in A_1 \times \cdots \times A_n$, alors $P = 0$.*

Démonstration. — Si $n = 1$, cela suit du fait qu'un polynôme de degré d admet au plus d racines dans E. Supposons que le lemme est vrai pour $n-1$, prenons $P \neq 0$, et écrivons $P(X_1, \dots, X_n) = \sum_i P_i(X_2, \dots, X_n) X_1^i$. L'un des P_i est non nul et il existe donc $(x_2, \dots, x_n) \in A_2 \times \cdots \times A_n$ tels que $P_i(x_2, \dots, x_n) \neq 0$. Il suffit alors d'appliquer le cas $n = 1$ du lemme à $P(X_1, x_2, \dots, x_n)$. □

Écrivons $\mathrm{Gal}(F/K) = \{g_1, \dots, g_n\}$ avec $g_1 = \mathrm{Id}$.

Lemme 3.23. — *Il existe $e_1, \dots, e_n \in F$ tels que $\det(g_i(e_j)) \neq 0$.*

Démonstration. — La proposition 3.6 (l'indépendance linéaire des caractères) implique que les g_i sont F-linéairement indépendants : si les $\lambda_i \in F$ sont tels que $\sum_{i=1}^n \lambda_i g_i(x) = 0$ pour tout $x \in F$, alors $\lambda_i = 0$ pour tout i.

Soit $P \subset F^n$ l'ensemble des $(g_1(x), \dots, g_n(x))$ avec $x \in F$. C'est une partie du F-espace vectoriel F^n qui n'est contenue dans aucun hyperplan de F^n par l'indépendance linéaire des g_i, et P contient donc une base de F^n (on prend $p_1 \neq 0 \in P$ puis $p_2 \notin \langle p_1 \rangle$, puis $p_3 \notin \langle p_1, p_2 \rangle$, etc). □

Démonstration du théorème 3.21. — Fixons une telle famille $e_1, \dots, e_n \in F$. Soit

$$P(X_1, \dots, X_n) = \det\left(\sum_{k=1}^n X_k \cdot (g_j^{-1} g_i(e_k))_{i,j}\right) \in F[X_1, \dots, X_n].$$

Comme $(g_i(e_j))_{i,j} \in \mathrm{GL}_n(F)$, il existe un vecteur colonne $c = (c_1, \dots, c_n) \in F^n$ tel que $(g_i(e_j)) \cdot c = (1, 0, \dots, 0)$. On a alors $\sum_{k=1}^n c_k \cdot (g_j^{-1} g_i(e_k))_{i,j} = \mathrm{Id}$ et donc $P(c_1, \dots, c_n) \neq 0$. Le polynôme P est donc non nul, et par le lemme 3.22, il existe $b_1, \dots, b_n \in K^n$ tels que $P(b_1, \dots, b_n) \neq 0$. Soit $x = b_1 e_1 + \cdots + b_n e_n$, de telle sorte que $\det(g_j^{-1} g_i(x))_{i,j} \neq 0$. Montrons que $\{g_1(x), \dots, g_n(x)\}$ est une base de F sur K. Si l'on a $\sum_{i=1}^n a_i g_i(x) = 0$, avec les a_i dans K, alors on a aussi $\sum_{i=1}^n a_i g_j^{-1} g_i(x) = 0$ pour tout j. On a donc $(g_j^{-1} g_i(x))_{i,j} \cdot (a_1, \dots, a_n) = 0$ et donc $a_i = 0$ pour tout i. □

Soit $G = \mathrm{Gal}(F/K)$. Si x est tel que $\{g(x)\}_{g \in G}$ est une base de F sur K, et si $y \in F$, on peut écrire $y = \sum y_g \cdot g(x)$ avec $y_g \in K$. Si $h \in G$, alors $h(y) = \sum y_g \cdot hg(x) = \sum y_{h^{-1}g} \cdot g(x)$.

On en déduit que $h(y) = y$ si et seulement si $y_{h^{-1}g} = y_g$ pour tout g. Par exemple, si H est un sous-groupe de G, alors $y \in F^H$ si et seulement si y_g ne dépend que $H \cdot g$.

On en déduit aussi la structure de F comme représentation K-linéaire de G : on trouve que c'est la représentation régulière de G.

3.8. La trace et la norme. — Soit K un corps, et L une extension algébriquement close de K dans laquelle on travaille. Soit F/K une extension finie de corps, $F \subset L$. Si $x \in F$, alors on a la multiplication par x, $m_x : F \to F$, donnée par $m_x(a) = xa$. C'est un endomorphisme F-linéaire de F. On a $m_{x+y} = m_x + m_y$ et $m_{xy} = m_x m_y$ et $m_{P(x)} = P(m_x)$ si $P(X) \in F[X]$.

On pose $\mathrm{Tr}_{F/K}(x) = \mathrm{Tr}(m_x)$ (m_x vu comme endomorphisme K-linéaire de F) et de même $\mathrm{N}_{F/K}(x) = \det(m_x)$. On a $\mathrm{Tr}_{F/K}(x)$, $\mathrm{N}_{F/K}(x) \in K$ et $\mathrm{Tr}_{F/K}(x+y) = \mathrm{Tr}_{F/K}(x) + \mathrm{Tr}_{F/K}(y)$ et $\mathrm{N}_{F/K}(xy) = \mathrm{N}_{F/K}(x)\,\mathrm{N}_{F/K}(y)$.

Proposition 3.24. — *Si F/K est séparable, alors $\mathrm{Tr}_{F/K}(x) = \sum_{\sigma \in \mathrm{Hom}_K(F,L)} \sigma(x)$ et $\mathrm{N}_{F/K}(x) = \prod_{\sigma \in \mathrm{Hom}_K(F,L)} \sigma(x)$.*

Démonstration. — Soit $P(X) = P_{\min,x}(X)$, de sorte que P est aussi le polynôme minimal de m_x. Soit $E = K(x)$ et $d = [E : K]$. En prenant comme base de E la famille $1, x, \ldots, x^{d-1}$, on voit que $\mathrm{Tr}(m_x : E \to E)$ est moins le coefficient de X^{d-1} dans $P_{\min,x}(X)$. Comme x est séparable, P est à racines simples, et ses racines sont les $\sigma(x)$ avec $\sigma \in \mathrm{Hom}_K(E, L)$. On a donc $\mathrm{Tr}(m_x : E \to E) = \sum_{\sigma \in \mathrm{Hom}_K(E,L)} \sigma(x)$.

Si on écrit $F = E \cdot f_1 \oplus \cdots E \cdot f_r$ alors chaque $E \cdot f_i$ est stable par m_x et donc $\mathrm{Tr}(m_x : F \to F) = r \cdot \mathrm{Tr}(m_x : E \to E)$. Comme F/K est séparable, chaque $\sigma \in \mathrm{Hom}_K(E, L)$ s'étend, par le théorème 2.27, en r plongements K-linéaires distincts de F dans L. On a donc $\sum_{\tau \in \mathrm{Hom}_K(F,L)} \tau(x) = r \cdot \sum_{\sigma \in \mathrm{Hom}_K(E,L)} \sigma(x)$. La formule pour la trace en découle, et la démonstration pour la norme est la même. □

Si F/K est une extension galoisienne, on a donc $\mathrm{Tr}_{F/K}(x) = \sum_{g \in \mathrm{Gal}(F/K)} g(x)$ et $\mathrm{N}_{F/K}(x) = \prod_{g \in \mathrm{Gal}(F/K)} g(x)$.

Proposition 3.25. — *Si F/K n'est pas séparable, alors $\mathrm{Tr}_{F/K}(x) = 0$ pour tout $x \in F$.*

Démonstration. — Comme dans la démonstration de la proposition 3.24, on pose $E = K(x)$ et alors $\mathrm{Tr}_{F/K}(x) = [F : E] \cdot \mathrm{Tr}(m_x : E \to E)$. Soit p la caractéristique de K.

Soit $x \in F$ qui n'est pas séparable sur K. Comme avant, $\mathrm{Tr}(m_x : E \to E)$ est moins le coefficient de X^{d-1} dans $P_{\min,x}(X)$. Or, par le lemme 2.26, celui-ci est de la forme $Q(X^p)$ et donc $\mathrm{Tr}(m_x : E \to E) = 0$, ce qui fait que $\mathrm{Tr}_{F/K}(x) = 0$.

Si $x \in F$ est séparable sur K, alors $\mathrm{Tr}_{F/K}(x) = [F : E] \cdot \mathrm{Tr}(m_x : E \to E)$. Comme F/E n'est pas séparable, son degré est divisible par p (si $y \in F$ n'est pas séparable sur E, alors $P_{\min,y}(X) = Q(X^p)$ et donc $[F : E]$ est divisible par p) et donc $\mathrm{Tr}_{F/K}(x) = 0$. □

La trace permet de définir une forme K-bilinéaire $\langle \cdot, \cdot \rangle : F \times F \to K$, par la formule $\langle x, y \rangle = \mathrm{Tr}_{F/K}(xy)$.

Proposition 3.26. — *La forme bilinéaire donnée par la trace est non dégénérée si et seulement si F/K est séparable.*

Démonstration. — La proposition 3.25 implique que si F/K n'est pas séparable, alors $\langle \cdot, \cdot \rangle$ est en fait nul.

Supposons que K est de caractéristique 0. Si $x \in F^\times$, alors $\langle x, 1/x \rangle = [F : K] \neq 0$ et donc la forme est non dégénérée. Si F/K est séparable mais K est de caractéristique $\neq 0$, cet argument ne marche plus nécéssairement. Soit x un élément primitif pour F, et $M = (\sigma(x^i))_{\sigma,i}$. Comme les $\sigma(x)$ sont distincts, $\det(M) \neq 0$. La matrice de $\langle \cdot, \cdot \rangle$ dans la base $1, x, \ldots, x^{d-1}$ est $M \cdot {}^tM$ et elle est donc non singulière. □

Proposition 3.27. — *Si $F/E/K$ est une tour, alors* $\mathrm{Tr}_{F/K} = \mathrm{Tr}_{E/K} \circ \mathrm{Tr}_{F/E}$.

Démonstration. — Écrivons $F = \oplus E \cdot f_i$ et $E = \oplus K \cdot e_k$, de sorte que $F = \oplus K \cdot f_i e_k$. Si $x \in F$, alors $x f_i = \sum_j x_{ij} f_j$ avec $x_{ij} \in E$ et $x_{ij} e_k = \sum_\ell x_{ij,k\ell} e_\ell$ avec $x_{ij,k\ell} \in K$ de sorte que $x f_i e_k = \sum_{j,\ell} x_{ij,k\ell} f_j e_\ell$.

On a alors $\mathrm{Tr}_{F/E}(x) = \sum_i x_{ii}$ et $\mathrm{Tr}_{E/K}(x_{ii}) = \sum_k x_{ii,kk}$ et $\mathrm{Tr}_{F/K}(x) = \sum_{i,k} x_{ii,kk}$. □

La même idée permet de montrer que $\mathrm{N}_{F/K} = \mathrm{N}_{E/K} \circ \mathrm{N}_{F/E}$. Étendre les scalaires et choisir une base de F sur E dans laquelle $\mathrm{Mat}(m_x)$ est triangulaire supérieure. Les $m_{x_{ii}}$ commutent et sont donc cotrigonalisables, dans une base de E sur K. On a alors $\mathrm{N}_{F/E}(x) = \prod_i x_{ii}$ et $\mathrm{N}_{E/K}(x_{ii}) = \prod_k x_{ii,kk}$ et $\mathrm{N}_{F/K}(x) = \prod_{i,k} x_{ii,kk}$.

Laurent Berger, UMPA, ENS de Lyon, UMR 5669 du CNRS
E-mail : laurent.berger@ens-lyon.fr • *Url :* http://perso.ens-lyon.fr/laurent.berger/