TD n°6.

Un corps est dit parfait si $Car(k) = 0$ ou si $p := Car(k) > 0$ et $\mathrm{Frob}_p : K \to K$ est surjectif ($\mathrm{Frob}_p(x) = x^p$).

1 Extensions transcendantes

Exercice 1. Soit k un corps et $K = k(X)$ le corps des fractions rationnelles.

a) Soit $F \in K\backslash k$. On écrit $F = \frac{P(X)}{Q(X)}$, avec $P, Q \in k[X]$ premiers entre eux.

i) Montrer que X est algébrique sur $k(F)$ (on pourra considérer $R(T) := P(T) - F(X)Q(T) \in k(F)[T]$).

ii) En déduire que F est transcendant sur k.

iii) Montrer que $[K : k(F)] = \max(\deg(P), \deg(Q))$ (on pourra montrer que $R(T)$ est irréductible dans $k[F][T]$).

b) Soit $\phi : \mathrm{GL}_2(k) \to \mathrm{Aut}_k(K)$ le morphisme de groupe défini par

$$\phi\begin{pmatrix} a & b \\ c & d \end{pmatrix}(R) = R\left(\frac{aX+b}{cX+d}\right).$$

Montrer que ϕ est surjectif, et que $\ker(\phi) = k^\times$.

Solution. a) i) Evaluons $R \in k(F)[T] \subset k(X)[T]$ en X : $R(X) = P(X) - F(X)Q(X) = 0$ donc R est un polynôme annulateur non nulde X dans $k(F)[T]$, donc X est algébrique sur $k(F)$. De plus $[k(X) : k(F)] \leq \deg(R) = \max(\deg(P), \deg(Q))$.

ii) Si F est algébrique sur k, $[k(F) : k]$ est fini. Or $[k(X) : k(F)]$ est fini donc par transitivité des degrés, $[k(X) : k]$ est fini, ce qui est absurde.

iii) On a déjà l'inégalité $[k(X) : k(F)] \leq \deg(R) = \max(\deg(P), \deg(Q))$. Pour avoir l'égalité il suffit de montrer que $R \in k(F)[T]$ est le polynôme minimal de X, ou de manière équivalente, que $R \in k(F)[T]$ est irréductible. Comme F est transcendant sur k, $k[F]$ est un anneau de polynôme à une variable (en l'occurrence F) sur k, c'est donc un anneau principal, et a fortiori factoriel. Il suffit alors de montrer que R est irréductible dans $k[F][T] \simeq k[T][F]$. Or vu comme polynôme en F à coefficient dans $k[T]$, R est de degré 1 en F, donc est irréductible dans $k(T)[F]$. De plus $\mathrm{pgcd}(P, Q) = 1$, donc R est primitif en tant que pôlynôme de $k[T][F]$, donc R est irréductible dans $k[T][F] \simeq k[F][T$, donc dans $k(F)[T]$. D'où le résultat.

b) Soit ϕ in $\mathrm{Aut}_k(K)$, et $F = \phi(X)$. Alors si $R(X) = \frac{P(X)}{Q(X)}$, $\phi(R) = R(F)$. Il suffit donc de montrer que F est de la forme $\frac{aX+b}{cX+d}$. (Remarquons que si $F \in K$, pour que $R \to R(F)$ définissent bien un morphisme de corps, il faut et il suffit que si $Q \neq 0 \in k[X]$, $Q(F) \neq 0$, c'est-à-dire F n'est pas algébrique sur k. D'après a)ii), c'est toujours le cas si F n'est pas constant).
Ecrivons $F = \frac{P}{Q}$ avec P et Q premiers entre eux. Comme $k(F)$ est l'image de ϕ, par bijectivité de ϕ, $k(F) = K$. D'après a)iii),on a donc $\max(\deg(P), \deg(Q)) = 1$, donc P est de la forme $aX + b$ et Q de la forme $cX + d$. Comme F n'est pas une fraction rationnelle constante, (a, b) et $(c, d$ ne sont pas colinéaire, et la matrice de l'énoncé est bien dans $\mathrm{GL}_2(k)$.

2 Caractéristique non nulle

Exercice 2. Algorithme de Berlekamp

a) Soit A une $\mathbb{F}_p$-algèbre. Montrer que $\mathrm{Frob}_p : A \to A$ définie par $f(x) = x^p$ est $\mathbb{F}_p$-linéaire.

b) Montrer que si A est un corps, alors $E := \ker(\mathrm{Frob}_p - \mathrm{Id}_A)$ est un sous-$\mathbb{F}_p$-espace vectoriel de A de dimension 1.

c) Montrer que si $A = K_1 \times \cdots K_n$ est un produit de n corps, alors $E := \ker(\mathrm{Frob}_p - \mathrm{Id}_A)$ est un sous-$\mathbb{F}_p$-espace vectoriel de A de dimension n.

d) Soit $P \in \mathbb{F}_p[X]$ tel que $\mathrm{pgcd}(P, P') = 1$. On pose $A = \mathbb{F}_p[X]/(P)$. Montrer que $E := \ker(\mathrm{Frob}_p - \mathrm{Id}_A)$ est un sous-espace vectoriel de A de dimension le nombre de facteurs irréductibles de P.

Solution. a) Si $a, b \in \mathbb{F}_p$, alors $\mathrm{Frob}_p(ax+by) = \sum_{k=0}^{p} \binom{p}{k} a^k x^k b^{p-k} y^{p-k} = a^p x^p + b^p y^p$ car les coefficients binomiaux pour $k \neq 0, p$ sont divisibles par p. Or $a^p = a$ et $b^p = b$ d'après le petit théorème de Fermat, donc Frob_p est bien $\mathbb{F}_p$ linéaire.

b) E est l'ensemble des racines de $X^p - X$. Comme A est un corps, il y a au plus p telles racines. Les éléments de $\mathbb{F}_p \subset A$ sont de telles racines, et donc $E = \mathbb{F}_p$ est bien un $\mathbb{F}_p$-espace vectoriel de dimension 1.

c) $(x_1, \cdots, x_n) \in E$ si et seulement si $x_i^p = x_i$ pour tout i, si et seulement si $x_i \in \mathbb{F}_p$ d'après la question précédente. Donc $E = \mathbb{F}_p \times \cdots \times \mathbb{F}_p$ est de dimension n.

d) Comme $\mathrm{pgcd}(P, P') = 1$, les facteurs irréductibles de P apparaissent avec multiplicité 1 dans la factorisation de P. Donc $P = Q_1 \cdots Q_n$ où les Q_i sont tous distincts. Le théorème des restes chinois affirme que $A = \prod_i \mathbb{F}_p[X]/Q_i$ et $K_i = \mathbb{F}_p[X]/Q_i$ est un corps puisque Q_i est irréductible. La question précédente nous dit donc que E est de dimension n sur $\mathbb{F}_p$.

Exercice 3. Soit p un nombre premier et $a \in \mathbb{F}_p$. Soit $P = X^p - X - a \in \mathbb{F}_p[X]$.

a) Si $a = 0$, donner la décomposition en facteur irréductible de P. On suppose dorénavant $a \neq 0$.

b) Montrer que $P(X+1) = P(X)$.

c) Soit Q un facteur irréductible de P. Montrer que $Q(X+1)$ est aussi un facteur irréductible de P.

d) Montrer que $Q(X+1) = Q(X)$ (on pourra considérer une action de $\mathbb{Z}/p\mathbb{Z}$ sur l'ensemble des facteurs irréductibles de P).

e) Montrer que si $R \in \mathbb{F}_p[X]$ est de degré $\leq p-1$ et $R(X+1) = R(X)$, alors R est un polynôme constant.

f) En déduire que P est irréductible.

g) Soit $b \in \mathbb{Z}$ premier à p. Montrer que $X^p - X - b$ est un polynôme irréductible de $\mathbb{Q}[X]$.

Solution. a) Si $x \in \mathbb{F}_p$, $P(x) = 0$ donc $rod_{x \in \mathbb{F}_p}(X - x)$ divise P, et comme les deux polynômes sont de même degré et de même coefficient dominant, ils sont égaux.

b) $P(X+1) = (X+1)^p - (X+1) - a = X^p + 1 - X - 1 - a = X^p - X - a$.

c) L'application $\mathbb{F}_p[X] \to \mathbb{F}_p[X]$ qui à R associe $R(X+1)$ est un isomorphisme d'anneaux, donc préserve l'irréductibilité et la relation de divisibilité. Donc $Q(X+1)$ est irréductible et $Q(X+1)$ divise $P(X+1) = P$, comme voulu.

d) On considère l'action $k.Q \mapsto Q(X+k)$. Le stabilisateur de Q est un sous-groupe de $\mathbb{Z}/p\mathbb{Z}$, c'est donc soit $\mathbb{Z}/p\mathbb{Z}$ (auquel cas $Q(X+1) = Q$ comme voulu), soit $\{0\}$. Si le stabilisateur est $\{0\}$, alors l'orbite de Q est de cardinal p. Or comme P est de degré p, s'il a au moins p facteurs irréductibles, ils doivent être de degré 1, et donc P devrait avoir une racine. Or si $x \in \mathbb{F}_p$, $P(x) = -a \neq 0$. Contradiction.

e) Soit z une racine de R dans une extensions K de $\mathbb{F}_p$. Alors $(z+a)_{a \in \mathbb{F}_p}$ est une famille de p racines distinctes de R, ce qui contredit $\deg R < p-1$.

f) Si Q est un facteur irréductible de P, alors $Q(X+1) = Q(X)$ d'après d), donc $\deg Q \geq p$ d'après e, ce qui prouve que P est irréductible.

g) Si $P = X^p - X - b$ était réductible, son image $\bar{P}$ dans $\mathbb{F}_p[X]$ par réduction modulo p serait aussi réductible puisque P est unitaire, ce qui est en contradiction avec f). Donc P est irréductible dans $\mathbb{Z}[X]$ donc dans $\mathbb{Q}[X]$

Exercice 4. Soient X et Y deux indéterminées et p un nombre premier. On pose

$$K = \mathbb{F}_p(X^p, Y^p) \quad \text{et} \quad L = \mathbb{F}_p(X, Y).$$

(ı) Montrer que L est une extension finie de K de degré p^2.
(ıı) Montrer qu'il n'existe pas d'élément $\theta \in L$ tel que $L = K(\theta)$.

Solution. (ı) L'élément X est algébrique sur K de degré p. En effet, considérons le polynôme $F = T^p - X^p \in K[T]$. On a $F = (T-X)^p$, de sorte que X est la seule racine de F dans une clôture algébrique de K. Puisque X n'appartient pas à K, l'élément X^p n'est pas une puissance p-ième dans K. D'après l'exercice **??**, F est donc irréductible sur K, et est ainsi le polynôme minimal de X sur K. De même, Y est algébrique sur $K(X)$ de degré p, comme on le constate en considérant le polynôme $T^p - Y^p \in K(X)[T]$ qui est irréductible sur $K(X)$. Compte tenu du fait que l'on a $L = K(X, Y)$, on en déduit le résultat.
(ıı) Supposons qu'il existe $\theta \in L$ tel que $L = K(\theta)$. Il existe des éléments F et G dans $\mathbb{F}_p[X, Y]$ tels que l'on ait

$$\theta = \frac{F(X, Y)}{G(X, Y)}.$$

Puisque L est de caractéristique p, on a

$$\theta^p = \frac{F(X^p, Y^p)}{G(X^p, Y^p)},$$

et donc θ^p appartient à K. On en déduit que le degré de θ sur K est au plus p, ce qui contredit le fait que L/K soit de degré p^2. D'où le résultat.

Exercice 5. Soient K un corps , $F = X^3 - 3X - 1 \in K[X]$ et α une racine de F dans une clôture algébrique de K. Montrer que $K(\alpha)$ est une extension séparable de K.

Solution. Supposons la caractéristique de K différente de 3. Le polynôme dérivé de F, qui est $3(X^2 - 1)$, est premier avec F, ce qui montre que F est séparable dans ce cas et donc que α est séparable sur K. Si la caractéristique de K vaut 3, on a $F = (X - 1)^3$, d'où $\alpha = 1$ puis $K(\alpha) = K$.

Exercice 6. Soient K un corps de caractéristique un nombre premier p et f un polynôme irréductible sur K. Montrer que f n'est pas séparable si et seulement si il existe g dans $K[X]$ tel que $f(X) = g(X^p)$.

Solution. Si f est de la forme $g(X^p)$, le polynôme dérivé de f est nul, donc f est inséparable. Inversement, supposons f inséparable. Posons $f = \sum_{i=0}^{n} a_i X^i$. On a

$$f' = \sum_{i=1}^{n} i a_i X^{i-1}.$$

D'après l'hypothèse faite, on a $f' = 0$, d'où $ia_i = 0$ pour $i = 1, \cdots, n$. Si a_i n'est pas nul, i est donc divisible par p, ce qui entraîne le résultat.

Exercice 7. Soient K un corps de caractéristique un nombre premier p et L une extension finie de K de degré non divisible par p. Montrer que L est séparable sur K.

Solution. Soient α un élément de L et F son polynôme minimal sur K. Il s'agit de montrer que F est séparable. Dans le cas contraire, F étant irréductible, il existe $G \in K[X]$ tel que $F(X) = G(X^p)$ (exercice 6). Il en résulte que le degré de F est multiple de p, par suite p divise le degré de L sur K. D'où une contradiction et le résultat.

Exercice 8. Soient $K = \mathbb{F}_p(X)$ et $P = T^p - X \in K[T]$. Montrer que P n'est pas séparable.

Solution. On a $P' = 0$. P est irréductible dans $k[X]$. En effet, si $P = P_1 \cdot P_2$, alors $P_1(0)P_2(0) = X$, donc $P_1(0) = X$, par exemple. Mais, si α est une racine de P, alors dans $K(\alpha)$, on a $P = t^p - \alpha^p = (t - \alpha)^p$. Donc $P_1 = (t - \alpha)^n$ et $X = \alpha^n = \alpha^p$, donc $p = n$ et $P_1 = P$. P est irréductible dans $k[X]$ donc aussi dans $k(X)$ (lemme de Gauss) et donc non séparable.

Exercice 9. Soit k un corps, $P \in k[X]$ un polynôme irréductible et L une extension finie de k. Soit Ω une extension algébriquement close de k.

a) Montrer que P est séparable si et seulement si $\Omega \otimes_k k[X]/(P)$ est un anneau réduit.

b) Montrer que L est une extension séparable de k si et seulement si $\Omega \otimes_k L$ est un anneau réduit.

Exercice 10. Montrer que $K = \mathbb{F}_p(X)$ n'est pas un corps parfait.

Solution. Comme $A = \mathbb{F}_p[X]$ est factoriel (même principal),$K = \mathrm{Frac}(A)$ et X est irréductible, le polynôme $T^p - X$ est irréductible dans $K[T]$, donc n'a pas de racine. Donc X n'est pas dans l'image du frobenius.

Exercice 11. Soit K un corps parfait et $P \in K[X]$. Montrer que si P est irréductible, alors $\mathrm{pgcd}(P, P') = 1$. Soit K un corps qui n'est pas parfait. Montrer qu'il existe un polynôme irréductible $P \in K[X]$ irréductible tel que $P' = 0$.

Solution. Si $P' \neq 0$, alors $\deg \mathrm{pgcd}(P, P') \leq \deg P' < \deg P$, et $\mathrm{pgcd}(P, P')|P$, donc si P est irréductible $\mathrm{pgcd}(P, P') = 1$. Il suffit donc de montrer que $P' \neq 0$ (ce qui est évident si $p := carK = 0$, on suppose dorénavant $p \neq 0$). Supposons $P' = 0$ et écrivons $P = \sum_k a_k X^k$. Alors $P' = \sum_k k a_k X^{k-1} = 0$ donc $a_k = 0$ si k n'est pas divisible par p. Donc $P = \sum_j a_{pj} X^{pj}$. Comme K est supposé parfait, il existe b_j tel que $b_j^p = a_p j$. Alors $P = \sum_j (b_j X^j)^p = (\sum_j b_j X^j)^p$, ce qui contredit l'irréductibilité de P.

Exercice 12. Soit K un corps parfait de caractéristique $p > 0$ et K' une extension finie de K.

a) Soient $(x_i)_i$ une base du K-espace vectoriel K' et $f : K' \to K'$ l'unique application K-linéaire telle que $f(x_i) = x_i^p$ pour tout i. Montrer que f est injective.

b) En déduire que K' est parfait.

c) on ne suppose plus K'/K finie, mais seulement algébrique. Montrer que K' est parfait.

Solution. a) Soit $y = \sum_i a_i x_i \in \ker f$ avec $a_i \in K$. Comme K est parfait, soit $b_i \in K$ tel que $b_i^p = a_i$. Alors $0 = f(y) = (\sum_i b_i x_i)^p$, donc comme (x_i) est une famille libre, pour tout i, $b_i = 0$, donc $a_i = 0$, donc $y = 0$.

b) Soit $y \in K'$. Comme K' est de dimension finie sur K, l'injectvité de f implique sa surjectivité. Il existe donc $z = \sum_i a_i x_i$ avec $a_i \in K$ tel que $f(z) = y$. Comme K est parfait, il existe $b_i \in K$ tel que $b_i^p = a_i$. On a alors $y = (\sum_i b_i x_i)^p$, ce qui prouve que K' est parfait.

c) Soit $y \in K'$. Alors $K(y)$ est une extension finie de K, donc $K(y)$ est parfait d'après 2. Il existe donc $z \in K(y) \subset K'$ tel que $z^p = y$, ce qui montre que K' est parfait.

Exercice 13. Soit K un corps de caractéristique $p > 0$.

a) Montrer qu'il existe une extension K' de K tel que K soit un corps parfait (on pourra prendre pour K' une clôture algébrique de K) .

b) On note $K^{\mathrm{pf}} = \{x \in K' : \exists n \in \mathbb{N}, x^{p^n} \in K\}$. Montrer que K^{pf} est un sous-corps parfait de K' contenant K.

c) Montrer que K^{pf} vérifie la propriété universelle suivante : pour toute extension L de K telle que L soit un corps parfait, il existe un unique morphisme de K-algèbres $K^{\mathrm{pf}} \to L$.

Solution. a) Soit K' une clôture algébrique de K. Soit $x \in K'$. Comme K' est algébriquement clos, le polynôme $X^p - x$ admet une racine, et donc x est dans l'image du frobenius. Donc K' est parfait.

b) Si $x, y \in K^{\mathrm{pf}}$, il existe n, m tels que $x^{p^n}, y^{p^m} \in K$. On peut supposer $n = m$ quitte à les remplacer par le maximum des deux. Alors $(x-y)^{p^n} = x^{p^n} - y^{p^n} \in K$ et si $y \neq 0$, $(x/y)^{p^n} = x^{p^n}/y^{p^n} \in K$, donc K^{pf} est un sous-corps de K'. De plus si $x \in K$, $x^{p^0} = x \in K$ donc K^{pf} contient K.

Enfin, si $x \in K^{\mathrm{pf}}$, soit n tel que $x^{p^n} \in K$. Comme K' est parfait il existe $y \in K'$ tel que $y^p = x$. Alors $y^{p^{n+1}} = x^{p^n} \in K$ donc $y \in K^{\mathrm{pf}}$, ce qui montre que K^{pf} est parfait.

c) Soit L comme dans l'énoncé. Soit $x \in K^{\mathrm{pf}}$. Il existe n tel que $x^{p^n} \in K \subset L$. Comme L est parfait le polynôme $X^{p^n} - x^{p^n}$ admet une racine y, unique par injectivité du frobenius.

Soit f un morphisme de K-algèbres $K^{\mathrm{pf}} \to L$. Alors $f(x)^{p^n} = f(x^{p^n}) = y^{p^n}$, donc par injectivité du frobenius, $f(x) = y$, ce qui montre l'unicité de f.

Réciproquement, posons $f(x) = y$ (ceci ne dépend pas du choix de n). Si $x_1, x_2 \in K^{\mathrm{pf}}$, il existe n tels que $x_1^{p^n}, x_2^{p^n} \in K$. Alors $(f(x_1) + f(x_2))^{p^n} = f(x_1)^{p^n} + f(x^2)^{p^n} = x_1^{p^n} + x_2^{p^n} = (x_1 + x_2)^{p^n} = f(x_1 + x_2)^{p^n}$, et donc par injectivité du frobenius f est additive. La multiplicativité de f se prouve de la même façon.

3 Extensions galoisiennes

Exercice 14. Soit $n \in \mathbb{N}^*$. Soit $\Phi_n = \prod_{k \in (\mathbb{Z}/n\mathbb{Z})^*} (X - e^{2i\pi k/n}) \in \mathbb{C}[X]$.

a) Montrer que $X^n - 1 = \prod_{d|n} \Phi_d$. En déduire que $\Phi_n \in \mathbb{Z}[X]$.

b) Soit ζ une racine primitive n^{e}de 1 et p un nombre premier premier à n. Soit f et g les polynômes minimaux unitaire sur $\mathbb{Q}$ de ζ et $\zeta' = \zeta^p$. On suppose $f \neq g$.

i) Montrer que $fg | \Phi_n$ et $f | g(X^p)$.

ii) Montrer que l'image de Φ_n dans $\mathbb{F}_p[X]$ a un facteur irréductible ayant multiplicité au moins deux, et en déduire une contradiction.

c) En déduire que Φ_n est un polynôme irréductible.

d) Montrer que $\mathbb{Q}(e^{2i\pi/n})$ est une extension galoisienne de $\mathbb{Q}$ et décrire son groupe de Galois.

e) Soit K une extension finie de $\mathbb{Q}$. Montrer que K ne contient qu'un nombre fini de racines de 1.

Solution. a) Soit μ_∞ le groupe multiplicatif des racines de 1, $\mu^{(n)}$ l'ensemble des éléments de μ_∞ dont l'ordre multiplicatif est n, et μ_n l'ensemble des racines n^{es}de 1 (c'est-à-dire dont l'ordre multiplicatif divise n). Alors $X^n - 1 = \prod_{\zeta \in \mu_n} (X - \zeta)$ et $\Phi_n = \prod_{\zeta \in \mu^{(n)}} (X - \zeta)$. Or μ_n est l'union disjointe des $\mathfrak{m}^{(d)}$ pour d divisant n, donc

$$X^n - 1 = \prod_{\zeta \in \mu_n} (X - \zeta) = \prod_{d|n} \prod_{\zeta \in \mu^{(d)}} (X - \zeta) = \prod_{d|n} \Phi_d.$$

Φ_n est le quotient de $X^n - 1 \in \mathbb{Z}[X]$ par $\prod_{d|n, d \neq n} \Phi_d$, qui par récurrence est un polynôme unitaire de $\mathbb{Z}[X]$, donc la division euclidienne par un polynôme unitaire, nous dit que Φ_n est à coefficient s dans $\mathbb{Z}$.

b) i) Comme $\Phi_n(\zeta)=0$, $f|\Phi_n$, de même $g|\Phi_n$. Or, en tant que polynômes minimaux, f et g sont irréductibles, donc l'hypothèse $f\neq g$ implique qu'ils sont premiers entre eux. Donc $fg|\Phi_n$.

De même, $g(\zeta^p)=0$, donc ζ est une racine de $g(X^p)$ donc $f|g(X^p)$.

ii) Soit h un facteur irréductible de $\bar{f}$. Donc $h|\bar{f}|\bar{g}(X^p)=\bar{g}^p$. Comme h est irréductible, $h|g$. Donc $h^2|fg|\Phi_n|X^n-1$. Donc $h|\operatorname{pgcd}(X^n-1,nX^{n-1})=1$ car n est premier à p. Contradiction.

c) Soit k premier à n, et soit $k=\prod_i p_i^{\alpha_i}$. En appliquant b) $\sum_i \alpha_i$ fois, on en déduit que $e^{2i\pi k/n}$ est racine du polynôme minimal f de $e^{2i\pi/n}$. Donc $\Phi_n|f$ et donc Φ_n est bien irréductible.

d) Si x est un conjugué de $\zeta=e^{2i\pi/n}$, alors x est une racine de Φ_n, donc de la forme $e^{2i\pi k/n}=\zeta^k\in\mathbb{Q}(\zeta)$. Donc $\mathbb{Q}(\zeta)$ contient tous les conjugués de ζ donc est une extension normale de $\mathbb{Q}$. Comme on est en caractéristique 0, c'est une extension galoisienne.

Soit $G=\operatorname{Gal}(\mathbb{Q}(\zeta)/\mathbb{Q})$. D'après la question précédente, les conjugués de ζ sont exactement les ζ^k avec $k\in(\mathbb{Z}/n\mathbb{Z})^\times$. Il existe donc $g_k\in G$ tel que $g(\zeta)=\zeta^k$, unique puisque $\mathbb{Q}(\zeta)$ est engendrée par ζ. Donc $G=\{g_k\}_{k\in(\mathbb{Z}/n\mathbb{Z})^\times}$. Décrivons la loi de groupe de G. On a $g_kg_{k'}(\zeta)=g_k(\zeta^{k'})=g_k(\zeta)^{k'}=\zeta^{kk'}$. Donc la bijection $(\mathbb{Z}/n\mathbb{Z})^\times\to G$ qui envoie k sur g_k est un isomorphisme de groupe. Donc $G\simeq(\mathbb{Z}/n\mathbb{Z})^\times$.

Exercice 15. Soit a un entier sans facteur carré, différent de $0,1$ et -1. Soit p un nombre premier. Soit K un corps de décomposition de X^p-a sur $\mathbb{Q}$. Calculer $[K:\mathbb{Q}]$.
Soit $G=\operatorname{Gal}(K/\mathbb{Q})$. Montrer que G a un sous-groupe distingué H isomorphe à $\mathbb{Z}/p\mathbb{Z}$ tel que G/H soit isomorphe à $(\mathbb{Z}/p\mathbb{Z})^*$.

Solution. Le polynôme X^p-a est irréductible d'après le critère d'eisenstein, donc si α est une racine p^{e}de a, $\mathbb{Q}(\alpha)/\mathbb{Q}$ est une extension de degré p.
Soit $\zeta=e^{2i\pi/p}$. Alors les conjugués de α sont les $\alpha_k=\zeta^k\alpha$, avec $k\in\mathbb{Z}/p\mathbb{Z}$. Donc $\zeta=\alpha_1/\alpha_0\in K=\mathbb{Q}(\alpha_0,\cdots,\alpha_{p-1})$. Réciproquement $\alpha_k\in\mathbb{Q}(\alpha,\zeta)$, donc $K=\mathbb{Q}(\alpha,\zeta)$.
Or $[\mathbb{Q}(\zeta):\mathbb{Q}]=p-1$ est premier à $p=[\mathbb{Q}(\alpha):\mathbb{Q}]$ donc $[K:\mathbb{Q}]=[\mathbb{Q}(\zeta):\mathbb{Q}][\mathbb{Q}(\alpha):\mathbb{Q}]=p(p-1)$.
Comme $\mathbb{Q}(\zeta)/\mathbb{Q}$ est une extension galoisienne de groupe de Galois $N=(\mathbb{Z}/p\mathbb{Z})^\times$, $N=G/H$ où $H=\operatorname{Gal}(K:\mathbb{Q}(\zeta))$. Comme $[\mathbb{Q}(\zeta)(\alpha):\mathbb{Q}(\zeta)]=[\mathbb{Q}(\alpha):\mathbb{Q}]$, X^p-a est encore le polynôme minimal de α dans $\mathbb{Q}(\zeta)[X]$, donc les conjugués de α sont les α_k. Comme dans l'exercice précédent, il existe un unique $h_k\in H$ tel que $h_k(\alpha)=\alpha_k$ et l'application $\phi:\mathbb{Z}/p\mathbb{Z}\to H$ qui envoie k sur h_k est donc bijective. Or $h_{k'}h_k(\alpha)=h_{k'}(\zeta^k\alpha)=\zeta^kh_{k'}(\alpha)=\zeta^{k+k'}\alpha$, ce qui prouve que ϕ est un isomorphisme de groupe.

Exercice 16. Soit $K=\mathbb{Q}(\sqrt{2},\sqrt{3},\sqrt{5})$. Montrer que K est une extension galoisienne de $\mathbb{Q}$ et décrire son groupe de Galois.

Solution. Comme les conjugués de $\sqrt{d}$ sont $\pm\sqrt(d)$ (si d n'est pas un carré), K contient les conjugués de $\sqrt{2},\sqrt{3}$ et $\sqrt{5}$ donc est galoisienne.
$\mathbb{Q}(\sqrt(d))/\mathbb{Q}$ est une extension galoisienne de groupe de Galois $G_d=\{1,\sigma_d\}$ où $\sigma(a+b\sqrt{d})=a-b\sqrt{d}$.
Si $\sqrt(3)\in\mathbb{Q}(\sqrt(2)$, on aurait $\sigma_2(\sqrt{3})=\pm\sqrt{3}$, et donc $\sqrt{3}\in\mathbb{Q}$ ou $\in\mathbb{Q}\sqrt{2}$, ce qui n'est pas possible. Donc $[\mathbb{Q}(\sqrt{3},\sqrt{2}):\mathbb{Q}]=4$ et a pour groupe de galois $G_2\times G_3\simeq\{\pm1\}^2$ où $(e,f)(a+b\sqrt{2}+c\sqrt{3}+d\sqrt{6})=a+be\sqrt{2}+cf\sqrt{3}+def\sqrt{6}$ si $e,f\in\{\pm1\}$.
Si $\sqrt{5}\in\mathbb{Q}(\sqrt{3},\sqrt{2})$, on aurait un morphisme de groupe (surjectif) $\chi:G_2\times G_3\to\mathbb{Z}/2\mathbb{Z}$ tel que $\sigma(\sqrt{5})=(-1)^{\chi(\sigma)}\sqrt{5}$. Or $\{x\in\mathbb{Q}(\sqrt{3},\sqrt{2}),\sigma(x)=(-1)^{\chi(\sigma)}x\}=\sqrt{2^{\chi(\sigma_2)}3^{\chi(\sigma_3)}}\mathbb{Q}$ et donc $5\in 2^{\chi(\sigma_2)}3^{\chi(\sigma_3)}(\mathbb{Q}^\times)^2$, ce qui n'est pas possible d'après l'unicité de la factorisation en facteurs premiers.
Donc $\mathbb{Q}(\sqrt{5},\sqrt{3},\sqrt{2})$ est une extension galoisienne de degré 8 de $\mathbb{Q}$, et son groupe de Galois est $(\mathbb{Z}/2\mathbb{Z})^3$.

Exercice 17. Soient $p_1,\cdots,p_n$ des nombres premiers distincts deux à deux. Montrer que $\mathbb{Q}(\sqrt{p_1},\cdots,\sqrt{p_n})$ est une extension galoisienne de $\mathbb{Q}$ et décrire son groupe de Galois.

Solution. $K:=\mathbb{Q}(\sqrt{p_1},\cdots,\sqrt{p_n})$ est le corps de décomposition de $\prod_i(X^2-p_i)$ sur $\mathbb{Q}$, c'est donc une extension normale. Comme on est en caractéristique 0 l'extension est forcément séparable. Donc K est bien une extension galoisienne de $\mathbb{Q}$.
Comme dans l'exercice précédent, on a un morphisme $f:\operatorname{Gal}(K/\mathbb{Q})\to\{\pm1\}^n$ qui à ϕ associe $(\frac{\phi(\sqrt{p_i})}{\sqrt{p_i}})_i$ (on a $\phi(\sqrt{p_i})$ qui doit être conjugué de $\sqrt{p_i}$, donc de la forme $\pm\sqrt{p_i}$). Ce morphisme est injectif. En effet si $\phi\in\operatorname{Ker}(f)$, $\phi(\sqrt{p_i})=\sqrt{p_i}$ pour tout i ; comme K est engendré par les $\sqrt{p_i}$, ϕ est l'identité. Pour la surjectivité, il suffit de comparer les cardinaux des deux groupes : il suffit de montrer que $[K:\mathbb{Q}]=2^n$.
On raisonne par récurrence en supposant que $[K':\mathbb{Q}]=2^{n-1}$ (on a posé $K'=\mathbb{Q}(\sqrt{p_1},\cdots,\sqrt{p_{n-1}})$). En particulier le morphisme $f':\operatorname{Gal}(K'/\mathbb{Q})\to\{\pm1\}^{n-1}$ (défini de la même façon que pour K) est bijectif. Par transitivité des degrés, il suffit de montrer que $[K=K'(\sqrt{p_n}):K']=2$. Comme $X^2-p_n\in K'[X]$ annule $\sqrt{p_n}$ et est de degré 2, $[K:K']\leq 2$. Il suffit donc de montrer que $\sqrt{p_n}\notin K'$. Supposons par l'absurde que $p_n=a^2$ avec

$a \in K'$. Alors si $\phi \in \mathrm{Gal}(K'/\mathbb{Q})$, $\phi(a) = \pm a$. Pour $i \leq n-1$, notons $\phi_i \in \mathrm{Gal}(K'/\mathbb{Q})$ l'unique automorphisme tel que, pour $k \leq n-1$, $\phi_i(\sqrt{p_k}) = 1$ si $k \neq i$ et $\phi_i(\sqrt{p_k}) = -1$ (l'existence et l'unicité découlent de la bijectivité de f'). Notons $I = \{i \leq n-1, \phi_i(a) = -a\}$. Alors $a \in \bigcap_{i\in I} \mathrm{Ker}(\phi_i + \mathrm{Id}) \cap \bigcap_{i\notin I} \mathrm{Ker}(\phi_i - \mathrm{Id}) = \sqrt{\prod_{i\in I} p_i}\mathbb{Q}$. Donc $\frac{\prod_{i\in I} p_i}{p_n}$ est un carré dans $\mathbb{Z}$, ce qui n'est pas possible (il suffit de regarder la valuation p_n-adique).

Exercice 18. Soient f un polynôme irréductible de $\mathbb{Q}[X]$ et K le corps de décomposition de f dans $\mathbb{C}$. On suppose que le groupe de Galois de K sur $\mathbb{Q}$ est abélien. Montrer que pour toute racine α de f, on a $K = \mathbb{Q}(\alpha)$.

Solution. Posons $G = \mathrm{Gal}(K/\mathbb{Q})$. Soient α une racine de f dans $\mathbb{C}$ et σ un élément de $\mathrm{Gal}\big(K/\mathbb{Q}(\alpha)\big)$. Soit τ un élément de G. On a $\tau(\alpha) = \tau \circ \sigma(\alpha)$, d'où puisque G est abélien, $\sigma \circ \tau(\alpha) = \tau(\alpha)$. L'extension $K/\mathbb{Q}(\alpha)$ étant galoisienne, on en déduit que $\tau(\alpha)$ est dans $\mathbb{Q}(\alpha)$. Par ailleurs, f étant irréductible, G agit transitivement sur l'ensemble des racines de f. Autrement dit, pour toute racine β de f il existe $\tau \in G$ tel que $\tau(\alpha) = \beta$. Ainsi, les racines de f sont dans $\mathbb{Q}(\alpha)$, d'où $K = \mathbb{Q}(\alpha)$.