École Polytechnique 2022-2023

Algèbre et théorie de Galois

Corrigé de la Feuille d'exercices 9

Exercice 1. Soit $n \geq 2$. Supposons qu'il existe une extension galoisienne $\mathbf{Q} \subset K \subset L$ dont le groupe de Galois $G = \mathrm{Gal}(L/\mathbf{Q})$ est cyclique d'ordre 2^n. Comme K est quadratique imaginaire, la conjugaison complexe ρ est un élément d'ordre 2 dans $\mathrm{Gal}(L/\mathbf{Q})$; c'est le seul car un groupe cyclique d'ordre pair ne contient qu'un seul élément d'ordre 2. D'après la correspondance de Galois, la sous-extension K correspond au sous-groupe

$$H = \{\sigma \in G \mid \sigma|_K = \mathrm{id}\} \subset G,$$

qui est d'ordre $[L\colon K] = 2^{n-1}$. Comme $n \geq 2$, c'est encore un groupe cyclique d'ordre pair et contient donc ρ. Or, $\rho|_K$ est l'automorphisme non trivial de K, contradiction. On remarquera que cet argument montre plus généralement qu'on ne peut pas plonger K dans une extension galoisienne cyclique d'ordre un multiple de 4.

Exercice 2.

(i) Sur une clôture algébrique Ω de K, on a $X^p - a = (X - z_1)\cdots(X - z_p)$ avec $z_i^p = a$. Comme $X^p - a$ n'a pas de racine dans K par hypothèse, s'il est irréductible, alors il existe des polynômes $P, Q \in K[X]$ tels que $X^p - a = PQ$ et que $1 < n = \deg P < p$. Quite à permuter les z_i, on peut supposer $P = (X - z_1)\cdots(X - z_n)$. Alors $b = z_1 \cdots z_n$ appartient à K et $b^p = a^n$. Comme p et n sont premiers entre eux, il existe par Bézout des entiers u, v tels que $1 = up + vn$. Mais alors $a = a^{up+vn} = (a^u b^v)^p$ est une puissance p-ième dans K.

(ii) On pourra consulter le Théorème 9.1 dans VI, §9, pp. 297-298 de S. Lang, *Algebra*, Graduate Texts in Mathematics 211, Springer-Verlag.

(iii) L'extension K/k est galoisienne car K est algébriquement clos de caractéristique zéro. Posons $G = \mathrm{Gal}(K/k)$ et supposons qu'il existe un nombre premier p divisant l'ordre de G. Par le théorème de Cauchy, G contient un sous-groupe H d'ordre p. Alors $F = K^H \subset K$ est une sous-extension telle que $[K\colon F] = p$; elle contient toutes les racines de l'unité d'ordre p car $[F[\zeta_p]\colon F] \leq p - 1$. Comme $\mathrm{Gal}(K/F) = H$ est cyclique d'ordre p, d'après la caractérisation des extensions cycliques vue dans le cours, K est le corps de racines d'un polynôme $X^p - a$ avec $a \in F$. Le polynôme $X^{p^2} - a$ est alors nécessairement réductible; d'après (ii), on a $p = 2$ et $a = -4b^4$ pour $b \in F$. Mais le corps de racines de $X^2 + 4b^4$ est F car -1 est un carré dans k, donc dans F. Cette contradiction montre que G est d'ordre 1, d'où $K = k$.

(iv) On applique ce qui précède à la sous-extension $k[\sqrt{-1}]$, dans laquelle -1 est un carré.

Exercice 3.

(i) Par construction, $\sigma(N_{L/K}(x)) = N_{L/K}(x)$ pour tout $\sigma \in \mathrm{Gal}(L/K)$, d'où $N_{L/K}(x) \in K$. On remarquera que $x \mapsto N_{L/K}(x)$ est un morphisme de groupes multiplicatifs $L^\times \to K^\times$.

(ii) Supposons qu'il existe une relation $a_1\sigma_1 + \cdots + a_m\sigma_m = 0$ avec $a_i \in L$ pas tous nuls et m minimal. Sans perte de généralité, on peut supposer $a_2 \neq 0$. Comme σ_1 et σ_2 sont distincts, il existe $y \in L^\times$ tel que $\sigma_1(y) \neq \sigma_2(y)$. Les σ_i étant multiplicatifs, on a

$$0 = a_1\sigma_1(yx) + \cdots + a_n\sigma_n(yx) = a_1\sigma_1(y)\sigma_1(x) + \cdots + a_m\sigma_m(y)\sigma_m(x)$$

pour tout $x \in L^\times$, d'où la relation

$$a_1\sigma_1 + a_2\frac{\sigma_2(y)}{\sigma_1(y)}\cdots + a_m\frac{\sigma_m(y)}{\sigma_1(y)}\sigma_m = 0$$

après avoir divisé par $\sigma_1(y)$. En soustrayant à celle-ci la relation de départ, on trouve

$$\left(a_2\frac{\sigma_2(y)}{\sigma_1(y)} - a_2\right)\sigma_2 + \cdots + \left(a_m\frac{\sigma_m(y)}{\sigma_1(y)} - a_m\right)\sigma_m = 0.$$

Comme le premier coefficient est non nul, on a trouvé une relation de plus petite longueur, contradiction avec le choix de m minimal.

(iii) Si un tel $y \in L^\times$ existe, alors on a $N_{L/K}(x) = N_{L/K}(y)/N_{L/K}(\sigma^{-1}(y)) = 1$ car $y \in L$ et son image par un élément de G ont la même norme. Réciproquement, supposons $N_{L/K}(x) = 1$. Comme les éléments $\mathrm{Id}, \sigma, \ldots, \sigma^{n-1}$ sont distincts, l'application

$$\mathrm{Id} + x\sigma + x\sigma(x)\sigma^2 + \cdots + x\cdots\sigma^{n-2}(x)\sigma^{n-1}$$

n'est pas identiquement nulle d'après (ii). Il existe donc $z \in L$ tel que

$$y = z + x\sigma(z) + x\sigma(x)\sigma^2(z) + \cdots + x\cdots\sigma^{n-2}(x)\sigma^{n-1}(z)$$

n'est pas nul. En appliquant σ à cet élément et en multipliant par x on trouve

$$x\sigma(y) = x\sigma(z) + x\sigma(x)\sigma^2(z) + x\sigma(x)\sigma^2(x)\sigma^3(z) + \cdots + \underbrace{x\sigma(x)\cdots\sigma^{n-1}(x)}_{N_{L/K}(x)}\underbrace{\sigma^n(z)}_{z} = y.$$

(iv) Puisque L/K est de degré n et que ζ appartient à K, on a $N_{L/K}(\zeta) = \zeta^n = 1$. D'après (iii), il existe $y \in L^\times$ tel que $\sigma(y) = \zeta^{-1}y$. Comme $\zeta \in K$, on a $\sigma^i(y) = \zeta^{-i}y$ pour $i = 1, \ldots, n-1$. Par conséquent, y a n conjugués distincts, d'où $[K[y]\colon K] \geq n$, donc $L = K[y]$ car $K \subset K[y] \subset L$ et $[L\colon K] = n$. Enfin, au vu des égalités $\sigma(y^n) = \sigma(y)^n = (\zeta^{-1}y)^n = y^n$, l'élément y^n est fixe par le groupe de Galois de L/K et appartient donc à K. On a ainsi montré que toutes les extensions cycliques de degré n de K sont obtenues en extrayant la racine n-ième d'un élément.

Exercice 4.

(i) Soit $x \in L$. Alors, pour tout $\sigma \in G$ on a $\sigma(\mathrm{tr}_{L/K}(x)) = \sum_{\tau\in G}\sigma\tau(x) = \sum_{\tau\in G}\tau(x) = \mathrm{tr}_{L/K}(x)$. On en déduit que $\mathrm{tr}_{L/K}(x) \in L^G = K$ donc que $\mathrm{tr}_{L/K}$ a son image dans K. Que ce soit un morphisme de groupes additifs est immédiat on vérifie même que $\mathrm{tr}_{L/K}$ est K-linéaire.

(ii) D'après la question (ii) de l'exercice 3 (indépendance linéaire des $\sigma \in G$), on peut trouver $y \in L$ tel que $\lambda := \mathrm{tr}_{L/K}(y) \neq 0$. Posons $x = y/\lambda$. Alors, puisque $\lambda \in K$, on a $\mathrm{tr}_{L/K}(x) = \lambda^{-1}\mathrm{tr}_{L/K}(y) = 1$.

(iii) Soit $x \in L$ et posons $c_\sigma = \sigma(x) - x$ pour $\sigma \in G$. Pour $\sigma, \tau \in G$, on a

$$c_{\sigma\tau} = \sigma\tau(x) - x = \sigma(\tau(x) - x) + \sigma(x) - x = \sigma(c_\tau) + c_\sigma$$

i.e. on a bien $(c_\sigma)_\sigma \in Z^1(G, L)$.

Réciproquement, soit $(c_\sigma)_\sigma \in Z^1(G, L)$. Choisissons $y \in L$ tel que $\mathrm{tr}_{L/K}(y) = 1$ et posons $x = -\sum_{\tau\in G}\tau(y)c_\tau$. Alors, pour tout $\sigma \in G$, on a

$$\begin{aligned}\sigma(x) &= -\sum_{\tau\in G}\sigma\tau(y)\sigma(c_\tau) = -\sum_{\tau\in G}\sigma\tau(y)(c_{\sigma\tau} - c_\sigma)\\ &= -\sum_{\tau\in G}\tau(y)(c_\tau - c_\sigma) = x + \mathrm{tr}_{L/K}(y)c_\sigma = x + c_\sigma\end{aligned}$$

c'est-à-dire $c_\sigma = \sigma(x) - x$.

(iv) On remarque d'abord que, puisque $\mathbf{F}_p = \mathbf{Z}/p\mathbf{Z} \subset K = L^G$, les morphismes de groupes $G \to \mathbf{Z}/p\mathbf{Z}$ sont exactement les éléments $(c_\sigma)_\sigma \in Z^1(G, L)$ avec $c_\sigma \in \mathbf{Z}/p\mathbf{Z}$ pour tout $\sigma \in G$.

Soit $y \in L$ tel que $a := y^p - y \in K$. Alors, les racines du polynôme $X^p - X - a$ sont les $y + k$ pour $k \in \mathbf{F}_p = \mathbf{Z}/p\mathbf{Z}$. Puisque $\sigma(y)$ est aussi racine de $X^p - X - a$, il s'en suit que $\sigma(y) - y \in \mathbf{Z}/p\mathbf{Z}$ pour tout $\sigma \in G$. D'après la question précédente, $\sigma \in G \mapsto \sigma(y) - y$ défini donc bien un morphisme $G \to \mathbf{Z}/p\mathbf{Z}$.

Réciproquement, si $G \to \mathbf{Z}/p\mathbf{Z}$, $\sigma \mapsto c_\sigma$, est un morphisme de groupe, d'après la question précédente il existe $y \in L$ tel que $c_\sigma = \sigma(y) - y$ pour tout $\sigma \in G$. Si le morphisme $\sigma \mapsto c_\sigma$ est trivial on a $y \in K$. Sinon, l'image de $\sigma \in G \mapsto \sigma(y) - y$ est $\mathbf{F}_p$ donc les conjugués de y sont les $y + k$ pour $k \in \mathbf{F}_p$. Or, l'unique polynôme de degré p dont les racines sont les $y + k$ pour $k \in \mathbf{F}_p$ est $X^p - X - (y^p - y)$ et il s'en suit que $y^p - y \in K$.

(v) A L/K une extension finie galoisienne contenue dans $\overline{K}$ on associe le sous-$\mathbf{F}_p$-espace vectoriel $V(L) = (F - Id)(L) \cap K/(F - Id)(K)$ de $K/(F - Id)(K)$. D'après la question précédente on a une application surjective $V(L) \to \mathrm{Hom}(G_L, \mathbf{F}_p)$ (où $G_L = Gal(L/K)$) qui envoie $x + (F - Id)(K) \in V(L)$ sur le morphisme $\sigma \mapsto \sigma(y) - y$ pour $y \in L$ un élément tel que $F(y) - y \in x + (F - Id)(K)$. On vérifie aisément que cette application est $\mathbf{F}_p$-linéaire et injective car le morphisme $\sigma \mapsto \sigma(y) - y$ est trivial si et seulement si $y \in K$. L'application précédente est donc un isomorphisme $V(L) \simeq \mathrm{Hom}(G_L, \mathbf{F}_p)$. En particulier, on voit que si G_L est un groupe abélien de p-torsion on a $|V(L)| = |G_L|$.

Réciproquement, à $V \subset K/(F - Id)(K)$ un sous-$\mathbf{F}_p$-espace vectoriel de dimension finie on associe l'extension finie $L_V = K[y_x \mid x \in V]$ où pour tout $x \in V$, y_x est une racine dans $\overline{K}$ du polynôme $X^p - X - \tilde{x}$ pour un choix de relèvement $\tilde{x}$ de x dans K. Puisque pour $a \in K$ les racines de $X^p - X - \tilde{x} - (F - Id)(a)$ sont les $y_x + a + k$ pour $k \in \mathbf{F}_p$, on voit que l'extension L_V ne dépend pas du choix des y_x et est galoisienne. De plus, on dispose d'un morphisme injectif $G_V = Gal(L_V/K) \to V^* = Hom(V, \mathbf{F}_p)$ qui envoie σ sur le morphisme $x \in V \mapsto \sigma(y_x) - y_x$. En particulier, on voit que G_V est un groupe abélien de p-torsion et $|G_V| \leqslant |V|$.

Montrons maintenant que ces deux constructions, $L \mapsto V_L$ et $V \mapsto L_V$, induisent des bijections réciproques

$$\left\{ \begin{array}{l} \text{extensions galoisiennes } K \subset L \subset \overline{K} \\ \text{tq } G_L \text{ est un groupe abélien de } p\text{-torsion} \end{array} \right\} \simeq \left\{ \begin{array}{l} \text{sous} - \mathbf{F}_p - \text{espace vectoriel} \\ V \subset K/(F - Id)(K) \text{ de dimension finie} \end{array} \right\}.$$

Pour $V \subset K/(F - Id)(K)$ un sous-$\mathbf{F}_p$-espace vectoriel de dimension finie, il est clair que $V \subseteq V(L_V)$. Or, puisque $G_{L_V} = G_V$ est un groupe abélien de p-torsion, on a

$$|V(L_V)| = |G_{L_V}| = |G_V| \leqslant |V|$$

d'où $V = V(L_V)$. De façon similaire, pour $K \subset L \subset \overline{K}$ une extension galoisienne finie dont le groupe de Galois G_L est un groupe abélien de p-torsion, il est clair que $L_{V(L)} \subset L$. Or, on a

$$[L_{V(L)} : K] = |G_{L_{V(L)}}| = |V(L_{V(L)})| = |V(L)| = |G_L| = [L : K]$$

donc $L_{V(L)} = L$.

Exercice 5.

Soit f ce polynôme et notons (x_i) ses racines dans un corps de décomposition. Le discriminant $\Delta(f)$ est égal à

$$(-1)^{\frac{n(n-1)}{2}} \prod_i f'(x_i).$$

Or, pour chaque i, on a

$$x_i f'(x_i) = a(1 - n)x_i - nb,$$

de sorte que

$$(-1)^n b(-1)^{\frac{n(n-1)}{2}}\Delta(f) = \prod_i \big(a(1-n)x_i - nb\big).$$

La formule résulte alors, simplifications faites, de l'égalité

$$\prod_i (ux_i + v) = \sum_i u^i \sigma_i(x_1, \ldots, x_n) v^{n-i},$$

où les σ_j sont les fonctions symétriques élémentaires, soit ici

$$(-1)^n b u^n + (-1)^{n-1} a u^{n-1} v + v^n.$$

En effet, on en déduit que

$$(-1)^{\frac{n(n-1)}{2}}\Delta(f) = \big(a(1-n)\big)^n + a\big(a(1-n)\big)^{n-1} n + b^{n-1} n^n.$$

(La division par b est licite : on peut traiter b comme une variable, en considérant $P \in \mathbf{Z}[a,b][X]$.)

Exercice 6.

(i) Cela signifie que $\delta = \prod_{i<j}(\alpha_i - \alpha_j) \in k$, et donc que pour tout $\sigma \in G$, on a $\sigma(\delta) = \delta$. Comme $\sigma(\delta) = \varepsilon_\sigma \cdot \delta$ — où ε_σ est la signature de σ (vu comme élément du groupe S_3 des permutations des racines) — et que $\delta \neq 0$, on en déduit que pour tout $\sigma \in G$, on a l'égalité $\varepsilon_\sigma = 1$ *dans* k. Ainsi, *si* k *est de caractéristique* $\neq 2$, on a $G \subset A_3$.

(ii) Le polynôme f est manifestement la somme des éléments de l'orbite de $Z_1 Z_2^2$ sous l'action du 3-cycle (123). Il est donc invariant par $A_3 = <(123)>$. D'autre part, $f_- = (12)\cdot f \neq f$. Ceci suffit pour conclure.

(iii) Les éléments $f + f_-$ et $f \cdot f_-$ sont invariants par l'action de S_3, si bien que les coefficients de $R_f(P)$ sont des fonctions symétriques en les $\alpha_1, \alpha_2, \alpha_3$, et donc des polynômes en les coefficients a, b de P. On vérifierait par le calcul que si $Q = X^3 + a_1 X^2 + a_2 X + a_3$, alors

$$R_f(Q) = T^2 + (a_1 a_2 - 3a_3)T + (a_1^3 a_3 + a_2^3 - 6a_1 a_2 a_3 + 9a_3^2).$$

Dans notre cas, on a plus simplement $R_f(P) = T^2 - 3bT + (a^3 + 9b^2)$ car

$$f(\alpha_1,\alpha_2,\alpha_3) + f_-(\alpha_1,\alpha_2,\alpha_3) = \alpha_1\alpha_2(\alpha_1+\alpha_2) + \alpha_2\alpha_3(\alpha_2+\alpha_3) + \alpha_3\alpha_1(\alpha_3+\alpha_1) = 3b$$

et

$$f(\alpha_1,\alpha_2,\alpha_3)\cdot f_-(\alpha_1,\alpha_2,\alpha_3) = \big((\alpha_1\alpha_2)^3 + (\alpha_2\alpha_3)^3 + (\alpha_3\alpha_1)^3\big) + 3(\alpha_1\alpha_2\alpha_3)^2 + (\alpha_1\alpha_2\alpha_3)\big(\alpha_1^3 + \alpha_2^3 + \alpha_3^3\big)$$

vaut

$$(a^3 + 3b^2) + 3(-b)^2 + (-b)(-3b) = a^3 + 9b^2.$$

(iv) Commençons par observer que le polynôme $R_f(P)$ est séparable, car

$$f_-(\alpha_1,\alpha_2,\alpha_3) - f(\alpha_1,\alpha_2,\alpha_3) = (\alpha_1-\alpha_2)(-\alpha_1\alpha_2 - \alpha_3^2 + \alpha_3(\alpha_1+\alpha_2)) = (\alpha_1-\alpha_2)(\alpha_1-\alpha_3)(\alpha_2-\alpha_3).$$

(Alternativement, on calcule son discriminant $\Delta(R) = (3b)^2 - 4(a^3+9b^2) = -4a^3 - 27b^2 = \Delta(P)$.) Il en résulte immédiatement de ce qui précède que $G \subset A_3$ si et seulement si $R_f(P)$ a une racine dans k. Lorsque k est de caractéristique 2, on obtient immédiatement l'équivalence annoncée en divisant le polynôme par b^2, qui est non nul.