École polytechnique 2022-2023
Théorie de Galois

Feuille d'exercices 6

Soient k un corps parfait et Ω une clôture algébrique de k. On rappelle qu'une sous-extension finie K/k de Ω est *galoisienne* si, pour chaque $x \in K$, tous les k-conjugués de x dans Ω appartiennent à K. D'après un résultat du cours, il est équivalent de demander que l'inclusion naturelle $\mathrm{Hom}_k(K,K) \subset \mathrm{Hom}_k(K,\Omega)$ soit une égalité, de sorte que $|\mathrm{Hom}_k(K,K)| = [K:k]$. Le groupe $\mathrm{Gal}(K/k) = \mathrm{Hom}_k(K,K)$ est appelé *groupe de Galois* de K/k. Si $x \in K$, les k-conjugués de x sont alors permutés transitivement par $\mathrm{Gal}(K/k)$.

Si $P \in k[X]$, on note R_P l'ensemble de ses racines dans Ω et $\mathrm{Gal}(P,k)$ le groupe de Galois de l'extension galoisienne $k[R_P]$ sur k.

Exercice 1. Soit $P \in k[X]$ un polynôme irréductible de degré n et soit $G = \mathrm{Gal}(P,k)$.

(i) Rappeler pourquoi $|R_P| = n$.

Sur un corps parfait k tout polynôme irréductible a des racines simples. Cela implique que le cardinal de R_P est n.

(ii) En déduire que n divise $|G|$ et que $|G|$ divise $n!$.

L'ordre du groupe de Galois G est le degré du corps des racines $k[R_P]$. D'un côté, ce corps contient comme sous-extension le corps de rupture $k[X]/(P)$ qui est de degré n car P est irréductible, donc n divise $|G|$ par le théorème de la base télescopique. D'un autre côté, G est un sous-groupe du groupe symétrique $\mathfrak{S}_n$ puisque les automorphismes de k-algèbres $k[R_P] \to k[R_P]$ permutent les racines de P ; par le théorème de Lagrange, $|G|$ divise $n!$.

Exercice 2. Soit K une extension galoisienne de k.

(i) Soient $k \subseteq F_1 \subseteq K$ et $k \subseteq F_2 \subseteq K$ des sous-extensions de K. On note F_1F_2 le *compositum* de F_1 et F_2, c'est-à-dire, la plus petite sous-extension de K contenant F_1 et F_2. Montrer que

$$\mathrm{Gal}(K/F_1F_2) = \mathrm{Gal}(K/F_1) \cap \mathrm{Gal}(K/F_2).$$

L'inclusion $\mathrm{Gal}(K/F_1F_2) \subseteq \mathrm{Gal}(K/F_1) \cap \mathrm{Gal}(K/F_2)$ est évidente. Réciproquement, si $\sigma \in \mathrm{Gal}(K/k)$ est un automorphisme fixant les éléments de F_1 et F_2, alors σ fixe les éléments de F_1F_2 aussi (par exemple, si $F_2 = k[x]$, alors $F_1F_2 = F_1[x]$ et σ fixe $x \in F_2$ ainsi que F_1).

(ii) Soit $k \subseteq F \subseteq K$ une sous-extension de K. Notons L la plus petite sous-extension galoisienne de K contenant F . Montrer que

$$\mathrm{Gal}(K/L) = \bigcap_{\sigma \in \mathrm{Gal}(K/k)} \sigma \mathrm{Gal}(K/F)\sigma^{-1}.$$

On observe d'abord que L est le compositum des corps $\sigma(F)$ pour $\sigma \in \mathrm{Gal}(K/k)$, donc $\mathrm{Gal}(K/L) = \bigcap_{\sigma \in \mathrm{Gal}(K/k)} \mathrm{Gal}(K/\sigma(F))$ d'après (i). Or, $\mathrm{Gal}(K/\sigma(F)) = \sigma \mathrm{Gal}(K/F)\sigma^{-1}$.

Exercice 3. Soient $K_1 \subset \Omega$ et $K_2 \subset \Omega$ des extensions galoisiennes de k.

(i) Montrer que $K_1 \cap K_2$ et K_1K_2 sont aussi galoisiennes sur k.

Soit $x \in K_1 \cap K_2$. Comme K_1 et K_2 sont galoisiennes, tous les k-conjugués de x dans Ω appartiennent à K_1 et à K_2, donc à $K_1 \cap K_2$. Pour traiter le cas du compositum K_1K_2, on utilise

le fait que les extensions galoisiennes sont exactement les corps de racines $k[R_P]$ des polynômes. Si $K_1 = k[R_{P_1}]$ et $K_2 = k[R_{P_2}]$, alors $K_1K_2 = k[R_{P_1P_2}]$ est galoisienne.

(ii) Montrer que $\mathrm{Gal}(K_1K_2/K_2)$ s'identifie à $\mathrm{Gal}(K_1/K_1 \cap K_2)$.

L'extension K_1K_2/K_2 est galoisienne car K_1K_2/k l'est. L'application $\mathrm{Gal}(K_1K_2/K_2) \to \mathrm{Gal}(K_1/k)$ qui envoie σ sur $\sigma|_{K_1}$ est un morphisme de groupes. Il est injectif car si $\sigma|_{K_1}$ est l'identité, alors σ est trivial sur K_1 et sur K_2, donc sur K_1K_2. Si l'on désigne par H son image, alors H fixe $K_1 \cap K_2$. De plus, si $x \in K_1$ est fixé par H, alors x est aussi fixé par $\mathrm{Gal}(K_1K_2/K_2)$, d'où $x \in K_1 \cap K_2$. Par le lemme d'Artin, on conclut : $H = \mathrm{Gal}(K_1/K_1 \cap K_2)$.

(iii) En déduire que $[K_1K_2 \colon k] = [K_1 \colon k] \cdot [K_2 \colon k]$ si et seulement si $K_1 \cap K_2 = k$.

Par le théorème de la base télescopique, $[K_1K_2 \colon k] = [K_1K_2 \colon K_2] \cdot [K_2 \colon k]$. Comme K_1K_2 est galoisienne sur k, l'extension K_1K_2/K_2 est galoisienne de degré égal à l'ordre de $\mathrm{Gal}(K_1K_2/K_2)$. Par (ii), ceci est égal à $[K_1 \colon K_1 \cap K_2]$, donc égal à $[K_1 \colon k]$ si et seulement si $K_1 \cap K_2 = k$.

(iv) Montrer qu'il y a un morphisme injectif

$$\mathrm{Gal}(K_1K_2/k) \to \mathrm{Gal}(K_1/k) \times \mathrm{Gal}(K_2/k)$$

qui est un isomorphisme si et seulement si $K_1 \cap K_2 = k$.

Soit $\varphi \colon \mathrm{Gal}(K_1K_2/k) \to \mathrm{Gal}(K_1/k) \times \mathrm{Gal}(K_2/k)$ l'application qui envoie σ sur $(\sigma|_{K_1}, \sigma|_{K_2})$; c'est clairement un morphisme de groupes. Si $\sigma \in \ker \varphi$, alors σ est l'identité sur K_1 et K_2, donc sur K_1K_2 également ; cela montre que φ est injectif. C'est un isomorphisme si et seulement si les groupes $\mathrm{Gal}(K_1K_2/k)$ et $\mathrm{Gal}(K_1/k) \times \mathrm{Gal}(K_2/k)$ ont le même ordre, autrement dit, si $[K_1K_2 \colon k] = [K_1 \colon k] \cdot [K_2 \colon k]$. D'après la question précédente, c'est le cas si et seulement si $K_1 \cap K_2 = k$.

Exercice 4. Soit $x = \sqrt{1+\sqrt{2}} \in \mathbf{R}$.

(i) Montrer que $[\mathbf{Q}[x] : \mathbf{Q}] = 4$ et déterminer les conjugués de x dans $\mathbf{C}$.

Le nombre x est annulé par le polynôme de degré quatre $P = X^4 - 2X^2 - 1 \in \mathbf{Q}[X]$, dont les racines complexes sont x, $-x$, $\sqrt{1-\sqrt{2}}$ et $-\sqrt{1-\sqrt{2}}$. Comme aucune d'entre elles n'est un nombre rationnel (autrement on aurait $\sqrt{2} \in \mathbf{Q}$), si P était réductible, il serait produit de deux polynômes quadratiques à coefficients rationnels. Or, il n'y a parmi les quatre racines aucune paire dont la somme et le produit soient des nombres rationnels. Il s'ensuit que P est irréductible, d'où $[\mathbf{Q}[x] : \mathbf{Q}] = 4$ et les conjugués de x sont les racines de P.

(ii) Montrer que $\mathbf{Q}[x]/\mathbf{Q}$ n'est pas galoisienne.

Puisque $\mathbf{Q}[x]$ est un sous-corps de $\mathbf{R}$ et que parmi les conjugués de x il y a des nombres qui ne sont pas réels, l'extension n'est pas galoisienne.

(iii) Montrer que $\mathbf{Q}[x]/\mathbf{Q}[\sqrt{2}]$ et $\mathbf{Q}[\sqrt{2}]$ sont galoisiennes.

Le polynôme minimal de x sur $\mathbf{Q}[\sqrt{2}]$ est $X^2 - 1 - \sqrt{2} = 0$, dont l'autre racine $-x$ appartient également à $\mathbf{Q}[x]$; c'est donc une extension galoisienne. De même, $\sqrt{2}$ a polynôme minimal $X^2 - 2 \in \mathbf{Q}[X]$ et l'autre racine $-\sqrt{2}$ appartient à $\mathbf{Q}[\sqrt{2}]$. (En fait, toute extension quadratique d'un corps de caractéristique distincte de 2 est galoisienne.)

(iv) Vérifier que $\mathbf{Q}[x, i]/\mathbf{Q}$ est galoisienne de degré 8.

Comme les générateurs x et i sont annulés par un polynôme de degré 4 et un polynôme de degré 2 respectivement, on a $[\mathbf{Q}[x, i] \colon \mathbf{Q}] \leq 8$. D'un autre côté, $\mathbf{Q}[x] \subsetneq \mathbf{Q}[x, i]$ est une sous-extension propre de degré 4 sur $\mathbf{Q}$, d'où $[\mathbf{Q}[x, i] \colon \mathbf{Q}] = 8$ par le théorème de la base télescopique. Pour démontrer qu'il s'agit d'une extension galoisienne, il suffit de vérifier que tous les conjugués complexes des générateurs appartiennent à $\mathbf{Q}[x, i]$: c'est évident pour i et c'est vrai pour x parce que $\sqrt{1-\sqrt{2}} = i \cdot \sqrt{\sqrt{2}-1} = i/x$.

(v) Montrer qu'en revanche $\mathbf{Q}[\sqrt{2+\sqrt{2}}]/\mathbf{Q}$ est galoisienne de degré 4.

Le polynôme minimal de $\alpha = \sqrt{2+\sqrt{2}}$ est $X^4 - 4X^2 + 2 \in \mathbf{Q}[X]$, qui est irréductible par le critère d'Eisenstein. Les conjugués de α dans $\mathbf{C}$ sont donc $\alpha, -\alpha, \sqrt{2-\sqrt{2}}, -\sqrt{2-\sqrt{2}}$. Ils appartiennent tous à $\mathbf{Q}[\sqrt{2+\sqrt{2}}]$ au vu de l'identité

$$\sqrt{2-\sqrt{2}} = \frac{\sqrt{2}}{\sqrt{2+\sqrt{2}}} = \frac{\alpha^2-2}{\alpha}.$$

(vi) Montrer que $\mathrm{Gal}(\mathbf{Q}[\sqrt{2+\sqrt{2}}]/\mathbf{Q})$ est cyclique d'ordre 4.

Voir exercice 5, (ii) dans la feuille 3.

Exercice 5. Soit $P \in \mathbf{Q}[X]$ le polynôme cubique unitaire dont les racines sont

$$x_1 = 2\cos(2\pi/7), \quad x_2 = 2\cos(4\pi/7), \quad x_3 = 2\cos(6\pi/7).$$

(i) Vérifier que $P = X^3 + X^2 - 2X - 1$.

Soient x une racine primitive de l'unité d'ordre 6 et $y = x + x^{-1}$. Comme $y^2 = x^2 + x^{-2} + 2$ et $y^3 = x^3 + x^{-3} + 3y$, la relation $1 + x + \cdots + x^6 = 0$ donne

$$0 = 1 + x + x^{-1} + x^2 + x^{-2} + x^3 + x^{-3} = 1 + y + y^2 - 2 + y^3 - 3y = y^3 + y^2 - 2y - 1.$$

Vu que $x_j = \xi^j + \xi^{-j}$ avec $\xi = e^{\frac{2i\pi}{7}}$, la formule pour P en découle.

(ii) Montrer que P est irréductible.

D'après le lemme de Gauss, il suffit de voir que P n'a pas de racines entières. Comme $x_1x_2x_3 = 1$, une telle racine serait forcément 1 ou -1, pas ces nombres ne sont pas de racines. (Une autre méthode : on peut réduire P modulo 3 et observer que $X^3 + X^2 - 2X - 1 \in \mathbf{F}_3[X]$ est un polynôme irréductible car il est de degré 3 et n'a pas de racine.)

(iii) Montrer que $\mathbf{Q}[x_1]$ est un corps de décomposition de P.

Montrons que les racines x_2 et x_3 appartiennent à $\mathbf{Q}[x_1]$. En effet,

$$x_2 = 2\mathrm{Re}(\xi^2) = 2\cos^2(2\pi/7) - 2\sin^2(2\pi/7) = -2 + 4\cos^2(2\pi/7) = x_1^2 - 2,$$

puis $x_3 \in \mathbf{Q}[x_1]$ car le produit $x_1x_2x_3$ vaut 1.

(iv) En déduire $\mathrm{Gal}(P, \mathbf{Q})$.

C'est le groupe cyclique d'ordre 3.

Exercice 6. Soient $f = X^4 - 4X^2 - 1 \in \mathbf{Q}[X]$ et $g = Y^2 - 4Y - 1 \in \mathbf{Q}[Y]$.

(i) Pourquoi le groupe $\mathrm{Gal}(g, \mathbf{Q})$ est-il un quotient de $G = \mathrm{Gal}(f, \mathbf{Q})$?

Comme $f(X) = g(X^2)$, on a l'inclusion $\mathbf{Q}[R_g] \subset \mathbf{Q}[R_f]$ et l'application de restriction

$$G = \mathrm{Gal}(\mathbf{Q}[R_f]/\mathbf{Q}) \longrightarrow \mathrm{Gal}(\mathbf{Q}[R_g]/\mathbf{Q}) = \mathrm{Gal}(g, \mathbf{Q})$$

est surjective par le théorème du prolongement des morphismes.

(ii) Montrer que G est un sous-groupe de $\mathfrak{S}_{R_f}$ *compatible* avec la partition

$$\left\{\left\{\sqrt{2+\sqrt{5}}, -\sqrt{2+\sqrt{5}}\right\}, \left\{\sqrt{2-\sqrt{5}}, -\sqrt{2-\sqrt{5}}\right\}\right\}$$

de R_f. (On dit qu'une permutation σ d'un ensemble fini E est *compatible* avec une partition de E lorsque $x \sim y$ implique $\sigma(x) \sim \sigma(y)$ pour $\sim$ la relation d'équivalence dont les classes sont la partition considérée.)

On a $R_g = \{2+\sqrt{5}, 2-\sqrt{5}\}$ et $R_f = \{\sqrt{2+\sqrt{5}}, -\sqrt{2+\sqrt{5}}, \sqrt{2-\sqrt{5}}, -\sqrt{2-\sqrt{5}}\}$. Les groupes $\mathrm{Gal}(g, \mathbf{Q})$ et $\mathrm{Gal}(f, \mathbf{Q})$ permutent R_g et R_f respectivement. Soient $x, y \in R_f$ et $\sigma \in G$. Si $x \sim y$, alors $x^2 = y^2$ et, puisque $\sigma(x)^2 = \sigma(x^2)$ et que $x^2 \in R_g$, on a également $\sigma(x) \sim \sigma(y)$.

(iii) En déduire que G est contenu dans le groupe diédral du carré, c'est-à-dire le groupe des isométries du plan conservant le carré.

Le groupe diédral du carré est le sous-groupe des permutations de l'ensemble des sommets qui sont compatible avec la partition $\{\{a, c\}, \{b, d\}\}$, où (a, c) et (b, d) sont des paires de sommets opposés.

(iv) Montrer qu'il existe un élément $\sigma \in G$ tel que $\sigma(\sqrt{2+\sqrt{5}})$ est égal à $\sqrt{2-\sqrt{5}}$ ou $-\sqrt{2-\sqrt{5}}$.

Le groupe G étant un quotient de $\mathrm{Gal}(g, \mathbf{Q}) = \mathbf{Z}/2\mathbf{Z}$, il existe $\sigma \in G$ dont la restriction à $\mathbf{Q}[R_g] = \mathbf{Q}[\sqrt{5}]$ est l'automorphisme non trivial qui envoie $2+\sqrt{5}$ sur $2-\sqrt{5}$. On a alors $\sigma(\sqrt{2+\sqrt{5}})^2 = \sigma(2+\sqrt{5}) = 2-\sqrt{5}$, d'où la propriété voulue.

(v) Montrer qu'il existe un élément $\tau \in G$ échangeant $\sqrt{2-\sqrt{5}}$ et $-\sqrt{2-\sqrt{5}}$ mais fixant $\sqrt{2+\sqrt{5}}$.

Comme $\sqrt{2+\sqrt{5}} \in \mathbf{R}$ mais $\sqrt{2-\sqrt{5}} \in i\mathbf{R}$, le morphisme de $\mathbf{Q}$-algèbres $\tau\colon \mathbf{Q}[R_f] \to \mathbf{Q}[R_f]$ donné par la conjugaison complexe a la propriété voulue.

(vi) En déduire que G est le groupe diédral tout entier.

Les éléments σ et τ correspondent, respectivement, à une rotation d'angle $\pi/2$ et à une réflexion par rapport à l'une des diagonales du carré, les deux générateurs du groupe diédral.

Exercice 7. Soit $P \in k[X]$ un polynôme irréductible de degré n et $K = k[R_P]$.

(i) Montrer que si $\mathrm{Gal}(K/k)$ est abélien alors $[K : k] = n$.

Soit x une racine de P, et $L = k[x] \subseteq K$. Alors $[L : k] = n$, et L correspond à un sous-groupe H de G. Puisque G est abélien, il est distingué et l'extension L/k est donc galoisienne. Le corps L contient donc toutes les racines de P : on a $L = K$, et $[K : k] = n$.

(ii) La réciproque est-elle vraie ?

Non ! L'extension de degré six $K = \mathbf{Q}[\sqrt[3]{2}, e^{\frac{2i\pi}{3}}]$ est galoisienne de groupe de Galois non abélien $\mathfrak{S}_3$ d'après l'exercice 4 de la feuille 4. Le polynôme minimal P d'un élément primitif $x \in K$ est irréductible de degré 6 et $K = \mathbf{Q}[R_P]$.