École polytechnique 2022-2023
Théorie de Galois

Corrigé de la feuille d'exercices 4

Exercice 1. (*Sous-groupes finis du groupe multiplicatif d'un corps*)

(i) Soient G un groupe et x, y deux éléments d'ordre fini de G. On suppose que $xy = yx$ et que les ordres respectifs n et m de x et y sont premiers entre eux. Montrer que xy est d'ordre fini nm.

Comme x et y commutent, $(xy)^k = x^k y^k$ pour tout entier k. En particulier, $(xy)^{nm} = 1$ et l'ordre de xy divise donc nm. Soit k un entier tel que $(xy)^k = 1$. Alors $x^k = y^{-k}$ est un élément de G dont l'ordre divise n et m, donc $x^k = y^k = 1$ car n et m sont premiers entre eux. Par conséquent, $n \mid k$ et $m \mid k$, puis $nm \mid k$ en utilisant encore que n et m sont premiers entre eux. On a ainsi démontré que l'ordre de xy est nm.

On fixe dorénavant un corps k et $G \subset k^*$ un sous-groupe fini (multiplicatif).

(ii) Si $n = |G|$, montrer que $X^n - 1$ est scindé dans $k[X]$, ses racines étant exactement les éléments de G. En déduire que, pour tout d divisant n, le polynôme $X^d - 1$ est scindé à racines distinctes dans G.

Comme un polynôme de degré n possède au plus n racines distinctes et comme $\alpha^n = 1$ pour tout élément $\alpha \in G$, on a $X^n - 1 = \prod_{\alpha \in G}(X - \alpha)$ dans $k[X]$. Si d divise n, les racines de $X^d - 1$ sont les racines de $X^n - 1$ telles que $\alpha^d = 1$; elles sont donc toutes distinctes et $X^d - 1$ est scindé.

(iii) Conclure que G est un groupe cyclique d'ordre n.

(On pourra commencer par montrer que, si p^r divise n avec p premier, alors G admet un élément d'ordre p^r, puis on construira un élément d'ordre n dans G.)

Soit $e = p_1^{a_1} \cdots p_r^{a_r}$ l'exposant de G, c'est-à-dire, le plus petit common multiple des ordres des éléments de G. Par définition, G contient des éléments d'ordre divisible par $p_i^{a_i}$ et donc des éléments d'ordre exactement égal à $p_i^{a_i}$ en prenant des puissances convenables. D'après (i), le produit x de ces derniers est d'ordre e. Si $\langle x \rangle$ désigne le sous-groupe cyclique de G engendré par x, on a $\langle x \rangle \subseteq G \subseteq \{\alpha \in k \mid \alpha^e = 1\}$. Or, le groupe à droite a ordre au plus e par la partie (ii) et $\langle x \rangle$ a ordre exactement e, d'où $G = \langle x \rangle$.

(iv) En déduire que, si k est un corps fini, alors k^* est cyclique (*Théorème de Gauss*).

Si k est fini, on peut prendre $G = k^*$ dans ce qui précède.

Exercice 2. Soient P un polynôme irréductible dans $k[X]$ de degré d et L son corps de décomposition dans une clôture algébrique fixée de k.

(i) Montrer que $[L : k] \leq d!$. À quelle condition a-t-on égalité ?

Soient $\alpha_1, \ldots, \alpha_d$ les d racines (pas nécessairement distinctes) de P dans une clôture algébrique $\bar{k}$ de k. L'extension $k[\alpha_1]$ de k a degré $\leq d$ et le polynôme P se factorise comme $(X - \alpha_1)P_1(x)$ sur $k[\alpha_1]$. L'extension $k[\alpha_1, \alpha_2]$ de $k[\alpha_1]$ a donc degré $\leq d - 1$, et ainsi de suite. Par le théorème de la base télescopique, on trouve

$$[k[\alpha_1, \ldots, \alpha_d] \colon k] \leq d(d-1)(d-2) \cdots 2 \cdot 1 = d!.$$

On a égalité si toutes les racines sont distinctes (e.g. si k est de caractéristique zéro) et si le polynôme $P(X)/(X - \alpha_1) \ldots (X - \alpha_i)$ est irréductible sur $k[\alpha_1, \ldots, \alpha_i]$ pour tout i.

(ii) Donner un exemple du cas d'égalité avec $d = 3$.

Le corps de décomposition de $P = X^3 - 2$ est l'extension de degré six $L = \mathbf{Q}[\sqrt[3]{2}, e^{2i\pi/3}]$, voir l'exercice 4. On remarquera que, dans ce cas, $\mathrm{Hom}_{\mathbf{Q}\text{-alg}}(L, L) \simeq \mathfrak{S}_3$.

Exercice 3. Posons $j = e^{2i\pi/3}$ et considérons les extensions $K = \mathbf{Q}[\sqrt[3]{2}]$ et $L = K[j]$.

(i) Calculer $[K : \mathbf{Q}]$ et déterminer $\mathrm{Hom}_{\mathbf{Q}\text{-alg}}(K, K)$.

Le polynôme $X^3 - 2 \in \mathbf{Q}[X]$ est irréductible par le critère d'Eisenstein avec $p = 2$ et annule $\sqrt[3]{2}$, d'où $[K : \mathbf{Q}] = 3$. Parmi les $\mathbf{Q}$-conjugués de $\sqrt[3]{2}$, à savoir $\sqrt[3]{2}$, $\sqrt[3]{2}j$ et $\sqrt[3]{2}j^2$, seul $\sqrt[3]{2}$ appartient à $K \subset \mathbf{R}$. Il s'ensuit que $\mathrm{Hom}_{\mathbf{Q}\text{-alg}}(K, K)$ est réduit à l'identité.

(ii) Déterminer $\mathrm{Hom}_{\mathbf{Q}[j]\text{-alg}}(L, L)$.

L'extension $L = \mathbf{Q}[\sqrt[3]{2}, j]$ est de degré 6 sur $\mathbf{Q}$. En effet, on a d'un côté $[L : \mathbf{Q}] \leq 6$ car les générateurs sont annulés par les polynômes $X^3 - 2$ et $X^2 + X + 1$ et, d'un autre côté, $[L : \mathbf{Q}]$ est divisible par 6 car L contient la sous-extension de degré trois K et la sous-extension de degré deux $\mathbf{Q}[j] = \mathbf{Q}[\sqrt{-3}]$. Par conséquent, le polynôme $X^3 - 2$ reste irréductible sur $\mathbf{Q}[j]$ et L est isomorphe à la $\mathbf{Q}[j]$-algèbre $\mathbf{Q}[j][X]/(X^3 - 2)$. Le groupe $\mathrm{Hom}_{\mathbf{Q}[\rho]\text{-alg}}(L, L)$ est formé des morphismes $\mathrm{Id}, \sigma, \sigma^2$, où $\sigma(\sqrt[3]{2}) = \sqrt[3]{2}j$; il est donc isomorphe à $\mathbf{Z}/3\mathbf{Z}$.

(iii) Montrer que $\mathrm{Hom}_{\mathbf{Q}\text{-alg}}(L, L)$ est isomorphe au groupe $\mathfrak{S}_3$.

L'extension de degré six L est engendrée par $\sqrt[3]{2}$, qui a pour $\mathbf{Q}$-conjugués $\sqrt[3]{2}$, $\sqrt[3]{2}j$ et $\sqrt[3]{2}j^2$, et par j, dont les $\mathbf{Q}$-conjugués sont j et j^2. Un morphisme $\sigma : L \to L$ est donc déterminé par les images de $\sqrt[3]{2}$ et de j, et il y au plus six possibilités. Tout morphisme de $\mathbf{Q}[j]$-algèbres $L \to L$ étant en particulier un morphisme de $\mathbf{Q}$-algèbres, le groupe que l'on veut calculer contient les éléments $\mathrm{Id}, \sigma, \sigma^2$. De plus, comme $L \subset \mathbf{C}$ est stable sous la conjugaison complexe car $\sqrt[3]{2} \in \mathbf{R}$ et $\bar{j} = j^2$, il contient également le morphisme $\tau : L \to L$ qui envoie un élément de L vers son conjugué. On a ainsi trouvé six éléments distincts

$$\mathrm{Id}, \sigma, \sigma^2, \tau, \sigma\tau, \sigma^2\tau.$$

On peut ensuite, par exemple, vérifier la relation $\sigma\tau = \tau\sigma^2$ en calculant les images des générateurs et ceci montre que $\mathrm{Hom}_{\mathbf{Q}\text{-alg}}(L, L)$ est isomorphe au groupe symétrique $\mathfrak{S}_3$. On aurait pu aussi remarquer que ce n'est pas un groupe abélien et que $\mathfrak{S}_3$ est le seul groupe non abélien d'ordre six.

Exercice 4. Soit $P(X) = X^3 - X - 1 \in \mathbf{Q}[X]$.

(i) Montrer que P est irréductible sur $\mathbf{Q}$.

Comme P est de degré 3, il suffit de voir qu'il n'a pas de racines dans $\mathbf{Q}$. Supposons que α est une telle racine et écrivons-la sous la forme p/q avec p et q premiers entre eux. La relation $\alpha^3 = \alpha + 1$ implique $p^3 = pq^2 + q^3$, ce qui montre que q divise p et p divise q. Les seule possibilités sont donc $\alpha = 1$ ou $\alpha = -1$, qui ne sont pas racines de P.

Alternativement, on peut réduire P modulo 3 et observer que le polynôme $X^3 - X - 1$ est irréductible sur $\mathbf{F}_3[X]$ car il n'a pas de racine.

(ii) Soit $L = \mathbf{Q}[X]/(P)$ l'extension de degré 3 de $\mathbf{Q}$ correspondante. Montrer que, si x désigne la classe de X dans L, on a l'égalité $\mathbf{Q}[x] = \mathbf{Q}[x^2]$ dans L et exprimer x comme un polynôme en x^2.

Comme $L/\mathbf{Q}$ est de degré impair, on a $\mathbf{Q}[x] = \mathbf{Q}[x^2]$ d'après l'exercice 3 de la feuille 3. L'élément $x \in L$ satisfait la relation $x^3 = x + 1$, d'où $x = (x^2)^2 - x^2$ en multipliant par x.

(iii) Montrer que P possède une unique racine réelle, qui est un *nombre de Pisot-Vijayaraghavan*[1].

La dérivée $P'(X) = 3X^2 - 1$ étant positive sur $]-\infty, -1/\sqrt{3}] \cup [1/\sqrt{3}, +\infty[$ et négative sur $]-1/\sqrt{3}, 1/\sqrt{3}[$, la fonction P est croissante sur la première réunion d'intervalles et décroissante sur le deuxième intervalle. Comme $P(-1/\sqrt{3}) < 0$, il y a une seule racine réelle θ, qui vérifie $\theta > 1$ car $P(1) < 0$. Soient z et $\bar{z}$ les autres racines complexes de P. Puisque le produit des trois racines vaut 1, on a $|z| < 1$.

Exercice 5. Soient k un corps de caractéristique p et $a \in k$.

(i) Soit $P(X) = X^p - X - a \in k[X]$. Montrer P est irréductible si et seulement s'il ne possède pas de racine.

Il est toujours vrai qu'un polynôme irréductible de degré plus grand que 2 sur un corps k n'a pas de racine dans k. Montrons la réciproque pour le polynôme donné. Vu l'égalité

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

si α est une racine de P dans une clôture algébrique $\bar{k}$ de k, alors toutes les racines sont $\alpha + i$ pour $i = 0, \dots, p-1$. Supposons que P n'est pas irréductible, c'est-à-dire, qu'il s'écrit comme un produit $f(X)g(X)$ avec f de degré $1 \leq d \leq p-1$. On a alors

$$f(X) = \prod_{i \in I}(X - \alpha - i) = X^d - (d\alpha + \sum_{i \in I} i)X^{d-1} + \dots$$

pour une partie $I \subset \{0, \dots, p-1\}$ de cardinal d. Puisque $d\alpha + \sum_{i \in I} i \in k$ en tant que coefficient du polynôme f et que $d \neq 0$, on en déduit $\alpha \in k$.

(ii) Si P est irréductible et K est un corps de rupture de P, que dire du groupe $\mathrm{Hom}_{k\text{-alg}}(K, K)$?

Le raisonnement précédent montre que, si K est un corps de rupture de P, alors K est aussi un corps de décomposition ; en fait, $K = k(\alpha)$ pour une racine α de P et les k-conjugués de α sont les $\alpha + i$. Il s'ensuit que $\mathrm{Hom}_{k\text{-alg}}(K, K)$ est le groupe cyclique $\mathbf{Z}/p\mathbf{Z}$.

Exercice 6. Soient k un corps et $f = T^d - a_1T^{d-1} + a_2T^{d-2} + \dots + (-1)^d a_d \in k[T]$ un polynôme unitaire de degré d. Soit

$$A = k[X_1, \dots, X_d]/\big((\sum_i X_i) - a_1, (\sum_{i<j} X_iX_j) - a_2, \dots, \prod_i X_i - a_n\big).$$

le quotient de l'anneau de polynômes $k[X_1, \dots, X_d]$ par l'idéal engendré par les

$$\sum_{i_1 < \dots < i_r} X_{i_1} \cdots X_{i_r} - a_r$$

pour $1 \leq r \leq d$.

---

1. On appelle *nombre de Pisot-Vijayaraghavan* toute racine réelle positive d'un polynôme unitaire à coefficients entiers dont les autres racines sont des nombres complexes de module strictement inférieur à un. On peut montrer que la racine réelle

$$\sqrt[3]{\frac{1}{2} + \frac{1}{6}\sqrt{\frac{23}{3}}} + \sqrt[3]{\frac{1}{2} - \frac{1}{6}\sqrt{\frac{23}{3}}} \simeq 1,324717957244746025960$$

de P est le plus petit tel nombre.

(i) Montrer que, par construction, l'image de f dans $A[T]$ est *scindée* sur A : on a l'égalité

$$f = \prod_{i=1}^{d} (T - x_i)$$

dans $A[T]$, où les x_i, $1 \leq i \leq d$, désignent les images des X_i dans A par la surjection canonique $k[X_1, \ldots, X_d] \twoheadrightarrow A$.

Dans l'anneau des polynômes à coefficients dans $k[X_1, \ldots, X_d]$, on a l'égalité

$$\prod_{i=1}^{d} (T - X_i) = T^d - (\sum_i X_i) T^{d-1} + (\sum_{i<j} X_i X_j) T^{d-2} - \cdots + (-1)^d \prod_i X_i$$

dont l'image par la surjection canonique $k[X_1, \ldots, X_d] \twoheadrightarrow A$ donne

$$\prod_{i=1}^{d} (T - x_i) = T^d - a_1 T^{d-1} + a_2 T^{d-2} - \cdots + (-1)^d a_d = f$$

(ii) Soit $\mathfrak{m}$ un idéal maximal de A. Montrer que $A/\mathfrak{m}$ est un *corps de décomposition* de f sur k. Comme $\mathfrak{m}$ est maximal, $L = A/\mathfrak{m}$ est un corps contenant k sur lequel le polynôme f est scindé : si $\bar{x_i}$ désigne l'image de x_i dans L, on a $f = \prod_{i=1}^{d} (T - \bar{x_i})$ dans $L[T]$. Or si $k[\bar{x}_1, \ldots, \bar{x_d}]$ était un sous-corps propre de L, le noyau de la projection $A \to k[\bar{x}_1, \ldots, \bar{x_d}]$ serait un idéal strictement inclus entre $\mathfrak{m}$ et A.