École Polytechnique 2022-2023

Algèbre et théorie de Galois

Corrigé de la Feuille d'exercices 7

Exercice 1. Puisque f est irréductible, B est un corps. Le polynôme $X^p - X$ a donc au plus p racines dans B et puisqu'il annule tous les éléments de $\mathbf{F}_p$, on a $\mathrm{Ker}(F - \mathrm{Id} : B \to B) = \mathbf{F}_p$.

La réciproque est fausse. En effet, tout élément de $B = \mathbf{F}_p[T]/(T^2)$ s'écrit sous la forme $x = \alpha + \beta T$ où $\alpha, \beta \in \mathbf{F}_p$. On a alors $x^p = \alpha^p + \beta^p T^p = \alpha$ (car $T^p = 0$ dans $\mathbf{F}_p[T]/(T^2)$) donc $x^p = x \Leftrightarrow \beta = 0$ i.e. on a encore $\mathrm{Ker}(F - \mathrm{Id} : B \to B) = \mathbf{F}_p$.

Exercice 2.

(i) Puisque les éléments de $\mathbf{F}_{q^n}$ sont exactement les racines du polynôme $X^{q^n} - X$, $\mathbf{F}_{q^n}$ est le corps de décomposition de $X^{q^n} - X$ et l'extension $\mathbf{F}_{q^n}/\mathbf{F}_q$ est par conséquent galoisienne. De plus, le sous-corps de $\mathbf{F}_{q^n}$ fixé par $F_q : x \mapsto x^q$ est exactement $\mathbf{F}_q$ donc le groupe de Galois de l'extension $\mathbf{F}_{q^n}/\mathbf{F}_q$ est cyclique engendré par F_q (d'après correspondance de Galois). Ce groupe est aussi d'ordre le degré de l'extension $\mathbf{F}_{q^n}/\mathbf{F}_q$ c'est-à-dire n.

(ii) Puisque $Gal(\mathbf{F}_{q^n}/\mathbf{F}_q) = \langle F_q \rangle$ est d'ordre n, ses sous-groupes sont de la forme $\langle F_q^d \rangle$ pour d un diviseur de n. La sous-extension fixée par $\langle F_q^d \rangle$ est l'ensemble des éléments $x \in \mathbf{F}_{q^n}$ vérifiant $x^{q^d} = x$ c'est-à-dire $\mathbf{F}_{q^d}$.

Exercice 3. Soit $x = \sqrt[4]{2}$, et $K = \mathbf{Q}[x, i]$.

(i) Les racines du polynôme $P(X) = X^4 - 2$ sont x, $-x$, ix et $-ix$. Ainsi, on voit que K est le corps de décomposition de P sur $\mathbf{Q}$ et l'extension $K/\mathbf{Q}$ est par conséquent galoisienne. De plus, P est irréductible sur $\mathbf{Q}$ (par le critère d'Eisenstein) d'où $[\mathbf{Q}[x] : \mathbf{Q}] = \deg(P) = 4$. D'autre part, puisque i vérifie l'équation $i^2 + 1 = 0$ l'extension $K/\mathbf{Q}[x]$ est de degré au plus 2 mais $i \notin \mathbf{Q}[x]$ (car $\mathbf{Q}[x] \subset \mathbf{R}$) donc $[K : \mathbf{Q}[x]] = 2$. Par téléscopage on obtient

$$[K : \mathbf{Q}] = [K : \mathbf{Q}[x]][\mathbf{Q}[x] : \mathbf{Q}] = 8.$$

Puisque K est le corps de décomposition de P, l'action de $\mathrm{Gal}(K/\mathbf{Q})$ sur l'ensemble de ses racines $\{x, -x, ix, -ix\}$ donne un morphisme injectif $\varphi : \mathrm{Gal}(K/\mathbf{Q}) \to \mathfrak{S}_4$. L'image de ce morphisme préserve la partition $\{\{x, -x\}, \{ix, -ix\}\}$. Or, on vérifie aisément que le sous-groupe des permutations préservant cette partition est isomorphe au groupe D_4. Comme $|\mathrm{Gal}(K/\mathbf{Q})| = |D_4| = 8$, φ induit donc un isomorphisme $\mathrm{Gal}(K/\mathbf{Q}) \simeq D_4$.
Alternativement, on peut aussi construire un isomorphisme explicite comme suit. La conjugaison complexe induit un élément σ de $\mathrm{Gal}(K/\mathbf{Q})$ qui fixe x, $-x$ et échange ix avec $-ix$. D'autre part, puisque P est irréductible, on sait que l'action de $\mathrm{Gal}(K/\mathbf{Q})$ sur $\{x, -x, ix, -ix\}$ est transitive. En particulier, il existe $\tau \in \mathrm{Gal}(K/\mathbf{Q})$ qui envoie x sur ix. On a alors $\tau(-x) = -\tau(x) = -ix$ et $\tau(ix)$ vaut x ou $-x$. Quitte à remplacer τ par $\tau\sigma$ on peut supposer que $\tau(ix) = -x$ et donc $\tau(-ix) = x$. Le sous-groupe engendré par σ et τ est alors isomorphe à D_4 (placer x, ix, $-x$, $-ix$ aux sommets d'un carré dans cet ordre: σ correspond à la symétrie par rapport à la diagonale passant par x et $-x$ tandis que τ est une rotation d'angle 45) donc égal à $\mathrm{Gal}(K/\mathbf{Q})$ car ce dernier est d'ordre 8.

(ii) Avec les notations de la question précédente, les sous-groupes de $\mathrm{Gal}(K/\mathbf{Q})$ sont les suivants:

- $\mathrm{Gal}(K/\mathbf{Q})$, d'ordre 8;

- $\langle\tau\rangle$, $\langle\sigma,\tau^2\rangle$ et $\langle\tau\sigma,\tau^2\rangle$, d'ordres 4;
- $\langle\tau^2\rangle$, $\langle\sigma\rangle$, $\langle\tau\sigma\rangle$, $\langle\tau^2\sigma\rangle$ et $\langle\tau^3\sigma\rangle$, d'ordres 2;
- $\{1\}$, d'ordre 1.

Les sous-extensions correspondantes, via la correspondance de Galois, sont:

- $K^{\mathrm{Gal}(K/\mathbf{Q})} = \mathbf{Q}$ de degré 1;
- $K^{\langle\tau\rangle} = \mathbf{Q}[i]$, $K^{\langle\sigma,\tau^2\rangle} = \mathbf{Q}[x^2] = \mathbf{Q}[\sqrt{2}]$ et $K^{\langle\tau\sigma,\tau^2\rangle} = \mathbf{Q}[ix^2] = \mathbf{Q}[\sqrt{-2}]$ de degré 2;
- $K^{\langle\tau^2\rangle} = \mathbf{Q}[i,x^2]$, $K^{\langle\sigma\rangle} = \mathbf{Q}[x]$, $K^{\langle\tau\sigma\rangle} = \mathbf{Q}[ix^2, x+ix]$, $K^{\langle\tau^2\sigma\rangle} = \mathbf{Q}[ix,x^2]$ et $K^{\langle\tau^3\sigma\rangle} = \mathbf{Q}[x-ix,ix^2]$ de degrés 4;
- $K^{\{1\}} = K$ de degré 8.

Exercice 4.

(i) Soit $x \in K$ non réel. Alors $K = \mathbf{R}[x]$ et le polynôme minimal π_x de x sur $\mathbf{R}$ est irréductible de degré 2 donc de la forme $\pi_x(X) = (X-a)^2 + b$ avec $a, b \in \mathbf{R}$, $b > 0$. On a alors

$$K \simeq \mathbf{R}[X]/((X-a)^2+b) \simeq \mathbf{R}[Y]/(Y^2+b) \simeq \mathbf{R}[Z]/(Z^2+1) \simeq \mathbf{C}.$$

(ii) Soit $x \in K$ et π_x son polynôme minimal sur $\mathbf{R}$. Alors $[\mathbf{R}[x] : \mathbf{R}] = \deg(\pi_x)$ divise $[K : \mathbf{R}]$, donc $\deg(\pi_x)$ est impair. D'après le théorème des valeurs intermédiaires, un polynôme réel de degré impair a au moins une racine réelle. Comme π_x est irréductible, il est donc de degré 1. Donc $\pi_x = X - x$ et x est réel. Tous les éléments de K sont par conséquent réels et $K = \mathbf{R}$.

(iii) Supposons que K soit une extension de degré 2 de $\mathbf{C}$ et soit $x \in K$ non complexe. Alors, le polynôme minimal π_x de x sur $\mathbf{C}$ est irréductible de degré 2. Or, on sait calculer explicitement les racines d'un polynôme de degré 2 à coefficients et elles sont toutes complexes. Contradiction.

(iv) Soit $G = \mathrm{Gal}(K/\mathbf{R})$ le groupe de Galois de l'extension. Écrivons $|G| = 2^n m$ où $n \in \mathbf{N}$ et $m \in \mathbf{N}^*$ est impair. D'après le résultat admis de théorie des groupes, G admet un sous-groupe P de cardinal 2^n. Choisissons de plus une suite de sous-groupes $P_1 \subset \ldots \subset P_n = P$ avec $|P_i| = 2^i$. Posons $K_i = K^{P_{n+1-i}}$ pour $1 \leqslant i \leqslant n$. Puisque la correspondance de Galois est décroissante, on obtient une tour d'extensions

$$\mathbf{R} \subset K_1 \subset \ldots \subset K_\alpha = K.$$

De plus, $[K_1 : \mathbf{R}] = |G|/|P| = m$ est impair et $[K_{i+1} : K_i] = |P_{n+1-i}|/|P_{n-i}| = 2$ pour tout $1 \leqslant i \leqslant n-1$.

(v) D'après la première question, on a $K_1 = \mathbf{R}$ et d'après la deuxième question, si $n \geqslant 2$, $K_2 \simeq \mathbf{C}$. Il s'ensuit, d'après la question (iii), que K_2 n'admet pas d'extension de degré 2 donc forcément $n \leqslant 2$ et on en déduit que $K = \mathbf{R}$ ou $K \simeq \mathbf{C}$. D'autre part, pour toute extension finie $k/\mathbf{R}$ il existe une extension galoisienne $K/\mathbf{R}$ telle que $k \subset K$ et il s'ensuit que les seules extensions finies de $\mathbf{R}$ sont, à isomorphisme près, $\mathbf{R}$ et $\mathbf{C}$. En particulier, $\mathbf{C}$ n'a pas d'extension finie non triviale et le résultat s'en déduit.

Exercice 5.

(i) Supposons qu'il existe $x \in \mathbf{Q}[\sqrt{21}]$ tel que $x^2 = 5 + \sqrt{21}$. En décomposant $x = a + b\sqrt{21}$, où $a, b \in \mathbf{Q}$, on obtient

$$5 + \sqrt{21} = (a + b\sqrt{21})^2 = a^2 + 21b^2 + 2ab\sqrt{21}.$$

D'où $a^2 + 21b^2 = 5$ et $2ab = 1$ donc $a^2 + \frac{21}{4a^2} = 5$ puis $a^4 - 5a^2 + \frac{21}{4} = 0$. On en tire que $a^2 = (5 \pm 2)/2$ et a ne peut pas être dans $\mathbf{Q}$, contradiction.

Soient

$$z = \sqrt{5 + \sqrt{21}} \text{ et } K = \mathbf{Q}[z].$$

(ii) On remarque que $\mathbf{Q}[\sqrt{21}] = \mathbf{Q}[z^2] \subset K$. D'après la question précédente on a $[K : \mathbf{Q}[\sqrt{21}]] = 2$ donc

$$[K : \mathbf{Q}] = [K : \mathbf{Q}[\sqrt{21}]] \times [\mathbf{Q}[\sqrt{21}] : \mathbf{Q}] = 4.$$

(iii) On calcule

$$zz' = \sqrt{(5 + \sqrt{21})(5 - \sqrt{21})} = \sqrt{25 - 21} = 2.$$

Ainsi, $z' = \frac{2}{z} \in K$. D'autre part, on a $z^2 - 5 = \sqrt{21}$ et z est racine du polynôme $P(X) = (X^2 - 5)^2 - 21$. Puisque z est de degré 4 sur $\mathbf{Q}$ (question (ii)), il s'en suit que P est le polynôme minimal de z sur $\mathbf{Q}$. Les conjugués de z sur $\mathbf{Q}$ sont les racines de P c'est-à-dire z, $-z$, z' et $-z'$. D'après ce qu'on vient de voir, tous ces conjugués sont dans K donc $K/\mathbf{Q}$ est galoisienne.

(iv) Puisque le groupe de Galois agit transitivement sur l'ensemble des conjugués de z, un tel élément g existe bien. De plus, comme z engendre K sur $\mathbf{Q}$ un tel élément est unique.

(v) Idem.

(vi) On a

$$g(z') = g(2/z) = 2/g(z) = -2/z = -z'.$$

De façon similaire,

$$h(z') = h(2/z) = 2/h(z) = 2/z' = z.$$

Puisque z engendre K, pour montrer que g et h commutent il suffit de vérifier que $g(h(z)) = h(g(z))$. Or, d'après ce qui précède, on a $g(h(z)) = g(z') = -z'$ et $h(g(z)) = h(-z) = -h(z) = -z'$. Ainsi, g et h commutent et comme ils sont tous les deux d'ordre 2 (car $g(g(z)) = h(h(z)) = z$), ils engendrent un sous-groupe de G isomorphe à $(\mathbf{Z}/2\mathbf{Z})^2$. Or, G est d'ordre $[K : \mathbf{Q}] = 4$ donc $G \simeq (\mathbf{Z}/2\mathbf{Z})^2$.

(vii) D'après la question précédente, les sous-groupes de G sont G, $\langle g \rangle$, $\langle h \rangle$, $\langle gh \rangle$ et $\{1\}$. D'après la correspondance de Galois, les sous-corps de K sont donc

$$K^G = \mathbf{Q},\ K^{\langle g \rangle} = \mathbf{Q}[\sqrt{21}],\ K^{\langle h \rangle} = \mathbf{Q}[z+z'] = \mathbf{Q}[\sqrt{14}],\ K^{\langle gh \rangle} = \mathbf{Q}[z-z'] = \mathbf{Q}[\sqrt{6}],\ K^{\{1\}} = K$$

où on a remarqué que $(z + z')^2 = z^2 + (z')^2 + 2zz' = 5 + \sqrt{21} + 5 - \sqrt{21} + 4 = 14$ et de façon similaire $(z - z')^2 = 6$.

Exercice 6. On considère le polynôme

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

(i) Puisque P est de degré 3, il suffit de montrer qu'il n'admet pas de racine rationnelle. Or si $\frac{p}{q}$ est racines de P avec $p, q \in \mathbf{Z}^*$ premiers entre eux, on a $p^3 - 3pq^2 - 4q^3 = 0$ donc

$q = 1$ et $p \mid 4$ or on vérifie aisément que ni 1, ni -1, ni 2, ni -2, ni 4 ni -4 ne sont racines de P.

(ii) Puisque $x^3 = 2 + \sqrt{3}$, on a $\mathbf{Q}[\sqrt{3}] \subset \mathbf{Q}[x]$ donc $2 = [\mathbf{Q}[\sqrt{3}] : \mathbf{Q}]$ divise $[\mathbf{Q}[x] : \mathbf{Q}]$.

(iii) Il s'agit de montrer que $[\mathbf{Q}[x] : \mathbf{Q}[\sqrt{3}]] = 3$. Or, x est annulé par le polynôme $T^3 - (2 + \sqrt{3})$ et il suffit de montrer que ce dernier est irréductible dans $\mathbf{Q}[\sqrt{3}][T]$ ou, ce qui revient au même, que $2 + \sqrt{3}$ n'est pas un cube dans $\mathbf{Q}[\sqrt{3}]$. Supposons que contraire que $2 + \sqrt{3} = (\frac{a}{q} + \frac{b}{q}\sqrt{3})^3$ où $a, b \in \mathbf{Z}$, $q \in \mathbf{N}^*$. On ne perd rien à supposer que a, b et q sont premiers entre eux dans leur ensemble. En développant, on obtient $2q^3 = a^3 + 9ab^2$ et $q^3 = 3a^2b + 3b^3$. De la dernière égalité on tire $3 \mid q$ d'où, par la première identité, $3 \mid a$ et enfin $3 \mid b$ à nouveau par la deuxième égalité ce qui contredit le fait que a, b et q sont premiers entre eux.

Une autre façon de procéder est de remarquer que x est annulé par le polynôme $Q(X) = (X^3 - 2)^2 - 3$ de degré 6. Or, on vérifie aisément que $Q(X + 2)$ satisfait au critère d'Eisenstein pour le premier $p = 3$ donc Q est irréductible dans $\mathbf{Q}[T]$.

(iv) Le polynôme minimal de x sur $\mathbf{Q}$ est $(X^3-2)^2-3$ donc jx (où on a posé $j = e^{2i\pi/3}$) est un conjugués de x sur $\mathbf{Q}$. Or $jx \notin \mathbf{Q}[x]$ car $\mathbf{Q}[x] \subset \mathbf{R}$ et $j \notin \mathbf{R}$. Donc $\mathbf{Q}[x]/\mathbf{Q}$ n'est pas galoisienne.

(v) Les conjugués de x sont les racines de $(X^3 - 2)^2 - 3$ c'est-à-dire x, jx, j^2x, y, jy et j^2y où on a posé $y = \sqrt[3]{2 - \sqrt{3}}$. Parmi ceux-ci seul y est réel et distinct de x.

(vi) On a $xy = \sqrt[3]{4 - 3} = 1$ i.e. $y = x^{-1}$ et il en découle que $\mathbf{Q}[x] = \mathbf{Q}[y]$.

(vii) On remarque que $X^3P(X + \frac{1}{X}) = (X^3 - 2)^2 - 3$ donc les racines de P sont $x + x^{-1} = x + y$, $jx + (jx)^{-1} = jx + j^2y$ et $j^2x + (j^2x)^{-1} = j^2x + jy$. Par conséquent, $K = \mathbf{Q}[x + y, jx + j^2y, j^2x + jy]$.

(viii) Le groupe de Galois de $K/\mathbf{Q}$ est un sous-groupe de S_3 donc le degré divise 6. Mais K contient strictement $\mathbf{Q}[x + y]$ (car $\mathbf{Q}[x, y] \subset \mathbf{R}$ et $jx + j^2y \notin \mathbf{R}$) qui est de degré 3 sur $\mathbf{Q}$ (puisque c'est un corps de rupture de P sur $\mathbf{Q}$) donc $[K : \mathbf{Q}] = 6$.