École Polytechnique 2022-2023

Algèbre et théorie de Galois

Corrigé de la Feuille d'exercices 3

Exercice 1.

(i) X^2-d est un polynôme annulateur de $\sqrt{d}$. Si il était réductible, il aurait une racine dans $\mathbf{Q}$, ce qui n'est pas. Donc $[\mathbf{Q}[\sqrt{d}]:\mathbf{Q}]=2$. Les conjugués sont $\sqrt{d}$ et $-\sqrt{d}$. Notons que si d est négatif, $\sqrt{d}$ est un imaginaire pur.

(ii) Si a/b est un carré d'un nombre rationnel, la conclusion est claire. Réciproquement, supposons $\sqrt{a}=\alpha+\beta\sqrt{b}$ avec $\alpha,\beta\in\mathbf{Q}$. En prenant le carré, on obtient que $2\alpha\beta\sqrt{b}\in\mathbf{Q}$. Or $\sqrt{b}\notin\mathbf{Q}$ par hypothèse. Donc $\alpha=0$ ou $\beta=0$. Mais $\beta\neq 0$ car $\sqrt{a}\notin\mathbf{Q}$ par hypothèse. Donc $\alpha=0$ et $\sqrt{a}/\sqrt{b}\in\mathbf{Q}$.

(iii) Il existe x dans K de degré 2 sur $\mathbf{Q}$: il existe $\alpha,\beta\in\mathbf{Q}$ avec $x^2+\alpha x+\beta=0$. Alors $(x+\alpha/2)^2\in\mathbf{Q}$ est de la forme p/q avec p,q entiers. Donc $K=\mathbf{Q}[\sqrt{p/q}]=\mathbf{Q}[\sqrt{pq}]$. Soit d l'entier obtenu à partir de pq en supprimant les facteurs carrés (c'est le produit, sans puissance, des nombres premiers apparaissant dans pq, avec le signe de pq). Alors $K=\mathbf{Q}[\sqrt{d}]$. On obtient l'existence. L'unicité découle de la question (ii).

Exercice 2

(i) Les polynômes X^2-2 et X^5-5 étant irréductibles dans $\mathbf{Q}[X]$ (d'après le critère d'Eisenstein), nous avons $[\mathbf{Q}[\sqrt{5}]:\mathbf{Q}]=2$ et $[\mathbf{Q}[\sqrt[5]{2}]:\mathbf{Q}]=5$. Donc 10 divise $[K:\mathbf{Q}]$. Puis le théorème de la base télescopique donne :

$$[K:\mathbf{Q}]=[K:\mathbf{Q}[\sqrt{5}]][\mathbf{Q}[\sqrt{5}]:\mathbf{Q}]=2[K:\mathbf{Q}[\sqrt{5}]]\leq 10.$$

(ii) On a un morphisme d'algèbre surjectif

$$\Psi:\mathbf{Q}[X,Y]\to K$$

tel que $\Psi(P)=P(\sqrt{5},\sqrt[5]{2})$. Le noyau contient l'idéal I engendré par X^2-5 et Y^5-2, donc on obtient un morphisme surjectif

$$\tilde{\Psi}:\mathbf{Q}[X,Y]/I\to K.$$

En comparant les dimensions, on obtient que c'est un isomorphisme.

(iii) On a clairement $\mathbf{Q}[\sqrt[3]{2},\sqrt{2}]\subseteq\mathbf{Q}[\sqrt[6]{2}]$. Puis X^6-2 annule $\sqrt[6]{2}$ et $[\mathbf{Q}[\sqrt[6]{2}]:\mathbf{Q}]\leq 6$. Mais $[\mathbf{Q}[\sqrt{2}]:\mathbf{Q}]=2$ et $[\mathbf{Q}[\sqrt[3]{2}]:\mathbf{Q}]=3$, donc $[\mathbf{Q}[\sqrt[3]{2},\sqrt{2}]:\mathbf{Q}]=6$ d'après le théorème de la base télescopique. Ceci permet de conclure.

Exercice 3

On a l'inclusion évidente $K[x^2]\subseteq K[x]$ et $X^2-x^2\in(K[x^2])[X]$ annule x, donc le degré $[K[x]:K[x^2]]$ est 1 ou 2. Mais ce degré divise $[L:K]$ impair d'après le théorème de la base télescopique. C'est donc 1.

Exercice 4

(i) D'après l'exercice 1, les extensions $\mathbf{Q}[\sqrt{7}]/\mathbf{Q}$ et $\mathbf{Q}[\sqrt{5}]/\mathbf{Q}$ sont de degré 2 et distinctes. Le théorème de la base télescopique implique donc que $[K:\mathbf{Q}]=4$ et que $\{1,\sqrt{5},\sqrt{7},\sqrt{35}\}$ est une base de K sur $\mathbf{Q}$.

(ii) On utilise l'exercice 1. Comme l'extension est de degré 4, un sous-corps non trivial est une extension quadratique de la forme $\mathbf{Q}[\sqrt{d}]$ avec d entier sans facteurs carrés. On a une décomposition $\sqrt{d} = \alpha + \beta\sqrt{5}$ avec $\alpha, \beta \in \mathbf{Q}[\sqrt{7}]$. Le coefficient de $\sqrt{5}$ dans le carré est nul donc $\alpha\beta = 0$. Si $\beta = 0$, $\sqrt{d} \in \mathbf{Q}[\sqrt{7}]$ et $d = 7$. Sinon $\alpha = 0$ et $\sqrt{d} = \lambda\sqrt{5} + \mu\sqrt{35}$ avec $\lambda, \mu \in \mathbf{Q}$. De même, en prenant le carré, on obtient que $d = 5$ ou $d = 35$. Au final il y a 5 sous-corps : $\mathbf{Q}$, $\mathbf{Q}[\sqrt{5}]$, $\mathbf{Q}[\sqrt{7}]$, $\mathbf{Q}[\sqrt{35}]$ et K.

(iii) On écrit $x = a+b\sqrt{5}+c\sqrt{7}+d\sqrt{35}$ avec $a, b, c, d \in \mathbf{Q}$. La condition est que x n'est pas dans un des sous-corps propres ci-dessus, c'est-à-dire qu'au moins deux coefficients parmi b, c, d sont non nuls.

(iv) Comme il engendre K d'après la dernière question, il a 4 conjugués : les racines de $(X^2 - 12)^2 - 140$ qui sont $\sqrt{5} + \sqrt{7}$, $\sqrt{5} - \sqrt{7}$, $-\sqrt{5} + \sqrt{7}$, $-\sqrt{5} - \sqrt{7}$.

(v) Pour $k = K$ il n'y a que $\sqrt{5} + \sqrt{7}$. Pour $k = \mathbf{Q}[\sqrt{5}]$, le polynôme minimal est $(X - \sqrt{5})^2 - 7$ et les conjugués sont $\sqrt{5}+\sqrt{7}$ et $\sqrt{5}-\sqrt{7}$. De même, pour $k = \mathbf{Q}[\sqrt{7}]$, les conjugués sont $\sqrt{5}+\sqrt{7}$ et $-\sqrt{5}+\sqrt{7}$. Enfin pour $k = \mathbf{Q}[\sqrt{35}]$, le polynôme minimal est $X^2 - 2\sqrt{35} - 7$ et les conjugués sont $\sqrt{5}+\sqrt{7}$ et $-\sqrt{5}-\sqrt{7}$.

Exercice 5

(i) On a un polynôme annulateur $(X^2 - 2)^2 - 2 = X^4 - 4X^2 + 2$ irréductible par Eisenstein. Les conjugués sont donc $\sqrt{2+\sqrt{2}}$, $-\sqrt{2+\sqrt{2}}$, $\sqrt{2-\sqrt{2}}$, $-\sqrt{2-\sqrt{2}}$.

(ii) Notons que les conjugués sont tous dans K car $\sqrt{2+\sqrt{2}}\sqrt{2-\sqrt{2}} = \sqrt{2} \in K$.

Chaque élément est un morphisme injectif comme morphisme défini sur un corps. En dimension finie, on obtient un isomorphisme. Donc on obtient un groupe. Un élément est caractérisé par l'image de $\sqrt{2+\sqrt{2}}$, on obtient un groupe d'ordre 4. Soit σ dans le groupe tel que $\sigma(\sqrt{2+\sqrt{2}}) = \sqrt{2-\sqrt{2}}$. En prenant le carré, $\sigma(\sqrt{2}) = -\sqrt{2}$. Donc $\sqrt{2-\sqrt{2}}\sigma(\sqrt{2-\sqrt{2}}) = -\sqrt{2}$ et $\sigma(\sqrt{2-\sqrt{2}}) = -\sqrt{2+\sqrt{2}}$. Donc $\sigma^2 \neq \mathrm{Id}$, donc σ est d'ordre 4 et engendre le groupe qui est cyclique.

(iii) Un sous-corps non trivial est une extension quadratique $\mathbf{Q}[\sqrt{d}]$. On peut écrire $\sqrt{d} = \lambda\sqrt{2+\sqrt{2}}+\mu$ avec $\lambda, \mu \in \mathbf{Q}[\sqrt{2}]$. En prenant le carré, on obtient $\lambda\mu = 0$. Si $\mu = 0$, écrivons $\lambda = x + y\sqrt{2}$ avec $x, y \in \mathbf{Q}$. Alors $d = (x+y\sqrt{2})^2(2+\sqrt{2})$, et le coefficient de $\sqrt{2}$ est $0 = x^2 + 2y^2 + 4xy$. Si $x \neq 0$, on obtient $0 = 1 + 2(y/x)^2 + 4y/x$, solution rationnelle d'une équation quadratique de discriminant $\Delta = 8 \notin \mathbf{Q}^2$, contradition. C'est analogue si $y \neq 0$. Dans tous les cas $\lambda = 0$. Donc $d = 2$. Au final on obtient $\mathbf{Q}[\sqrt{2}]$ seul sous-corps propre.

Exercice 6.

(i) On suit l'indication : $\Phi_p(X + 1)$ satisfait le critère d'Eisenstein pour le nombre premier p. Il est irréductible si et seulement si $\Phi_p(X)$ l'est.

(ii) $\Phi_p(X)$ annule $e^{2i\pi/p}$ donc $[\mathbf{Q}[e^{2i\pi/p}] : \mathbf{Q}] = p - 1$. Si $p = 2$, $\cos(2\pi/p) = -1$ et $[\mathbf{Q}[\cos(2\pi/p)] : \mathbf{Q}] = 1$. Si $p > 2$, $e^{2i\pi/p}$ n'est pas réel. Notons que $\mathbf{Q}[\cos(2\pi/p)] \subset \mathbf{Q}[e^{2i\pi/p}]$ d'après les relations d'Euler :

$$\cos(2\pi/p) = \frac{e^{2i\pi/p} + e^{-2i\pi/p}}{2}.$$

De plus ceci donne un polynôme annulateur de $e^{2i\pi/p}$ de degré 2, à savoir $X^2 - 2X\cos(2\pi/p) + 1$. Donc $[\mathbf{Q}[e^{2i\pi/p}] : \mathbf{Q}[\cos(2\pi/p)]] = 2$. Le théorème de la base télescopique donne donc

$$[\mathbf{Q}[\cos(2\pi/p)] : \mathbf{Q}] = \frac{p-1}{2}.$$

Exercice 7.

(i) $\mathbf{Q}[x]$ contient $\sqrt{3}$ donc le degré est divisible par 2.

(ii) On a $(x^3-2)^2-3=0$ donc le degré est au plus 6. Considérons $Q(X)=X^3-(2+\sqrt{3})$ et montrons qu'il est irréductible dans $(\mathbf{Q}[\sqrt{3}])[X]$. Sinon, il aurait une racine $(p+p'\sqrt{3})/q$ avec $p'\neq 0$, $2q^3=p^3+9p'$, $q^3=3(p^2p'+(p')^3)$ et $p\wedge p'\wedge q=1$. Alors $3|q$ donc $3|p$. La première égalité implique que $3|p'$. Contradiction. Donc le degré de x sur $\mathbf{Q}[\sqrt{3}]$ est 3 et donc degré sur $\mathbf{Q}$ est divible par 3. C'est donc 6.

Exercice 8.

(i) C'est une conséquence directe du Lemme de Gauss.

(ii) On peut supposer $z\notin\mathbf{Q}$. Ecrivons $z=a+ib$. Alors le polynôme minimal de z est $X^2-2aX+(a^2+b^2)$. Si $a,b\in\mathbf{Z}$, ce polynôme est clairement à coefficients entiers. Réciproquement, supposons que $a^2+b^2=A$ et $2a=B$ sont entiers. Alors $a=B/2$ et $A=B^2/4+b^2$.
On réécrit $4A-B^2=4b^2$ est entier, et donc $2b$ également. Notons $c=2b$. On a donc $4A=B^2+c^2$ et tous les éléments sont entiers. Si B est impair, c également, et B^2+c^2 est égal à 2 modulo 4, contradiction. Donc B et c sont pairs, et a,b sont entiers.