École Polytechnique 2009-2010

Théorie de Galois

Corrigé de la Feuille d'exercices 1

Exercice 1.

(i) Soit I un idéal non nul de $k[X]$. Soit P un polynôme non nul de I de degré minimal. Alors pour $Q \in I \setminus \{0\}$, écrivons la division euclidienne $Q = AP + B$ de Q par P, avec $\deg(B) < \deg(P)$. Alors $B = Q - AP \in I$. Donc $B = 0$ car P est de degré minimal. Donc P engendre I. Maintenant si un autre polynôme R engendre I, alors R divise P et P divise R. Donc ils sont de même degré et il existe $\lambda \in k^*$ tel que $R = \lambda P$. Ainsi les polynômes générateurs de I sont les multiples non nuls de P. Parmi ceux-ci, il y a un seul polynôme unitaire.

(ii) L'algébricité de x implique immédiatement que $I_x \neq \{0\}$. Maintenant comme pour P, Q polynômes on a $(PQ)(x) = P(x)Q(x)$ et $(P+Q)(x) = P(x)+Q(x)$, I_x est clairement un idéal.

(iii) Si Π_x n'était pas irréductible, on aurait une factorisation $\Pi_x = QR$ avec $Q, R \in k[X]$ tels que $\deg(Q), \deg(R) < \deg(\Pi_x)$. Alors $Q(x)R(x) = 0$, et comme k est un corps, $Q(x) = 0$ ou $R(x) = 0$. On a donc un polynôme de I_x non nul de degré strictement inférieur à celui de P, contradiction.

(iv) Pour P, Q polynômes et $\lambda \in k$ on a $(PQ)(x) = P(x)Q(x)$ et $(P+\lambda Q)(x) = P(x)+\lambda Q(x)$, donc $k[x]$ est clairement une sous-k-algèbre de K. Soit $\mathcal{B} = \{1, \cdots, x^{\deg(\Pi_x)-1}\}$. Pour $P \in k[X]$, écrivons la division euclidienne $P = A\Pi_x + B$ de P par Π_x, avec $\deg(B) < \deg(\Pi_x)$. Alors $P(x) = B(x) \in \mathrm{Vect}(\mathcal{B})$. Donc $\mathcal{B}$ est génératrice. Maintenant si $\mathcal{B}$ était liée, on aurait un polynôme P annulateur de x tel que $\deg(P) \leq \deg(\Pi_x)-1$, contradiction. Donc on obtient une base de $k[x]$ et $[k[x] : k] = \deg(\Pi_x)$.

(v) Il ne reste plus qu'à montrer que $y \in k[x] \setminus \{0\}$ admet un inverse dans $k[x]$. D'après (iv), il existe $P \in k[X]$ tel que $y = P(x)$ et $\deg(P) < \deg(\Pi_x)$. Or d'après (iii), Π_x est irréductible. Comme Π_x ne divise pas P, ils sont premiers entre eux. Le théorème de Bézout donne $Q, R \in k[X]$ tels que $PQ + \Pi_x R = 1$. On alors $P(x)Q(x) = 1$, et $Q(x) \in k[x]$ est un inverse de y. Notons qu'en utilisant l'algorithme d'Euclide étendu aux coefficients de Bézout, on obtient une méthode théorique de calcul de l'inverse.

Exercice 2.

(i) On a $(\sqrt{7})^2 - 7 = 0$ et $(e^{2i\pi/17})^{17} - 1 = 0$. Soit $x = \sqrt{2} + \sqrt[3]{5}$. Alors $(x - \sqrt{2})^3 = 5$, c'est à dire $x^3 + 6x - 5 = 2\sqrt{2} + 3\sqrt{2}x^2$ et $(x^3 + 6x - 5)^6 - 2(2 + 3x^2)^2 = 0$. Donc x est algébrique sur $\mathbf{Q}$ de degré au plus 6.

(ii) Soit $z = a + ib \in \mathbf{C}$ avec $a, b \in \mathbf{R}$. Alors $(z - a)^2 + b^2 = 0$.

Exercice 3.

(i) Si $X^3 - 2$ n'était pas irréductible sur $\mathbf{Q}$, il aurait une racine dans $\mathbf{Q}$ car son degré est 3. Une telle racine est de la forme p/q avec $p, q \in \mathbf{Z}$ premiers entre eux. Alors $p^3 = 2q^3$ et p est pair. On peut écrire $p = 2p'$ et donc $q^3 = 4(p')^3$. Donc q est pair, contradiction.

(ii) D'après (i), $X^3 - 2$ est le polynôme minimal de $\sqrt[3]{2}$ sur $\mathbf{Q}$ qui est donc de degré 3. Si $\sqrt[3]{2} = a + b\sqrt{c}$ avec $a, b, c \in \mathbf{Q}$, on aurait $(\sqrt[3]{2} - a)^2 - b^2 c = 0$ et $\sqrt[3]{2}$ serait de degré au plus 2 sur $\mathbf{Q}$, contradiction.

(iii) Comme $\mathbf{Q}[\sqrt[3]{2}]$ est un corps de dimension 3 sur $\mathbf{Q}$, on connait l'existence de tels $a, b, c \in \mathbf{Q}$. On développe $1 = (\sqrt[3]{4} - 1)(a + b\sqrt[3]{2} + c\sqrt[3]{4})$, ce qui donne $1 = (-a + 2b) + \sqrt[3]{2}(-b + 2c) + \sqrt[3]{4}(a - c)$. En identifiant les coefficients sur la base $(1, \sqrt[3]{2}, \sqrt[3]{4})$ et en résolvant le système on obtient $a = c = 1/3$ et $b = 2/3$.

Exercice 4.

(i) Si $[L : k] < \infty$, on a $[K : k] < \infty$ car K est un sous k-espace vectoriel de L. De plus, si L contenait une famille libre pour K, elle serait libre pour k, ce qui n'est pas possible. Donc $[L : K] < \infty$. Maintenant si $[L : K] < \infty$ et $[K : k] < \infty$, soit $(a_i)_{1\leq i\leq N}$ (resp. $(b_j)_{1\leq j\leq M}$) une base de K sur k (resp. de L sur K). Alors un $x \in L$ s'écrit $x = \sum_{1\leq j\leq M} \lambda_j b_j$ avec $\lambda_j \in K$. Chaque λ_j s'écrit $\lambda_j = \sum_{1\leq i\leq n} \mu_{i,j} a_i$ avec $\mu_{i,j} \in k$, et donc $x = \sum_{1\leq i\leq N, 1\leq j\leq M} \mu_{i,j} a_i b_j$. Donc $\{a_i b_j\}_{1\leq i\leq N, 1\leq j\leq M}$ génère L sur k et donc $[L : k] < \infty$. Montrons de plus qu'on obtient une base. Si on a une combinaison linéaire $0 = \sum_{1\leq i\leq N, 1\leq j\leq M} \mu_{i,j} a_i b_j$ sur k, alors $0 = \sum_{1\leq i\leq N} (\sum_{1\leq j\leq M} \mu_{i,j} a_i) b_j$. Par liberté des b_j sur K, on obtient $\sum_{1\leq j\leq M} \mu_{i,j} a_i = 0$ pour chaque i. Par liberté des a_i sur k, tous les $\mu_{i,j}$ sont nuls. Donc la famille est libre. La relation sur les dimension en découle directement.

(ii) On applique le résultat précédent avec $K = k[x]$ et $L = k[x, y]$. On obtient

$$[k[x, y] : k] = [k[x] : k][(k[x])[y] : k[x]].$$

Il suffit donc de montrer que $[(k[x])[y] : k[x]] \leq [k[y] : k]$. Ceci est clair car le polynôme minimal de y sur k est un polynôme à coefficient dans $k[x]$ et donc est un polynôme annulateur sur $k[x]$. Maintenant $x+y, xy \in k[x, y]$, donc $[k[x+y] : k] < \infty$ et $[k[xy] : k] < \infty$. Donc $x + y$ et xy sont algébriques sur k.

Exercice 5

(i) Comme $[K : k] = 2$, on peut compléter $\{1\}$ en une base $\{1, z\}$ de K sur k. Alors il existe $\lambda, \mu \in k$ tels que $z^2 = \lambda z + \mu$. Comme la caractéristique de k n'est pas 2, ceci s'écrit $(z - \frac{\lambda}{2})^2 = \mu + \frac{\lambda}{4}$. On pose $x = z - \frac{\lambda}{2}$. Alors par construction $x^2 \in k$. De plus comme $z \notin k$, on a $x \notin k$ et $K = k[x]$.

(ii) Pour un tel autre y, on a $\lambda, \mu \in k$ tels que $y = \lambda x + \mu$. Alors $2\lambda\mu x = y^2 - \lambda^2 x^2 - \mu^2 \in k$. Comme $x \notin k$ et la caractéristique est différente de 2, ceci implique $\lambda = 0$ ou $\mu = 0$. Si $\lambda = 0$, $y = \mu \in k$, contradiction. Donc $\mu = 0$ et $y = \lambda x$ avec $\lambda \neq 0$ car $y \neq 0$.

(iii) D'après ce qui précède, une telle extension K s'écrit $K = \mathbf{Q}[\sqrt{\frac{p}{q}}]$ avec $p, q \in \mathbf{Z}$ premiers entre eux. En multipliant par $q \in \mathbf{Q}$, on voit que $K = \mathbf{Q}[\sqrt{pq}]$. Si $pq = r^2 p' q'$ avec $p', q', r \in \mathbf{Z}$, on a $K = \mathbf{Q}[r\sqrt{p'q'}] = \mathbf{Q}[\sqrt{p'q'}]$. Donc $K = \mathbf{Q}[\sqrt{n}]$ avec $n \neq 1$ dans $\mathbf{Z}$ sans facteur carré. Si c'est vrai pour un autre m, d'après (ii) on a $\sqrt{n} = \frac{s}{t}\sqrt{m}$ avec $s, t \in \mathbf{Z}$ premiers entre eux. Alors $nt^2 = ms^2$ et le Lemme de Gauss implique que s^2 divise n et t^2 divise m. Comme m et n n'ont pas de facteur carré, on en déduit $s^2 = t^2 = 1$ et $m = n$.

Exercice 6

(i) Si D a une équation de la forme $y = Ax + B$ avec $A, B \in \mathbf{R}$, on a par hypothèse $x_1 \neq x_2 \in k$ tels que $Ax_1 + B, Ax_2 + B \in k$. Donc $A, B \in k$. Sinon D a une équation de la forme $x = A$. Comme la droite contient un point de k^2, on obtient $A \in k$.

C a une équation $(x - x_0)^2 + (y - y_0)^2 = R^2$ avec $(x_0, y_0) \in k^2$ les coordonnées du centre. Comme C contient un point de k^2, on obtient $R^2 \in k$, d'où le résultat.

(ii) Dans le premier cas, on écrit une équation de la droite $aX + bY + c = 0$ et du cercle $X^2 + Y^2 + dX + eY + f = 0$ avec $a, b, c, d, e, f \in k$. Si $b \neq 0$, on écrit $y = -c/b - ax/b$ et on substitue y dans l'équation du cercle. On obtient une équation de degré au plus 2 et $[k[x] : k] \leq 2$. Comme $y \in k[x]$, on a aussi $[k[y] : k] \leq 2$. Le raisonnement est analogue si $a \neq 0$.

Dans le cas de deux cercles, le raisonnement est analogue en commencant par soustraire les deux équations de cercle pour obtenir une relation du type $(d-d')x+(e-e')y+(f-f') = 0$.

(iii) Si la condition de la définition du cours est satisfaite, on obtient la suite de

corps $k_0, \cdots, k_n$ en appliquant successivement le résultat de (ii) aux points $P_1, P_2, \cdots$. Réciproquement, l'extension $k_{i-1} \subset k_i$ est quadratique est donc d'après l'exercice 5 on a $k_i = k_{i-1}[x]$ avec $x^2 \in k_{i-1}^*$. D'après le cours, x est constructible, et on peut donc conclure par récurrence sur n.

(iv) Considérons deux éléments x, y constructibles avec des suites de corps comme ci-dessus $k_0, \cdots, k_n$ et $k'_0, \cdots, k'_{n'}$ qui leurs sont respectivement associées. Alors on définit une nouvelle suite de corps $K_0 = k_0, \cdots, K_n = k_n$, $K_{n+1} = k_n[k'_1], \cdots, K_{[n+n']} = k_n[k_{n'}]$. On supprime les corps redondant dans la suite, et on obtient une suite comme dans l'énoncé. Or $x + y, xy, x^{-1} \in k_n k_{n'}$, ils sont donc constructibles.

De plus, si x est constructible, le degré de x divise $[k_n : k_0]$ qui vaut 2^n par le théorème de la base télescopique. Donc x est algébrique et son degré est une puissance de 2.

(v) Dans ce cas, le degré de $\cos\frac{2\pi}{p}$ est de la forme 2^n. Mais ce degré est $(p-1)/2$ d'après l'exercice suivant, donc $p - 1 = 2^{n+1}$.

Exercice 7

(i) Le critère d'Eisenstein avec $p = 19$ donne le résultat immédiatement.

(ii) Comme $\Phi_p(X) = \frac{X^p-1}{X-1}$, on a $\Phi_p(X+1) = \frac{(X+1)^p-1}{X} = \sum_{1\leq k\leq p} C_p^k X^{k-1}$. Le critère d'Eisenstein avec p s'applique à ce polynôme, donc $\Phi_p(X+1)$ est irréductible, donc $\Phi_p(X)$ aussi.

(iii) On suppose que $p > 2$. D'après ce qui précède, $\Phi_p(X)$ est le polynôme minimal de $x = e^{2i\pi/p}$ sur $\mathbf{Q}$ donc son degré est $p - 1$. Maintenant, $\cos(2\pi/p) = \frac{x+x^{-1}}{2}$ donc $\mathbf{Q}[\cos(2\pi/p)] \subset \mathbf{Q}[x]$. Mais aussi $x^2 - 2x\cos(2\pi/p) + 1 = 0$ donc $[\mathbf{Q}[x] : \mathbf{Q}[\cos(2\pi/p)]]$ divise 2. Ce n'est pas 1 car x n'est pas réel. Donc $[\mathbf{Q}[x] : \mathbf{Q}[\cos(2\pi/p)]] = 2$ et d'après le théorème de la base téléscopique, $[\mathbf{Q}[\cos(2\pi/p)] : \mathbf{Q}] = \frac{[\mathbf{Q}[x]:\mathbf{Q}]}{[\mathbf{Q}[x]:\mathbf{Q}[\cos(2\pi/p)]]} = (p-1)/2$.

Exercice 8

(i) Si on a un corps intermédiaire $k \subset K' \subset K$, on a d'après le théorème de la base téléscopique $[K : k] = [K : K'][K' : k]$. Comme $[K : k]$ est premier, $[K : K'] = 1$ ou $[K' : k] = 1$, donc $K' = K$ ou $K' = k$.

(ii) On a $k \subset k[x^2] \subset k[x]$ et d'après le théorème de base téléscopique

$$[k[x] : k] = k[[x^2] : k][k[x] : k[x^2]].$$

Si $x \notin k[x^2]$, x est de degré 2 sur $k[x^2]$. Donc $[k[x] : k[x^2]] = 2$, contradiction car $[k[x] : k]$ est impair. Donc $k[x] = k[x^2]$.

(iii) Pour $1 \leq i \leq n$, soit $P_i(X) = \frac{P(X)}{(X-x_1)\cdots(X-x_{i-1})}$. Alors $P_i(X) \in (\mathbf{Q}[x_1, \cdots, x_{i-1}])[X]$, $\deg(P_i) = n - i + 1$ et $P_i(x_i) = 0$. Donc

$$[(\mathbf{Q}[x_1, \cdots, x_{i-1}])[x_i] : \mathbf{Q}[x_1, \cdots, x_{i-1}]] \leq n - i + 1.$$

En utilisant la base téléscopique, on obtient

$$[\mathbf{Q}[x_1, \cdots, x_n] : \mathbf{Q}] = [\mathbf{Q}[x_1] : \mathbf{Q}][\mathbf{Q}[x_1, x_2] : \mathbf{Q}[x_1]] \cdots [\mathbf{Q}[x_1, \cdots, x_n] : \mathbf{Q}[x_1, \cdots, x_{n-1}]],$$

d'où le résultat.