École Polytechnique
Algèbre et théorie de Galois MAT 451

Corrigé du contrôle classant 2018

Ce corrigé constitue un ensemble d'indications pour résoudre les exercices.

Il ne s'agit en aucun cas d'un modèle de rédaction pour le contrôle classant.

Exercice 1.

1) Cours : $1 + X + \cdots + X^{p-1}$.

2) On a $\phi_{p^r}(X) = \frac{X^{p^r}-1}{X^{p^{r-1}}-1} = 1 + X^{p^{r-1}} + \cdots + X^{(p-1)p^{r-1}}$.

3) $\phi_6(X) = (X^6 - 1)(X^2 - 1)^{-1}(X^2 + X + 1)^{-1} = X^2 - X + 1$. Il y a un coefficient négatif.

4) Le discriminant est -3, le polynôme est irréductible dans $\mathbf{R}[X]$, donc dans $\mathbf{Q}[X]$.

5) Oui car 3 est un nombre premier de Fermat.

6) Le groupe de Galois est d'ordre 2. L'élément non trivial est la conjugaison complexe.

7) Le degré est $\phi(12) = 4$.

8) Les corps de décomposition K_3, K_4 respectivement de $\phi_3(X)$ et de $\phi_4(X)$.

9) On regarde les projection sur les quotients par $\mathrm{Gal}(K/K_3)$ et $\mathrm{Gal}(K/K_4)$.

10) Le sous corps engendré par K_3 et K_4 est K. Donc un élément dans le noyau du morphisme Φ est l'identité et Φ est injectif. Par cardinalité on obtient un isomorphisme.

11) Cours.

12) C'est le groupe de Klein, engendré par les double transpositions. En effet les éléments d'ordre 2 de S_4 sont les transpositions et les doubles transpositions. Mais un élément de G dont l'image dans S_4 a un point fixe est l'identité.

Exercice 2.

1) Le polynôme $P(X + 1)$ satisfait le critère d'Eisenstein avec le nombre premier 2.

2) Cours.

3) Pour $\alpha = \sqrt{6+\sqrt{11}}$ et $\beta = \sqrt{6-\sqrt{11}}$, les racines du polynômes sont $\pm\alpha$ et $\pm\beta$.

4) Comme $\alpha\beta = 5$, on peut choisir α comme générateur. Donc K est le corps de rupture de P de degré 4.

5) Les 4 éléments du groupe de Galois sont caractériés par leur image sur α qui est dans $\{\pm\alpha, \pm\beta\}$. On vérifie qu'ils sont tous d'ordre au plus 2.

6) Ce qui précède implique que le groupe ne contient pas d'élément d'ordre 4.

7) Cours.

8) Non en vertue des relations entre $\pm\alpha$ et $\pm\beta$.

9) Le groupe est donc isomorphe à $(\mathbf{Z}/2\mathbf{Z})^2$ qui contient 5 sous-groupes.

10) La correspondance de Galois implique qu'il y a 5 sous-corps.

11) Les sous-corps triviaux et les corps engendrés par $\sqrt{11}$, $\sqrt{22}$ et $\sqrt{2}$.

Exercice 3.

1) $K = \mathbf{R}$, $L = \mathbf{C}$, $q(X_1, X_2) = X_1^2 + X_2^2$. Alors q n'a pas de zéro non trivial dans $\mathbf{R}$, par contre $(i, 1)$ est un zéro dans $\mathbf{C}$.

2) C'est le théorème de l'élément primitif.

3) Supposons $n = 2$. Si $a_{1,1} = a_{2,2} = 0$, alors $a_{1,2} \neq 0$ et $x_1 = 0$ ou $x_2 = 0$. Sinon on peut supposer $a_{1,1} \neq 0$. On en déduit que le degré de x_1 sur $K[x_2]$ et 1 ou 2, mais comme le degré impair, on obtient $x_1 \in K[x_2]$.

4) Supposons $n = 3$. On peut supposer que $x_1 \neq 0$. Alors en divisant par x_1^2, on obtient la relation $q(1, x_2/x_1, x_3/x_1) = 0$. On peut supposer que x_2/x_1 intervient effectivement dans la relation. Alors on obtient comme ci-dessus que $x_2/x_1 \in K[x_3/x_1]$.

5) L'énoncé contra-posé est : si q est anisotrope (sans zéro non-trivial) dans K, elle l'est aussi dans L extension de degré impair. Si cet énoncé était faux, alors on peut considérer un triplet (K, L, q) pour lequel ça ne fonctionne pas avec $[L : K]$ de degré minimal. Alors pour $x \in L \setminus K$, ça ne fonctionne pas non plus pour le triple $(K, K[x], q)$. Donc pour une raison de degré, $L = K[x]$.

6) Pour chaque i, il existe un polynôme $Q_i(X) \in K[X]$ de degré au plus $d-1$ tel que $x_i = P_i(\alpha)$. Alors il suffit de considérer Q le PGCD des Q_i et $P_i = Q_i/Q$.

7) Soit $\alpha_i \in K$ le coefficient de P_i devant X^δ. Alors $(\alpha_1, \cdots, \alpha_n) \neq (0, \cdots, 0)$. Comme le coefficient de Q devant $X^{2\delta}$ est $\sum_{i,j} a_{i,j}\alpha_i\alpha_j$, on obtient $q(\alpha_1, \cdots, \alpha_n) = 0$.

8) Le degré d de P étant impair et Q de degré pair, et comme $2d > 2\delta$, il existe un facteur irréductible R de Q dans $K[X]$ différent de P et de degré impair. Alors $\deg(R) < d$ et on peut choisir $L' = K[X]/(P_1)$.

9) En considérant dans la question 5 un triplet dans une extension de degré minimal, on obtient une contradiction.

Exercice 4

On a vu en PC l'existence d'une extension dont S_n est le groupe de Galois. On montre alors que tout groupe fini est isomorphe au sous-groupe d'un groupe symétrique (en utilisant l'action fidèle du groupe sur lui-même par multiplication à gauche).