École Polytechnique
Algèbre et théorie de Galois MAT 451

Corrigé du contrôle classant 2019

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) Soit $x \in L \setminus K$ et

$$Q(X) = X^2 + \lambda X + \mu$$

son polynôme minimal sur K. Comme Q est irréductible, on a $\mu \neq 0$. Si $\lambda = 0$, on a $\mu = x^2$ et donc $Q(X) = (X - x)^2$ non séparable, donc non irréductible, contradiction.

2) On considère x et Q comme ci-dessus. On considère x' un autre générateur de L de la forme $x' = \alpha x + \beta$ avec $\alpha \in K^*$ et $\beta \in K$. Il suffit de montrer qu'on peut choisir α et β pour que $(x')^2 - x' \in K$. Ceci équivaut à

$$\alpha^2 x^2 + \beta^2 - \alpha x - \beta = (\alpha^2\lambda - \alpha)x + \alpha^2\mu + \beta^2 - \beta \in K,$$

et $\alpha^2\lambda - \alpha = 0$. Ceci équivaut à $\alpha = \lambda^{-1}$ (on a vu en 1 que $\lambda \neq 0$). On pose donc $x' = x\lambda^{-1} + \beta$.

3) Le groupe de Galois est d'ordre 2, il suffit donc de donner la matrice de l'élément σ qui n'est pas l'identité. On a $\sigma(1) = 1$ et $\sigma(b)$ est le conjugué de b non égal à b. Mais $P(b + 1) = b^2 + 1 - b - 1 + a = P(b) = 0$. Donc la matrice de σ est $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$.

4) Les extensions sont égales si et seulement si l'une est incluse dans l'autre, ce qui équivaut à l'existence de $\alpha \in K^*$, $\beta \in K$ avec $b' = \alpha b + \beta$. Ceci équivaut à $(\alpha b + \beta)^2 - \alpha b - \beta + a' = 0$, ou encore $(\alpha^2 - \alpha)b + \alpha^2 a + \beta^2 - \beta + a' = 0$. Ceci équivaut à $\alpha = 1$ et $a - a' = \beta^2 - \beta$.

5) Pour $K = \mathbf{F}_2$, il n'y a qu'une seulle valeur possible pour a qui est 1. L'expression $\beta^2 - \beta$ est nulle pour tous $\beta \in \mathbf{F}_2$. Ceci est cohérent avec le fait que K n'a qu'une seule extension quadratique, $\mathbf{F}_4$. C'est le corps de

décomposition du polynôme X^2-X+1. On note aussi que $Fr(b) = b^2 = b+1$ est bien le conjugué de b.

6) Pour $N \geq 1$, $\mathbf{F}_{2^N}$ n'a aussi qu'une seule extension de degré 2, $\mathbf{F}_{2^{N+1}}$. Or $\mu^2 - \mu$ prend 2^{N-1} valeurs distinctes quand μ parcourt $\mathbf{F}_{2^{N-1}}$ (car une valeur n'est atteinte qu'au plus deux fois et μ, $\mu + 1$ donnent la même valeur). Il y a donc au plus 2^{N-1} polynômes irréductibles dans $\mathbf{F}_{2^N}$ de la forme $X^2 - X + a$. D'après l'analyse de la section 5, pour un tel polynôme irréductible, les polynômes $X^2 - X + (a + \mu)$ avec μ comme ci-dessus est aussi irréductible. Il y a donc exactement 2^{N-1} tels polynômes. On peut aussi compter le nombre de polynômes de cette forme : 2^N, et le nombre de polynômes réductibles de cette forme : 2^{N-1}. La différence est bien 2^{N-1}. C'est bien cohérent.

7) Soient α, β les racines du polynôme dans une clôture algébrique. Ces éléments sont conjugués sur $\mathbf{F}_{2^N}$ et donc $\beta = \alpha^{(2^N)}$. Alors $\alpha+\beta = a$ devient $\alpha^{(2^N)} + \alpha + a = 0$. On a la même relation pour β.

8) On obtient comme en 8, en écrivant q à la place de 2^N, que f irréductible divise $X^q + X + a$. Réciproquement, $X^{(2^n)} + X + a$ est premier avec sa dérivée donc séparable. Donc si f le divise, il a deux racines distinctes. Pour α une de ces racines, on a $\alpha^q = b - \alpha = \beta$ racine de f. Donc $\alpha^q \neq \beta$ et $\alpha \notin \mathbf{F}_q$. Le polynôme est bien irréductible.

Exercice 2.

1) C'est un cours comme pour le Lemme d'Artin.

2) On a $K \subset L^{G_x}$ et $x \in L^{G_x}$.

3) Comme G agit transitivement sur $G.x$, l'application est uniquement déterminée par les propriétés. Maintenant, pour $z = g.x \in G.x$, posons $\phi(z) = g.y$. Si $g.x = g'.x$, on a $g(g')^{-1} \in G_x$ et donc $g.y = g'.y$ par hypothèse. Donc ϕ est bine définie. On vérifie alors directement les propriétés.

4) L'unicité est claire car deux polylômes á coefficients dans un corps de degré strictiement inférieur à $|G.x|$ et qui coincident en $|G.x|$ points sont égaux. Pour l'existence, on écrit $P(y) = \phi(y)$ pour $y \in G.x$ ce qui donne $|G.x|$ équations en les coefficients de P. C'est un système linéaire de Vandermonde (voir le prémisse du sujet), qui est inversible.

5) On a maintenant $y = P(x)$ et les coefficients de P sont invariants sont l'action de G car pour $g \in G$, le polynôme P^g obtenu à partir de P en appliquant g aux coefficients satisfait les propriétés de la question 4. Donc $P(X) \in K[X]$ et $y \in K[x]$.

Exercice 3.

1) C'est une conséquence du théorême de Langrange dans le groupe additif de l'anneau.

2) L'application naturelle de la caractéristique est surjective, on en déduit le résultat.

3) Si c'est un corps c'est $\mathbf{F}_{p^2}$. Sinon il admet un sous corps premier isomorphe à $\mathbf{F}_p$. C'est donc un quotient de $\mathbf{F}_p[X]$ par un polynôme $P(X)$

4) On a les anneaux : $\mathbf{F}_p \times \mathbf{F}_p$, $\mathbf{Z}/(p^2\mathbf{Z})$, $\mathbf{F}_{p^2}$ et $\mathbf{F}_p[X]/(X^2)$. Le deuxième est de caractéristique p^2, les trois autres de caractéristique p. Le troisième est un corps, pas les deux autres anneaux de caractéristique p car $(1,0)(0,1) = 0$ pour le premier et $\overline{X}^p = 0$ pour le dernier. Enfin $\mathbf{F}_p \times \mathbf{F}_p$ n'a pas d'élément non nul nilpotent. Réciproquement, d'après les question précendent, il suffit de consider un anneau de caractéristique p qui n'est pas un corps. C'est donc un quotient de $\mathbf{F}_p[X]$ par un polynôme $P(X)$ de degré 2 réductible : $P(X) = (X-\alpha)(X-\beta)$. Si $P(X) = (X-\alpha)^2$ est un carré, on obtient un corps isomorphe à $\mathbf{F}_p[X]/(X^2)$. Sinon, $(X-\alpha)$ et $(X-\beta)$ est le lemme chinois implique qu'on obtient un anneau isomorphe à $\mathbf{F}_p \times \mathbf{F}_p$.

Exercice 4.

On a $P(0) = 1$ et l'ensemble des racines de P est invariant par la transformation $x \mapsto x^{-1}$. Notons donc $\{(x_1, x_1^{-1}), (x_2, x_2^{-1}), \cdots, (x_d, x_d^{-1})\}$ l'ensemble des racines. Le groupe de Galois est un sous-groupe de l'ensemble des permutations σ de ces racines. De plus, il suffit de connaître l'image de $x_1, \cdots, x_d$. Il y a $2d$ possibilités pour $\sigma(x_1)$. Puis $2d-2$ possibilités pour $\sigma(x_2)$, toutes les racines sauf $\sigma(x_1)$ et $\sigma(x_1)^{-1}$. Puis $2d-4$ possibilités pour $\sigma(x_3)$. Au final, on obtient le majorant

$$2d.2(d-1).2(d-2)\cdots 2 = 2^d d!.$$