Université de Bordeaux **Master Mathématiques fondamentales**
Semestre 7 **Théorie de Galois et représentations**

DM n°2 (année 2022/2023) - corrigé

Exercice 1. (1) Soit $\alpha \in K$: écrivons $\alpha = \frac{u(t)}{v(t)}$ avec $u(t), v(t) \in \mathbf{F}_p[t]$, $v(t)$ unitaire et $\mathsf{pgcd}(u(t), v(t)) = 1$. Si $P(\alpha) = 0$, on a $tu(t)^p - tu(t)v(t)^{p-1} - v(t)^p = 0$, ce qui implique que $u(t) \mid v(t)^p$, de sorte que $u(t) \in \mathbf{F}_p^\times$, et $v(t) \mid tu(t)^p$, d'où $v(t) \mid t$ puisque $\mathsf{pgcd}(u(t), v(t)) = 1$. On a bien sûr $\alpha \notin \mathbf{F}_p$ (parce que $\lambda^p = \lambda$ pour tout $\lambda \in \mathbf{F}_p$) : on a nécessairement $\alpha = \frac{\lambda}{t}$ avec $\lambda \in \mathbf{F}_p^\times$, et $t\lambda^p - (\lambda - 1)t^p$, soit encore $\lambda = (\lambda - 1)t^{p-1}$, ce qui est impossible. Il en résulte que P n'a pas de racine dans K.
(2) Si $\lambda \in \mathbf{F}_p$, on a $P(\alpha + \lambda) = (\alpha + \lambda)^p - (\alpha + \lambda) - \frac{1}{t} = \alpha^p + \lambda^p - \alpha - \lambda - \frac{1}{t} = P(\alpha) + \lambda^p - \lambda$ (la deuxième égalité provient du fait que l'élévation à la puissance p est un morphisme d'anneaux en caractéristique p). Comme $P(\alpha) = 0$ et $\lambda^p = \lambda$ (parce que $\lambda \in \mathbf{F}_p$), on a donc $P(\alpha + \lambda) = 0$. Les éléments $\alpha + \lambda$ pour $\lambda \in \mathbf{F}_p$ fournissent p racines distinctes de P : ce sont donc les racines de P dans $\overline{K}$. Cela montre que P est séparable.
(3) Soit $Q(X) \in K[X]$ un diviseur unitaire de $P(X)$: il existe $I \subset \mathbf{F}_p$ tel que $Q(X) = \prod\limits_{\lambda \in I}(X - \alpha - \lambda)$. Si $d = \#I = \deg(Q)$, le coefficient de X^{d-1} de Q est $-d\alpha - \sum\limits_{\lambda \in I} \lambda \in K$: on a donc $d\alpha \in K$. Si $0 < d < p$, l'image de d dans K est inversible, ce qui implique que $\alpha \in K$, contredisant la question (1). On a donc $d \in \{0, p\}$, ce qui prouve que P est irréductible dans $K[X]$.
(4) Comme L est le corps de décomposition sur K d'un polynôme séparable, l'extension L/K est galoisienne. L'ensemble des racines de P est $\alpha + \mathbf{F}_p$ et $\mathbf{F}_p \subset K$, on a $L = K(\alpha)$: comme P est irréductible dans $K[X]$, on a donc $[L : K] = p$. Comme p est premier, le groupe $\mathrm{Gal}(L/K)$ est donc cyclique d'ordre p.

Exercice 2. (1) Écrivons $K = \mathbf{C}(\alpha_1, \ldots, \alpha_r)$ (en fait, on peut prendre $r = 1$ en vertu du théorème de l'élément primitif). Posons $P = \prod\limits_{k=1}^{r} P_{\alpha_k, \mathbf{R}} \in \mathbf{R}[X]$ (où $P_{\alpha, \mathbf{R}}$ désigne le polynôme minimal de α sur $\mathbf{R}$), et notons L un corps de décomposition de P sur K. L'extension $L/\mathbf{R}$ est galoisienne comme corps de décomposition d'un polynôme en caractéristique 0 (le corps L est une *clôture normale* de K sur $\mathbf{R}$).
(2) Soit $f(X) \in \mathbf{R}[X]$ de degré impair. Quitte à le diviser par son coefficient dominant, on peut le supposer unitaire. On a $\lim\limits_{t \to \infty} f(t) = +\infty$ et $\lim\limits_{t \to -\infty} f(t) = -\infty$. Comme une application polynômiale est continue, le théorème des valeurs intermédiaires implique que f s'annule sur $\mathbf{R}$. Si $\deg(f) > 1$, cela implique que f n'est pas irréductible dans $\mathbf{R}[X]$ (c'est le seul endroit du raisonnement où on fait de l'analyse).
(3) Soit $F/\mathbf{R}$ de degré impair. Si $\alpha \in F$, on a $\deg(P_{\alpha, \mathbf{R}}) = [\mathbf{R}(\alpha) : \mathbf{R}] \mid [F : \mathbf{R}]$ donc $P_{\alpha, \mathbf{R}}$ est de degré impair. Comme il est irréductible dans $\mathbf{R}[X]$, la question précédente implique que $\deg(P_{\alpha, \mathbf{R}}) = 1$, *i.e.* que $\alpha \in \mathbf{R}$. On a donc nécessairement $F = \mathbf{R}$.
(4) Si $F = L^S$, la correspondance de Galois implique que $[F : \mathbf{R}] = (G : S)$ est impair : la question précédente montre que $F = \mathbf{R}$, et donc que $(G : S) = 1$, *i.e.* $G = S$.
(5) H est un sous-groupe de $G = S$, qui est un 2-groupe : c'est donc un 2-groupe lui aussi.
(6) Procédons par récurrence sur r, le cas $r = 1$ étant trivial : supposons $r > 1$. Le centre de H est non trivial : il existe un sous-groupe distingué strict H_0 de H (si H est abélien, tout sous-groupe strict convient, sinon on prend $H_0 = \mathsf{Z}(H)$). L'hypothèse de récurrence appliquée au 2-groupe H/H_0 implique l'existence d'un sous-groupe H' d'indice 2 dans H (et contenant H_0).
(7) Posons $M = L^{H'}$: par construction, on a $[M : \mathbf{C}] = (H : H') = 2$: si $\alpha \in M \setminus \mathbf{C}$, on a $M = \mathbf{C}(\alpha)$, et le polynôme minimal de α sur $\mathbf{C}$ est de degré 2. Il existe donc $a, b \in \mathbf{C}$ tels que $\alpha^2 + a\alpha + b = 0$, soit $\big(\alpha + \frac{a}{2}\big)^2 + b - \frac{a^2}{4} = 0$, *i.e.* $\beta^2 = \gamma$ où $\beta = \alpha + \frac{a}{2}$ et $\gamma = \frac{a^2}{4} - b \in \mathbf{C}$. Or on sait extraire des racines carrées dans $\mathbf{C}$: écrivons $\gamma = u + iv$ avec $u, v \in \mathbf{R}$. Si $z = x + iy$ avec $x, y \in \mathbf{R}$, on a $z^2 = \gamma$ si et seulement si $x^2 - y^2 = u$ et $2xy = v$, et $(x^2 + y^2)^2 = u^2 + v^2$ *i.e.* $x^2 + y^2 = \sqrt{u^2 + v^2}$: on en déduit que $x^2 = \frac{\sqrt{u^2+v^2}+u}{2} \in \mathbf{R}_{\geq 0}$ et $y^2 = \frac{\sqrt{u^2+v^2}-u}{2} \in \mathbf{R}_{\geq 0}$, le signe de xy étant celui de v. Cela implique donc que $\beta \in \mathbf{C}$, d'où $\alpha \in \mathbf{C}$: absurde.
(8) L'hypothèse $r > 0$ étant contradictoire, on a $r = 0$, *i.e.* $\#H = [L : \mathbf{C}] = 1$: on a $L = \mathbf{C}$, donc $K = \mathbf{C}$. On a montré que $\mathbf{C}$ n'a pas d'extension finie non triviale : il est algébriquement clos.