École polytechnique 2022-2023
Théorie de Galois

Feuille d'exercices 5

Exercice 1. Soit Ω une clôture algébrique de k. Si α est une racine de f dans Ω, elle est de degré exactement d sur $\mathbb{F}_p$ donc appartient à l'unique sous-corps de cardinal q de Ω, qui est k. Le polynôme est donc scindé sur k. (Voir l'exercice 5 pour une description plus précise des conjugués de α.)

Exercice 2. Soit $K/\mathbb{F}_p$ une extension de degré d ; on sait qu'une telle extension existe : considérer un corps de décomposition de $T^q - T$, où $q = p^d$. Le groupe multiplicatif $K^\times$ étant cyclique, il existe $x \in K$ tel que $K^\times = <x> = \{x^i \,|\, 0 \leq i < q-1\}$; en particulier, $K = \mathbb{F}_p[x]$ (« théorème de l'élément primitif »). Le polynôme minimal de x sur $\mathbb{F}_p$ est donc un polynôme irréductible de degré $[K : \mathbb{F}_p] = d$.

Exercice 3. (i) L'inclusion du terme de gauche dans le terme de droite est le petit théorème de Fermat (ou l'additivité du morphisme de Frobenius). Le terme de droite est de cardinal au plus p car il s'agit de l'ensemble des racines (dans un corps) d'un polynôme de degré p. Ainsi, de même qu'un élément $z \in \mathbb{C}$ est réel si et seulement si $\overline{z} = z$, un élément $x \in \Omega$ est dans $\mathbb{F}_p$ si et seulement si $x^p = x$. On va appliquer ce critère à $\sqrt{-1}$ et $\sqrt{2}$.

(ii) Existence de ζ « $= \sqrt{-1}$ » : le corps Ω est algébriquement clos. Il appartient à $\mathbb{F}_p$ si et seulement si -1 est un carré dans $\mathbb{F}_p$ (d'autre racine étant $-\zeta$) ; d'après ce qui précède cela revient à dire qu'il est fixe par l'endomorphisme de Frobenius. Comme ζ^p ne dépend que de p (mod 4), car $\zeta^4 = 1$, le résultat en découle aussitôt.

(iii) Si $\zeta^4 = -1$ (racine primitive 8-ième de l'unité), on a $(\zeta + \zeta^{-1})^2 = 2$ (vrai dans n'importe quel anneau). Ainsi, $\zeta + \zeta^{-1}$« $= \sqrt{2}$ » (comme sur les complexes) et 2 est un carré dans $\mathbb{F}_p$ si et seulement si $\zeta + \zeta^{-1} \in \mathbb{F}_p$, si et seulement si $\zeta + \zeta^{-1}$ est fixe par Frobenius. Par additivité de ce dernier, cela est équivalent à la condition :

$$\zeta^p + \zeta^{-p} = \zeta + \zeta^{-1}.$$

Le terme de gauche ne dépend que de p (mod 8). Pour conclure, il faut vérifier que $\zeta^3 + \zeta^{-3} \neq \zeta + \zeta^{-1}$. Or, $\zeta^3 + \zeta^{-3}$ est l'autre racine carré de 2 : on a $\zeta^3 + \zeta^{-3} = -(\zeta + \zeta^{-1})$ car $\zeta^4 = -1$. (L'inégalité annoncée résulte du fait que $-1 \neq 1$ (car $p \neq 2$) et $\zeta + \zeta^{-1} \neq 0$.)

Exercice 4. (i) De même qu'un nombre entier n est composé si et seulement si il a un facteur premier $\leq \sqrt{n}$, un polynôme P est réductible si et seulement si il est divisible par un polynôme irréductible de degré $r \leq d/2$; un tel polynôme a une racine dans $\mathbb{F}_{p^r}$. Réciproquement, le polynôme minimal d'un élément de $\mathbb{F}_{p^r}$ est de degré un diviseur de r (en particulier, inférieur ou égal à r). Ceci suffit pour conclure.

(ii) Le polynôme $X^2 + X + 1 = (X^3 - 1)/(X - 1)$ est irréductible sur $\mathbb{F}_2$; le quotient $\mathbb{F}_2[X]/(X^2 + X + 1)$ est donc un corps à 4 éléments et la classe j de X satisfait $j^2 = j + 1$ (et donc $j^3 = 1$).

(iii) Pour tester si un polynôme f de degré 5 sur $\mathbb{F}_2$ est irréductible, il suffit d'après ce qui précède de vérifier que les trois éléments $f(0)$, $f(1)$ et $f(j)$ [calculé dans $\mathbb{F}^4$] sont non nuls. (On utilise le fait que j et j^2 sont conjugués sur $\mathbb{F}^2$: $f(j) = 0$ si et seulement si $f(j^2) = 0$.) Il est alors immédiat de vérifier que parmi les $2^5 = 32$ polynômes unitaires de degré 5, seuls les 6 de la liste sont irréductibles.

On montre d'ailleurs immédiatement que si ℓ est premier, il y a toujours exactement $(p^\ell - p)/\ell$ polynômes irréductibles unitaires de degré ℓ. (Si ℓ n'est pas premier, il existe une formule explicite, due à Gauß.) Remarquer également que cet ensemble est stable par la substitution palindromique $f(X) \mapsto X^\ell f(1/X)$.

Exercice 5. (i) Soit $K = \mathbb{F}_p[x] \subseteq \Omega$, dont on cherche à calculer le degré sur $\mathbb{F}_p$. (Degré que l'on peut aussi interpréter comme le degré du polynôme minimal de x sur $\mathbb{F}_p$.) C'est un corps de cardinal une puissance q de p. Or, dans Ω, les sous-corps finis sont exactement les ensembles de points fixes d'une puissance de l'endomorphisme de Frobenius. La conclusion résulte alors du fait que K est fixe par Frob_p^d si et seulement si x l'est.

(ii) Soit $q = p^d$ le cardinal de $K = \mathbb{F}_p[x]$. On a $x^q = x$ d'où $x^{q-1} = 1$. En particulier, l'ordre (multiplicatif) N de x divise $q-1$ et est donc premier à q (donc p). D'autre part, on a vu que le degré d est le plus petit entier $\delta \geq 1$ tel que $x^{p^\delta} = x$, c'est-à-dire $x^{p^\delta - 1} = 1$. Puisque N est l'ordre de x, ceci est encore équivalent à $N | p^\delta - 1$, c'est-à-dire $p^\delta \equiv 1 \pmod{N}$.

(iii) De même que pour tout $z \in \mathbb{C}$, le polynôme $(X-z)(X-\overline{z})$ est à coefficients réels car invariant sous l'action de la conjugaison complexe, le polynôme $\prod_{0 \leq n < d} \left(X - \mathrm{Frob}_p^n(x)\right)$ est à coefficients dans $\mathbb{F}_p$, car invariant sous Frobenius. Comme il est de degré d, c'est le polynôme minimal de x (sur $\mathbb{F}_p$).

(iv) Soit α une racine dans Ω d'un tel polynôme. D'après ce qui précède, son degré est égal au cardinal de l'orbite du Frobenius agissant sur α. Or, par hypothèse, on a $\mathrm{Frob}_p(\alpha) = \alpha + a$ et donc $\mathrm{Frob}_p^n(\alpha) = \alpha + na$. (On utilise l'additivité du Frobenius et le fait que a soit fixe.) Pour conclure, il suffit d'observer que $\alpha + na = \alpha$ si et seulement si $p | n$; l'élément α est de degré p sur $\mathbb{F}_p$ et son polynôme minimal est $X^p - X - a$.

Exercice 6. (i) [Rappel d'une feuille précédente.] Comme $\Phi_p(X) = (X^p - 1)/(X-1)$, le polynôme $P = \Phi_p(X+1)$ n'est autre que $((X+1)^p - 1)/X$. Vérifions le critère d'Eisenstein pour P et le nombre premier p. On a $P(0) = \Phi_p(1) = p$, non divisible par p^2 et, $P \equiv X^{p-1} \pmod{p}$. Il est donc irréductible.

(ii) Soit ζ une racine de $\Phi_{p,\ell}$ dans un clôture algébrique de $\mathbb{F}_\ell$; c'est une racine primitive p-ième de l'unité. Ainsi, avec les notations de l'exercice précédent, on a $N = p$, et le degré de ζ sur $\mathbb{F}_\ell$ est l'ordre (multiplicatif) d de ℓ dans $\mathbb{Z}/p\mathbb{Z}$. Ainsi, les facteurs irréductibles de $\Phi_{p,\ell}$ ont tous le même degré. La conclusion résulte alors du fait que le polynôme $\Phi_{p,\ell}$ est sans racine multiple : c'est déjà le cas $X^p - 1 \pmod{\ell}$.

(iii) D'après ce qui précède, $\Phi_{p,\ell}$ est irréductible si et seulement si ℓ est d'ordre $p-1$ dans $\mathbb{F}_p^\times$. Comme ce dernier est de cardinal $p-1$, on a l'équivalence.

(iv) Résulte trivialement de (ii).

(v) Il s'agit de montrer que le polynôme Φ_p a une racine modulo ℓ pour une infinité de ℓ. C'est un fait général :

> Soit $P \in \mathbb{Z}[T]$ un polynôme non constant. Il existe une infinité de nombres premiers ℓ tels que P ait une racine dans $\mathbb{F}_\ell$.

Commençons par observer que l'on peut supposer que $P(0) = 1$ car, si $a = P(0) \neq 0$, on a $P(aT) = aQ(T)$, où $Q(0) = 1$, et si Q a une racine modulo un nombre premier ℓ, il en est de même de P. Supposons par l'absurde que les $P(n)$, pour $n \in \mathbb{N}$, n'aient qu'un nombre fini de diviseurs premiers $\ell_1, \ell_2, \ldots, \ell_r$. Pour chaque $n \in \mathbb{N}$, l'entier $P(n\ell_1\ell_2\cdots\ell_r)$ est congru à $P(0) = 1$ modulo chaque ℓ_i. Il en résulte que $P(n\ell_1\ell_2\cdots\ell_r)$ est premier à chacun des ℓ_i. Or, si n est grand, $P(n\ell_1\ell_2\cdots\ell_r)$ est grand (en valeur absolue) donc a un diviseur premier. Absurde.

Exercice 7. (i) $p = 5$. La question revient à déterminer le plus petit p tel que le polynôme cyclotomique

$\Phi_{23} = (T^{23}-1)/(T-1)$ soit irréductible sur $\mathbb{F}_p$. D'après l'exercice précédent, on veut donc que p soit un générateur de $(\mathbb{Z}/23\mathbb{Z})^\times$. Pour $p=2$, les puissances sont $1, 2, 8, 16, 32, 64, 128, 256 = 3, 6, 12, 24 = 1$; pour $p=3$, on a $1, 3, 27 = 4, 12, 36 = 13, 39 = 16, 48 = 2, 6, 18 = -5, -15 = 8, 24 = 1$. Dans ces deux cas, l'ordre n'est pas 22. Par contre, c'est le cas si $p=5$.

(ii) $p = 2, 3, 5, 11, 13, 19, 29, 37, 53, 59, \ldots$ On se demande maintenant pour quels p le polynôme Φ_p est irréductible sur $\mathbb{F}_2$, c'est-à-dire quand 2 est primitif dans $(\mathbb{Z}/p\mathbb{Z})^\times$. On vérifie à la main que $p = 3, 5$ conviennent mais pas 7 (car $2^3 = 1$), ni 17 (car $2^4 = -1$). On trouve par des calculs semblables les valeurs ci-dessus.

Exercice 8. Soient $n_1 = p$ et $n_2 = \binom{p}{2}$ les nombres de polynômes unitaires irréductibles de degré respectivement 1 et 2. Alors, le nombre cherché est

$$\sum_{a+2b=d} \left(\!\binom{n_1}{a}\!\right)\left(\!\binom{n_2}{b}\!\right)$$

où $\left(\!\binom{n}{r}\!\right) = \binom{r+n-1}{r}$ est le cardinal des multiensembles de cardinal r pris dans un ensemble de cardinal n. Par exemple, pour $d=3$, on trouve $(2p^3+p)/3$, qui est bien égal à $p^3 - (p^3-p)/3$ (cf. remarque dans la correction de l'exercice 3). La probabilité est donc $2/3 + 1/3p^2$. Lorsque $p=2$ et d quelconque, on trouve $2^{-d}\sum_{a+2b=d}(a+1)$. Par exemple, pour $d=3$, on (re)trouve $3/4$.