École polytechnique 2022-2023
Théorie de Galois

Feuille d'exercices 10

Exercice 1.

Soit $p \neq 2, 5$. Le groupe de Galois d'une extension de corps finis étant déterminé par son degré, il s'agit de trouver le degré d'un corps de décomposition de $(f \mod p)$, c'est-à-dire le plus petit entier $d \geq 1$ tel que le groupe (cyclique) $\mathbb{F}_{p^d}^\times$ contienne les 10 racines 10-ièmes de l'unité. Ceci se produit si et seulement si $p^d - 1$ est divisible par 10 : l'entier d est l'ordre de p dans $(\mathbb{Z}/10\mathbb{Z})^\times \simeq \mathbb{Z}/4\mathbb{Z}$. Modulo 10, il y a 4 possibilités pour p ; s'il est congru respectivement à $1, 3, 7 = -3, 9 = -1$ modulo 10, son ordre est, respectivement, $1, 4, 4, 2$. Les groupes de Galois correspondants sont $\{0\}$, $\mathbb{Z}/4\mathbb{Z}$, $\mathbb{Z}/4\mathbb{Z}$ et $\mathbb{Z}/2\mathbb{Z}$.

Exercice 2.

(i) Appliquer par exemple le critère d'Eisenstein[-Schönemann] pour $p = 2$, ou constater qu'il est irréductible sur $\mathbb{F}_3$.

(ii) [Méthode analytique] Une étude de fonction permet de voir que le polynôme P a trois racines réelles. Par exemple, parce P' a deux racines réelles et que $P(0) > 0 > P(1)$, de sorte que les valeurs de P en les deux extrema locaux sont de signes opposés. La conjugaison complexe induit donc bien une transposition (des deux racines non réelles conjuguées).

[Méthode algébrique] Le polynôme $(X^2 - 7X - 118) \in \mathbb{F}_{257}[X]$ est irréductible car son discriminant, 7, n'est pas un carré (modulo 257), comme on peut le voir par un calcul laborieux, montrant que les résidus quadratiques sont $\{0, 1, 2, 4, 8, 9, 11, 13, 15, 16, 17, 18, \ldots, 248, 249, 253, 255, 256\}$, ou bien en utilisant la *loi de réciprocité quadratique*, si on la connaît. Il résulte alors du théorème de réduction modulo p (Dedekind) que le groupe de Galois de P contient une transposition.

(iii) Il résulte de (i) que G contient un 5-cycle. En effet, il agit transitivement sur les racines donc (équation aux classes) est de cardinal divisible par 5 et un élément d'ordre 5 de S_5 — dont l'existence est assurée par Cauchy — est un 5-cycle. (Variante : utiliser le théorème de réduction modulo $p = 3$.) D'autre part, il résulte de (ii) qu'il contient également une transposition.

On vérifie que tout sous-groupe de S_5 contenant deux tels éléments, que l'on peut supposer être (01234) et $(0x)$ avec $x \neq 0$, est S_5 tout entier. Ceci est également vrai si on remplace 5 par un nombre premier quelconque et résulte du fait que l'on a aussi la transposition $(x2x)$ — en conjuguant par la translation $t \to t + x$ — donc $(02x)$ et, plus généralement tous les $(0kx)$. Voir l'exercice 4 de la feuille 1 pour les détails.

Exercice 3.

Posons $P = X^5 - X - 1$ et $G = \mathrm{Gal}(P, \mathbf{Q})$. D'après le cours, le polynôme P est résoluble par radicaux si et seulement si le groupe G est résoluble. On calcule G en réduisant modulo 2 et 3. La décomposition de $\bar{P} \in \mathbf{F}_2[X]$ en facteurs irréductibles étant $(X^2 + X + 1)(X^3 + X^2 + 1)$, on sait par le théorème de la réduction modulo p que $G \subset \mathfrak{S}_5$ contient une transposition. D'ailleurs, la réduction $\bar{P} \in \mathbf{F}_3[X]$ est irréductible et G contient donc un 5-cycle d'après le théorème de la réduction modulo p. Comme une transposition et un 5-cycle engendrent $\mathfrak{S}_5$, on conclut $G = \mathfrak{S}_5$. Or, ce groupe n'est pas résoluble.

Exercice 4.

(i) Soient U_p l'ensemble des racines p-ièmes de 1 et ξ une racine primitive. Le discriminant est

$$(-1)^{p(p-1)/2} \prod_{\omega \in U_p} \omega \prod_{\omega' \in U_p \setminus \{\omega\}} (1 - \omega' \omega^{-1})$$

$$= (-1)^{p(p-1)/2} \left(\prod_{\omega \in U_p} \omega \right) \times \left(\prod_{\omega'' \in U_p \setminus \{1\}} (1 - \omega'') \right)^p .$$

Le premier facteur est

$$(-1)^{p(p-1)/2}\xi^{p(p-1)/2} = (-1)^{(p-1)/2}.$$

Le deuxième facteur est $(P'(1))^p$ avec $P(X) = X^p - 1$, c'est donc p^p.

(ii) Une racine carrée du discriminant est dans le corps de décomposition du polynôme, c'est-à-dire $\mathbb{Q}[\exp(\frac{2i\pi}{p})]$. On conclut car, p étant impair,

$$\mathbb{Q}\left[\sqrt{(-1)^{\frac{p-1}{2}}p}\right] = \mathbb{Q}\left[\sqrt{(-1)^{\frac{p-1}{2}}p^p}\right].$$

(iii) Une extension quadratique de $\mathbb{Q}$ est de la forme $\mathbb{Q}[\sqrt{d}]$ avec d sans facteur carré. On écrit

$$d = \epsilon\mu p_1 p_2 \cdots p_m.$$

avec les p_i des nombres premiers impairs distinces, $\epsilon = -1$ ou 1, $\mu = 2$ ou 1. On alors $\mathbb{Q}[\sqrt{d}]$ dans

$$\mathbb{Q}[i, \sqrt{2}, \sqrt{p_1}, \cdots, \sqrt{p_m}] \subset \mathbb{Q}[e^{\frac{i\pi}{2}}, e^{\frac{i\pi}{4}}, e^{\frac{2i\pi}{p_1}}, \cdots, e^{\frac{2i\pi}{p_m}}] \subset \mathbb{Q}[e^{\frac{2i\pi}{N}}]$$

avec

$$N = 4p_1 p_2 \cdots p_m.$$

Exercice 5. (i) Φ_n divise $X^n - 1$, et ce polynôme est à racines simples dans $\mathbb{F}_p$ si p ne divise pas n.

(ii) L'élément $Frob_p$ est bien défini à conjugaison près. Puisque le groupe de Galois est abélien, il est bien défini.

(iii) Soit $A = \mathbb{Z}[\zeta_n] \simeq \mathbb{Z}[X]/\Phi_n(X)$. Soit g l'élément du groupe de Galois envoyant ζ_n sur ζ_n^p. On vérifie que g induit le Frobenius sur A/pA. L'élément $Frob_p$ correspond donc à p avec l'isomorphisme $\mathrm{Gal}(K/\mathbb{Q}) \simeq (\mathbb{Z}/n\mathbb{Z})^\times$.

(iv) Soit a premier à n : il est dans $(\mathbb{Z}/n\mathbb{Z})^\times \simeq \mathrm{Gal}(K/\mathbb{Q})$
Soit $g \in G$ l'élément correspondant à a. D'après le théorème de Cebotarev, il existe une infinité de nombres premiers p tels que $Frob_p = g$. D'après ce qui précède, cette condition est équivalente à $p = a \pmod n$.

Exercice 6.

(i) Comme on l'a vu dans la feuille 5 (exercice 4), il suffit de vérifier qu'il ne s'annule pas en $0, 1, j \in \mathbb{F}_4$.

(ii) Le sous-groupe engendré par deux tels éléments est de cardinal au moins $4 \times 3 = 12$. Il ne peut y avoir égalité car le seul sous-groupe d'indice 2 est A_4, qui ne contient pas de 4-cycle. Le seul diviseur de 24 strictement supérieur à 12 est 24.

(iii) Modulo 2, ce polynôme est irréductible, de sorte que le groupe de Galois contient un 4-cycle (par le théorème de réduction modulo p). Modulo 3, il a une unique racine (simple) ; par ce même théorème, on obtient l'existence d'un 3-cycle. Finalement, le groupe de Galois est S_4.

Exercice 7.

(i) Il résulte du théorème des restes chinois — d'après lequel $\mathbb{Z}/(2\dot{3}\cdot p)\mathbb{Z} \simeq \mathbb{F}_2 \times \mathbb{F}_3 \times \mathbb{F}_p$ — que les trois conditions sont indépendantes : il suffit donc de montrer que l'on peut satisfaire chacune d'entre elles. Or,

(a) il existe dans $\mathbb{F}_2[X]$ des polynômes irréductibles de tout degré, en particulier d ;

(b) il existe dans $\mathbb{F}_3[X]$ des polynômes irréductibles de tout degré, en particulier $d-1$;

(c) il existe dans $\mathbb{F}_p[X]$ un polynôme irréductible de degré 2, et $d-2$ polynômes unitaires de degré 1 car $p = |\mathbb{F}_p| \geq d-2$.

(ii) D'après le théorème de réduction modulo p, le groupe de Galois de f contient un d-cycle, un $(d-1)$-cycle et une transposition. Trois tels éléments engendrent S_d. En conjuguant par le d-cycle, qui agit transitivement, on peut supposer que (a) la transposition est $(1x)$, avec $1 < x \leq d$, et que (b) le $(d-1)$-cycle laisse fixe l'élément 1. La conjugaison par ce $(d-1)$-cycle permet d'obtenir toutes les transpositions $(1y)$, pour $y \neq x$; elles engendrent S_d.

Exercice 8.

La signature du Frobenius F agissant sur les racines de $f = f_1 \cdot \cdots \cdot f_r$ (décomposition en irréductibles) dans un corps de décomposition est égale à $(-1)^{d_1-1} \dots (-1)^{d_r-1} = (-1)^{d-r}$. Or, cette signature est égale à 1 si et seulement si F est une permutation paire, ce qui est équivalent au fait que le discriminant soit un carré.