

Feuille d'exercices 7

Exercice 1. (i) Soit $P = p_1 p_2 \cdots p_r$ un produit de nombres premiers distincts. Soit $f \in \mathbf{Z}/P[X]$ un polynôme unitaire et $f_i \in \mathbf{F}_{p_i}[X]$ sa réduction modulo p_i ($1 \leq i \leq r$). Montrer que f est réductible si et seulement si chaque f_i l'est.

(ii) Soient $p \geq 3$ un nombre premier et $d \geq 1$ un entier. Montrer que la proportion des polynômes à coefficients dans $\mathbf{F}_p$ irréductibles unitaires de degré d est au moins égale à $\frac{1}{2d}$.

(iii) En déduire que quand N tend vers $+\infty$, la proportion des polynômes f unitaires de degré d à coefficients entiers dans $[-N, N]$ qui sont *réductibles* tend vers 0. (Indication : on pourra commencer par montrer que chaque pour chaque $\varepsilon > 0$, il existe P comme ci-dessus tel que le nombre polynômes réductibles unitaires de $\mathbf{Z}/P[X]$ de degré d soit au plus εP^d puis considérer $N \geq P$ et le cardinal des fibres de la projection $f \mapsto f \bmod P$.)

Exercice 2. (i) Soit $d \geq 2$ un entier et $p \geq d - 2$ un nombre premier différent de 2 et 3. Montrer qu'il existe un polynôme $f \in \mathbf{Z}[X]$ unitaire de degré d tel que :

- la réduction modulo 2 de f soit irréductible dans $\mathbf{F}_2[X]$,
- la réduction modulo 3 de f soit de la forme $XQ(X)$ où $Q(X) \in \mathbf{F}_3[X]$ est irréductible,
- la réduction modulo p de f ait un facteur irréductible de degré 2 et $d - 2$ racines distinctes dans $\mathbf{F}_p$.

(ii) Montrer que le groupe de Galois sur $\mathbf{Q}$ de f est isomorphe au groupe symétrique $\mathfrak{S}_d$.

En combinant les techniques des deux exercices précédents, on peut montrer que « la plupart » des polynômes unitaires de degré d ont pour groupe de Galois $\mathfrak{S}_d$ (*Die Seltenheit der Gleichungen mit Affekt*, van der Waerden, 1933).

Exercice 3. (i) Montrer que le polynôme $1 + X + X^2 + X^3 + X^4 \in \mathbf{F}_2[X]$ n'a pas de racine dans $\mathbf{F}_4$, puis qu'il est irréductible.

(ii) Montrer qu'un 4-cycle et un 3-cycle engendrent $\mathfrak{S}_4$.

(iii) Déterminer le groupe de Galois sur $\mathbf{Q}$ du polynôme $X^4 + X^3 - X^2 + X - 1$.

Exercice 4. Soit K une extension finie de $\mathbf{R}$, on veut montrer que K est égal à $\mathbf{R}$ ou isomorphe à $\mathbf{C}$ (théorème de d'Alembert-Gauß).

(i) Montrer que si $K/\mathbf{R}$ est de degré 2, alors $K \simeq \mathbf{C}$.

(ii) Montrer que si $K/\mathbf{R}$ est de degré impair, alors $K = \mathbf{R}$.

(iii) Montrer que $\mathbf{C}$ n'admet pas d'extension de degré 2.

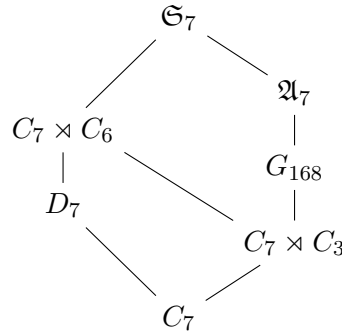
(iv) Supposons $K/\mathbf{R}$ galoisienne finie. Montrer l'existence d'une tour d'extensions

$$\mathbf{R} \subset K_1 \subset K_2 \subset \cdots \subset K_n = K$$

telle que $[K_1 : \mathbf{R}]$ est impair et, pour $i = 1, \dots, n - 1$, $[K_{i+1} : K_i] = 2$. (On pourra utiliser le théorème de Sylow : « si $|G| = p^\alpha m$ avec p premier et $(p, m) = 1$ alors G contient un sous-groupe d'ordre p^α ».)

(v) Conclure.

Exercice 5. On admet que les sous-groupes transitifs de $\mathfrak{S}_7$ sont, à conjugaison près, représentés par le schéma suivant :



où :

- G_{168} (d'ordre 168) est le groupe $\text{GL}_3(\mathbf{F}_2)$; il agit sur les 7 droites et est abstraitement isomorphe à $\text{PSL}_2(\mathbf{F}_7)$;
- $C_7 \rtimes C_6$ (d'ordre 42) est le groupe $\text{AGL}(\mathbf{F}_7)$ des fonctions affines $x \mapsto ax + b$ sur $\mathbf{F}_7$ (avec $a \in \mathbf{F}_7^\times$ et $b \in \mathbf{F}_7$);
- $C_7 \rtimes C_3$ (d'ordre 21) est le groupe des fonctions affines de la forme $x \mapsto ax + b$ sur $\mathbf{F}_7$ avec $a \in \{1, 2, 4\}$ (et $b \in \mathbf{F}_7$);
- le $D_7 = C_7 \rtimes C_2$ (d'ordre 14) le groupe diédral de l'heptagone, qui est aussi le groupe des fonctions affines de la forme $x \mapsto ax + b$ sur $\mathbf{F}_7$ avec $a \in \{1, -1\}$ (et $b \in \mathbf{F}_7$);
- C_7 (d'ordre 7) est le groupe cyclique.

(i) Soit $f = X^7 - 7X + 3 \in \mathbf{Z}[X]$ dont on note $x_0, \dots, x_6$ les racines dans un corps de décomposition K sur $\mathbf{Q}$. Montrer que f est irréductible.

(ii) On admet que f a exactement trois racines dans $\mathbf{F}_{107}$. Que peut-on en déduire sur le groupe de Galois G de f ?

(iii) Montrer que le polynôme de degré 35

$$g(T) = \prod_{i < j < k} (T - (x_i + x_j + x_k))$$

appartient à $\mathbf{Q}[X]$ et est *séparable*. (Indication : pour le second point, on pourra utiliser l'existence d'un 7-cycle dans le groupe de Galois G de f et le fait que le polynôme cyclotomique $\Phi_7(Z) = 1 + Z + \dots + Z^6$ est irréductible.)

(iv) Montrer que G_{168} agit 2-fois transitivement mais pas 3-fois transitivement sur les droites de $\mathbf{F}_2^3$. Montrer que $\mathfrak{A}_7$ agit 3-fois transitivement sur $\{1, \dots, 7\}$.

(v) On admet que g est divisible par le polynôme $T^7 + 14T^4 - 42T^2 - 21T + 9$. En déduire que le groupe de Galois G n'est ni le groupe alterné $\mathfrak{A}_7$ ni $\mathfrak{S}_7$. Conclure.