École Polytechnique 2009-2010

Théorie de Galois

Feuille d'exercices 8

Exercice 1. (i) Soit p un nombre premier. Montrer que pour tout entier $d \geq 1$, il existe un polynôme irréductible de degré d dans $\mathbf{F}_p[X]$.

(On pourra considérer un élément bien choisi du corps fini de cardinal p^d.)

(ii) Soient $n \geq 2$ un entier et $\ell > n+1$ un nombre premier. Montrer qu'il existe un polynôme $P \in \mathbf{Z}[X]$ unitaire de degré n tel que :

- la réduction modulo 2 de P soit irréductible dans $\mathbf{F}_2[X]$,

- la réduction modulo 3 de P soit de la forme $XQ(X)$ où $Q(X) \in \mathbf{F}_3[X]$ est irréductible,

- la réduction modulo ℓ de P ait un facteur irréductible de degré 2 et $n-2$ racines distinctes dans $\mathbf{F}_\ell$.

(iii) Soient $a, b, c \in \mathfrak{S}_n$ où a est un n-cycle, b un $n-1$-cycle et c une transposition. Montrer que a, b et c engendrent $\mathfrak{S}_n$. (On pourra montrer qu'il existe $\sigma \in \langle a \rangle$ tel que le point fixe de $\sigma b \sigma^{-1}$ n'est pas fixé par c.)

(iv) Montrer que P est irréductible dans $\mathbf{Q}[X]$, et que son groupe de Galois sur $\mathbf{Q}$ est isomorphe au groupe symétrique $\mathfrak{S}_n$.

Exercice 2. (i) Montrer que $\mathbf{F}_4 = \mathbf{F}_2[j]$ où $j \in \mathbf{F}_4$ est un élément tel que $1 + j + j^2 = 0$.

(ii) 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.

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

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

Exercice 3. Déterminer par réduction modulo p le groupe de Galois sur $\mathbf{Q}$ du polynôme

$$X^4 + 4X^3 + 12X^2 + 24X + 24.$$

Donnée : son discriminant est $2^{12}3^4$.

Sous-groupes transitifs de $\mathfrak{A}_5$. Soit G un sous-groupe de $\mathfrak{A}_5$ agissant transitivement sur l'ensemble $\{1, 2, 3, 4, 5\}$. On montrera dans l'ex. 5 que G est l'un des groupes suivants :

- le groupe cyclique engendré par un 5-cycle,

- le normalisateur dans $\mathfrak{A}_5$ du sous-groupe engendré par un 5-cycle[1],

- $\mathfrak{A}_5$.

Exercice 4. (i) Déterminer le groupe de Galois sur $\mathbf{Q}$ du polynôme $X^5 - 5X + 12$. On pourra utiliser la classification ci-dessus et les renseignements suivants (les x_i sont les racines complexes de ce polynôme) :

- $X^5 + 2X - 2$ est irréductible dans $\mathbf{F}_7[X]$,

[1] C'est-à-dire que si c est le 5-cycle en question, $G = \{g \in \mathfrak{A}_5,\ gcg^{-1} \in \langle c \rangle\}$. En fait, on verra qu'il existe une double-transposition $\tau \in G$ telle que $\tau c \tau^{-1} = c^{-1}$ et $G = \langle \tau, c \rangle$.

- le discriminant de $X^5 - 5X + 12$ vaut $2^{12}5^6$,

- $\prod_{1 \leq i < j \leq 5}(X - (x_i + x_j)) = (X^5 - 5X^3 - 10X^2 + 30X - 36)(X^5 + 5X^3 + 10X^2 + 10X + 4)$.

(ii) Montrer que les racines de $X^5 - 5X + 12$ s'expriment comme sommes de radicaux emboîtés.

(iii) Expliquer brièvement comment vous feriez pour vérifier chacune des informations données du (i).

Exercice 5. On se propose de démontrer la classification énoncée plus haut des sous-groupes transitifs de $\mathfrak{A}_5$.

(i) Montrer que si $d \leq 4$, un morphisme de groupes $\mathfrak{A}_5 \to \mathfrak{S}_d$ est nécessairement trivial.

(ii) En déduire que $\mathfrak{A}_5$ n'a pas de sous-groupe d'indice ≤ 4. (Considérer l'action par translations à gauche de G sur G/H.)

(iii) Montrer que si $G \subset \mathfrak{A}_5$ est un sous-groupe transitif, alors soit $G = \mathfrak{A}_5$, soit G est engendré par un 5-cycle, soit $|G| = 10$.

On suppose désormais que $|G| = 10$.

(iv) Montrer que G contient un 5-cycle c et une double-transposition τ.

(v) Montrer que $\langle c \rangle$ est d'indice 2 dans G, en déduire que c'est un sous-groupe distingué de G.

(vi) Montrer que $\tau c \tau^{-1} = c^{-1}$.

(vii) Conclure.

Exercice 6. (Polynôme d'Artin-Schreier) Soient p un nombre premier et $a \in \mathbf{F}_p^*$. Montrer que $X^p - X - a$ est irréductible dans $\mathbf{F}_p[X]$.

(Si Ω est une clôture algébrique de $\mathbf{F}_p$ et $x \in \Omega$ est une racine de ce polynôme, on pourra remarquer que les autres racines sont les $x + i$, $i \in \mathbf{F}_p^*$.)