Partiel Algèbre 2

Responsable : Mr O. DEBARRE

Important : vous avez droit de consulter le cours et d'utiliser sans démonstration ses résultats (sauf ceux des exercices ou des TD). Si vous voulez utiliser des résultats hors du cours, il faut les démontrer (sauf mention explicite du contraire). Il n'est pas nécessaire de faire tous les exercices pour avoir la note maximale.

Exercice 1. a) Quel est le groupe de Galois d'un corps de décomposition du polynôme $X^3 - 10$ sur $\mathbf{Q}$? Sur $\mathbf{Q}(\sqrt{-3})$?

b) Trouver un polynôme de groupe de Galois $\mathbf{Z}/4\mathbf{Z}$ sur $\mathbf{Q}$. Même question avec $\mathbf{Z}/3\mathbf{Z}$.

Exercice 2. Soient p et q deux nombres premiers distincts, avec p impair. Soit $K \supset \mathbf{F}_q$ un corps de décomposition du polynôme séparable $X^p - 1 \in \mathbf{F}_q[X]$ et soit ω une racine primitive p-ième de l'unité dans K. On a $\omega^p = 1$, donc l'écriture ω^i, où $i \in \mathbf{Z}/p\mathbf{Z}$, a un sens. Pour toute partie Z de $\mathbf{Z}/p\mathbf{Z}$, on pose $P_Z(X) := \prod_{i\in Z}(X - \omega^i) \in K[X]$. Pour tout entier r premier à p, on note aussi $rZ \subset \mathbf{Z}/p\mathbf{Z}$ l'image de Z par la bijection $z \mapsto rz$ de $\mathbf{Z}/p\mathbf{Z}$.

a) Montrer l'équivalence :

$$P_Z(X) \in \mathbf{F}_q[X] \iff qZ = Z.$$

b) Quels sont les degrés des facteurs irréductibles de $X^7 - 1$ dans $\mathbf{F}_2[X]$? Dans $\mathbf{F}_3[X]$? De $X^{17} - 1$ dans $\mathbf{F}_2[X]$?

On pose

$$Z_p^+ = \{x \in (\mathbf{Z}/p\mathbf{Z})^* \mid \exists y \in (\mathbf{Z}/p\mathbf{Z})^* \quad x = y^2\} \qquad et \qquad Z_p^- = (\mathbf{Z}/p\mathbf{Z})^* - Z_p^+$$

et on suppose à partir de maintenant que la classe de q modulo p est dans Z_p^+.

c) Quels sont les cardinaux de Z_p^+ et de Z_p^- ?

d) Montrer $P_{Z_p^\pm}(X) \in \mathbf{F}_q[X]$. En déduire que le polynôme cyclotomique $\Phi_p(X) := \frac{X^p-1}{X-1}$ n'est pas irréductible dans $\mathbf{F}_q[X]$.

On suppose à partir de maintenant $q = 2$ et p tel que $2 \in Z_p^+$.

e) On pose $Q^\pm(X) := \sum_{i\in Z_p^\pm} X^i \in \mathbf{F}_2[X]$. Calculer $Q^+(X)^2$ et en déduire $\{Q^+(\omega), Q^-(\omega)\} = \{0, 1\}$.

On suppose à partir de maintenant $Q^+(\omega) = 0$ et $Q^-(\omega) = 1$, ce qu'on peut toujours faire quitte à changer de racine primitive ω.

f) Montrer $P_{Z_p^\pm} = \Phi_p \wedge Q^\pm$.

g) Décomposer le polynôme $X^7 - 1$ en produit de facteurs irréductibles dans $\mathbf{F}_2[X]$. *Si vous calculez bien,* même question avec $X^{17} - 1$.

Exercice 3. Soit $K \hookrightarrow L$ une extension finie de corps.

a) Si $K \neq L$ et que tout élément de $L - K$ est inséparable sur K, montrer que la caractéristique de K est un nombre premier p, que $[L : K]_s = 1$, et que $[L : K]$ est une puissance de p.

b) On revient au cas général. Montrer que $[L : K]_s$ divise $[L : K]$ et que soit le quotient est 1, soit la caractéristique de K un nombre premier p et le quotient est une puissance de p (*Indication :* on pourra introduire la clôture séparable de K dans L et utiliser a)).

Exercice 4. Soit $\overline{\mathbf{Q}}$ une clôture algébrique de $\mathbf{Q}$ et soit $a \in \overline{\mathbf{Q}} - \mathbf{Q}$.

a) Montrer qu'il existe un sous-corps $K \subset \overline{\mathbf{Q}}$ tel que $a \notin K$ et que tout sous-corps de $\overline{\mathbf{Q}}$ contenant strictement K contient a ; on dit que K est un sous-corps de $\overline{\mathbf{Q}}$ maximal sans a (*Indication :* utiliser le lemme de Zorn).

On choisit un nombre premier p divisant $[K(a) : K]$. Soit $K \subset L \subset \overline{\mathbf{Q}}$ une extension finie non triviale de K. On note M la clôture normale de L dans $\overline{\mathbf{Q}}$ et $G := \mathrm{Gal}(M/K)$.

b) Montrer que p divise $[L : K]$.

c) Montrer que $[L : K]$ est une puissance de p (*Indication :* on pourra appliquer la théorie de Galois à l'extension $K \subset M$ et utiliser (sans le démontrer !) le théorème de Sylow donné plus bas).

d) Montrer que $[K(a) : K] = p$ et que $K(a)$ est la seule sous-extension de $K \subset \overline{\mathbf{Q}}$ de degré p sur K (*Indication :* on pourra utiliser la théorie de Galois et appliquer le théorème de Sylow donné plus bas).

e) Montrer que G est cyclique, puis que toute extension finie de K est galoisienne cyclique (*Indication :* on pourra utiliser le théorème de Sylow donné plus bas).

f) Montrer qu'il existe $b \in K(a)$, avec $b^p \in K$, tel que $K(a) = K(b)$.

Théorème de Sylow. *Soit p un nombre premier et soit G un groupe fini de cardinal mp^r, avec $m \wedge p = 1$. Il existe un sous-groupe de G de cardinal p^r. Plus précisément, pour tout sous-groupe H de G de cardinal p^s, avec $0 \leq s \leq r$, et tout $s \leq t \leq r$, il existe un sous-groupe de G contenant H et de cardinal p^t.*