Université Lyon 1
M1G. Anneaux et corps commutatifs.

Le 17 mai 2017

PARTIEL

Durée : 1h30

Documents non admis.
Les résultats d'une question peuvent être utilisés pour les questions suivantes.

Problème 1

Soit $P(X) = X^3 + X + 1 \in \mathbb{F}_2[X]$, où $\mathbb{F}_2 = \mathbb{Z}/2\mathbb{Z}$ est les corps à deux éléments.

1. Montrer que P est irréductible sur $\mathbb{F}_2$.
2. Construire le corps $\mathbb{F}_8$ à l'aide de P, et donner la liste de ses éléments.
3. Donner la table de multiplication de $\mathbb{F}_8$, ainsi qu'un élément générateur du groupe multiplicatif.
4. Donner le groupe de Galois $\mathrm{Gal}(\mathbb{F}_8/\mathbb{F}_2)$, et expliciter ses éléments. L'extension $\mathbb{F}_8/\mathbb{F}_2$, est-elle galoisienne ? Justifier.

Problème 2

1. Soit L une extension galoisienne finie de K. Montrer qu'il y a une sous-extension unique maximale $K \leq M \leq L$ telle que M/K est abélienne (c'est-à-dire $\mathrm{Gal}(M/K)$ est abélien).
2. Soit $\zeta \in \mathbb{C}$ une racine de l'unité. Rappeler pourquoi $\mathbb{Q}(\zeta)$ est une extension abélienne, et donner $\mathrm{Gal}(\mathbb{Q}(\zeta)/\mathbb{Q})$.
3. Soit p premier. Montrer qu'il existe une extension cyclique de $\mathbb{Q}$ de degré p.
(Indication : Vous pouvez utiliser qu'un groupe abélien G d'ordre divisible par p a un sous-groupe d'indice p.)
4. (a) Soit ζ une racine primitive $15^{\text{ième}}$. Estc-e que $\mathrm{Gal}(\mathbb{Q}(\zeta)/\mathbb{Q})$ est cyclique ?
   (b) Soit a une racine $15^{\text{ième}}$ de 2. Quel est le degé $[\mathbb{Q}(a,\zeta) : \mathbb{Q}]$?
   (c) Expliciter le groupe $\mathrm{Gal}(\mathbb{Q}(a,\zeta)/\mathbb{Q})$.

Problème 3

1. Soit $(I, \leq)$ un bon ordre, et $\leq^p$ l'ordre partiel sur I^n donné par $(i_1, \ldots, i_n) \leq (j_1, \ldots, j_n)$ ssi $i_k \leq j_k$ pour tout $k = 1, \ldots, n$. Montrer que toute complétion de $\leq^p$ en un ordre total sur I^n est un bon ordre.
2. (a) Donner la définition d'une base de Gröbner. Pourquoi est-ce que cette définition dépend de l'ordre monomial choisi ?
   (b) Soit $f = x + z$, $g = x - y$ et $I = (f, g) \triangleleft \mathbb{Q}[x, y, z]$. Montrer que f, g est une base de Gröbner pour l'ordre lexicographique avec $x < y < z$, mais pas pour l'ordre lexicographique avec $z < y < x$.
   (c) Une base $\mathcal{G}$ de Gröbner d'un idéal I est *réduite* si $\mathrm{cd}(g) = 1$ et g est réduit par rapport à $\mathcal{G} \setminus \{g\}$ pour tout $g \in \mathcal{G}$. Montrer que tout idéal admet une unique base de Gröbner réduite.
   (Indication : Pour l'unicité, considérer un polynôme de multidegré minimal qui est dans une des deux bases mais pas dans l'autre.)
3. Calculer une base de Gröbner de l'idéal $(x^2 + y, x^4 + 2x^2y + y^2z) \triangleleft \mathbb{Q}[x, y, z]$ à l'aide de l'algorithme de Buchberger, avec l'ordre lexicographique et $x > y > z$.