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.

Solution.

1. Comme P est de degré 3, il suffit de montrer que P n'a pas de racine dans $\mathbb{F}_2$. Or, $P(0) = P(1) = 1$. Donc P est irréductible sur $\mathbb{F}_2$.
2. Comme $P \in \mathbb{F}_2[X]$ est irréductible de degré 3, on a $\mathbb{F}_8 = \mathbb{F}_{2^3} = \mathbb{F}_2(\theta) \cong \mathbb{F}_2[X]/(P)$, où $\theta \in \mathbb{F}_8$ est une racine de P qui correspond à l'élément $X + (P)$ dans $\mathbb{F}_2[X]/(P)$. On a $\mathbb{F}_8 = \{a + b\theta + c\theta^2 : a, b, c \in \mathbb{F}_2\}$.
3. On a $\theta^3 = \theta + 1$, $\theta^4 = \theta^2 + \theta$, $\theta^6 = \theta^{-1} = \theta^2 + 1$ et $\theta^5 = \theta + \theta^{-1} = \theta^2 + \theta + 1$. Donc θ est générateur multiplicatif, et

$\cdot$	1	θ	θ^2	$\theta+1$	$\theta^2+\theta$	$\theta^2+\theta+1$	θ^2+1
1	1	θ	θ^2	$\theta+1$	$\theta^2+\theta$	$\theta^2+\theta+1$	θ^2+1
θ	θ	θ^2	$\theta+1$	$\theta^2+\theta$	$\theta^2+\theta+1$	θ^2+1	1
θ^2	θ^2	$\theta+1$	$\theta^2+\theta$	$\theta^2+\theta+1$	θ^2+1	1	θ
$\theta+1$	$\theta+1$	$\theta^2+\theta$	$\theta^2+\theta+1$	θ^2+1	1	θ	θ^2
$\theta^2+\theta$	$\theta^2+\theta$	$\theta^2+\theta+1$	θ^2+1	1	θ	θ^2	$\theta+1$
$\theta^2+\theta+1$	$\theta^2+\theta+1$	θ^2+1	1	θ	θ^2	$\theta+1$	$\theta^2+\theta$
θ^2+1	θ^2+1	1	θ	θ^2	$\theta+1$	$\theta^2+\theta$	$\theta^2+\theta+1$

4. Comme $P(\theta) = 0$ et P est invariant sous le Frobelius $\sigma : x \mapsto x^2$, les deux autres racines de P sont θ^2 et $(\theta^2)^2 = \theta^4 = \theta^2 + \theta$. Toues les racines de P sont dans $\mathbb{F}_8$, qui est donc le corps de rupture de P, et normal. Comme $\mathbb{F}_2$ est parfait, l'extension $\mathbb{F}_8/\mathbb{F}_2$ ets galoisienne. (Alternativement, toute extension finie d'un corps fini est galoisienne.) Le groupe $\mathrm{Gal}(\mathbb{F}_8/\mathbb{F}_2)$ est cyclique d'ordre 3; ses éléments sont $1 =$id, $\sigma =$Frob et σ^2, avec $\sigma^3 = 1$, puisque le groupe de Galois sur un corps fini $\mathbb{F}_q$ est cyclique et engendré par le Frobenius $x \mapsto x^q$.

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 $15^{\text{ième}}$. Est-ce 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 $\mathrm{Gal}(\mathbb{Q}(a,\zeta)/\mathbb{Q})$.

Solution.

1. Puisque les sous-extensions normales abéliennes de L/K correspondent aux quotients abéliens $\mathrm{Gal}(L/K)/N$ par un sous-groupe N par la correspondance de Galois qui inverse les inclusions, le quotient maximal abélien $\mathrm{Gal}(L/K)/\mathrm{Gal}(L/K)'$ correspond à l'unique sous-extension abélienne maximale $L^{\mathrm{Gal}(L/K)'}$ de K.

2. Si ζ est une racine primitive n-me de l'unité, ses conjugués par un automorphisme de $\mathbb{C}$ sont aussi des racines primitives n-mes de l'unité, qui sont des puissances ζ^k avec $\mathrm{pgcd}(n,k)=1$. Ils sont donc dans $\mathbb{Q}(\zeta)$, qui est ainsi galoisien fini sur $\mathbb{Q}$. Si $\sigma,\tau\in\mathrm{Gal}(\mathbb{Q}(\zeta)/\mathbb{Q})$ avec $\sigma(\zeta)=\zeta^m$ et $\tau(\zeta)=\zeta^n$, alors $(\sigma\circ\tau)(\zeta)=\zeta^{mn}=(\tau\circ\sigma)(\zeta)$. Comme tout élément de $\mathrm{Gal}(\mathbb{Q}(\zeta)/\mathbb{Q})$ est déterminé par son action sur ζ, le groupe $\mathrm{Gal}(\mathbb{Q}(\zeta)/\mathbb{Q})$ est abélien.

   Comme le polynôme cyclotomique $\Phi_n(X)$, qui a comme racines les racines primitives n-mes de l'unité, est irréductible sur $\mathbb{Q}$ (théorème du cours), toute autre racine primitive n-me de l'unité est conjugué de ζ par un élément du groupe de Galois. On a ainsi $\mathrm{Gal}(\mathbb{Q}(\zeta)/\mathbb{Q})\cong\left(\mathbb{Z}/n\mathbb{Z}\right)^\times$.

3. Soit $n=p^2$, et ζ racine primitive n-me. Alors $\mathbb{Q}(\zeta)$ est une extension abélienne de degré

$$|\mathrm{Gal}(\mathbb{Q}(\zeta)/\mathbb{Q})| = |\left(\mathbb{Z}/n\mathbb{Z}\right)^\times| = \phi(n)=\phi(p^2)=(p-1)p.$$

   Soit N sous-groupe de $\mathrm{Gal}(\mathbb{Q}(\zeta)/\mathbb{Q})$ d'indice p. Alors N est distingué. Par la correspondance de Galois le corps fixe $\mathbb{Q}(\zeta)^N$ est une extension galoisienne de degré p, de groupe de Galois $\mathrm{Gal}(\mathbb{Q}(\zeta)/\mathbb{Q})/N$, qui est abélien. (Alternativement, tout groupe d'ordre premier est abélien.)

4. (a) On a $\mathrm{pgcd}(4,15)=1$. Il y a donc $\sigma\in\mathrm{Gal}(\mathbb{Q}(\zeta)/\mathbb{Q})$ avec $\sigma(\zeta)=\zeta^4$, d'où $\sigma^2(\zeta)=\zeta^{4^2}=\zeta^{16}=\zeta$. Ainsi il y a au moins deux involutions dans $\mathrm{Gal}(\mathbb{Q}(\zeta)/\mathbb{Q})$, à savoir σ et $\sigma':\zeta\mapsto\zeta^{-1}$. Donc $\mathrm{Gal}(\mathbb{Q}(\zeta)/\mathbb{Q})$ ne peut pas être cyclique.

   (b) Le polynôme $X^{15}-2$ est irréductibre sur $\mathbb{Q}$ d'après Eisenstein avec $p=2$. Donc $[\mathbb{Q}(a):\mathbb{Q}]=15$. D'autre part, $[\mathbb{Q}(\zeta):\mathbb{Q}]=\varphi(15)=(3-1)(5-1)=8$. Comme $\mathrm{pgcd}(15,8)=1$, on a $[\mathbb{Q}(a,\zeta):\mathbb{Q})]=8\cdot 15=120$.

   (c) $\mathbb{Q}(a,\zeta)$ est le corps de rupture de P sur $\mathbb{Q}$. L'extension est donc normale. Il y a un sous-corps normal $\mathbb{Q}(\zeta)$, qui correspond à un sous-groupe distingué $N=\mathrm{Gal}(\mathbb{Q}(a,\zeta)/\mathbb{Q}(\zeta))$ de $G=\mathrm{Gal}(\mathbb{Q}(a,\zeta)/\mathbb{Q})$; on a $G/N\cong\mathrm{Gal}(\mathbb{Q}(\zeta)/\mathbb{Q})\cong\left(\mathbb{Z}/15\mathbb{Z}\right)^\times$. Or, comme P reste irréductible sur $\mathbb{Q}(\zeta)$, on a $\mathrm{Gal}(\mathbb{Q}(a,\zeta)/\mathbb{Q}(\zeta))$ est cyclique d'ordre 15, engendré par $a\mapsto a\zeta$. En total,

$$\begin{aligned}\mathrm{Gal}(\mathbb{Q}(a,\zeta)/\mathbb{Q}) &\cong \left(\mathbb{Z}/15\mathbb{Z}\right)^+ \rtimes \left(\mathbb{Z}/15\mathbb{Z}\right)^\times \\ &\cong \{f_{b,c} : b\in\left(\mathbb{Z}/15\mathbb{Z}\right)^\times,\ c\in\mathbb{Z}/15\mathbb{Z}\}\end{aligned}$$

   où $f_{b,c}: Z/15\mathbb{Z}\to\mathbb{Z}/15\mathbb{Z}$ est donné par $x\mapsto bx+c$.

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 $I=(f,g)\lhd\mathbb{Q}[x,y,z]$. 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 $(x^2+y, x^4+2x^2y+y^2z)\lhd\mathbb{Q}[x,y,z]$ à l'aide de l'algorithme de Buchberger, avec l'ordre lexicographique et $x>y>z$.

Solution.

1. On montre d'abord que toute suite infinie $(i_n : n \in \mathbb{N})$ dans I a une sous-suite faiblement croissante: On prend $i_{n_0} = \min\{i_n : n \in \mathbb{N}\}$, et $i_{n_{k+1}} = \min\{i_n : n > n_k\}$.

   Soit $\leq$ une complétion de $\leq^p$ en ordre total sur I^n. Supposons pour une contradiction qu'il y ait une chaîne infinie descendante $(\bar{k}_i : i \in \mathbb{N})$. Alors il y a une sous-suite infinie telle que la suite des premières coordonnées est faiblement croissante, une sous-suite infinie de celle-ci telle que la suite des deuxièmes coordonnées est faiblement croissante, etc. On obtient une sous-suite infinie qui est faiblement croissante pour toutes les coordonnées ; elle est donc faiblement croissante, ce qui donne la contradiction recherchée.

2. (a) $\{f_i : i \in I\}$ est une base de Gröbner d'un idéal I de $K[\bar{X}]$ si $I = (f_i : i \in I)$ et $(td(f) : f \in I) = (td(f_i) : i \in I)$, où $td(f)$ est le terme dominant par rapport à un ordre monomial sur l'ensemble des monômes en $\bar{X}$. Cette définition dépend de l'ordre monomial choisi puisque le terme dominant d'un polynôme en dépend.

   (b) Dans l'ordre lexicographique avec $x < y < z$ on a $td(f) = z$ et $td(g) = -y$. Si $h \in (f, g)$ mais $td(h) \notin (td(f), td(g)) = (y, z)$, alors $h \in \mathbb{Q}[x]$. Comme $h \in I$ il y a $h_1, h_2 \in \mathbb{Q}[x, y, z]$ avec

   $$h(x) = h_1(x, y, z)(x + z) + h_2(x, y, z)(x - y).$$

   Donc $h(x) = h_1(x, x, z)(x + z)$ et $0 = \deg_z(h) = \deg_z(h_1) + 1 > 0$, une contradiction. Donc $\{f, g\}$ est une base de Gröbner de I pour l'ordre lexicographique avec $x < y < z$.

   Dans l'ordre lexicographique avec $x > y > z$ on a $td(f) = td(g) = x$, mais $y + z = f - g \in I$ avec $td(y + z) = y \notin (x)$. Donc $\{f, g\}$ n'est pas une base de Gröbner de I pour l'ordre lexicographique avec $x > y > z$.

   (c) On définit un ordre total $\leq$ sur les polynômes par l'ordre lexicographique sur les uplets des multidegrés de ses termes. Comme les multidegrés sont bien ordonnés, et les uplets sont en ordre descendant, c'est un bon ordre. De plus, si g' est une réduction de g, on a $g' \leq g$, avec égalité si et suelement si $g' = g$.

   Étant donné une base de Gröbner $\mathcal{G}$ et $g \in \mathcal{G}$, si g' est la réduction de g par rapport à $\mathcal{G} \setminus \{g\}$, alors $(\mathcal{G} \setminus \{g\}) \cup \{g'\}$ est toujours une base de Gröbner. On réduit donc chaque polynôme dans $\mathcal{G}$ par rapport aux autres et on itère ; comme à chaque réduction propre on remplace un polynôme par un autre qui est strictement plus petit, on s'arrête après un nombre fini d'itérations. On normalise les polynômes pour obtenir une base réduite.

   Soient $\mathcal{G}$ et $\mathcal{G}'$ deux bases réduites différentes, et $f \in \mathcal{G} \triangle \mathcal{G}'$ un polynôme de multidegré minimal, disons $f \in \mathcal{G} \setminus \mathcal{G}'$. Puisque $f \in (\mathcal{G})$, on a que f se réduit en 0 par rapport à $\mathcal{G}'$. Or, seuls les polynômes de multidegré strictement inférieur à celui de f peuvent intervenir dans cette réduction, et ces polynômes sont également dans $\mathcal{G}$ par minimalité. Donc f se réduit en 0 par rapport à $\mathcal{G} \setminus \{f\}$, ce qui contredit le fait que $\mathcal{G}$ est réduit.