Université Rennes 1, Année 2013-2014, Master 1 Math ALGB : Algèbre générale de base

Examen de deuxième session

Seuls les résultats du cours pourront être admis. Documents et calculatrices ne sont pas autorisés. Le barème envisagé, indiqué entre parenthèses, est donné à titre indicatif.

Justifiez toutes vos réponses !

Exercice 1 (Total : 7 points) Soit M l'ensemble des polynômes $P \in \mathbb{R}[X]$ tels que $P(\mathbb{Z}) \subset \mathbb{Z}$.

1. Montrez que M est un $\mathbb{Z}$-module. (1 point)
2. On pose $H_0 = 1$ et $H_n = \frac{X(X-1)\ldots(X-n+1)}{n!}$ pour $n \geqslant 1$ entier. Montrez que $H_n \in M$. (2 points)
3. Montrez que $\{H_n\}_{n\geqslant 0}$ est une famille libre du $\mathbb{Z}$-module M. (2 points)
4. Montrez que $\{H_n\}_{n\geqslant 0}$ est une famille génératrice. Indication : montrer que pour tout $P \in M$ de degré n, il existe $\lambda_0, \ldots, \lambda_n$ réels tels que $P = \sum_{k=0}^{n} \lambda_k H_k$, puis que $\lambda_k \in \mathbb{Z}$ pour tout k. (2 points)

Exercice 2 (Total : 4 points)

1. Soit $g = X^4 + X + 1 \in \mathbb{F}_2[X]$, montrer que $K = \mathbb{F}_2[X]/(g)$ est un corps. (1 point)
2. Donner tous les générateurs du groupe multiplicatif K^*. (1,5 points)
3. Déterminer les polynômes minimaux sur $\mathbb{F}_2$ de α^2, α^4 et α^5. (1,5 points)

Exercice 3 (Total : 3 points)

1. Effectuez la division euclidienne de 2014 par 19. (0,5 point)
2. Exprimez le groupe G des éléments inversibles de l'anneau $\mathbb{Z}/2014\mathbb{Z}$ sous la forme d'un produit de groupes cycliques. (2 points)
3. Donnez les facteurs invariants du groupe G. (0,5 point)

Exercice 4 (Total 6 points)

1. Montrer que $f = X^4 - 5 \in \mathbb{Q}[X]$ est irréductible sur $\mathbb{Q}$ et que $K = \mathbb{Q}(\sqrt[4]{5}, i)$ (avec $i^2 = -1$) est un corps de décomposition de f sur $\mathbb{Q}$. (0.5 point)
2. Montrer que l'extension $K/\mathbb{Q}$ est galoisienne et calculer $[K : \mathbb{Q}]$. (1.5 points)
   Indication : utiliser $i \notin \mathbb{R}$.
3. Parmi les extensions de corps suivantes, lesquelles sont normales ? (1.5 points)
   (a) $\mathbb{Q}(i)/\mathbb{Q}$;
   (b) $\mathbb{Q}(\sqrt[4]{5})/\mathbb{Q}$;
   (c) $\mathbb{Q}(i, \sqrt[4]{5})/\mathbb{Q}(i)$.
4. Déterminer le groupe de Galois de f sur les corps (1.5 points)
   (a) $\mathbb{Q}(\sqrt[4]{5})$;
   (b) $\mathbb{Q}(i)$.
5. Déterminer explicitement les automorphismes du groupe de Galois de f sur $\mathbb{Q}$. (1 point)

Corrigé Ex. 1

1. Le polynôme nul est dans M et la somme de deux polynômes de $\mathbb{R}[X]$ est dans M. Ainsi M est un sous-groupe de $\mathbb{R}[X]$, c'est en particulier un groupe commutatif i.e. un $\mathbb{Z}$-module.
2. Soit $m \in \mathbb{Z}$. Si $m \geqslant n$, on a $H_n(m) = \binom{m}{n}$ qui est entier. Si $0 \leqslant m \leqslant n-1$, on a $H_n(m) = 0$ et si $m < 0$, on a $H_n(m) = (1/n!)(m)(m-1)\dots(m-n+1) = (1/n!)(-1)^n(-m)(-m+1)\dots(-m+n-1) = (-1)^n\binom{-m+n-1}{n}$ qui est entier. Dans tous les cas $H_n(m) \in \mathbb{Z}$, donc $H_n \in M$.
3. Dans le $\mathbb{R}$-espace vectoriel $\mathbb{R}[X]$, la famille $\{H_n\}_{n\geqslant 0}$ est étagée par les degrés (i.e. à degrés tous distincts), donc c'est une famille libre. Ainsi toute combinaison linéaire finie des H_n à coefficients réels nulle a ses coefficients nuls ; ceci est vrai en particulier si les coefficients sont dans $\mathbb{Z}$, donc $\{H_n\}_{n\geqslant 0}$ est une famille libre du $\mathbb{Z}$-module M.
4. Dans $\mathbb{R}_n[X] = \{Q \in \mathbb{R}[X], \deg(Q) \leqslant n\}$ la famille $\{H_k\}_{k\leqslant n}$ est libre et de cardinal $n+1$ c'est donc une $\mathbb{R}$-base. Ceci montre que pour tout $P \in M$ de degré n il existe $\lambda_0, \dots, \lambda_n$ réels et uniques tels que $P = \sum_{k=0}^{n} \lambda_k H_k$. Montrons par récurrence sur $k \leqslant n$ que $\lambda_k \in \mathbb{Z}$. Pour $k = 0$ c'est vrai car $P(0) = \lambda_0$ qui est dans $\mathbb{Z}$ puisque $P \in M$. Pour $k \geqslant 1$ il suffit de calculer $P(k) = \lambda_0 + \lambda_1 H_1(k) + \dots + \lambda_{k-1}H_{k-1}(k) + \lambda_k$, puisque $H_k(k) = 1$ et $H_k(\ell) = 0$ si $\ell > k$. Ainsi $\lambda_k = P(k) - \lambda_0 - \lambda_1 H_1(k) - \dots - \lambda_{k-1}H_{k-1}(k) \in \mathbb{Z}$.

Corrigé Ex. 2

1. Comme g n'a pas de racine dans $\mathbb{F}_2$ il est soit irréductible soit le produit de deux polynôme de degré 2. Comme $h = X^2 + X + 1$ est l'unique polynôme irréductible de degré 2 de $\mathbb{F}_2[X]$ et que $h^2 = X^4 + X^2 + 1 \neq g$, le polynôme g est irréductible et d'après le cours K est un corps. .
2. Comme K^* est un groupe cyclique d'ordre $2^4 - 1 = 15$, les éléments qui ne sont pas d'ordre 1, 3, 5 sont tous des générateurs. Pour $\alpha = \overline{X}$ nous obtenons dans la $\mathbb{F}_2$base $(1, \overline{X}, \overline{X}^2, \overline{X}^3)$ l'écriture unique $\alpha = \overline{X}$, $\alpha^2 = \overline{X}^2$, $\alpha^3 = \overline{X}^3 \neq 1$, $\alpha^4 = \overline{X} + 1$, $\alpha^5 = \overline{X}^2 + \overline{X} \neq 1$. Les générateurs sont donc les puissances α^m de α avec m et 15 premiers entre eux.
3. Comme $\alpha^4 + \alpha + 1 = 0$ nous obtenons également $(\alpha^4 + \alpha + 1)^2 = (\alpha^2)^4 + (\alpha^2) + 1 = 0$ et de la même manière $(\alpha^4)^4 + (\alpha^4) + 1 = 0$. Le polynôme minimal de α^2 et α^4 est donc g. Les deux éléments α^3 et $(\alpha^3)^2$ d'ordre 3 de K^* sont dans $\mathbb{F}_4 \subset K$ mais pas dans $\mathbb{F}_2$. Leur polynôme minimal est donc $h = X^2 + X + 1$.

Corrigé Ex. 3

1. $2014 = 19 \times 106$.
2. La factorisation complète de 2014 est $2014 = 2 \times 19 \times 53$ et c'est donc un produit de 3 nombres premiers distincts. On en déduit que $\mathbb{Z}/2014\mathbb{Z} \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/19\mathbb{Z} \times \mathbb{Z}/53\mathbb{Z}$. Comme le groupe des inversibles d'un anneau produit $A = B \times C$ est le produit $G = A^* = B^* \times C^*$ des groupes des inversibles des facteurs B et C, on en déduit que :

$$G = (\mathbb{Z}/2014\mathbb{Z})^* \simeq (\mathbb{Z}/2\mathbb{Z})^* \times (\mathbb{Z}/19\mathbb{Z})^* \times (\mathbb{Z}/53\mathbb{Z})^* \simeq \mathbb{Z}/18\mathbb{Z} \times \mathbb{Z}/52\mathbb{Z}.$$

3. On a $G \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/3^2\mathbb{Z} \times \mathbb{Z}/2^2\mathbb{Z} \times \mathbb{Z}/13\mathbb{Z} \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/(2^2 \cdot 3^2 \cdot 13)\mathbb{Z}$, ainsi les facteurs invariants de G sont $d_1 = 2$ et $d_2 = 2^2 \cdot 3^2 \cdot 13 = 468$.

Corrigé Ex. 4

1. Eisenstein avec le premier 5. Les racines $\sqrt[4]{5}, -\sqrt[4]{5}, i\sqrt[4]{5}, -i\sqrt[4]{5}$ sont toutes dans $\mathbb{Q}(\sqrt[4]{5}, i)$. Comme $\mathbb{Q}(\sqrt[4]{5}, i) = \mathbb{Q}(\sqrt[4]{5}, -\sqrt[4]{5}, i\sqrt[4]{5}, -i\sqrt[4]{5})$ il en résulte que K est un corps de décomposition de f.

2. En tant que corps de décomposition d'un polynôme séparable (caractéristique zéro) l'extension $K/\mathbb{Q}$ est galoisienne. Le polynôme f étant irréductible il est le polynôme minimal de $\sqrt[4]{5}$ sur $\mathbb{Q}$ et nous obtenons $[\mathbb{Q}(\sqrt[4]{5}) : \mathbb{Q}] = 4$. Il en résulte

$$[K : \mathbb{Q}] = [\mathbb{Q}(\sqrt[4]{5})(i) : \mathbb{Q}(\sqrt[4]{5})][\mathbb{Q}(\sqrt[4]{5}) : \mathbb{Q}] = [\mathbb{Q}(\sqrt[4]{5})(i) : \mathbb{Q}(\sqrt[4]{5})] \cdot 4$$

il suffit de noter que $i \notin \mathbb{Q}(\sqrt[4]{5}) \subset \mathbb{R}$ (i n'est pas réel) pour en déduire que $[K : \mathbb{Q}] = 8$.

3. (a) $\mathbb{Q}(i)/\mathbb{Q}$: une extension de degré 2 est toujours normale car un polynôme irréductible qui possède une racine dans l'extension est de degré $\leqslant 2$ et donc scindé.
   (b) $\mathbb{Q}(\sqrt[4]{5})/\mathbb{Q}$: le polynôme irréductible $f \in \mathbb{Q}[X]$ possède une racine dans $\mathbb{Q}(\sqrt[4]{5})$ mais il n'est pas scindé sur $\mathbb{Q}(\sqrt[4]{5})$ car $i \notin \mathbb{R}$. Ainsi $\mathbb{Q}(\sqrt[4]{5})/\mathbb{Q}$ n'est pas une extension normale.
   (c) $\mathbb{Q}(i, \sqrt[4]{5})/\mathbb{Q}(i) : \mathbb{Q}(i, \sqrt[4]{5})$ est le corps de décomposition de $f \in \mathbb{Q}(i)[X]$ et donc est une extension normale.
4. (a) La deuxième question montre que $[K : \mathbb{Q}(\sqrt[4]{5})] = 2$ et le groupe de Galois est donc d'ordre 2.
   (b) La deuxième question montre que $[K : \mathbb{Q}(i)] = 4$. D'après le cours le groupe de Galois d'un polynôme $X^n - b$ sur un corps de caractéristique zéro qui contient une racine n-ième de l'unité est cyclique. Il s'agit donc du groupe cyclique d'ordre 4.
5. $\sigma \in G(K/\mathbb{Q})$ est uniquement déterminé par son action sur i et sur $\sqrt[4]{5}$. Comme le groupe de Galois permute les racines d'un polynôme il en résulte 4 possibilités pour l'image de $\sqrt[4]{5}$ et deux pour l'image de i. Puisque $|G(K/\mathbb{Q})| = [K : \mathbb{Q}] = 8$ toutes ces combinaisons donnent des automorphismes distincts de $G(K/\mathbb{Q})$.