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

Examen de première session

16 décembre 2013

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 (3,5 points) Montrer que les anneaux $R_1 = \mathbb{F}_3[X]/(X^2+2X+2)$ et $R_2 = \mathbb{F}_3[X]/(X^2+X+2)$ sont isomorphes et donner un isomorphisme explicite entre ces deux anneaux.

Corrigé. Comme ils n'ont pas de racine dans $\{\overline{0}, \overline{1}, \overline{-1}\}$ les polynômes X^2+2X+2 et X^2+X+2 sont irréductibles dans $\mathbb{F}_3$ et les deux anneaux sont des corps. On travaille dans la $\mathbb{F}_3$-base $(1, \overline{X})$ du corps R_1.

- 1re alternative : Il y a $(3^2-3)/2 = 3$ polynômes irréductibles dans $\mathbb{F}_3$ et il manque donc X^2+1. Le morphisme de Frobenius envoie une racine sur une racine et donc $\overline{X} \in R_1$ et $\overline{X}^3 = 2\overline{X}+1 \in R_1$ sont zéros de $X^2+2X+2 \in \mathbb{F}_3$. Pour $\overline{X}^2 = \overline{X}+1 \notin \mathbb{F}_3$ on a $\overline{X}^4 = \overline{X}^2 + 2\overline{X} + 1 = 2$ (en particulier $\overline{X}^4 = -1$ est zéro de $X+1 \in \mathbb{F}_3[X]$) et donc $\overline{X}^2$ et $(\overline{X}^2)^3$ (image sous Frobenius de $\overline{X}^2$) sont racines de $X^2+1 \in \mathbb{F}_3[X]$. Il en résulte que $\overline{X}^5 = -\overline{X}$ et $\overline{X}^7$ sont les deux zéros de $X^2+X+2 \in \mathbb{F}_3[X]$ dans R_1, et en particulier $R_1 = \mathbb{F}_3(\overline{X}^5)$.
- 2e alternative : un zéro $a+b\overline{X}$ de $X^2+X+2=0$ dans R_1 satisfait

$$a^2 + 2ab\overline{X} + b^2(\overline{X}+1) + a + b\overline{X} + 2 = (a^2+b^2+a+2) + (2ab+b^2+b)\overline{X}.$$

  Dans la $\mathbb{F}_3$-base $(1, \overline{X})$ les deux coefficients sont nuls. Comme $X^2+X+2=0$ n'a pas de zéro dans $\mathbb{F}_3$ il faut $b \neq 0$ et donc $a = b+1$ qui entraine $(b^2+2b+1)+b^2+(b+1)+2 = 2b^2+1 = 2(b^2-1) = 2(b+1)(b-1) = 0$. Les deux zéros sont donc $2+\overline{X}$ et $-\overline{X}$.

Ce qui permet de représenter $R_1 = \mathbb{F}_3(-\overline{X})$ et R_2 comme deux corps de rupture d'un même polynôme $X^2+X+2 \in \mathbb{F}_3[X]$. D'après le cours il existe un $\mathbb{F}_3$-isomorphisme entre R_1 et R_2 qui envoie $-\overline{X} = \overline{X}^5 \in R_1$ sur $\overline{X} \in R_2$.

Exercice 2 (3 points) Donnez la forme de Smith de la matrice à coefficients dans $\mathbb{Z}$:

$$A = \begin{pmatrix} 12 & -6 & 2 \\ 75 & -41 & 13 \\ 19 & -3 & 3 \end{pmatrix}.$$

A quel groupe est isomorphe le groupe $M = \mathbb{Z}^3/A(\mathbb{Z}^3)$?

Corrigé. On désigne par $\sim$ la relation d'équivalence définie par $A \sim B$ si et seulement s'il existe deux matrices P, Q dans $\mathrm{GL}_3(\mathbb{Z})$ telles que $B = PAQ$. Alors, par transformations par opérations élémentaires

sur les lignes et les colonnes on a :

$$\begin{pmatrix}12 & -6 & 2\\ 75 & -41 & 13\\ 19 & -3 & 3\end{pmatrix} \overset{L1\to L1-L3}{\sim} \begin{pmatrix}-7 & -3 & -1\\ 75 & -41 & 13\\ 19 & -3 & 3\end{pmatrix} \overset{C1\leftrightarrow C3}{\sim} \begin{pmatrix}-1 & -3 & -7\\ 13 & -41 & 75\\ 3 & -3 & 19\end{pmatrix}$$

$$\overset{\substack{L2\to L2+13L1\\ L3\to L3+3L1}}{\sim} \begin{pmatrix}-1 & -3 & -7\\ 0 & -80 & -16\\ 0 & -12 & -2\end{pmatrix} \overset{\times(-\mathrm{I}_3)}{\sim} \begin{pmatrix}1 & 3 & 7\\ 0 & 80 & 16\\ 0 & 12 & 2\end{pmatrix}$$

$$\overset{\substack{C2\to C2-3C1\\ C3\to C3-7C1}}{\sim} \begin{pmatrix}1 & 0 & 0\\ 0 & 80 & 16\\ 0 & 12 & 2\end{pmatrix} \overset{\substack{L2\leftrightarrow L3\\ C2\leftrightarrow C3}}{\sim} \begin{pmatrix}1 & 0 & 0\\ 0 & 2 & 12\\ 0 & 16 & 80\end{pmatrix}$$

$$\overset{L3\to L3-8L2}{\sim} \begin{pmatrix}1 & 0 & 0\\ 0 & 2 & 12\\ 0 & 0 & -16\end{pmatrix} \overset{C3\to C3-6C2}{\sim} \begin{pmatrix}1 & 0 & 0\\ 0 & 2 & 0\\ 0 & 0 & -16\end{pmatrix}.$$

Cette dernière matrice est la forme normale de Smith. Il existe donc des bases $\{e_1, e_2, e_3\}$ et $\{f_1, f_2, f_3\}$ de $\mathbb{Z}^3$, données par les matrices P, Q des opérations sur les lignes resp. sur les colonnes, telles que $A(e_1) = f_1$, $A(e_2) = 2f_2$ et $A(e_3) = -16f_3$. Ainsi :

$$\begin{aligned}\mathbb{Z}^3/A(\mathbb{Z}^3) &\simeq (\mathbb{Z}f_1 \oplus \mathbb{Z}f_2 \oplus \mathbb{Z}f_3)/(\mathbb{Z}f_1 \oplus \mathbb{Z}2f_2 \oplus \mathbb{Z}(-16f_3))\\ &\simeq \mathbb{Z}/\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/16\mathbb{Z} \simeq \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/16\mathbb{Z}.\end{aligned}$$

Exercice 3 (total 6,5 points) Soit $f = X^6 - 7 \in \mathbb{Q}[X]$ et K un corps de décomposition $\mathcal{D}_{f,\mathbb{Q}}$ de f.

1. Montrer qu'il existe deux racines primitives 6es de l'unité dans $\mathbb{C}$ et qu'elles sont zéros du polynôme $X^2 - X + 1 \in \mathbb{Q}[X]$ dont on montrera qu'il est irréductible. (1 pt)
2. Montrer que l'extension $K/\mathbb{Q}$ est galoisienne et calculer $[K : \mathbb{Q}]$. (1,5 pt)
3. Donner l'ordre de $G(K/\mathbb{Q})$. Donner l'ordre des sous-groupes suivants de $G(K/\mathbb{Q})$ en précisant lesquels sont distingués : $G(K/\mathbb{Q}(\sqrt[6]{7}))$ et $G(K/\mathbb{Q}(\xi))$ où ξ est zéro de $X^2 - X + 1 \in \mathbb{Q}[X]$. (2,5 pts)
4. Donner des générateurs du groupe de Galois $G(K/\mathbb{Q})$. Le groupe $G(K/\mathbb{Q})$ est-il abélien ? (1,5 pt)

Corrigé.

1. Solution a) : $\xi = e^{2i\pi/6}$ est une racine primitive de l'unité, et les autres sont de la forme ξ^i avec i et 6 premiers entre eux, ce qui monture que les deux racines primitives de 'unité sont ξ et ξ^5. Avec $\xi = e^{2i\pi/6} = \frac{1}{2} + \frac{\sqrt{3}}{2}i$ et $\xi^5 = \overline{\xi}$ le polynôme minimal de ξ est $(X - \xi)(X - \xi^5) = X^2 - X + 1$. Pour ontrer l'irréductibilité on note que l'image $X^2 + X + 1 \in \mathbb{F}_2[X]$ sous $\varphi_{X\to X}\mathbb{Z}[X] \to \mathbb{F}_2[X]$ est irréductible.

   Solution b) : Les racines primitives 6es de l'unité sont zéros de $X^6 - 1$ mais pas de $(X^3 - 1)/(X - 1)$, $(X^2 - 1)/(X - 1)$ ou $X - 1$. Il en existe donc $6 - 2 - 1 - 1 = 2$ et elles sont zéros de $X^2 - X + 1$ dont on montre qu'il est irréductible comme ci-dessus.

2. Les zéros de f sont $\xi^i \sqrt[6]{7}$ avec $i =\in \{1, \ldots, 6\}$ et donc $K = \mathbb{Q}(\xi, \sqrt[6]{7})$ est le corps e décomposition de $X^6 - 7$. Comme $\xi \notin \mathbb{R}$ on a $\xi \notin \mathbb{Q}(\sqrt[6]{7})$, le point précédent t montre que $[\mathbb{Q}(\sqrt[6]{7})(\xi) : \mathbb{Q}(\sqrt[6]{7})] = 2$. Comme $f \in \mathbb{Q}[X]$ est irréductible (Eisenstein avec le premier 7 dans $\mathbb{Z}$), il en résulte que

$$[K : \mathbb{Q}] = [\mathbb{Q}(\sqrt[6]{7})(\xi) : \mathbb{Q}(\sqrt[6]{7})][\mathbb{Q}(\sqrt[6]{7}) : \mathbb{Q}] = 2 \cdot 6.$$

Comme $\mathbb{Q}$ est de caractéristique 0 l'extension $K/\mathbb{Q}$ est séparable et comme K est corps de décomposition d'un polynôme de $\mathbb{Q}$, l'extension $K/\mathbb{Q}$ est galoisienne. D'après le cours l'ordre de $G(K/\mathbb{Q})$ est $[K : \mathbb{Q}] = 12$.

3. — Le point précédent montre que $[K : \mathbb{Q}(\sqrt[6]{7})] = 2$. Comme K est le corps de décomposition de $X^6 - 7$ sur $\mathbb{Q}$, c'est aussi le corps de décomposition de $X^6 - 7$ sur $\mathbb{Q}(\sqrt[6]{7})$. La caractéristique de $\mathbb{Q}$ étant nulle l'extension est séparable et donc $K/\mathbb{Q}(\sqrt[6]{7})$ est une extension galoisienne. D'après le cours l'ordre de $G(K/\mathbb{Q}(\sqrt[6]{7}))$ est $[K : \mathbb{Q}(\sqrt[6]{7})] = 2$. L'extension $\mathbb{Q}(\sqrt[6]{7})/\mathbb{Q}$ n'est pas normale car elle contient un zéro du polynôme irréductible $\mathbb{Q}[X]$, mais pas le zéro $\xi \sqrt[6]{7}$ qui n'est pas réel. Par correspondance de Galois le sous-groupe $G(K/\mathbb{Q}(\sqrt[4]{7})$ n'est pas distingué dans $G(K/\mathbb{Q})$.

— Comme $\xi^5 \in \mathbb{Q}(\xi)$, $\mathbb{Q}(\xi)$ est le corps de décomposition de $X^2 - X + 1 \in \mathbb{Q}[X]$. Comme $\mathbb{Q}(\xi)$ est aussi de caractéristique 0, l'extension $\mathbb{Q}(\xi)/\mathbb{Q}$ est galoisienne. Par correspondance de Galois le groupe $G(K/\mathbb{Q}(\xi))$ est un sous-groupe distingué de $G(K/\mathbb{Q})$ d'indice $[\mathbb{Q}(\xi) : \mathbb{Q}] = 2$ et donc d'ordre 6.

4. Le groupe de Galois $G(K/\mathbb{Q})$ envoie un zéro d'un polynôme irréductible de $\mathbb{Q}[X]$ sur un autre zéro de ce polynôme. Pour $\sigma \in G(K/\mathbb{Q})$ nous obtenons $\sigma(\xi) \in \{\xi, \xi^5\}$ et $\sigma(\sqrt[4]{7}) = \xi^i \sqrt[4]{7}$ avec $i \in \{1, \ldots, 6\}$, ce qui livre 12 possibilités. Le lemme de la base télescopique montre qu'un $\mathbb{Q}$-automorphisme de $K = \mathbb{Q}(\xi, \sqrt[4]{7})$ est uniquement déterminé par les images de ξ et de $\sqrt[4]{7}$. Comme l'ordre de $G(K/\mathbb{Q})$ est 12, les possibilités précédentes livrent toutes des automorphsimes $G(K/\mathbb{Q})$. Les deux automorphismes définis par $\sigma_1(\xi) = \xi^5, \sigma_1(\sqrt[4]{7}) = \sqrt[4]{7}$ et $\sigma_2(\xi) = \xi, \sigma_2(\sqrt[4]{7}) = \xi \sqrt[4]{7}$ engendrent $G(K/\mathbb{Q})$. Comme $\sigma_1\sigma_2 \neq \sigma_2\sigma_1$ le groupe est non abélien.

Exercice 4 (total 7 points) Soient $n, a, b \geqslant 1$ des entiers. On note $\mathbb{Z}/n\mathbb{Z}$ le groupe abélien des entiers modulo n. On note $(\mathbb{Z}/n\mathbb{Z})^\times$ le groupe abélien des éléments inversibles de l'anneau des entiers modulo n, et on rappelle que lorsque n est une puissance d'un nombre premier $p \geqslant 3$ c'est un groupe cyclique. L'objet de cet exercice est de comparer les deux groupes abéliens finis :

$$M = \mathbb{Z}/a\mathbb{Z} \times (\mathbb{Z}/b\mathbb{Z})^\times \quad \text{et} \quad N = \mathbb{Z}/b\mathbb{Z} \times (\mathbb{Z}/a\mathbb{Z})^\times.$$

1. Dans cette question, on suppose que $a = 75$ et $b = 135$.
   (a) Montrez que M et N ont même cardinal. (1 pt)
   (b) Montrez que M et N ne sont pas isomorphes. (1,5 pts)
2. Dans cette question, on suppose que $a = p^\alpha$ et $b = p^\beta$ sont des puissances d'un même nombre premier $p \geqslant 3$.
   (a) Montrez que M et N ont même cardinal. (0,5 pt)
   (b) Énoncez le théorème de structure des $\mathbb{Z}$-modules de type fini dans le cas particulier des modules finis dont le cardinal est une puissance de p. (2 pts)
   (c) Déduisez de la question précédente que M et N sont isomorphes si et seulement si $\alpha = \beta$. (2 pts)

Corrigé. 1. (a) On observe que $75 = 3.5^2$ et $135 = 3^3.5$. On en déduit que

$$\varphi(75) = \varphi(3)\varphi(5^2) = 2.5.(5-1) = 2^3.5 \quad \text{et} \quad \varphi(135) = \varphi(3^3)\varphi(5) = 3^2.(3-1).4 = 2^3.3^2,$$

donc

$$\mathrm{card}(M) = 75\varphi(135) = 2^3.3^3.5^2 \quad \text{et} \quad \mathrm{card}(N) = 135\varphi(75) = 2^3.3^3.5^2.$$

Ces cardinaux sont donc égaux (à 5400, si on fait le calcul).

1. (b) Pour abréger, notons $\mathbb{Z}/n$ au lieu de $\mathbb{Z}/n\mathbb{Z}$. En utilisant les théorèmes classiques relatifs à $\mathbb{Z}/n$:

(i) le théorème des restes chinois,
(ii) le fait que $(\mathbb{Z}/n \times \mathbb{Z}/m)^\times \simeq (\mathbb{Z}/n)^\times \times (\mathbb{Z}/m)^\times$, et
(iii) le fait que $(\mathbb{Z}/p^\alpha)^\times \simeq \mathbb{Z}/p^{\alpha-1} \times \mathbb{Z}/(p-1)$,

on trouve $M \simeq \mathbb{Z}/3 \times \mathbb{Z}/25 \times \mathbb{Z}/9 \times \mathbb{Z}/2 \times \mathbb{Z}/4$ et $N \simeq \mathbb{Z}/3^3 \times \mathbb{Z}/5 \times \mathbb{Z}/2 \times \mathbb{Z}/5 \times \mathbb{Z}/4$. On voit qu'il y a un élément d'ordre 27 dans N mais pas dans M, donc ces groupes ne sont pas isomorphes. On peut aussi pousser plus loin l'analyse et donner les facteurs invariants de ces groupes :

$$M \simeq (\mathbb{Z}/2 \times \mathbb{Z}/4) \times (\mathbb{Z}/3 \times \mathbb{Z}/9) \times (\mathbb{Z}/25) \simeq \mathbb{Z}/6 \times \mathbb{Z}/900$$

et

$$N \simeq (\mathbb{Z}/2 \times \mathbb{Z}/4) \times (\mathbb{Z}/5 \times \mathbb{Z}/5) \times \mathbb{Z}/3^3 \simeq \mathbb{Z}/10 \times \mathbb{Z}/540.$$

Comme les facteurs invariants sont différents, les modules M et N ne sont pas isomorphes.

2. (a) Le cardinal de M est $a\varphi(b) = p^\alpha p^{\beta-1}(p-1)$. Celui de N est $b\varphi(a) = p^\beta p^{\alpha-1}(p-1)$. Ces deux cardinaux sont égaux à $p^{\alpha+\beta-1}(p-1)$.

2. (b) Soit M un groupe abélien fini dont l'ordre est une puissance de p. Le théorème de structure des $\mathbb{Z}$-modules de type fini appliqué à un tel M affirme qu'il existe une unique suite croissante $1 \leqslant \alpha_1 \leqslant \alpha_2 \leqslant \cdots \leqslant \alpha_r$ telle que :

$$M \simeq \mathbb{Z}/p^{\alpha_1}\mathbb{Z} \oplus \mathbb{Z}/p^{\alpha_2}\mathbb{Z} \oplus \cdots \oplus \mathbb{Z}/p^{\alpha_r}\mathbb{Z}.$$

Les entiers $p^{\alpha_1}, \ldots, p^{\alpha_r}$ sont les facteurs invariants de M.

2. (c) Si $\alpha = \beta$, il est clair que M et N sont isomorphes ; nous écartons ce cas dans la suite. En utilisant de nouveau les théorèmes classiques comme dans 1. (b), on obtient :

$$M \simeq \mathbb{Z}/p^\alpha \times \mathbb{Z}/p^{\beta-1} \times \mathbb{Z}/(p-1) \quad \text{et} \quad N \simeq \mathbb{Z}/p^\beta \times \mathbb{Z}/p^{\alpha-1} \times \mathbb{Z}/(p-1).$$

Si $\alpha < \beta$, on a $\alpha \leqslant \beta - 1$ donc $M \simeq \mathbb{Z}/p^\alpha \times \mathbb{Z}/p^{\beta-1}(p-1)$ et $N \simeq \mathbb{Z}/p^{\alpha-1} \times \mathbb{Z}/p^\beta(p-1)$ ce qui montre que les facteurs invariants de M sont $(p^\alpha, p^{\beta-1}(p-1))$ et ceux de N sont $(p^{\alpha-1}, p^\beta(p-1))$. Ces listes de facteurs invariants sont distinctes, donc M et N ne sont pas isomorphes.

Si $\alpha > \beta$, tout se passe pareil en échangeant M, N et α, β. On voit que les facteurs invariants de M sont $(p^{\beta-1}, p^\alpha(p-1))$ et ceux de N sont $(p^\beta, p^{\alpha-1}(p-1))$ donc M et N ne sont pas isomorphes.