Université Rennes 1, Année 2013-2014, M1 Math ALGB (Algèbre générale de base)

Examen de première session, Corrigé

17 décembre 2014

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. (5 points) Soit $f = X^4 + 1 \in \mathbb{Q}[X]$.

1. Montrer que $f \in \mathbb{Q}[X]$ est irréductible. (1 pt)
2. Montrer que $K = \mathbb{Q}(i, \sqrt{2})$ est un corps de décomposition de f sur $\mathbb{Q}$. (2 pts)
3. En déduire (en justifiant) le groupe de Galois $G(K/\mathbb{Q})$ de f sur $\mathbb{Q}$ en explicitant tous les automorphismes de $G(K/\mathbb{Q})$. (1,5 pts)
4. Donner tous les corps intermédiaires F avec $\mathbb{Q} \subseteq F \subseteq K$ en précisant si $F/\mathbb{Q}$ ou K/F est une extension normale. (0,5 pt)

Corrigé 1.

1. *On considère l'isomorphisme d'anneaux $\varphi_{X\mapsto X+1} : \mathbb{Q}[X] \to \mathbb{Q}[X]$ (d'inverse $\varphi_{X\mapsto X-1}$). Alors $\varphi_{X\mapsto X+1}(f) = X^4 + 4X^3 + 6X^2 + 4X + 2$ est irréductible (Eisenstein dans $\mathbb{Z}[X]$ avec le premier 2) et donc f également.*
2. *Soit α une racine de f, alors $\alpha^2 = i$ ou $\alpha^2 = -i$. Sur le cercle unité on trouve les possibilités $\alpha_1 = \frac{\sqrt{2}}{2} + i\frac{\sqrt{2}}{2}$, $\alpha_2 = -\frac{\sqrt{2}}{2} - i\frac{\sqrt{2}}{2}$, $\alpha_3 = -\frac{\sqrt{2}}{2} + i\frac{\sqrt{2}}{2}$, $\alpha_4 = \frac{\sqrt{2}}{2} - i\frac{\sqrt{2}}{2}$ et il en résulte que $\mathbb{Q}(\alpha_1, \alpha_2, \alpha_3, \alpha_4) \subset K$. Comme $[K : \mathbb{Q}] = [\mathbb{Q}(i, \sqrt{2}) : \mathbb{Q}(\sqrt{2})][\mathbb{Q}(\sqrt{2}) : \mathbb{Q}]$ et que $i \notin \mathbb{Q}(\sqrt{2}) \subset \mathbb{R}$ nous obtenons $[\mathbb{Q}(i, \sqrt{2}) : \mathbb{Q}] = 4$. La première question montre que $[\mathbb{Q}(\alpha_1) : \mathbb{Q}] = \deg(f) = 4$ et donc $\mathbb{Q}(\alpha_1, \alpha_2, \alpha_3, \alpha_4) = K$, en particulier l'extension $K/\mathbb{Q}$ est galoisienne.*
3. *D'après le cours $|G(K/\mathbb{Q})| = 4$. Un automorphisme $\sigma \in G(K/\mathbb{Q})$ envoie une racine de $X^2 - 2$ et de $X^2 + 1$ sur une racine de ce même polynôme, ce qui donne les quatre possibilités $\sigma(\sqrt{2}) = \pm\sqrt{2}$ et $\sigma(i) = \pm i$ qui sont donc tous des automorphismes. Ces automorphismes sont tous d'ordre 2 ou 1 et le groupe est donc isomorphe à $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.*
   NB : Comme f est irréductible le groupe permute les racines transitivement et doit donc être le groupe engendré par les doubles transpositions de S_4.
4. *Pour σ_1 avec $\sigma_1(\sqrt{2}) = -\sqrt{2}, \sigma_1(i) = i$ et σ_2 avec $\sigma_2(i) = -i, \sigma_2(\sqrt{2}) = \sqrt{2}$ les sous groupes de $G(K/\mathbb{Q})$ sont $G(K/\mathbb{Q})$, $\{e, \sigma_1\}$, $\{e, \sigma_2\}$, $\{e, \sigma_1\sigma_2\}$ et $\{e\}$ dont les corps fixes F sont $\mathbb{Q}$, $\mathbb{Q}(i)$, $\mathbb{Q}(\sqrt{2})$, $\mathbb{Q}(i\sqrt{2})$ et K. Les extensions $F/\mathbb{Q}$ et K/F sont toutes normales car le groupe est abélien et donc tous les sous-groupes et tous les quotients sont distingués.*

Exercice 2. (5 points) Soient A un anneau principal, $M = A^n$ le A-module libre de rang $n \geq 1$ muni de sa base canonique (e_i), et $f : M \to M$ un endomorphisme A-linéaire. On note N l'image de f, δ son déterminant et F sa matrice dans la base (e_i). On suppose que f est injectif.

1. Le $\mathbb{Z}$-module N est-il libre ? de torsion ? En utilisant la formule de la comatrice, montrez que M/N est un module de δ-torsion. (1,5 pt)
2. On suppose que $A = \mathbb{Z}$. En utilisant le théorème de mise sous forme normale de Smith pour F, montrez que M/N est fini, de cardinal $|\delta|$. (2 pts)
3. Soient $f_1, f_2 : \mathbb{Z}^2 \to \mathbb{Z}^2$ les endomorphismes donnés par les matrices $F_1 = \left(\begin{smallmatrix} 7 & 3 \\ 1 & 3 \end{smallmatrix}\right)$ et $F_2 = \left(\begin{smallmatrix} 9 & 3 \\ 3 & 3 \end{smallmatrix}\right)$. Soient $N_i = f_i(\mathbb{Z}^2)$ avec $i = 1, 2$ les images. Les groupes M/N_1 et M/N_2 sont-ils isomorphes ? (1 pt)
4. On suppose que $A = k[X]$ est un anneau de polynômes sur un corps k fini à q éléments. Par la même méthode qu'en 2, montrez que M/N est fini, de cardinal q^n où $n = \deg(\delta)$. (0,5 pt)

Corrigé 2.

1. *Comme f est injectif, il induit un isomorphisme $M \simeq N$ donc N est libre de rang n. (Le fait que A soit un anneau principal n'est pas utilisé !) Comme de plus $n \geq 1$, alors N est libre et non nul, donc il n'est pas de torsion : n'importe lequel de ses éléments non nuls n'est pas de torsion. Maintenant notons F^* la transposée de la comatrice de F, et f^* l'endomorphisme associé. D'après la formule de la comatrice, on a $FX^* = \delta\, I_n$, ou encore $f f^* = \delta\, id_M$. Il en découle que $\delta x = f(f^*(x)) \in N$, pour tout $x \in M$. Ainsi $\delta \bar{x} = 0$ dans M/N, donc M/N est de δ-torsion.*
2. *D'après le théorème de mise sous forme normale de Smith, il existe une suite unique d'idéaux emboîtés $(d_1) \supset \cdots \supset (d_n) \neq (0)$ et deux matrices $P, Q \in SL_n(\mathbb{Z})$ tels que $F = PDQ$, où D est la matrice diagonale de coefficients diagonaux $d_1, \ldots, d_n$. Le fait que le nombre de facteurs invariants non nuls d_i est égal à n provient du fait que f est supposé injectif. Si on note v_i les vecteurs colonnes de P et u_i ceux de Q^{-1}, l'égalité $F = PDQ$ signifie que l'on a $f(u_i) = d_i v_i$ pour tout i. Il en découle que $N = \mathbb{Z}d_1 v_1 \oplus \cdots \oplus \mathbb{Z}d_n v_n \subset M = \mathbb{Z}v_1 \oplus \cdots \oplus \mathbb{Z}v_n$ et $M/N \simeq \oplus \mathbb{Z}/d_i\mathbb{Z}$. En particulier c'est un groupe fini de cardinal $|d_1 \cdots d_n| = |\det(D)| = |\det(F)| = |\delta|$.*
3. *Les facteurs invariants d'une matrice F de taille $(2, 2)$ sont le pgcd des coefficients de F et son déterminant. On trouve donc $(1, 18)$ pour F_1 et $(3, 6)$ pour F_2. Ainsi $M/N_1 \simeq \mathbb{Z}/18\mathbb{Z}$ et $M/N_2 \simeq \mathbb{Z}/3\mathbb{Z} \oplus \mathbb{Z}/6\mathbb{Z}$. Ce sont deux groupes de cardinal 18, de facteurs invariants différents donc non isomorphes.*
4. *La même méthode qu'en 2. montre que $N = Ad_1 v_1 \oplus \cdots \oplus Ad_n v_n \subset M = Av_1 \oplus \cdots \oplus Av_n$ où cette fois-ci $A = k[X]$ et les éléments d_i, u_i, v_i sont des polynômes. On trouve ici encore $M/N \simeq k[X]/(d_1) \oplus \cdots \oplus k[X]/(d_n)$. Chaque facteur $k[X]/(d_i)$ est un k-espace vectoriel de dimension $\deg(d_i)$, donc M/N est de dimension $\deg(d_1) + \cdots + \deg(d_n) = \deg(d_1 \cdots d_n) = \deg(\delta)$. Comme k est fini de cardinal q, cet espace vectoriel est fini de cardinal $q^{\deg(\delta)}$.*

Exercice 3. (5 points) Soient p un nombre premier et $n \geq 1$ un entier. Dans l'exercice on fixe une clôture algébrique $\overline{\mathbb{F}_p}$ de $\mathbb{F}_p$ et on note $\mathbb{F}_{p^n}$ l'unique sous-corps à p^n éléments de $\overline{\mathbb{F}_p}$.

1. Soit $f \in \mathbb{F}_p[X]$ de degré m un diviseur irréductible unitaire de $X^{p^n} - X \in \mathbb{F}_p[X]$, montrer que m divise n. (1 pt)
2. Montrer que pour tout diviseur d de n il existe un unique sous-groupe d'ordre d du groupe de Galois $G(\mathbb{F}_{p^n}/\mathbb{F}_p)$ (0,5 pt)
3. En déduire que les sous-corps de $\mathbb{F}_{p^n}$ sont les $\mathbb{F}_{p^m}$ avec m divise n. (2 pts)
4. En déduire que tout polynôme irréductible unitaire $f \in \mathbb{F}_p[X]$ dont le degré m divise n est un diviseur de $X^{p^n} - X \in \mathbb{F}_p[X]$. (1 pt)
5. En déduire que $X^{p^n} - X$ est le produit des polynômes irréductibles unitaires de $\mathbb{F}_p[X]$ dont le degré divise n. (0.5 pt)

Corrigé 3.

1. *Pour un zéro α de f nous avons $\mathbb{F}_p \subset \mathbb{F}_p(\alpha) \subset \mathbb{F}_{p^n}$ et donc $[\mathbb{F}_p(\alpha) : \mathbb{F}_p] = \deg(f)$ divise $[\mathbb{F}_{p^n} : \mathbb{F}_p] = n$.*
2. *D'après le cours l'ordre du groupe cyclique $G(\mathbb{F}_{p^n}/\mathbb{F}_p)$ est un groupe cyclique d'ordre n. Le groupe $G(\mathbb{F}_{p^n}/\mathbb{F}_p)$ étant cyclique il existe d'après le cours au plus un sous-groupe d'ordre d pour chaque diviseur d de n. Inversement si σ est un générateur d'ordre n du groupe alors pour $n = dm$ l'automorphisme σ^m engendre un sous-groupe d'ordre d de $G(\mathbb{F}_{p^n}/\mathbb{F}_p)$.*
3. *La correspondance de Galois livre une bijection entre les sous-groupes de $G(\mathbb{F}_{p^n}/\mathbb{F}_p)$ et les sous-corps de $\mathbb{F}_{p^n}$ (contenant $\mathbb{F}_p$)). A l'unique sous-groupe H d'ordre d et d'indice m correspond un unique sous-corps F avec $[F : \mathbb{F}_p] = m$. Comme $[F : \mathbb{F}_p] = m$ le corps F est d'ordre p^m et donc $F = \mathbb{F}_{p^m}$ (l'unique sous corps d'ordre p^m de $\overline{\mathbb{F}_p}$).*
4. *Le corps de rupture $\mathbb{F}_p[X]/(f)$ est un corps à p^m éléments et est donc un sous-corps de $\mathbb{F}_{p^n}$. Le polynôme $f \in \mathbb{F}_p[X]$ possède donc une racine dans $\mathbb{F}_{p^n}$. L'extension $\mathbb{F}_{p^n}/\mathbb{F}_p$ galoisienne étant normale, il en résulte que f est scindé dans $\mathbb{F}_{p^n}$ et donc les zéros de f sont tous des zéros de $X^{p^n} - X$. D'après le cours un corps fini est toujours séparable et $X^{p^n} - X$ est sans racines multiples. Donc f divise $X^{p^n} - X$.*
5. *Nous avons obtenu que le degré d'un diviseur irréductible unitaire de $X^{p^n} - X$ divise n et inversement tout polynôme irréductible unitaire dont le degré divise n est un diviseur de $X^{p^n} - X$. Comme $X^{p^n} - X$ est sans facteurs multiples et que dans l'anneau factoriel $\mathbb{F}_p[X]$ le polynôme unitaire $X^{p^n} - X$ est le produit de ses diviseurs irréductibles nous obtenons le résultat.*

Exercice 4. (5 points) On appelle *nombre d'or* le nombre complexe $\alpha = \frac{1+\sqrt{5}}{2}$. On note $A = \mathbb{Z}[\alpha]$ le sous-anneau de $\mathbb{Q}(\alpha)$ engendré par α.

1. Calculez le polynôme minimal f de α sur $\mathbb{Q}$ et montrez qu'il est à coefficients dans $\mathbb{Z}$. (0,5 pt)
2. Construisez un isomorphisme d'anneaux $u : \mathbb{Z}[X]/(f) \to A$. (1,5 pt)
3. Montrez que 2 est premier dans A et que 5 n'est pas premier dans A. (2 pts)
4. Soit $a = m + n\alpha \in A$, avec $(m, n) \in \mathbb{Z}^2$. Montrez que a est inversible dans A si et seulement si $m^2 + mn - n^2 = \pm 1$. Donnez un exemple d'élément inversible distinct de 1 et -1. (1 pt)

Corrigé 4.

1. *On a $2\alpha - 1 = \sqrt{5}$ donc $\alpha^2 - \alpha - 1 = 0$. Ainsi le polynôme $f = X^2 - X - 1$ annule α. Comme ses racines α et $1 - \alpha$ ne sont pas dans $\mathbb{Q}$, il est irréductible sur $\mathbb{Q}$. C'est donc le polynôme minimal de α sur $\mathbb{Q}$. Il est à coefficients dans $\mathbb{Z}$.*
2. *On définit un morphisme d'anneaux $v : \mathbb{Z}[X] \to A$ en envoyant X sur α. Par définition de A, ce morphisme est surjectif. Le polynôme f est dans le noyau de u, donc d'après le théorème de propriété universelle du quotient, v induit un morphisme surjectif $u : \mathbb{Z}[X]/(f) \to A$ tel que $u(x) = \alpha$, où x est la classe de X. Montrons que u est injectif. Par division euclidienne, tout élément de $\mathbb{Z}[X]/(f)$ s'écrit de manière unique sous la forme $m + nx$ avec $m + n \in \mathbb{Z}$. Si $u(m + nx) = m + n\alpha = 0$, alors comme $\{1, \alpha\}$ est une famille linéairement indépendante sur $\mathbb{Q}$ on en déduit que $m = n = 0$. Ceci montre que u est injectif, donc finalement un isomorphisme.*
3. *On a $A/(2) \simeq \mathbb{Z}[X]/(f, 2) \simeq \mathbb{F}_2[X]/(f)$ où l'on note encore $f = X^2 - X - 1$ le polynôme vu à coefficients dans $\mathbb{F}_2$. Comme f n'a pas de racine dans $\mathbb{F}_2$, il est irréductible dans $\mathbb{F}_2[X]$ donc le quotient $\mathbb{F}_2[X]/(f)$ est un anneau intègre. Ceci signifie que $2 \in A$ est premier. Maintenant, on a $A/(5) \simeq \mathbb{Z}[X]/(f, 5) \simeq \mathbb{F}_5[X]/(f)$ où l'on note encore $f = X^2 - X - 1 \in \mathbb{F}_5[X]$. Comme $f = (X - 3)^2$ dans $\mathbb{F}_5[X]$, l'anneau $\mathbb{F}_5[X]/(f)$ n'est pas intègre : l'élément $x - 3$ n'est pas nul mais son carré est nul. Ceci signifie que $5 \in A$ n'est pas premier.*
4. *L'élément $a = m + n\alpha$ est inversible si et seulement si le morphisme de $\mathbb{Z}$-modules m_a donné par la multiplication par a dans A est surjectif. Or on sait par la question 3. que A est un $\mathbb{Z}$-module libre de rang 2, de base $\{1, \alpha\}$. Il suffit donc d'écrire la matrice de m_a dans cette base et d'exprimer le fait que son déterminant doit être inversible dans $\mathbb{Z}$ i.e. égal à ± 1. La matrice en question est $\begin{pmatrix} m & n \\ n & m+n \end{pmatrix}$ et son déterminant vaut $m^2 + mn - n^2$. On obtient le critère demandé. À titre d'exemples, les éléments α et $1 + \alpha$ sont inversibles dans A. (*On pouvait aussi utiliser la norme habituelle en théorie des nombres : on introduit le conjugué $\bar{\alpha} = 1 - \alpha$, le morphisme de conjugaison $c : A \to A$ défini par $c(m + n\alpha) = m + n\bar{\alpha}$ et la norme $N(a) = a.c(a) = m^2 + mn - n^2$. C'est une application multiplicative et on montre que a est inversible ssi $N(a) = \pm 1$.*)*