Université de Rennes 1 Année universitaire 2019-2020
Licence de mathématiques
Module Anneaux et Arithmétique

Contrôle continu n°2
Mercredi 8 avril 2020, 16h15 – 17h30
Corrigé

Exercice 1

1 Soit a et b des entiers strictement positifs premiers entre eux. Soit G un groupe noté multiplicativement, d'élément neutre noté e, et x et y deux éléments de G d'ordre respectifs a et b et tels que $xy = yx$. Déterminer l'ordre de xy.

Correction *: Montrons que l'ordre de xy est égal à ab. Tout d'abord, comme on a $xy = yx$, on peut écrire $(xy)^{ab} = x^{ab}y^{ab}$. Ainsi*

$$(xy)^{ab} = x^{ab}y^{ab} = (x^a)^b(y^b)^a.$$

Comme x est d'ordre a, on a $x^a = e$. De même, comme y est d'ordre b, on a $y^b = e$. On a alors

$$(xy)^{ab} = (x^a)^b(y^b)^a = e^b.e^a = e.$$

Ainsi l'ordre de xy divise ab.

Soit à présent N un entier strictement positif tel que $(xy)^N = e$. Montrons que ab divise N. Comme $xy = yx$, on a $x^N y^N = e$. En élevant cette égalité à la puissance b, on obtient $x^{bN}y^{bN} = e$ Mais comme $y^b = e$, on a $y^{bN} = (y^b)^N = e$. Ainsi $x^{bN} = e$. Donc l'ordre de x divise bN. Ainsi a divise bN. Comme a et b sont supposés premiers entre eux, a divise N. Comme x et y jouent des rôles symétriques dans l'énoncé, on en déduit que b divise N. Comme a et b divise N et sont premiers entre eux, on en déduit que ab divise N.

En particulier ab divise l'ordre de xy. D'après ce qu'on a démontré au début, on en déduit que l'ordre de xy est égal à ab.

2 Donner *sans justification* la liste des polynômes de $\mathbf{F}_2[X]$ qui sont irréductibles de degré 2.

Correction *: Il n'y a qu'un polynôme irréductible de degré 2 sur $\mathbf{F}_2$, à savoir $X^2 + X + [1]_2$.*

3 Montrer que le polynôme $P_1 := X^4 + X + [1]_2$ est un élément irréductible de $\mathbf{F}_2[X]$.

Correction *: On a*

$$P_1([0]_2) = [0]_2^4 + [0]_2 + [1]_2 = [1]_2 \neq [0]_2$$
$$\text{et} \quad P_1([1]_2) = [1]_2^4 + [1]_2 + [1]_2 = [3]_2 = [1]_2 \neq [0]_2.$$

Ainsi P_1 n'a pas de racine dans $\mathbf{F}_2$. Si P_1 est réductible, il s'écrit $P_1 = Q_1R_1$, où Q_1 et R_1 sont des éléments de $\mathbf{F}_2[X]$ tels que $1 \leqslant \deg(Q_1), \deg(R_1) \leqslant \deg(P_1) - 1 = 3$. On a par ailleurs $\deg(Q_1) + \deg(R_1) = \deg(P_1) = 4$. Comme P_1 n'a pas de racine dans $\mathbf{F}_2$, Q_1 et R_1 n'en ont pas non plus, donc le cas $\{\deg(Q_1), \deg(R_1)\} = \{1, 3\}$ est exclu. Ainsi Q_1 et R_1 sont de degré 2 et comme ils n'ont pas de racine dans $\mathbf{F}_2$, ce sont donc des éléments irréductibles de $\mathbf{F}_2[X]$. D'après la question précédente, on a $Q_1 = R_1 = X^2 + X + [1]_2$, donc $P_1 = (X^2 + X + [1]_2)^2$. Comme $\mathbf{F}_2[X]$ est de caractéristique 2, on en déduit $P_1 = (X^2)^2 + X^2 + [1]_2^2 = X^4 + X^2 + [1]_2$, ce qui n'est pas vrai. Donc P_1 est bien un élément irréductible de $\mathbf{F}_2[X]$.

4 Soit $\mathbf{K} := \mathbf{F}_2[X]/\langle X^4 + X + [1]_2\rangle$. Donner *sans justification* la caractéristique et le cardinal de $\mathbf{K}$

Correction : *Le corps* $\mathbf{K}$ *est de caractéristique* 2 *et de cardinal* $2^4 = 16$.

5 On note α l'image de X dans $\mathbf{K}$ par le morphisme quotient. Soit $x := \alpha^2 + \alpha$ et $y := \alpha^3$. Calculer x^3. Montrer que $y^5 = [1]_2$. En déduire un générateur explicite du groupe $\mathbf{K}^\times$.
Correction : *On a* $P_1(\alpha) = 0$ *soit* $\alpha^4 = -\alpha - [1]_2 = \alpha + [1]_2$. *Ainsi, en utilisant aussi le fait que* $\mathbf{K}$ *est de caractéristique* 2, *on a*

$$x^3 = x.x^2 = x.(\alpha^4 + \alpha^2) = (\alpha^2 + \alpha)(\alpha^2 + \alpha + [1]_2)$$

soit

$$x^3 = \alpha^4 + \alpha^3 + \alpha^2 + \alpha^3 + \alpha^2 + \alpha = \alpha^4 + 2\alpha^3 + 2\alpha^2 + \alpha = 2\alpha + [1]_2 = [1]_2.$$

Par ailleurs, on a $y^5 = (y^2)^2.y$. *Or*

$$y^2 = (\alpha^3)^2 = \alpha^6 = \alpha^2(\alpha + [1]_2) = \alpha^3 + \alpha^2$$

donc

$$(y^2)^2 = \alpha^6 + \alpha^4 = \alpha^3 + \alpha^2 + \alpha + [1]_2.$$

Finalement

$$y^5 = y.y^4 = \alpha^3(\alpha^3 + \alpha^2 + \alpha + [1]_2) = \alpha^6 + \alpha^5 + \alpha^4 + \alpha^3 = (\alpha^3 + \alpha^2) + (\alpha^2 + \alpha) + (\alpha + [1]_2) + \alpha^3$$

$$\textit{soit} \quad y^5 = 2.\alpha^3 + 2.\alpha^2 + 2.\alpha + [1]_2 = [1]_2.$$

Comme $x^3 = [1]_2$, *l'ordre de* x *comme élément de* $\mathbf{K}^\times$ *divise* 3. *Comme* 3 *est premier, cet ordre est donc* 1 *ou* 3. *Mais comme* $\{[1]_2, \alpha, \alpha^2, \alpha^3\}$ *est une base du* $\mathbf{F}_2$*-espace vectoriel* $\mathbf{K}$, *on a* $x \neq [1]_2$. *Donc l'ordre de* x *comme élément de* $\mathbf{K}^\times$ *est* 3.

Un raisonnement strictement similaire montre que l'ordre de y *comme élément de* $\mathbf{K}^\times$ *est* 5.

Or 5 *et* 3 *sont premiers entre eux, et* $\mathbf{K}^\times$ *est un groupe commutatif. La première question montre donc que* xy *est un élément d'ordre* 15 *de* $\mathbf{K}^\times$. *Mais comme* $\mathbf{K}$ *est un corps et d'après la question 4,* $\mathbf{K}^\times$ *est de cardinal* $16 - 1 = 15$. *Donc* xy *est un générateur de* $\mathbf{K}^\times$. *On pouvait éventuellement calculer*

$$xy = (\alpha^2 + \alpha)\alpha^3 = \alpha^5 + \alpha^4 = \alpha^2 + \alpha + \alpha + [1]_2 = \alpha^2 + [1]_2.$$

6 Le polynôme $P_2 := X^3 + X^2 + X + [1]_2$ a-t-il une racine dans $\mathbf{K}$? Même question pour le polynôme $P_3 := X^3 + X^2 + [1]_2$.
Correction : *Le corps* $\mathbf{K}$ *contient* $\mathbf{F}_2$, *et on a* $P_2([1]_2) = [1]_2^3 + [1]_2^2 + [1]_2 + [1]_2 = [4]_2 = [0]_2$. *Ainsi* P_2 *a bien une racine dans* $\mathbf{K}$ *(question bonus : trouver toutes les racines de* P_2 *dans* $\mathbf{K}$*).*

Montrons par contre que le polynôme P_3 *n'a pas de racine dans* $\mathbf{K}$. *Tout d'abord, on vérifie facilement que* P_3 *n'a pas de racine dans* $\mathbf{F}_2$. *Comme ce polynôme est de degré* 3, *c'est un élément irréductible de* $\mathbf{F}_2[X]$. *Raisonnons par l'absurde en supposant que* P_3 *admet une racine* β *dans* $\mathbf{K}$.

Soit φ *l'unique morphisme de* $\mathbf{F}_2$*-algèbres de* $\mathbf{F}_2[X]$ *vers* $\mathbf{K}$ *qui envoie* X *sur* β. *Le noyau de* φ *est engendré par un polynôme* Q *de* $\mathbf{F}_2[X]$, *et contient par ailleurs* P_3. *En particulier* Q *divise* P_3. *Or* P_3 *est irréductible, donc soit* Q *est associé à* P *et* $\mathrm{Ker}(\varphi) = \langle P_3 \rangle$, *soit* Q *est inversible et* $\mathrm{Ker}(\varphi) = \mathbf{F}_2[X]$. *Mais cette dernière éventualité entraîne que* $\mathbf{K}$ *est l'anneau nul, ce qui est faux. Donc* $\mathrm{Ker}(\varphi) = \langle P_3 \rangle$, *et* φ *induit un isomorphisme de* $\mathbf{F}_2[X]/\langle P_3 \rangle$ *sur un sous-corps* $\mathbf{L}$ *de* $\mathbf{K}$. *Ainsi* $\mathbf{K}$ *est muni d'une structure de* $\mathbf{L}$*-espace vectoriel de dimension finie, et donc son cardinal est une puissance du cardinal de* $\mathbf{L}$. *Or* $\mathbf{L}$ *est de cardinal* $2^3 = 8$ *et* $\mathbf{K}$ *est de cardinal* 16 *:*

contradiction (on pouvait bien sûr pour la fin appliquer directement le théorème 15 du chapitre 4 du cours).

7 (question bonus) Montrer que $x^2 + x + [1]_2 = 0$. En déduire la liste explicite des éléments d'un sous corps de $\mathbf{K}$ de cardinal 4.
Correction : *Calculons*

$$x^2 + x + [1]_2 = (\alpha^2 + \alpha)^2 + (\alpha^2 + \alpha) + [1]_2 = \alpha^4 + 2\alpha^2 + \alpha + [1]_2 = 2\alpha + [2]_2 = [0]_2.$$

Ainsi x est une racine du polynôme $Q := X^2 + X + [1]_2$, qui est un polynôme de $\mathbf{F}_2[X]$ irréductible de degré 2 (question 2). L'unique morphisme de $\mathbf{F}_2$-algèbres de $\mathbf{F}_2[X]$ vers $\mathbf{K}$ qui envoie X sur x induit donc (cf. le raisonnement de la question précédente) un isomorphisme de $\mathbf{F}_2[X]/\langle Q\rangle$ sur un sous-corps $\mathbf{L}$ de $\mathbf{K}$, sous-corps qui est donc de cardinal $2^{\deg(Q)} = 4$. En utilisant la description explicite d'une base du $\mathbf{F}_2$-espace vectoriel $\mathbf{F}_2[X]/\langle Q\rangle$, on en déduit qu'on a $\mathbf{L} = \{[0]_2, [1]_2, x, [1]_2 + x\}$ soit $\mathbf{L} = \{[0]_2, [1]_2, \alpha^2 + \alpha, \alpha^2 + \alpha + [1]_2\}$

Exercice 2

Pour tout entier strictement positif a, on note A_a l'image dans $\mathbf{Q}$ de l'unique morphisme d'anneaux $\pi_a \colon \mathbf{Z}[X] \to \mathbf{Q}$ qui envoie X sur $\frac{1}{a}$.

1 Montrer que $A_a = \{\frac{b}{a^n}\}_{b\in\mathbf{Z},\, n\in\mathbf{N}}$.
Correction : *Montrons l'inclusion $\{\frac{b}{a^n}\}_{b\in\mathbf{Z},\, n\in\mathbf{N}} \subset A_a$. Soit $b \in \mathbf{Z}$ et $n \in \mathbf{N}$. Soit $P := bX^n \in \mathbf{Z}[X]$. Alors $\pi_a(P) = P\left(\frac{1}{a}\right) = \frac{b}{a^n}$. On en déduit l'inclusion annoncée.*
Montrons l'inclusion $A_a \subset \{\frac{b}{a^n}\}_{b\in\mathbf{Z},\, n\in\mathbf{N}}$. Soit $c \in A_a$ et $P \in \mathbf{Z}[X]$ tel que $c = \pi_a(P) = P\left(\frac{1}{a}\right)$. Écrivons $P = \sum_{i=0}^n a_i X^i$ avec $n \in \mathbf{N}$ et $(a_i) \in \mathbf{Z}^{n+1}$. On a donc

$$c = P\left(\frac{1}{a}\right) = \sum_{i=0}^{n} a_i \left(\frac{1}{a}\right)^i.$$

Posons $b := \sum_{i=0}^n a_i a^{n-i}$. On peut alors écrire

$$c = \sum_{i=0}^{n} \frac{a_i.a^{n-i}}{a^n} = \frac{b}{a^n}.$$

On en déduit l'inclusion annoncée.
Par double inclusion, on a donc bien montré l'égalité demandée.

2 Donner *sans justification* une partie multiplicative S de $\mathbf{Z}$ telle que A_a est isomorphe au localisé de $\mathbf{Z}$ par rapport à S. Donner *sans justification* le corps des fractions de A_a.
Correction : *On peut prendre $S = \{a^n\}_{n\in\mathbf{N}}$. Le corps des fractions de A_a est $\mathbf{Q}$.*

3 Soit $\mathbf{K}$ un corps et $P \in \mathbf{K}[X]$ un polynôme de degré 1. Montrer que l'anneau quotient $\mathbf{K}[X]/\langle P\rangle$ est isomorphe à $\mathbf{K}$. *En admettant* que le noyau de π_a est l'idéal de $\mathbf{Z}[X]$ engendré par $aX - 1$, en déduire, pour tout nombre premier p, une description simple du quotient A_a/pA_a.
Correction : *Pour la première question, soit $\alpha \in \mathbf{K}^\times$ et $x \in \mathbf{K}$ tels que $P = \alpha(X - x)$. Ainsi les polynômes P et $X - x$ sont associés, et on a donc $\langle P\rangle = \langle X - x\rangle$. Soit alors $\varphi \colon \mathbf{K}[X] \to \mathbf{K}$ l'unique morphisme de $\mathbf{K}$-algèbres qui envoie X sur x, en d'autres termes le morphisme d'évaluation en x. Un élément Q de $\mathbf{K}[X]$ est dans le noyau de φ si et seulement si $Q(x) = 0$ si et seulement si $X - x$ divise Q si et seulement si $Q \in \langle X - x\rangle$. Ainsi le noyau de φ est $\langle X - x\rangle$. Par ailleurs si*

$Q = \alpha \in \mathbf{K}$ est un polynôme constant, on a $Q(x) = \alpha$; ceci montre que φ est surjectif. Ainsi φ induit un isomorphisme de $\mathbf{K}[X]/\langle P\rangle = \mathbf{K}[X]/\langle X - x\rangle$ sur $\mathbf{K}$.

Pour la seconde question, si on admet la propriété annoncée, on sait que π_a est un morphisme d'image A_a et de noyau $\langle aX - 1\rangle$. On en déduit que A_a est isomorphe à l'anneau quotient $\mathbf{Z}[X]/\langle aX - 1\rangle$. Soit p un nombre premier. En utilisant les théorèmes d'isomorphismes, on en déduit que le quotient A_a/pA_a est isomorphe à $\mathbf{Z}[X]/\langle p, aX - 1\rangle$, puis à $(\mathbf{Z}/p\mathbf{Z})[X]/\langle [a]_p X - [1]_p\rangle$ Comme p est premier, $\mathbf{Z}/p\mathbf{Z}$ est un corps. Si p divise a, on a $[a]_p X - [1]_p = -[1]_p$ qui est donc un élément inversible de $(\mathbf{Z}/p\mathbf{Z})[X]$. Donc le quotient considéré est l'anneau nul. Si p ne divise pas a, le polynôme $[a]_p X - [1]_p$ est de degré 1. D'après la question précédente, le quotient considéré est isomorphe à $\mathbf{Z}/p\mathbf{Z}$.

En résumé, le quotient A_a/pA_a est l'anneau nul si p divise a, et $\mathbf{Z}/p\mathbf{Z}$ si p ne divise pas a.

4 Montrer que l'idéal engendré par 3 dans A_2 est premier. En déduire que les anneaux A_2 et A_3 ne sont pas isomorphes.

***Correction** : Soit $\mathcal{I}$ l'idéal engendré par 3 dans A_2. D'après la question précédente, le quotient $A_2/\mathcal{I}$ est isomorphe à $\mathbf{Z}/3\mathbf{Z}$, qui est corps. Ainsi $\mathcal{I}$ est un idéal maximal, donc premier, de A_2. Indiquons comment on pouvait montrer que $\mathcal{I}$ est premier sans utiliser la question précédente. Montrons d'abord que $\mathcal{I}$ est propre. Supposons le contraire, d'après la première question, il existe alors $b \in \mathbf{Z}$ et $n \in \mathbf{N}$ tel que $\frac{3b}{2^n} = 1$. On en déduit qu'on a $3b = 2^n$ donc 3 divise 2^n, donc 3 divise 2 d'après le lemme d'Euclide, contradiction. Donc $\mathcal{I}$ est un idéal propre. Soit à présent $c_1, c_2 \in A_2$ tel que $c_1, c_2 \in \mathcal{I}$. D'après la première question, il existe $b_1, b_2, b_3 \in \mathbf{Z}$ et $n_1, n_2, n_3 \in \mathbf{Z}$ tels que*

$$\frac{b_1}{2^{n_1}} \frac{b_2}{2^{n_2}} = \frac{3b_3}{2^{n_3}}.$$

On a donc $3b_3 2^{n_1+n_2} = b_1 b_2 2^{n_3}$. En particulier 3 divise $b_1 b_2 2^{n_3}$. Comme 3 est premier avec 2^{n_3}, 3 divise $b_1 b_2$. Comme 3 est premier, on en déduit que 3 divise b_1 ou 3 divise b_2. Ainsi $c_1 \in \mathcal{I}$ ou $c_2 \in \mathcal{I}$, et $\mathcal{I}$ est un idéal premier de A_2.

Raisonnons par l'absurde et supposons qu'il existe un isomorphisme d'anneaux φ de A_2 sur A_3. Comme φ est un morphisme de groupes, on a $\varphi(3) = \varphi(3 \cdot 1) = 3 \cdot \varphi(1) = 3 \cdot 1 = 3$. On en déduit, en utilisant le fait que φ est un isomorphisme, donc surjectif, que $\varphi(3A_2) = 3A_3$. Mais 3 est inversible dans A_3, donc $3A_3 = A_3$. Comme $3A_2$ est un idéal premier d'après la question précédente, donc propre, et que φ est injectif, l'égalité $\varphi(3A_2) = A_3$ est impossible.

5 Soit a et a' des entiers strictement positifs. Énoncer *sans démonstration* une condition nécessaire et suffisante, portant sur les facteurs premiers de a et a', pour que les anneaux A_a et $A_{a'}$ soient isomorphes.

***Correction** : Les anneaux A_a et $A_{a'}$ sont isomorphes si et seulement si a et a' ont exactement les mêmes facteurs premiers.*

6 (question bonus) Démontrer le résultat énoncé à la question précédente.

***Correction** : Remarque préliminaire : si A est un anneau et a, b sont des éléments de A tels que $ab \in A^\times$, alors a et b sont des élément de $A^\times$. En effet si c est l'inverse de ab dans A, on vérifie que a est inversible dans A d'inverse bc et b est inversible dans A d'inverse ac.*

Supposons que a et a' n'ont pas les mêmes facteurs premiers et montrons que les anneaux A_a et $A_{a'}$ ne sont pas isomorphes. Quitte à échanger a et a', on peut supposer qu'il existe un facteur premier p de a' qui ne divise pas a. D'après la question 3, pA_a est un idéal premier de A_a. Comme p divise a' et a' est inversible dans $A_{a'}$, d'après la remarque préliminaire, p est inversible dans $A_{a'}$. Ainsi $pA_{a'} = A_{a'}$. Si φ est un isomorphisme de A_a sur $A_{a'}$, on montre comme à la question 4 que $\varphi(pA_a) = pA_{a'}$ et on en déduit comme à la question 4 une contradiction.

Supposons que a et a' ont exactement les mêmes facteurs premiers et montrons que les anneaux A_a et $A_{a'}$ sont isomorphes. On va en fait montrer qu'ils sont égaux (comme sous-anneaux de $\mathbf{Q}$). Comme a et a' ont les mêmes facteurs premiers, en utilisant la décomposition en facteurs premiers, on constate qu'il existe un entier strictement positif N tel que a divise $(a')^N$. Soit $\alpha \in \mathbf{Z}$ tel que $(a')^N = \alpha.a$. On a alors $\frac{1}{a} = \frac{\alpha}{\alpha.a} = \frac{\alpha}{(a')^N}$. Ainsi $\frac{1}{a} \in A_{a'}$. Comme tout élément de A_a est un polynôme à coefficients entiers en $\frac{1}{a}$ et que $A_{a'}$ est un sous-anneau de $\mathbf{Q}$, on en déduit l'inclusion $A_a \subset A_{a'}$ Comme a et a' jouent des rôles symétriques, on en déduit aussitôt l'inclusion réciproque $A_{a'} \subset A_a$ et donc l'égalité annoncée.

7 (question bonus) Démontrer le résultat admis sur le noyau de π_a à la question 3. Le premier résultat de la question 3 est-il encore vrai si on remplace le corps $\mathbf{K}$ par un anneau intègre A quelconque ?

Correction : *On a $\pi_a(aX-1) = a\frac{1}{a} - 1 = 0$. Donc $aX - 1 \in \mathrm{Ker}(\pi_a)$ et comme $\mathrm{Ker}(\pi_a)$ est un idéal on a l'inclusion $\langle aX-1\rangle \subset \mathrm{Ker}(\pi_a)$.*

Montrons l'inclusion réciproque. Soit $P \in \mathrm{Ker}(\pi_a)$. La difficulté est que le polynôme $aX-1$ n'est pas un polynôme unitaire de $\mathbf{Z}[X]$ et qu'on ne peut donc pas effectuer la division euclidienne de P par ce polynôme dans $\mathbf{Z}[X]$ (ce qui permettrait de conclure en évaluant en $\frac{1}{a}$). Par contre on sait qu'il existe $Q \in \mathbf{Q}[X]$ tel que $P = Q(aX-1)$. Il s'agit pour conclure de montrer que $Q \in \mathbf{Z}[X]$. C'est immédiat en utilisant la notion de contenu du chapitre 5. On a $c(aX-1) = \mathrm{pgcd}(a,1) = 1$ et par ailleurs $c(P) = c(Q)c(aX-1)$ donc $c(Q) = c(P) \in \mathbf{Z}$ et finalement $Q \in \mathbf{Z}[X]$.

On peut aussi s'en tirer sans la notion de contenu (en particulier sans utiliser le fait que $\mathbf{Z}$ est factoriel) en écrivant $Q = \sum_{i=0}^{n} q_i X^i$ et en identifiant les coefficients dans l'égalité $P = Q(aX-1)$. On trouve de proche en proche que q_0, q_1,... q_n sont dans $\mathbf{Z}$.

Le premier résultat de la question 3 est faux si on remplace le corps $\mathbf{K}$ par un anneau intègre A quelconque, et l'énoncé de l'exercice lui-même fournit des contre-exemples. Considérons par exemple le quotient $\mathbf{Z}[X]/\langle 2X-1\rangle$. D'après la question 3, il est isomorphe à l'anneau A_2. D'après la question 5, il n'est pas isomorphe à $\mathbf{Z} = A_1$. Ou plus directement : si $\varphi\colon \mathbf{Z} \to A_2$ est un isomorphisme, c'est nécessairement l'unique morphisme de $\mathbf{Z}$ vers A_2. Mais ce dernier morphisme correspond à l'inclusion de $\mathbf{Z}$ dans A_2, et n'est donc pas surjectif, car $\frac{1}{2} \in A_2 \setminus \mathbf{Z}$.