Université de Poitiers, Année 2022-2023

3e année de Licence de Mathématiques, Anneaux

Corrigé de l'examen du mardi 2 mai 2023

Questions de cours (sur 5 points)

1. Donner la définition d'un anneau euclidien.

   Il fallait donner la définition 2.1 du chapitre "Anneaux de polynômes".

   Soit A un anneau intègre.

   - Un *stathme euclidien* est une application $\varphi : A^* \to \mathbb{N}$ qui vérifie les conditions :
     (1) pour tout couple d'éléments (a, b) de A avec b non nul, il existe des éléments q et r de A tels que $a = bq + r$ et soit $r = 0_A$, soit $\varphi(r) < \varphi(b)$;
     (2) pour tout couple d'éléments (a, b) de A^*, si b divise a, alors $\varphi(b) \leqslant \varphi(a)$.
   - Si un tel stathme euclidien existe, on dit que A est un *anneau euclidien.*

2. Démontrer que, dans un anneau euclidien, tous les éléments non nuls se décomposent en un produit d'un élément inversible par un produit d'éléments irréductibles.

   Il s'agissait de redonner la démonstration de la proposition 1.12 du chapitre "Arithmétique dans les anneaux".

   Soien A un anneau euclidien et φ un stathme euclidien sur A. Supposons que A ait un élément non nul qui ne se décompose pas en un produit d'un élément inversible par un produit d'éléments irréductibles. Alors il y a un plus petit $n \in \mathbb{N}$ tel qu'il existe $a \in A^*$ vérifiant $\varphi(a) = n$ et n'admettant aucune décomposition de la forme voulue. En particulier a n'est ni inversible, ni irréductible. Il se décompose donc en un produit $a = uv$ de deux éléments non inversibles u et v, qui sont non nuls puisque $a \neq 0_A$. La division euclidienne de u par a fournit $(q, r) \in A^2$ tel que $u = aq + r$ et soit $r = 0_A$, soit $\varphi(r) < \varphi(a)$. Or u divise a, donc il divise $r = u - aq$ et on a $\varphi(u) \leqslant \varphi(r)$, d'où $\varphi(u) < \varphi(a)$. De même on obtient $\varphi(v) < \varphi(a)$. Par minimalité de $\varphi(a)$, on en déduit que u et v ont une décomposition de la forme voulue, donc c'est aussi le cas de a, ce qui contredit notre hypothèse.

3. Soit A un anneau factoriel. Démontrer que tout produit de deux polynômes primitifs de $A[X]$ est un polynôme primitif.

   Il fallait réécrire la démonstration de la proposition 5.3 du chapitre "Arithmétique dans les anneaux".

   Soient $P = \sum_{i=0}^{m} a_i X^i$ et $Q = \sum_{i=0}^{n} b_i X^i$ deux polynômes primitifs dans $A[X]$. Soit p un élément irréductible de A. Comme P et Q sont primitifs, ils ne sont pas nuls et on peut supposer $m = \deg P$ et $n = \deg Q$. Aussi p ne peut pas diviser tous les coefficients $a_0, \ldots, a_m$, ni tous les coefficients $b_0, \ldots, b_n$. Il existe donc un plus petit entier entier $r \in \{0, \ldots, m\}$ et un plus petit entier $s \in \{0, \ldots, n\}$ tels que p ne divise pas a_r ni b_s.

Comme p est irréductible, p ne divise pas le produit $a_r b_s$. Or le coeffcient du terme de degré $r+s$ de PQ est

$$c_{r+s} = \sum_{\substack{i+j=r+s \\ 0\leqslant i\leqslant m, 0\leqslant j\leqslant n}} a_i b_j = \sum_{\substack{i=0 \\ 0\leqslant r+s-i\leqslant n}}^{r-1} a_i b_{r+s-i} + a_r b_s + \sum_{\substack{i=r+1 \\ 0\leqslant r+s-i\leqslant n}}^{m} a_i b_{r+s-i},$$

et p divise la première somme par minimalité de r, ainsi que la seconde somme par minimalité de s (car on a $r+s-i<s$ lorsque $i>r$). On en déduit que p ne divise pas c_{r+s}. Ceci démontre qu'aucun élément irréductible de A ne divise tous les coefficients de PQ, donc tout $PGCD$ de PQ est inversible et PQ est primitif.

Exercices

Exercice 1 (extrait du DM, sur 2 points)
Soit A un anneau commutatif. Pour tout idéal I de A, on définit

$$\sqrt{I} = \{x \in A \mid \exists n \in \mathbb{N},\ x^n \in I\}.$$

1. Démontrer que $\sqrt{I}$ est un idéal de A contenant I.

   Tout $x \in I$ vérifie $x^n = x \in I$ pour $n=1$, et appartient donc $\sqrt{I}$. On en déduit que $\sqrt{I}$ contient I.

   En particulier $\sqrt{I}$ est non vide. Aussi, pour tous x et y dans $\sqrt{I}$, il existe m et n dans $\mathbb{N}$ tels que $x^m \in I$ et $y^n \in I$. La formule du binôme donne

   $$(x+y)^{m+n} = \sum_{k=0}^{n} \binom{m+n}{k} x^k y^{m+n-k}.$$

   Or pour tout $k \in \{0,\dots,m\}$, on a $m-k \geqslant 0$ et y^{m-k} est donc défini. Comme I est un idéal de A, on obtient $\binom{m+n}{k} x^k y^{m+n-k} = y^n \left(\binom{m+n}{k} x^k y^{m-k}\right) \in I$. De même, pour tout $k \in \{m,\dots,m+n\}$, on a $k-m \geqslant 0$ et x^{k-m} est donc défini, et comme I est un idéal de A, on obtient $\binom{m+n}{k} x^k y^{m+n-k} = x^m \left(\binom{m+n}{k} x^{k-m} y^{m+n-k}\right) \in I$. Ainsi $(x+y)^{m+n}$ est une somme d'éléments de I et appartient donc à I, on en déduit que $x+y$ appartient à $\sqrt{I}$.

   Enfin, pour tout $x \in \sqrt{I}$, il existe $m \in \mathbb{N}$ tel que $x^m \in I$, donc on a $(-x)^m = (-1)^m x^m \in I$ et $-x \in I$. Ceci démontre que $\sqrt{I}$ est un sous-groupe de $(A,+)$.

   Pour tout $(a,x) \in A \times \sqrt{I}$, il existe $n \in \mathbb{N}$ tel que $x^n \in I$, et on a donc $(ax)^n = a^n x^n \in I$ car I est un idéal et $x^n \in I$. On en déduit que $ax \in \sqrt{I}$ et que I est un idéal de A.

2. Prouver que $\sqrt{\sqrt{I}} = \sqrt{I}$.

   D'après la question précédente on a $\sqrt{I} \subseteq \sqrt{\sqrt{I}}$.

   Aussi, pour tout $x \in \sqrt{\sqrt{I}}$, il existe $m \in \mathbb{N}$ tel que $x^m \in \sqrt{I}$ et il existe $n \in \mathbb{N}$ tel que $(x^m)^n \in I$. On a donc $x^{mn} \in I$ et $x \in \sqrt{I}$, d'où $\sqrt{\sqrt{I}} \subseteq \sqrt{I}$. On a donc bien $\sqrt{\sqrt{I}} = \sqrt{I}$.

Exercice 2 (extrait du TD, sur 4 points)
Voir la correction faite en TD : il s'agit de questions issues de l'exercice 10 de la fiche "Anneaux, morphismes" et de l'exercice 5 de la fiche "Anneaux euclidiens, principaux, factoriels".

Exercice 3 (sur 9 points)
Dans cet exercice, on identifie $\mathbb{Z}$ et l'ensemble des polynômes constants de $\mathbb{Z}[X]$: l'ensemble $\mathbb{Z}$ est donc un sous-anneau de $\mathbb{Z}[X]$.
Le but de cet exercice est de montrer que les idéaux premiers de $\mathbb{Z}[X]$ sont ceux de l'une des formes suivantes :

- $J = \{0\}$ *;*
- $J = p\mathbb{Z}[X]$ *pour un nombre premier p ;*
- $J = (P)$ *pour un polynôme primitif $P \in \mathbb{Z}[X]$ irréductible dans $\mathbb{Q}[X]$;*
- $J = (p, P)$ *pour un nombre premier p et $P \in \mathbb{Z}[X]$ irréductible dans $\mathbb{F}_p[X]$.*

1. (a) Soit A un anneau commutatif. À quelle condition $A[X]$ est-il un anneau intègre ?
   Il a été vu en cours que $A[X]$ est un anneau intègre si et seulement si A est intègre.
   (b) En déduire que $J = \{0\}$ est un idéal premier de $\mathbb{Z}[X]$.
   Comme $\mathbb{Z}$ est un anneau intègre, alors $\mathbb{Z}[X]/\{0\} \simeq \mathbb{Z}[X]$ est un anneau intègre, et $J = \{0\}$ est donc un idéal premier de $\mathbb{Z}[X]$.

2. (a) Soit $P \in \mathbb{Z}[X]$ un polynôme primitif. S'il est irréductible dans $\mathbb{Q}[X]$, pourquoi est-il un élément premier de $\mathbb{Z}[X]$?
   Comme $\mathbb{Q}$ est un corps, l'anneau $\mathbb{Q}[X]$ est euclidien (exemple 2.4 du chapitre "Anneaux de polynômes"), principal (théorème 2.7 du chapitre "Anneaux de polynômes") et à PGCD (exemple 3.3 du chapitre "Arithmétique dans les anneaux"). Ses éléments irréductibles sont donc premiers (proposition 3.8 du chapitre "Arithmétique dans les anneaux"), et P est donc premier dans $\mathbb{Q}[X]$. Or $\mathbb{Q}$ est le corps des fractions de l'anneau factoriel $\mathbb{Z}$ et $P \in \mathbb{Z}[X]$ est primitif, donc P est premier dans $\mathbb{Z}[X]$ (lemme 5.12 du chapitre "Arithmétique dans les anneaux").
   (b) En déduire que, si $J = (P)$ pour un polynôme primitif $P \in \mathbb{Z}[X]$ irréductible dans $\mathbb{Q}[X]$, alors J est un idéal premier de $\mathbb{Z}[X]$.
   D'après la question précédente, l'élément P est premier dans $\mathbb{Z}[X]$, donc l'idéal $J = (P)$ est premier (proposition 3.9 du chapitre "Anneaux intègres").

3. (a) Soient B un sous-anneau d'un anneau commutatif A, et I un idéal premier de A. Montrer que $I \cap B$ est un idéal premier de B.
   Comme B est un sous-anneau de A et I un idéal de A, ce sont des sous-groupes de $(A, +)$ et $I \cap B$ est donc aussi un sous-groupe de $(A, +)$. Aussi, pour tout $(x, a) \in (I \cap B) \times B$, on a $xa \in B$ puisque B est un sous-anneau de A, et de plus, comme $(x, a) \in I \times A$, on a $xa \in I$, donc xa appartient à $I \cap B$ et $I \cap B$ est un idéal de B. Montrons que $I \cap B$ est un idéal premier. Soit ab un produit de deux éléments a et b de B tel que $ab \in I \cap B$. Comme I est premier dans A et $ab \in I$, on a soit $a \in I$, soit $b \in I$. Ainsi on a $a \in I \cap B$ ou $b \in I \cap B$, et $I \cap B$ est donc un idéal premier.

(b) En déduire que, si J est un idéal premier de $\mathbb{Z}[X]$, on a soit $J \cap \mathbb{Z} = \{0\}$, soit $J \cap \mathbb{Z} = p\mathbb{Z}$ pour un nombre premier p.

Comme $\mathbb{Z}$ est un sous-anneau de $\mathbb{Z}[X]$, la question précédente dit que $J \cap \mathbb{Z}$ est un idéal premier de $\mathbb{Z}$. On a donc soit $J \cap \mathbb{Z} = \{0\}$, soit $J \cap \mathbb{Z} = p\mathbb{Z}$ pour un nombre premier p.

4. On fixe un idéal premier J non nul de $\mathbb{Z}[X]$ tel que $J \cap \mathbb{Z} = \{0\}$. On note d le plus petit entier pour lequel J possède un polynôme de degré d.

(a) Montrer qu'il y a un polynôme primitif P de degré d qui appartient à J.

Soit $U \in J$ un polynôme de degré d. Soit c un contenu de U, c'est-à-dire un PGCD des coefficients de U. Alors il existe un polynôme primitif P tel que $U = cP$ (lemme 5.4 du chapitre "Arithmétique dans les anneaux"). Comme U est non nul puisque son degré est $d \neq -\infty$, on a $c \neq 0$, et donc $c \notin J$ puisque $J \cap \mathbb{Z} = \{0\}$. Or J est un idéal premier et on a $cP = U \in J$, donc P appartient à J. De plus, comme $\mathbb{Z}$ est un anneau intègre, on a $d = \deg U = \deg c + \deg P = \deg P$, d'où le résultat.

(b) Démontrer que P est irréductible dans $\mathbb{Q}[X]$.

Supposons $P = UV$ pour deux polynômes U et V de $\mathbb{Q}[X]$. Soient $C(U)$ et $C(V)$ des contenus de U et V et soient U^* et V^* des polynômes primitifs tels que $U = C(U)U^*$ et $V = C(V)V^*$. D'après le lemme de Gauss (lemme 5.8 du chapitre "Arithmétique dans les anneaux"), l'élément $C(U)C(V)$ est un contenu de P, et comme P est primitif, on a $C(U)C(V) = \pm 1 \notin J$. Comme J est un idéal premier et comme $(C(U)C(V))U^*V^* = P \in J$, on en déduit qu'on a soit $U^* \in J$, soit $V^* \in J$.

Supposons $U^* \in J$. Comme $\mathbb{Z}$ est intègre, on a $\deg U^* + \deg V^* = \deg P = d$ et, par minimalité de d, on a $\deg U^* = d$ et $\deg V^* = 0$. Ainsi V^* est un polynôme constant, et comme il est primitif, on a $V^* = \pm 1$ et V^* est inversible dans $\mathbb{Z}[X]$. De même, si $V^* \in J$, alors U^* est inversible dans $\mathbb{Z}[X]$, donc P est irréductible dans $\mathbb{Q}[X]$.

(c) Soit $A \in J$. Pourquoi existe-t-il des polynômes Q et R dans $\mathbb{Q}[X]$ tels que $A = QP + R$ et $\deg R < d$?

Comme $\mathbb{Q}$ est un corps et P est non nul, le coefficient dominant de P est inversible dans $\mathbb{Q}$ et le théorème de la division euclidienne donne l'existence d'un unique couple (Q, R) de polynômes sur $\mathbb{Q}$ tel que $A = QP + R$ et $\deg R < d$.

(d) Démontrer que $R = 0$.

Comme A et P appartiennent à J, on a $R = A - QP \in J$, et la minimalité de d interdit à $\deg R$ d'être un entier, donc on a $\deg R = -\infty$ et $R = 0$.

(e) En déduire que $J = (P)$.

La question précédente montre que tout $A \in J$ est divisible par P, donc on a $J \subseteq (P)$. Or on a $P \in J$, donc $J = (P)$.

5. On fixe un idéal J de $\mathbb{Z}[X]$ tel que $J \cap \mathbb{Z} = p\mathbb{Z}$ pour un nombre premier p. On note $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$ et $\overline{a} = a + (p)$ la classe modulo (p) de tout $a \in \mathbb{Z}$. On considère le morphisme d'anneaux surjectif $\varphi : \mathbb{Z}[X] \to \mathbb{F}_p[X]$ qui, à tout polynôme $\sum_{k=0}^{m} a_k X^k \in \mathbb{Z}[X]$ associe le polynôme $\sum_{k=0}^{m} \overline{a_k} X^k \in \mathbb{F}_p[X]$.

   (a) Quel est le noyau de φ ? Pourquoi est-il contenu dans J ?

   Soit $P = \sum_{k=0}^{m} a_k X^k \in \mathbb{Z}[X]$. On a $P \in \operatorname{Ker}\varphi$ si et seulement si $\varphi(P) = 0_{\mathbb{F}_p[X]}$, ce qui équivaut à dire que $\sum_{k=0}^{m} \overline{a_k} X^k = 0_{\mathbb{F}_p[X]}$, ou encore que $\overline{a_k} = 0_{\mathbb{F}_p}$ pour tout $k \in \{0, \dots, m\}$. Ceci revient à dire que p divise a_k pour tout $k \in \{0, \dots, m\}$, donc que p divise P. On en déduit que $\operatorname{Ker}\varphi = p\mathbb{Z}[X]$.

   Comme J est un idéal de $\mathbb{Z}[X]$ contenant $p \in p\mathbb{Z} = J \cap \mathbb{Z}$, alors J contient $p\mathbb{Z}[X] = \operatorname{Ker}\varphi$.

   (b) En déduire que $p\mathbb{Z}[X]$ est un idéal premier de $\mathbb{Z}[X]$.

   Comme φ est un morphisme d'anneaux surjectif, on a $\mathbb{Z}[X]/p\mathbb{Z}[X] \simeq \mathbb{F}_p[X]$ d'après le théorème d'isomorphisme. Or $\mathbb{F}_p$ est un corps puisque p est un nombre premier, donc $\mathbb{F}_p[X]$ et $\mathbb{Z}[X]/p\mathbb{Z}[X]$ sont des anneaux intègres et $p\mathbb{Z}[X]$ est donc un idéal premier de $\mathbb{Z}[X]$.

   (c) Montrer qu'il existe $P \in \mathbb{Z}[X]$ tel que $J = (p, P)$.

   [*Indication : justifier d'abord l'existence de $P \in \mathbb{Z}[X]$ tel que $\varphi(J) = (\varphi(P))$.*]

   Comme $\mathbb{F}_p$ est un corps, l'anneau $\mathbb{F}_p[X]$ est principal, et l'idéal $\varphi(J)$ est donc principal. Ainsi il existe $\overline{P} \in \mathbb{F}_p[X]$ tel que $\varphi(J) = (\overline{P})$. On choisit $P \in J$ tel que $\varphi(P) = \overline{P}$. En particulier, on a $(p, P) \subseteq J$. Aussi, pour tout $Q \in J$, on a $\varphi(Q) \in (\overline{P})$, donc $\varphi(Q) = \overline{PU}$ pour $\overline{U} \in \mathbb{F}_p[X]$. Soit $U \in \mathbb{Z}[X]$ tel que $\varphi(U) = \overline{U}$. Alors on a $\varphi(Q) = \varphi(P)\varphi(U) = \varphi(PU)$ donc $Q - PU \in \operatorname{Ker}\varphi$ et il existe $V \in p\mathbb{Z}[X]$ tel que $Q = PU + pV$. On a donc $Q \in (p, P)$ et $J = (p, P)$.

   (d) On suppose $J \neq p\mathbb{Z}[X]$ et on fixe $P \in \mathbb{Z}[X]$ tel que, $J = (p, P)$. Montrer que J est premier si et seulement si $\varphi(P)$ est irréductible dans $\mathbb{F}_p[X]$.

   L'idéal J est premier si et seulement si $\mathbb{Z}[X]/J$ est intègre. Or J contient $p\mathbb{Z}[X]$, donc $\mathbb{Z}[X]/J$ est isomorphe à $(\mathbb{Z}[X]/p\mathbb{Z}[X])/(J/p\mathbb{Z}[X])$ (corollaire 6.19 du chapitre "Anneaux : généralités"). On considère la surjection canonique $\pi : \mathbb{F}_p[X] \to \mathbb{F}_p[X]/(\varphi(P))$. Alors $\pi \circ \varphi$ est un morphisme d'anneaux surjectif dont le noyau est $\varphi^{-1}((\varphi(P))) = (p, P) = J$. On en déduit que $\mathbb{Z}[X]/J$ est isomorphe à $\mathbb{F}_p[X]/(\varphi(P))$ et que J est premier si et seulement si $(\varphi(P))$ est un idéal premier de $\mathbb{F}_p[X]$. Or ceci est le cas si et seulement si $\varphi(P)$ est irréductible dans $\mathbb{F}_p[X]$, d'où le résultat.