Université de Poitiers, Année 2022-2023

3$^{\text{e}}$ année de Licence de Mathématiques, Anneaux

Corrigé du Contrôle continu du mercredi 22 février 2023

Questions de cours (5 points)

1. Donner la définition de la caractéristique d'un anneau.

   Il fallait donner la Définition 7.1 du chapitre "Anneaux : généralités".

   La *caractéristique* d'un anneau $(A, +, \times)$ est 0 si $n1_A \neq 0_A$ pour tout $n \in \mathbb{N}^*$, sinon c'est le plus petit entier $n \in \mathbb{N}^*$ tel que $n1_A = 0_A$. On la note $\mathrm{char}(A)$.

2. Soient A un anneau et $f : \mathbb{Z} \to A$ l'application définie pour tout $x \in \mathbb{Z}$ par $f(x) = x1_A$. Démontrer que f est un morphisme d'anneaux. Quel est son noyau ?

   Il s'agissait de retrouver la démonstration de la Proposition 7.5 du chapitre "Anneaux : généralités". Le noyau de ce morphisme est obtenu par le Lemme 7.8 du même chapitre.

   L'application f satisfait :

   - $f(1) = 1 \cdot 1_A = 1_A$;
   - pour tout $(a, b) \in \mathbb{Z}^2$, $f(a + b) = (a + b)1_A = a1_A + b1_A = f(a) + f(b)$;
   - pour tout $(a, b) \in \mathbb{Z}^2$, $f(ab) = (ab)1_A = a(b1_A) = a(1_A \cdot b1_A) = a1_A \cdot b1_A = f(a)f(b)$.

   Ainsi f est bien un morphisme d'anneaux. D'après le cours, son noyau est $\mathrm{Ker}\, f = char(A)\mathbb{Z}$.

3. Donner la définition d'un élément premier d'un anneau commutatif.

   Il fallait de donner la Définition 3.7 du chapitre "Anneaux intègres".

   Soient $(A, +, \times)$ un anneau commutatif et x un élément de A. On dit que x est *premier* si x est non nul et non inversible et si, lorsque x divise un produit ab d'éléments a et b de A, l'un des facteurs a ou b est divisible par x.

4. Démontrer qu'un élément non nul x d'un anneau commutatif A est premier si et seulement si l'idéal (x) est premier.

   Il fallait retrouver la démonstration de la Proposition 3.9 du chapitre "Anneaux intègres". Cette démonstration utilise le Lemme 3.5 du même chapitre qui dit que $(x) = xA$.

   Si x est premier, alors x n'est pas inversible donc on a $1_A \notin xA = (x)$ et $(x) \neq A$. Si un produit ab d'éléments a et b de A appartient à $(x) = xA$, alors ab est un multiple de x et l'élément x divise le produit ab. Or x est un élément premier de A, donc a ou b est divisible par x, autrement dit a ou b appartient à $xA = (x)$, ce qui signifie que l'idéal (x) est premier.

   Réciproquement, si (x) est un idéal premier, alors on a $(x) \neq A$, donc 1_A n'appartient pas à $(x) = xA$ et x n'est pas inversible. Soient a et b des éléments de A tels que x divise ab. Alors on a $ab \in xA = (x)$, et (x) étant premier, on a soit $a \in (x)$ soit $b \in (x)$. Ainsi, x divise a ou b et l'élément x est donc premier.

Exercices

Exercice 1 (5 points)

Voir la correction faite en TD : il s'agit d'une partie de l'exercice 2 de la fiche n°1.

Exercice 2 (5 points)

On considère les ensembles

$$A = \mathbb{Z}[\sqrt{2}] = \{a + b\sqrt{2}\ ;\ (a, b) \in \mathbb{Z}^2\} \quad \text{et} \quad \mathbb{Q}[\sqrt{2}] = \{a + b\sqrt{2}\ ;\ (a, b) \in \mathbb{Q}^2\}.$$

1. Justifier que tout élément de $\mathbb{Q}[\sqrt{2}]$ s'écrit d'une unique façon sous la forme $a+b\sqrt{2}$ pour $(a, b) \in \mathbb{Q}^2$.

   L'existence de l'écriture $a + b\sqrt{2}$ suit de la définition de $\mathbb{Q}[\sqrt{2}]$. Pour montrer l'unicité, on suppose que $a + b\sqrt{2} = c + d\sqrt{2}$ pour $(a, b, c, d) \in \mathbb{Q}^4$. Si on avait $b \neq d$, on aurait $\sqrt{2} = \frac{c-a}{b-d} \in \mathbb{Q}$, ce qui est incompatible avec l'irrationnalité de $\sqrt{2}$. On a donc $b = d$, or ceci implique $a = c$, d'où l'unicité de l'écriture.

2. Montrer que A est un sous-anneau de $\mathbb{R}$. En déduire que A est un anneau intègre.

   L'élément unité $1 = 1+0\sqrt{2}$ de $\mathbb{R}$ appartient à A. Aussi, pour tous éléments $x = a+b\sqrt{2}$ et $y = c + d\sqrt{2}$ de A avec $(a, b, c, d) \in \mathbb{Z}^4$, on a $x - y = (a - c) + (b - d)\sqrt{2} \in A$ et $xy = (ac + 2bd) + (ad + bc)\sqrt{2} \in A$, donc A est un sous-anneau de $\mathbb{R}$.

   En particulier A est un anneau, et cet anneau est intègre puisque c'est un sous-anneau d'un anneau intègre (l'anneau $\mathbb{R}$ est intègre car c'est un corps).

3. Montrer que 7 n'est pas un élément premier de A.

   [*Indication :* $-14 = (2 + 3\sqrt{2})(2 - 3\sqrt{2})$.]

   Notons d'abord que $7 = 7 + 0\sqrt{2}$ appartient à A et que c'est un élément non nul de A. De plus 7 n'est pas inversible puisque son inverse dans $\mathbb{R}$ est $\frac{1}{7} \notin A$. Enfin, on remarque que $(2 + 3\sqrt{2})(2 - 3\sqrt{2}) = 2^2 - (3\sqrt{2})^2 = -14$ et que 7 divise -14. Pourtant 7 ne divise pas $2 + 3\sqrt{2}$ dans A puisque l'équation $2 + 3\sqrt{2} = 7x$ a une unique solution $x = \frac{2}{7} + \frac{3}{7}\sqrt{2}$ dans $\mathbb{R}$ et elle n'appartient pas à A. Pour la même raison 7 ne divise pas $2 - 3\sqrt{2}$, ce qui démontre que 7 n'est pas un élément premier de A.

4. Montrer que $\mathbb{Q}[\sqrt{2}]$ est un corps.

   L'élément unité $1 = 1 + 0\sqrt{2}$ de $\mathbb{R}$ appartient à $\mathbb{Q}[\sqrt{2}]$. Aussi, pour tous éléments $x = a+b\sqrt{2}$ et $y = c+d\sqrt{2}$ de $\mathbb{Q}[\sqrt{2}]$ avec $(a, b, c, d) \in \mathbb{Q}^4$, on a $x-y = (a-c)+(b-d)\sqrt{2} \in \mathbb{Q}[\sqrt{2}]$ et $xy = (ac + 2bd) + (ad + bc)\sqrt{2} \in \mathbb{Q}[\sqrt{2}]$, donc $\mathbb{Q}[\sqrt{2}]$ est un sous-anneau de $\mathbb{R}$, et c'est en particulier un anneau.

   De plus, si $x = a + b\sqrt{2}$ est un élément non nul de $\mathbb{Q}[\sqrt{2}]$ avec $(a, b) \in \mathbb{Q}^2$, alors il a un unique inverse dans $\mathbb{R}$ et celui-ci est

   $$\frac{1}{x} = \frac{1}{a + b\sqrt{2}} = \frac{a - b\sqrt{2}}{(a + b\sqrt{2})(a - b\sqrt{2})} = \frac{a - b\sqrt{2}}{a^2 - 2b^2} = \frac{a}{a^2 - 2b^2} + \frac{-b}{a^2 - 2b^2}\sqrt{2} \in \mathbb{Q}[\sqrt{2}].$$

   On en déduit que tous les éléments non nuls de $\mathbb{Q}[\sqrt{2}]$ sont inversibles dans $\mathbb{Q}[\sqrt{2}]$, donc $\mathbb{Q}[\sqrt{2}]$ est un corps.

5. Justifier que $\mathbb{Q}[\sqrt{2}]$ est isomorphe au corps des fractions de A.

   Soit K_A le corps des fractions de A. Comme $\mathbb{Q}[\sqrt{2}]$ est un corps contenant A, il y a un sous-corps L de $\mathbb{Q}[\sqrt{2}]$ contenant A et isomorphe à K_A.

Soit $x = a + b\sqrt{2} \in \mathbb{Q}[\sqrt{2}]$ avec $a = \frac{p}{q}$ et $b = \frac{r}{s}$ pour $(p,q) \in \mathbb{Z} \times \mathbb{Z}^*$ et $(r,s) \in \mathbb{Z} \times \mathbb{Z}^*$. Alors on a $x = \frac{1}{qs}(ps + rq\sqrt{2})$. Comme $qs \in \mathbb{Z}^*$ est un élément non nul de $A \subseteq L$, et que L est un corps, son inverse $\frac{1}{qs}$ appartient à L. Comme $ps + rq\sqrt{2}$ appartient à $A \subseteq L$, l'élément $x = \frac{1}{qs}(ps + rq\sqrt{2})$ est un produit d'éléments de L, il appartient donc aussi à L. Ceci démontre que L contient $\mathbb{Q}[\sqrt{2}]$.

Comme L est un sous-corps de $\mathbb{Q}[\sqrt{2}]$, on obtient $\mathbb{Q}[\sqrt{2}] = L$ et $\mathbb{Q}[\sqrt{2}]$ est isomorphe au corps des fractions de A.

Exercice 3 (5 points)
Soit $A = \mathbb{R}^{\mathbb{N}}$ l'anneau des suites de nombres réels où la somme et le produit de toutes suites $(x_i)_{i\in\mathbb{N}}$ et $(y_i)_{i\in\mathbb{N}}$ sont définis par :

$$(x_i)_{i\in\mathbb{N}} + (y_i)_{i\in\mathbb{N}} = (x_i + y_i)_{i\in\mathbb{N}} \quad \text{et} \quad (x_i)_{i\in\mathbb{N}} \times (y_i)_{i\in\mathbb{N}} = (x_i y_i)_{i\in\mathbb{N}}.$$

1. Prouver que, pour tout $k \in \mathbb{N}$, l'ensemble $\mathfrak{M}_k = \{(x_i)_{i\in\mathbb{N}} \in A \mid x_k = 0\}$ est un idéal de A, puis qu'il s'agit d'un idéal *maximal* de A (⚠ *la maximalité est difficile à démontrer*).

   Soit $k \in \mathbb{N}$. Comme la suite nulle appartient à $\mathfrak{M}_k$, l'ensemble $\mathfrak{M}_k$ n'est pas vide. Aussi, si $(x_i)_{i\in\mathbb{N}}$ et $(y_i)_{i\in\mathbb{N}}$ sont deux suites appartenant à $\mathfrak{M}_k$, alors on a $x_k = y_k = 0$, donc on a $x_k - y_k = 0$ et $(x_i)_{i\in\mathbb{N}} - (y_i)_{i\in\mathbb{N}} = (x_i - y_i)_{i\in\mathbb{N}}$ appartient à $\mathfrak{M}_k$. Par conséquent $\mathfrak{M}_k$ est un sous-groupe de $(A,+)$. De plus, si $(x_i)_{i\in\mathbb{N}}$ est une suite appartenant à $\mathfrak{M}_k$ et $(y_i)_{i\in\mathbb{N}}$ une suite appartenant à A, alors on a $x_k = 0$ et $x_k y_k = 0$, donc la suite $(x_i)_{i\in\mathbb{N}}(y_i)_{i\in\mathbb{N}} = (x_i y_i)_{i\in\mathbb{N}}$ appartient à $\mathfrak{M}_k$. Ainsi $\mathfrak{M}_k$ est un idéal de A.

   Comme $\mathfrak{M}_k$ ne contient pas la suite constante 1_A ayant tous ses termes égaux à 1, c'est un idéal propre de A. Considérons un idéal I de A contenant strictement $\mathfrak{M}_k$. Soit $(x_i)_{i\in\mathbb{N}}$ un élément de I n'appartenant pas à $\mathfrak{M}_k$. Alors on a $x_k \neq 0$. Soit $(y_i)_{i\in\mathbb{N}}$ la suite de A définie par $y_k = x_k^{-1}$ et $y_i = 0$ pour $i \neq k$. Alors le produit $(z_i)_{i\in\mathbb{N}} = (x_i)_{i\in\mathbb{N}}(y_i)_{i\in\mathbb{N}}$ appartient à I puisque I est un idéal de A, et cette suite $(z_i)_{i\in\mathbb{N}}$ satisfait $z_k = x_k y_k = 1$ et $z_i = x_i y_i = 0$ pour $i \neq k$. De plus, la suite $(u_i)_{i\in\mathbb{N}}$ satisfaisant $u_k = 0$ et $u_i = 1$ pour $i \neq k$ appartient à $\mathfrak{M}_k \subseteq I$, donc la suite $1_A = (z_i)_{i\in\mathbb{N}} + (u_i)_{i\in\mathbb{N}}$ appartient à I puisque I est un idéal de A. Comme 1_A est l'élément neutre de A pour la multiplication, on en déduit que $I = A$, ce qui montre que l'idéal $\mathfrak{M}_k$ est maximal dans A.

2. Soit I l'ensemble des suites n'ayant qu'un nombre fini de termes non nuls. *On admet que I est un idéal de A.* Pourquoi l'idéal I n'est-il pas premier ?

   Soient $(x_i)_{i\in\mathbb{N}}$ et $(y_i)_{i\in\mathbb{N}}$ les éléments de A définis par $x_i = 1$ et $y_i = 0$ si i est pair et par $x_i = 0$ et $y_i = 1$ si i est impair. Ces deux suites ont un nombre infini de termes non nuls, elles n'appartiennent donc pas à I. Pourtant leur produit est la suite nulle (on a $x_i y_i = 0$ pour tout $i \in \mathbb{N}$), donc on a $(x_i)_{i\in\mathbb{N}}(y_i)_{i\in\mathbb{N}} \in I$, ce qui démontre que l'idéal I n'est pas premier.

3. Montrer qu'il existe un idéal maximal de A qui n'est pas de la forme $\mathfrak{M}_k$ pour $k \in \mathbb{N}$.

   Mis à part la suite nulle, aucune suite constante n'appartient à l'idéal I ci-dessus, donc I est un idéal propre de A. D'après le théorème de Krull, l'idéal I est contenu dans un idéal maximal M de A. Pour tout $k \in \mathbb{N}$, on note $s_k = (x_i)_{i\in\mathbb{N}}$ la suite définie par $x_k = 1$ et $x_i = 0$ pour $i \neq k$. On a donc $s_k \in I \subseteq M$ pour tout $k \in \mathbb{N}$. Or, pour tout $k \in \mathbb{N}$, on a $s_k \notin \mathfrak{M}_k$ et donc $M \neq \mathfrak{M}_k$. On en déduit que M est un idéal maximal de A qui n'est pas de la forme $\mathfrak{M}_k$ pour $k \in \mathbb{N}$.