Université de Rennes 1
Licence de mathématiques
Module Anneaux et Arithmétique

Année universitaire 2018-2019

Exemples de rédactions de solutions de certains exercices de la feuille 1

- *Exercice 1.1, feuille 1*

  Montrons que $(A^E, +)$ est un groupe commutatif. Montrons tout d'abord que $+$ est associative, c'est-à-dire montrons

  $$\forall (f,g,h) \in (A^E)^3,\ (f+g)+h = f+(g+h).$$

  Soit $(f,g,h) \in (A^E)^3$. Il s'agit de montrer

  $$\forall x \in E,\ ((f+g)+h)(x) = (f+(g+h))(x).$$

  Soit $x \in E$. Par définition de la loi $+$ sur A^E, on a

  $$((f+g)+h)(x) = (f+g)(x)+h(x) = (f(x)+g(x))+h(x)$$

  et

  $$(f+(g+h))(x) = f(x)+(g+h)(x) = f(x)+(g(x)+h(x)).$$

  Par associativité de la loi $+$ sur A, on a

  $$(f(x)+g(x))+h(x) = f(x)+(g(x)+h(x)).$$

  On a donc bien démontré

  $$\forall x \in E,\ ((f+g)+h)(x) = (f+(g+h))(x).$$

  On a donc bien démontré

  $$\forall (f,g,h) \in (A^E)^3,\ (f+g)+h = f+(g+h).$$

  Montrons que $+$ est commutative, c'est-à-dire montrons

  $$\forall (f,g) \in (A^E)^2,\ f+g = g+f.$$

  Soit $(f,g) \in (A^E)^2$. Il s'agit de montrer

  $$\forall x \in E,\ (f+g)(x) = (g+f)(x).$$

  Soit $x \in E$. Par définition de la loi $+$ sur A^E, on a

  $$(f+g)(x) = f(x)+g(x)$$

  et

  $$(g+f)(x) = g(x)+f(x).$$

  Par commutativité de la loi $+$ sur A, on a

  $$f(x)+g(x) = g(x)+f(x).$$

On a donc bien démontré

$$\forall x \in E,\ (f+g)(x) = (g+f)(x).$$

On a donc bien démontré

$$\forall (f,g) \in (A^E)^2,\ f+g = g+f.$$

Montrons que la loi $+$ sur A^E a un élément neutre. Soit f_0 la fonction constante sur E égale à 0_A. Montrons

$$\forall f \in A^E,\ f + f_0 = f.$$

Soit $f \in A^E$. Il s'agit de montrer

$$\forall x \in E,\ (f+f_0)(x) = f(x).$$

Soit $x \in E$. Par définitions de la loi $+$ sur A^E et de f_0, on a

$$(f+f_0)(x) = f(x) + 0_A$$

d'où, comme 0_A est l'élément neutre de la loi $+$ sur A,

$$(f+f_0)(x) = f(x).$$

On a donc bien démontré

$$\forall x \in E,\ (f+f_0)(x) = f(x).$$

On a donc bien démontré

$$\forall f \in A^E,\ f + f_0 = f.$$

Ainsi f_0 est un élément neutre pour la loi $+$ sur A^E
Montrons que tout élément de A^E admet un symétrique pour la loi $+$. Soit $f \in A^E$. Soit $g \in A^E$ l'application définie par

$$\forall x \in E, g(x) = -f(x).$$

Montrons que $f+g = g+f = f_0$. Comme la loi $+$ sur A^E est commutative, il suffit de montrer que $f+g = f_0$. Il s'agit de montrer

$$\forall x \in E, (f+g)(x) = f_0(x).$$

Soit $x \in E$. Par définitions de la loi $+$ sur A^E et de g, on a

$$(f+g)(x) = f(x) + g(x) = f(x) + (-f(x)).$$

Ainsi $(f+g)(x) = 0_A$, soit $(f+g)(x) = f_0(x)$ par définition de f_0. On a donc bien démontré

$$\forall x \in E, (f+g)(x) = f_0(x).$$

On a donc bien démontré que $f+g = f_0$. Ainsi f admet un symétrique pour la loi $+$ sur A^E. On a donc bien démontré que tout élément de A^E admettait un symétrique pour la loi $+$ sur A^E.
Par des méthodes strictement similaires, on démontre que la loi $\times$ sur A^E est associative, commutative, admet un élément neutre (qui est la fonction constante sur E égale à 1_A) et est distributive par rapport à la loi $+$ sur A^E.

- *Exercice 1.4, feuille 1*
Notons $\mathcal{B}$ l'ensemble des applications constantes de E vers A.
Montrons que $\mathcal{B}$ est un sous-groupe de $(A^E,+)$.
Soit $f,g\in\mathcal{B}$. Montrons que $f+g\in\mathcal{B}$. Par définition de $\mathcal{B}$, il existe $a\in A$ tel que

$$\forall x\in E,\ f(x)=a$$

et il existe $b\in A$ tel que

$$\forall x\in E,\ g(x)=b.$$

Soit $x\in E$. On a

$$(f+g)(x)=f(x)+g(x)=a+b.$$

Ainsi

$$\forall x\in E,\ (f+g)(x)=a+b$$

ce qui montre bien que $f+g\in\mathcal{B}$.
Soit $f\in\mathcal{B}$. Montrons que $-f\in\mathcal{B}$. Par définition de $\mathcal{B}$, il existe $a\in A$ tel que

$$\forall x\in E,\ f(x)=a.$$

Soit $x\in E$. Alors $(-f)(x)$ est l'opposé de $f(x)$ pour la loi $+$ sur A (*cf.* question 1 de l'exercice). Donc $-f(x)=-a$. Ainsi

$$\forall x\in E,\ (-f)(x)=a+b$$

ce qui montre bien que $-f\in\mathcal{B}$.
Enfin, l'élément neutre de la loi $+$ sur A^E, qui est la fonction constante sur E égale à 0_A, est bien un élément de $\mathcal{B}$. Ceci achève de montrer que $\mathcal{B}$ est un sous groupe de $(A^E,+)$.
Par une méthode strictement similaire, on montre que $\mathcal{B}$ est stable par la loi $\times$ sur A^E. Par ailleurs $\mathcal{B}$ contient l'élément neutre pour la loi $\times$ sur A^E ; en effet ce n'est autre que la fonction constante égale à 1_A sur E.
Ceci achève de montrer que $\mathcal{B}$ est un sous-anneau de A^E.
Pour montrer que $\mathcal{B}$ est isomorphe à A, on considère l'application

$$\varphi\colon\ \begin{array}{ccc} A & \longrightarrow & \mathcal{B} \\ a & \longmapsto & \varphi(a)\colon x\mapsto a \end{array}$$

Cette application est clairement bien définie. Montrons que c'est un morphisme d'anneaux.
En notant f_1 la fonction constante sur E égale à 1_A, il s'agit de montrer

$$\forall (a,b)\in A^2,\ \varphi(a+b)=\varphi(a)+\varphi(b)$$

$$\forall (a,b)\in A^2,\ \varphi(a\times b)=\varphi(a)\times\varphi(b)$$

$$\text{et}\varphi(1_A)=f_1.$$

La dernière propriété découle aussitôt des définitions de φ et de f_1. Montrons la deuxième propriété, la première se montre par une méthode similaire.
Soit $(a,b)\in A^2$. La fonction $\varphi(a\times b)$ est la fonction définie par

$$\forall x\in E,\ \varphi(a\times b)(x)=a\times b.$$

Soit $x\in E$. Par défintions de $\varphi(a)$, $\varphi(b)$ et de la loi $\times$ sur A^E, on a

$$(\varphi(a)\times\varphi(b))(x)=(\varphi(a)(x))\times(\varphi(b)(x))=a\times b.$$

On a donc démontré

$$\forall x \in E, \, \varphi(a \times b)(x) = (\varphi(a) \times \varphi(b))(x).$$

On a donc démontré $\varphi(a \times b) = \varphi(a) \times \varphi(b)$. On a donc démontré

$$\forall (a,b) \in A^2, \, \varphi(a \times b) = \varphi(a) \times \varphi(b).$$

Il reste à montrer que φ est un isomorphisme d'anneaux. En fait ceci ne vaut que si E est non vide (hypothèse oubliée dans l'énoncé). Il suffit d'après le cours de montrer que φ est bijective. Montrons que φ est injective. Soit $a, b \in A$ tel que $\varphi(a) = \varphi(b)$. Montrons que $a = b$. Soit $x \in E$ (E est un ensemble non vide). On a

$$a = \varphi(a)(x) = \varphi(b)(x) = b.$$

Donc φ est injective.
Montrons que φ est surjective. Soit $f \in \mathcal{B}$. Par définition de $\mathcal{B}$, il existe $a \in A$ tel que

$$\forall x \in E, \quad f(x) = a.$$

Pour un tel a, on a bien $\varphi(a) = f$. Donc φ est surjective.
Finalement φ est un morphisme d'anneaux bijectif de A vers $\mathcal{B}$, donc un isomorphisme d'anneaux de A sur $\mathcal{B}$.

- *Exercice 4.4, feuille 1*
  Montrons tout d'abord

$$\forall (a_1, a_2) \in A^2, \, (\psi \circ \varphi)(a_1 + a_2) = (\psi \circ \varphi)(a_1) + (\psi \circ \varphi)(a_2).$$

Soit $(a_1, a_1) \in A^2$. On a

$$(\psi \circ \varphi)(a_1 + a_2) = \psi(\varphi(a_1 + a_2))$$

Comme φ est un morphisme d'anneaux, on a

$$\varphi(a_1 + a_2) = \varphi(a_1) + \varphi(a_2).$$

Comme ψ est un morphisme d'anneaux, on a

$$\psi(\varphi(a_1 + a_2)) = \psi(\varphi(a_1)) + \psi(\varphi(a_2)).$$

Finalement on a

$$(\psi \circ \varphi)(a_1 + a_2) = \psi(\varphi(a_1)) + \psi(\varphi(a_2)) = (\psi \circ \varphi)(a_1) + (\psi \circ \varphi)(a_2).$$

On a bien montré

$$\forall (a_1, a_2) \in A^2, \, (\psi \circ \varphi)(a_1 + a_2) = (\psi \circ \varphi)(a_1) + (\psi \circ \varphi)(a_2).$$

Par une méthode strictement similaire, on montre

$$\forall (a_1, a_2) \in A^2, \, (\psi \circ \varphi)(a_1 \times a_2) = (\psi \circ \varphi)(a_1) \times (\psi \circ \varphi)(a_2).$$

Enfin, comme φ et ψ sont des morphismes d'anneaux, on a

$$(\psi \circ \varphi)(1_A) = \psi(\varphi(1_A)) = \psi(1_B) = 1_C.$$

Ainsi $\psi \circ \varphi$ est bien un morphisme d'anneaux.

- *Exercice 4.9, feuille 1*
  Montrons que $\varphi^{-1}(\mathcal{I})$ est un sous-groupe de A.
  Soit $x, y \in \varphi^{-1}(\mathcal{J})$. Montrons que $x+y \in \varphi^{-1}(\mathcal{J})$. Il s'agit de montrer que $\varphi(x+y) \in \mathcal{J}$. Or, comme φ est un morphisme d'anneaux, on a $\varphi(x+y) = \varphi(x)+\varphi(y)$. Par ailleurs, comme x et y sont dans $\varphi^{-1}(\mathcal{J})$, $\varphi(x)$ et $\varphi(y)$ sont dans $\mathcal{J}$. Comme $\mathcal{J}$ est un idéal de B, on a donc $\varphi(x)+\varphi(y) \in \mathcal{J}$, d'où $\varphi(x+y) \in \mathcal{J}$. Ainsi, on a démontré
  $$\forall (x,y) \in \varphi^{-1}(\mathcal{J})^2,\ x+y \in \varphi^{-1}(\mathcal{J}).$$
  Soit $x \in \varphi^{-1}(\mathcal{J})$. Montrons que $-x \in \varphi^{-1}(\mathcal{J})$. Il s'agit de montrer que $\varphi(-x) \in \mathcal{J}$. Or, comme φ est un morphisme d'anneaux, on a $\varphi(-x) = -\varphi(x)$. Par ailleurs, comme x est dans $\varphi^{-1}(\mathcal{J})$, $\varphi(x)$ est dans $\mathcal{J}$. Comme $\mathcal{J}$ est un idéal de B, on a donc $-\varphi(x) \in \mathcal{J}$, d'où $\varphi(-x) \in \mathcal{J}$. Ainsi, on a démontré
  $$\forall x \in \varphi^{-1}(\mathcal{J}),\ -x \in \varphi^{-1}(\mathcal{J}).$$
  Comme φ est un morphisme d'anneaux, on a $\varphi(0_A) = O_B$. Comme $\mathcal{J}$ est un idéal de B, on a $0_B \in \mathcal{J}$. Donc $0_A \in \varphi^{-1}(\mathcal{J})$.
  Ainsi, $\varphi^{-1}(\mathcal{I})$ est un sous-groupe de A.
  Soit $x \in \varphi^{-1}(\mathcal{J})$ et $y \in A$. Montrons que $xy \in \varphi^{-1}(\mathcal{J})$. Il s'agit de montrer que $\varphi(xy) \in \mathcal{J}$. Or, comme φ est un morphisme d'anneaux, on a $\varphi(xy) = \varphi(x)\varphi(y)$. Par ailleurs, comme x est dans $\varphi^{-1}(\mathcal{J})$, $\varphi(x)$ est dans $\mathcal{J}$. Comme $\mathcal{J}$ est un idéal de B, on a donc $\varphi(x)\varphi(y) \in \mathcal{J}$, d'où $\varphi(xy) \in \mathcal{J}$. Ainsi, on a démontré
  $$\forall (x,y) \in \varphi^{-1}(\mathcal{J}) \times A,\ xy \in \varphi^{-1}(\mathcal{J}).$$
  Ceci achève de montrer que $\varphi^{-1}(\mathcal{J})$ est un idéal de A.
  Montrons que $\varphi^{-1}(\mathcal{J})$ contient $\mathrm{Ker}(\varphi)$. Comme $\mathcal{J}$ est un idéal de B, $\mathcal{J}$ contient $\{0_B\}$. Donc $\varphi^{-1}(\mathcal{J})$ contient $\varphi^{-1}(\{0_B\}) = \mathrm{Ker}(\varphi)$.
- *Exercice 7.3.a, feuille 1*
  Montrons que $\mathbf{Z}_{(p)}$ est un sous-anneau de $\mathbf{Q}$. On montre seulement ici que $\mathbf{Z}_{(p)}$ est stable par addition. Le reste de la démonstration utilise des méthodes et raisonnements similaires.
  Soit $x, y \in \mathbf{Z}_{(p)}$. Par définition, il existe $a, b, c, d \in \mathbf{Z}$ tels que p ne divise ni b ni d et $x = \frac{a}{b}$, $y = \frac{c}{d}$. On a
  $$x+y = \frac{a}{b} + \frac{c}{d} = \frac{ad+bc}{bd}$$
  Évidemment, $ad+bc \in \mathbf{Z}$ et $bd \in \mathbf{Z}$. Par ailleurs, comme p ne divise ni b ni d, p ne divise par bd (lemme d'Euclide). Ceci montre bien que $x+y \in \mathbf{Z}_{(p)}$.
  Comme $\mathbf{Z}_{(p)}$ est un sous-anneau de $\mathbf{Q}$ et que $\mathbf{Q}$ est un anneau intègre, $\mathbf{Z}_{(p)}$ est un anneau intègre.
  Comme p ne divise pas 1 et que tout élément a de $\mathbf{Z}$ s'écrit $\frac{a}{1}$, on voit que $\mathbf{Z}_{(p)}$ contient $\mathbf{Z}$.
- *Exercice 7.3.b, feuille 1* On va montrer que
  $$\mathbf{Z}_{(p)}^{\times} = \left\{\frac{a}{b}\right\}_{a,\, b \in \mathbf{Z} \setminus p\mathbf{Z}}.$$
  Soit a, b des entiers non divisibles par p. Alors par défintion de $\mathbf{Z}_{(p)}$ on a $\frac{a}{b} \in \mathbf{Z}_{(p)}$ et $\frac{b}{a} \in \mathbf{Z}_{(p)}$. Comme $\frac{a}{b} \times \frac{b}{a} = 1$, ceci montre que $\frac{a}{b} \in \mathbf{Z}_{(p)}^{\times}$. Ceci montre l'inclusion
  $$\left\{\frac{a}{b}\right\}_{a,\, b \in \mathbf{Z} \setminus p\mathbf{Z}} \subset \mathbf{Z}_{(p)}^{\times}.$$

Soit à présent $x \in \mathbf{Z}_{(p)}^{\times}$. Il existe donc $y \in \mathbf{Z}_{(p)}$ tel que $xy = 1$. Soit $a, b, c, d \in \mathbf{Z}$ tels que p ne divise ni b ni d et $x = \frac{a}{b}$, $y = \frac{c}{d}$. Comme $xy = 1$, on a $ac = bd$. Comme p ne divise ni b ni d, p ne divise pas bd (lemme d'Euclide). Donc p ne divise pas a. Ceci montre l'inclusion

$$\mathbf{Z}_{(p)}^{\times} \subset \left\{ \frac{a}{b} \right\}_{a,\, b \in \mathbf{Z} \setminus p\mathbf{Z}}.$$

On a donc bien démontré

$$\mathbf{Z}_{(p)}^{\times} = \left\{ \frac{a}{b} \right\}_{a,\, b \in \mathbf{Z} \setminus p\mathbf{Z}}.$$

- *Exercice 10.2, feuille 1*
  Si $n = 0$, on a $\mathbf{Z}/n\mathbf{Z} = \mathbf{Z}$. Comme $\mathbf{Z}$ est intègre, la question 1 de l'exercice montre que l'ensemble des nilpotents de $\mathbf{Z}$ est réduit à $\{0\}$.
  Si $n = 1$, $\mathbf{Z}/n\mathbf{Z}$ est l'anneau nul. Son unique élément est clairement nilpotent.
  On suppose désormais $n \geqslant 2$. Soit n_0 le produit de tous les facteurs premiers de n. Ainsi si $n = 6$, $n_0 = 6$ et si $n = 20$, $n_0 = 10$.
  Soit $a \in \mathbf{Z}$. Montrons que $[a]_n$ est nilpotent si et seulement si n_0 divise a.
  Supposons $[a]$ nilpotent. Soit m un entier strictement positif tel que $[a]_n^m = [0]_n$. Comme $[a]_n^m = [a^m]_n$, on en déduit que n divise a^m. Par le lemme d'Euclide, tout facteur premier de n divise a. Donc n_0 divise a.
  Supposons que n_0 divise a. Soit m le plus grand exposant des facteurs premiers de n dans la décomposition de n en facteurs premiers. En particulier n divise n_0^m. Mais par ailleurs, comme n_0 divise a, n_0^m divise a^m, donc n divise a^m. Donc $[a]_n^m = [0]_n$.
  Finalement l'ensemble des éléments nilpotents de $\mathbf{Z}/n\mathbf{Z}$ est l'idéal de $\mathbf{Z}/n\mathbf{Z}$ engendré par $[n_0]_n$. Ceci montre au passage qu'il y a $\frac{n}{n_0}$ éléments nilpotents dans $\mathbf{Z}/n\mathbf{Z}$. En particulier $\mathbf{Z}/n\mathbf{Z}$ est réduit si et seulement si $n = n_0$ si et seulement si n est sans facteur carré.