Année universitaire 2013-2014 Licence 3 de mathématiques

Algèbre 4 - Devoir surveillé

Corrections

Tous les anneaux considérés ci-dessous sont commutatifs. Si a et b sont des éléments d'un anneau A, on note $\langle a, b\rangle$ l'idéal engendré par a et b.

Questions de cours

1. Soient A un anneau, $a, b \in A$. Rappeler la définition de $\mathrm{pgcd}(a, b)$.
   On dit que $d = \mathrm{pgcd}(a, b)$ si $d \mid a$, $d \mid b$ et pour tout d' vérifiant $d' \mid a$, $d' \mid b$ on a $d' \mid d$.

   Dans la suite on suppose que **l'anneau A est principal.**
2. Montrer l'existence de $\mathrm{pgcd}(a, b)$ pour tout $a, b \in A$. Montrer aussi que $\mathrm{pgcd}(a, b)$ peut s'écrire sous la forme $au + bv$, où $u, v \in A$.
   Puisque A est anneau principal, on a $\langle a, b\rangle = \langle d\rangle$ pour un certain $d \in A$. Une vérification immédiate montre que $d = \mathrm{pgcd}(a, b)$. Puisque $d \in \langle a, b\rangle$, on a $d = au + bv$ avec certains $u, v \in A$.
3. Démontrer le "théorème de Gauss" : si $a, b, c \in A$ vérifient
   $$a \mid bc, \qquad \mathrm{pgcd}(a, b) = 1,$$
   alors $a \mid c$.
   L'hypothèse $\mathrm{pgcd}(a, b) = 1$ implique $1 = au + bv$ avec certains $u, v \in A$, d'où $c = acu + bcv$. L'hypothèse $a \mid bc$ implique que $a \mid (acu + bcv)$, d'où le résultat.
4. Soit $\mathbb{F}_3$ le corps à 3 éléments. L'anneau $\mathbb{F}_3[t]$ est-il principal ?
   Oui : l'anneau de polynômes sur un corps est euclidien, donc principal.
5. Pour $f(t) = t^2 + t + 1 \in \mathbb{F}_3[t]$ et $g(t) = t^3 + t + 1 \in \mathbb{F}_3[t]$ déterminer $\mathrm{pgcd}\big(f(t), g(t)\big)$ et l'exprimer sous la forme $f(t)u(t) + g(t)v(t)$ avec $u(t), v(t) \in \mathbb{F}_3[t]$.
   En utilisant la division euclidienne on trouve
   $$\mathrm{pgcd}\big(f(t), g(t)\big) = t - 1 = f(t) - (t - 1)g(t).$$

Exercice 1 Soit n un entier naturel, $n \geq 2$, et soient $K_1, \ldots, K_n$ des corps. On considère l'anneau $A = K_1 \times \ldots \times K_n$.

1. L'anneau A est-il intègre ?
   Non : $(1, 0, 0, \ldots, 0) \cdot (0, 1, 0, \ldots, 0) = (0, 0, \ldots, 0) = 0_A$.
2. Soit S un sous-ensemble de $\{1, \ldots, n\}$. On pose
   $$I_S = \{(a_1, \ldots, a_n) \in A : a_i = 0 \text{ pour } i \in S\}.$$
   Montrer que I_S est un idéal de A.
   Supposons que $\mathbf{a} = (a_1, \ldots, a_n)$ et $\mathbf{b} = (b_1, \ldots, b_n)$ appartiennent à I_S, ce qui signifie que
   $$a_i = b_i = 0 \qquad (i \in S).$$
   Ceci implique que
   $$a_i - b_i = 0 \qquad (i \in S),$$
   ce qui montre que $\mathbf{a} - \mathbf{b} = (a_1 - b_1, \ldots, a_n - b_n) \in I_S$.
   De même, si $\mathbf{c} = (c_1, \ldots, c_n) \in A$, alors
   $$a_i c_i = 0 \qquad (i \in S),$$
   ce qui montre que $\mathbf{ac} \in I_S$. L'ensemble I_S est donc idéal.

3. Soit I un idéal de A. Est-il vrai que $I = I_S$ pour un certain $S \subset \{1, \dots, n\}$?
Oui : montrons que $I = I_S$ où

$$S = \{i \in \{1, \dots, n\} : a_i = 0 \text{ pour tout } (a_1, \dots, a_n) \in I\}.$$

Il est claire que $I \subset I_S$. Pour montrer que $I_S \subset I$, posons

$$e_i = (0, \dots, 0, \underset{i}{1}, 0 \dots 0)$$

(1 sur la i-ième position, et 0 sur les autres positions) et montrons tout d'abord que $e_i \in I$ pour tout $i \notin S$. Pour le voir, remarquons que, si $i \notin S$ alors il existe $\mathbf{a} = (a_1, \dots, a_n) \in I$ avec $a_i \neq 0$. Posons

$$\mathbf{b} = (0, \dots, 0, \underset{i}{a_i^{-1}}, 0 \dots 0) \in I$$

Alors $e_i = \mathbf{ab} \in I$.
Puis, tout $\mathbf{a} \in A$ s'exprime comme

$$\mathbf{a} = \sum_{1 \leq i \leq n} \mathbf{a} e_i.$$

Si $\mathbf{a} \in I_S$ alors $\mathbf{a} e_i = 0_A$ pour $i \in S$ et on obtient

$$\mathbf{a} = \sum_{i \notin S} \mathbf{a} e_i \in I,$$

ce qui montre que $I_S \subset I$.

4. L'anneau A n'admet-il qu'un nombre fini d'idéaux ? Si la réponse est « oui », déterminer ce nombre.

Par la question précédente tout idéal de A est de la forme I_S, et il est clair que $I_S \neq I_{S'}$ pour $S \neq S'$. Ceci montre que les idéaux de A sont en bijection avec les sous-ensembles de $\{1, \dots, n\}$. Puisque le nombre de ces derniers est 2^n, l'anneau A admet exactement 2^n idéaux.

5. Est-il vrai que tout idéal de A est principal ?
Oui : montrons que l'idéal I_S est engendré par $\varepsilon_S = (\varepsilon_1, \dots, \varepsilon_n)$, où $\varepsilon_i = 0$ pour $i \in S$ et $\varepsilon_i = 1$ pour $i \notin S$. Il est clair que $\varepsilon_S \in I_S$, ce qui montre que $\langle \varepsilon_S \rangle \subset I_S$. D'autre part, $\varepsilon_S = \sum_{i \notin S} e_i$, et, comme on a vu tout à l'heure, tout $\mathbf{a} \in I_S$ vérifie

$$\mathbf{a} = \sum_{i \notin S} \mathbf{a} e_i = \mathbf{a} \varepsilon_S \in \langle \varepsilon_S \rangle,$$

ce qui montre que $I_S \subset \langle \varepsilon_S \rangle$.

Exercice 2 On considère l'ensemble $\mathbb{Z}[\sqrt{2}]$ des nombres réels de la forme $x + y\sqrt{2}$ avec $x, y \in \mathbb{Z}$:

$$\mathbb{Z}[\sqrt{2}] = \{x + y\sqrt{2} : x, y \in \mathbb{Z}\}.$$

1. Montrer que $\mathbb{Z}[\sqrt{2}]$ (muni des lois habituelles) est un anneau.
Il faut montrer que pour $z_1, z_2 \in \mathbb{Z}[\sqrt{2}]$ on a $z_1 - z_2, z_1 z_2 \in \mathbb{Z}[\sqrt{2}]$. En écrivant $z_i = x_i + y_i\sqrt{2}$ avec $x_i, y_i \in \mathbb{Z}$, on obtient

$$z_1 - z_2 = (x_1 - y_1) + (x_2 - y_2)\sqrt{2} \in \mathbb{Z}[\sqrt{2}], \qquad z_1 z_2 = (x_1 x_2 + 2y_1 y_2) + (x_1 y_2 + y_1 x_1)\sqrt{2} \in \mathbb{Z}[\sqrt{2}].$$

2. Montrer que tout $z \in \mathbb{Z}[\sqrt{2}]$ s'écrit de façon unique sous la forme $x + y\sqrt{2}$ avec $x, y \in \mathbb{Z}$.
Supposons que $z = x_1 + y_1\sqrt{2} = x_2 + y_2\sqrt{2}$ avec $x_i, y_i \in \mathbb{Z}$ et montrons que $x_1 = x_2$ et $y_1 = y_2$. Si $y_1 \neq y_2$ alors $\sqrt{2} = \frac{x_1 - x_2}{y_2 - y_1} \in \mathbb{Q}$, ce qui n'est pas possible. On a donc $y_1 = y_2$ et $x_1 = z - y_1\sqrt{2} = z - y_2\sqrt{2} = x_2$.
3. Pour $z = x + y\sqrt{2} \in \mathbb{Z}[\sqrt{2}]$ on définit *le conjugué* de z par $\bar{z} = x - y\sqrt{2}$. (Attention : ce n'est pas la conjugaison complexe !)
   (a) Montrer que $z \mapsto \bar{z}$ définit un automorphisme de l'anneau $\mathbb{Z}[\sqrt{2}]$.
   L'application $z \mapsto \bar{z}$ est sa propre réciproque : $\bar{\bar{z}} = z$. In particulier, elle est inversible, donc bijective.
   Une vérification immédiate montre que $\overline{z_1 + z_2} = \bar{z}_1 + \bar{z}_2$ et $\overline{z_1 z_2} = \bar{z}_1 \bar{z}_2$; autrement dit, l'application $z \mapsto \bar{z}$ est morphisme d'anneaux. Comme elle est bijective, c'est un automorphisme.

(b) Montrer que $z\bar{z} \in \mathbb{Z}$ pour tout $z \in \mathbb{Z}[\sqrt{2}]$.
Pour $z = x + y\sqrt{2}$ on a $z\bar{z} = x^2 - 2y^2 \in \mathbb{Z}$.

(c) Montrer que $z \in \mathbb{Z}[\sqrt{2}]^\times$ si et seulement si $z\bar{z} \in \{1, -1\}$.
Si $z\bar{z} = \varepsilon \in \{1, -1\}$ alors $z^{-1} = \varepsilon\bar{z}$, d'où z est inversible.
Réciproquement, si z est inversible alors $(z\bar{z}) \cdot (z^{-1}\overline{z^{-1}}) = (zz^{-1}) \cdot \overline{(zz^{-1})} = 1\bar{1} = 1$. Ceci montre que $z\bar{z} \mid 1$, autrement dit $z\bar{z} \in \{1, -1\}$.

(d) Vérifier que $1 + \sqrt{2} \in \mathbb{Z}[\sqrt{2}]^\times$. Le groupe $\mathbb{Z}[\sqrt{2}]^\times$ est-il fini ou infini ?
On a $(1 + \sqrt{2})^{-1} = -1 + \sqrt{2} \in \mathbb{Z}[\sqrt{2}]$, ce qui montre que $1 + \sqrt{2} \in \mathbb{Z}[\sqrt{2}]^\times$. Le groupe $\mathbb{Z}[\sqrt{2}]^\times$ est infini, parce qu'il contient l'ensemble infini $\{(1 + \sqrt{2})^n : n \in \mathbb{Z}\}$.

4. On va montrer que le groupe multiplicatif $\mathbb{Z}[\sqrt{2}]^\times$ est engendré par $\theta = 1 + \sqrt{2}$ et -1. Autrement dit,
$$\mathbb{Z}[\sqrt{2}]^\times = \{\pm\theta^m : m \in \mathbb{Z}\}. \tag{1}$$

(a) Montrer que pour $z = x + y\sqrt{2}$ on a
$$x = \frac{z + \bar{z}}{2}, \qquad y = \frac{z - \bar{z}}{2\sqrt{2}}. \tag{2}$$
C'est évident.

(b) Soit $z \in \mathbb{Z}[\sqrt{2}]^\times$ vérifiant $1 \le z < \theta$. Montrer que $z = 1$.
Puisque $z \ge 1$ et $|z\bar{z}| = 1$ (voir question 3c), on a $-1 \le \bar{z} \le 1$. En utilisant (2), on trouve
$$x = \frac{z + \bar{z}}{2} \ge \frac{1 - 1}{2} = 0, \qquad x = \frac{z + \bar{z}}{2} < \frac{\theta + 1}{2} < 1,8.$$
Puisque $x \in \mathbb{Z}$, ceci implique que $x \in \{0, 1\}$. De la même façon on montre que
$$0 \le y \le \frac{\theta + 1}{2\sqrt{2}} < 1,3,$$
d'où $y \in \{0, 1\}$. On trouve que $z \in \{0, 1, \sqrt{2}, 1 + \sqrt{2}\}$. Puisque z est inversible et vérifie $1 \le z < \theta$, la seule possibilité est $z = 1$.

(c) Soit $\eta \in \mathbb{Z}[\sqrt{2}]^\times$. Montrer que $|\eta| = \theta^m$ pour un certain $m \in \mathbb{Z}$.
Posons $m = \lfloor \frac{\ln|\eta|}{\ln\theta} \rfloor$. Alors $0 \le \frac{\ln|\eta|}{\ln\theta} - m < 1$, d'où $1 \le |\eta|\theta^{-m} < \theta$. Par la question précédente on a $|\eta|\theta^{-m} = 1$.

(d) Conclure.
On vient de montrer que tout $\eta \in \mathbb{Z}[\sqrt{2}]^\times$ vérifie $|\eta| = \theta^m$ pour un certain $m \in \mathbb{Z}$. Puisque $\eta \in \mathbb{R}$, ceci implique que $\eta = \pm\theta^m$, ce qui démontre (1).

Exercice 3

1. Soient p un nombre premier et $\mathbb{F}_p$ le corps à p éléments. Montrer que les anneaux $\mathbb{Z}[t]/\langle t^3 + 2t + p, t^2 + 2\rangle$ et $\mathbb{F}_p[t]/\langle t^2 + 2\rangle$ sont isomorphes.
On utilise la propriété générale suivante. Soient A un anneau, I et J des idéaux de A et $\bar{J}$ l'image de J dans A/I. Alors
$$A/(I + J) \cong (A/I)/\bar{J}. \tag{3}$$
(Pour la démontrer on considère les morphismes naturels $A \to A/I \to (A/I)/\bar{J}$ et on montre que le noyau du morphisme composé est $I + J$.)
Dans notre cas $A = \mathbb{Z}[t]$. Puisque $t^3 + 2t + p = p + t(t^2 + 2)$, on a
$$\langle t^3 + 2t + p, t^2 + 2\rangle = \langle p, t^2 + 2\rangle = I + J, \qquad I = \langle p\rangle, \quad J = \langle t^2 + 2\rangle,$$
et donc $A/I = \mathbb{F}_p[t]$ et $\bar{J} = \langle t^2 + 2\rangle$, ce qui achève le résultat.

2. Montrer que l'anneau $\mathbb{R}[t, u]/\langle t^3 + 2t + u, t^2 + 2\rangle$ est isomorphe à $\mathbb{C}$.
De même, $A = \mathbb{R}[t, u]$,
$$\langle t^3 + 2t + u, t^2 + 2\rangle = \langle u, t^2 + 2\rangle = I + J, \qquad I = \langle u\rangle, \quad J = \langle t^2 + 2\rangle,$$
et donc $A/I = \mathbb{R}[t]$ et $\bar{J} = \langle t^2 + 2\rangle$, ce qui démontre que
$$\mathbb{R}[t, u]/\langle t^3 + 2t + u, t^2 + 2\rangle \cong \mathbb{R}[t]/\langle t^2 + 2\rangle.$$
Puis, le morphisme $\mathbb{R}[t] \to \mathbb{C}$ défini par $t \mapsto \sqrt{-2}$ est surjectif et son noyau est $\langle t^2 + 2\rangle$, ce qui démontre que $\mathbb{R}[t]/\langle t^2 + 2\rangle \cong \mathbb{C}$.