Université Aix-Marseille	2018–2019

Licence – Mathématiques
Algèbre 2

Partiel
corrigé

Exercice 1. (6 points)

1. - Un nombre $n \in \mathbb{Z}$ est premier s'il possède exactement quatre diviseurs distincts.
   - La multiplication dans $\frac{\mathbb{Z}}{n\mathbb{Z}}$ est définie, pour tout $k_1, k_2 \in \mathbb{Z}$, par $\overline{k_1}.\overline{k_2} := \overline{k_1.k_2}$.
   - Soit G un groupe. L'ordre de $g \in G$ est défini comme le cardinal de l'ensemble $\{g^k \mid k \in \mathbb{Z}\}$. Cela correspond également à au minimum de l'ensemble $\{k \in \mathbb{N}^* \mid g^k = e\}$, avec la convention que le minimum sur l'ensemble vide vaut ∞.
2. Le lemme de Gauss dit que, pour tous $a, b \in \mathbb{Z}^*$ et $c \in \mathbb{Z}$, si a divise $b.c$ et si a et b sont premier entre eux, alors a divise c. Pour le démontrer, on écrit $b.c = k.a$ avec $k \in \mathbb{Z}$ et utilise le théorème de Bachet–Bézout pour trouver $r, s \in \mathbb{Z}$ tels que $1 = r.a + s.b$. On a alors $c = c.1 = c.(r.a + s.b) = c.r.a + s.b.c = c.r.a + s.k.a = (c.r + s.k).a$, impliquant que a divise c.

Exercice 2.

1. Pour tout $a \in \mathbb{R}^*$ et $b \in \mathbb{R}$, on note $f_{a,b}$ l'application $(x \mapsto a.x + b)$. On peut remarquer que tous les éléments de $\mathrm{Aff}(\mathbb{R})$ sont inversibles, l'inverse de $f_{a,b} \in \mathrm{Aff}(\mathbb{R})$ étant $f_{\frac{1}{A},-\frac{b}{a}}$. On a donc $\mathrm{Aff}(\mathbb{R}) \subset \mathrm{Bij}(\mathbb{R})$, et il suffit donc de montrer que $\mathrm{Aff}(\mathbb{R})$ est un sous-groupe. On vient de voir que $\mathrm{Aff}(\mathbb{R})$ est stable par inverse, il ne reste plus qu'à montrer qu'il est stable par composition. Or, par calcul direct, on a $f_{a_1,b_1} \circ f_{a_2,b_2} = f_{a_1.a_2, a_1.b_2+b_1} \in \mathrm{Aff}(\mathbb{R})$ pour tous $f_{a_1,b_1}, f_{a_2,b_2} \in \mathrm{Aff}(\mathbb{R})$.
2. D'après le calcul précédent, on a $f_{1,1} \circ f_{2,1} = f_{2,2}$ tandis que $f_{2,1} \circ f_{1,1} = f_{2,3}$. Le groupe $\mathrm{Aff}(\mathbb{R})$ n'est donc pas abélien.

Exercice 3.

1. (a) On a $2.x_0^2 + 5y_0^2 = 1000$ et donc $2.x_0^2 = 1000 - 5.y_0^2 = 5.(200 - y_0^2)$; on en déduit que 5 divise $2.x_0^2$. Mais 5 et 2 sont premiers entre eux (par exemple car $1.5 - 2.2 = 1$), donc d'après le lemme de Gauss, 5 divise x_0^2. Or 5 est premier, donc d'après le lemme d'Euclide, 5 divise x_0. Il existe donc $x_1 \in \mathbb{Z}$ tels que $x_0 = 5.x_1$.

   Par un raisonnement totalement similaire, on montre que 2 divise y_0 et qu'il existe donc $y_1 \in \mathbb{Z}$ tel que $y_0 = y_1$.

   On a alors $1000 = 2.x_0^2 + 5y_0^2 = 2.5^2.x_1^2 + 5.2^2.y_1^2$ et, en divisant par 10, $5.x_1^2 + 2.y_1^2 = 100$.

   (b) Par le même raisonnement, on montre que 5 divise y_1, donc qu'il existe $y_2 \in \mathbb{Z}$ tel que $y_1 = 5.y_2$; et que 2 divise x_1, donc qu'il existe $x_2 \in \mathbb{Z}$ tel que $x_1 = 1.x_2$. On en déduit que $5.2^2.x_2^2 + 2.5^2.y_2^2 = 100$ et donc que $2.x_2^2 + 5.y_2^2 = 10$.

   (c) Toujours par le même raisonnement, on montre que 5 divise x_2 et que 2 divise y_2, et donc qu'il existe $x_3, y_3 \in \mathbb{Z}$ tels que $5.x_3^2 + 2.y_3^2 = 1$.
2. En supposons par l'absurde que l'équation (1) admet une solution entière, la question précédente montre que l'équation $5.x^2 + 2.y^2 = 1$ admet une solution entière. Or cette dernière n'a pas de solution entière. Si $|x| \geq 1$ on a en effet que $5.x^2 + 2.y^2 \geq 5$ et donc $5.x^2 + 2.y^2 \neq 1$, et si $|y| \geq 1$, que $5.x^2 + 2.y^2 \geq 2$ et donc que $5.x^2 + 2.y^2 \neq 1$. La seule solution possible serait donc $(x, y) = (0, 0)$, mais cette dernière n'est pas solution. On en déduit donc que l'équation (1) n'a pas de solution entière.

Exercice 4. (8 points)

1. (a) Par divisions euclidiennes successives, on a $17 = 1.13 + 4$ et $13 = 3.4 + 1$. On en déduit que $1 = 1.13 - 3.4 = 1.13 - 3.(17 - 1.13) = 4.13 - 3.17$.

   (b) On pose $\alpha := 52 = 4.13$ et $\beta = -51 = -3.17$. On a alors

$$\left\{ \begin{array}{l} \alpha = 4.13 = 1 + 3.17 \equiv 1 \ [17] \\ \alpha = 4.13 \equiv 0 \ [13] \end{array} \right. \quad \text{et} \quad \left\{ \begin{array}{l} \beta = -3.17 \equiv 0 \ [17] \\ \beta = -3.17 = 1 - 4.13 \equiv 1 \ [13] \end{array} \right. .$$

2. Par hypothèse, 13 divise $n_2 - n_1$. Il existe donc $k_1 \in \mathbb{Z}$ tel que $n_2 - n_1 = 13.k_1$. Mais par hypothèse, 17 divise également $n_2 - n_1 = 13.k_1$. Or, par le théorème de Bachet–Bézout, la question 1.(a) montre que 13 et 17 sont premiers entre eux. D'après le lemme de Gauss, on en déduit donc que 17 divise k_1, c'est-à-dire qu'il existe $k_2 \in \mathbb{Z}$ tel que $k_1 = 17.k_2$. On a de fait $n_2 - n_1 = 17.13.k_2 = 221.k_2$, et 221 divise donc $n_2 - n_1$.
3. Notons N le nombre de pièces d'or. D'après l'énoncé, on a $N \equiv 3$ [17] et $N \equiv 12$ [13]. Or $3.\alpha + 12.\beta = -456$ vérifie les même congruences. On en déduit que $N \equiv -456$ [17] et $N \equiv -456$ [13] et donc, d'après la question 2, que 221 divise $N + 456$. Autrement dit, il existe $k \in \mathbb{Z}$ tel que $N = 221.k - 456$. Mais par ailleurs, N étant un nombre de pièces d'or, on a $N \geq 0$. On en déduit que, en pièces d'or, le gain minimum du cuistot est

$$\min \mathbb{N} \cap \{221.k - 456 \mid k \in \mathbb{Z}\} = \min\{221.k - 456 \mid k \in \mathbb{Z}, k \geq 3\} = 221.3 - 456 = 207.$$