Université de Lille

FACULTÉ DES SCIENCES ET TECHNOLOGIES
Département de Mathématiques

M22 : Mathématiques fondamentales 2 — L1 SESI 2019–2020

Corrigé du devoir surveillé n° 2 – Partie Algèbre

Exercice 1.

1. (a) On a
$$a\left(\frac{p}{q}\right)^2 + b\left(\frac{p}{q}\right) + c = 0, \quad \text{soit encore} \quad ap^2 + bpq + cq^2 = 0.$$
On en déduit que $cq^2 = -p(ap + bq)$, donc p divise cq^2, et comme p et q sont premiers entre eux, on obtient que p divise c par le lemme de Gauss.
De même, on a $ap^2 = -q(bp+cq)$, donc q divise ap^2, et comme p et q sont premiers entre eux, on obtient que q divise a par le lemme de Gauss.

   (b) Supposons par l'absurde que a, b et c sont impairs. En particulier, d'après la question précédente, on en déduit que p et q sont aussi impairs. Mais alors ap^2, bpq et cq^2 sont impairs, et la somme de trois nombres impairs est un nombre impair, ce qui contredit l'égalité $ap^2 + bpq + cq^2 = 0$ puisque 0 est pair.

2. (a) Comme les trois coefficients de l'équation sont impairs alors, d'après la question précédente, on en déduit que l'équation n'admet aucune solution rationnelle.

   (b) On raisonne par analyse–synthèse. Tout d'abord, d'après le (a) de la question 1, si $x = \frac{p}{q}$ avec $(p, q) \in \mathbb{Z} \times \mathbb{N}^*$ et $\mathrm{PGCD}(p, q) = 1$ est solution de $x^2 + bx + 1 = 0$, alors p et q divisent 1, et donc $q = 1$ car $q \in \mathbb{N}^*$ et $p = \pm 1$. Ainsi, on a $x \in \{-1, 1\}$. Si $x = 1$ alors on obtient $b = -2$, et si $x = -1$ alors on obtient $b = 2$.
   Réciproquement, l'équation $x^2 + bx + 1 = 0$ admet des solutions rationnelles dans les deux cas suivants :
   — si $b = -2$, alors $x^2 - 2x + 1 = (x - 1)^2 = 0$ admet pour unique solution $x = 1$,
   — si $b = 2$, alors $x^2 + 2x + 1 = (x + 1)^2 = 0$ admet pour unique solution $x = -1$.

   (c) — S'il existe $m \in \mathbb{N}$ tel que $n = m^2$, alors $\sqrt{n} = \sqrt{m^2} = m \in \mathbb{N} \subset \mathbb{Q}$.
   — Réciproquement, si on suppose que $\sqrt{n} \in \mathbb{Q}$, alors l'équation $x^2 - n = 0$ admet une solution rationnelle $x = \frac{p}{q}$ avec $(p, q) \in \mathbb{Z} \times \mathbb{N}^*$ et $\mathrm{PGCD}(p, q) = 1$. Mais alors, d'après le (a) de la question 1, q divise 1 et donc $q = 1$ puisque $q \in \mathbb{N}^*$. Ainsi, on a $n = x^2 = p^2 = m^2$ avec $m = |p| \in \mathbb{N}$ puisque $p \in \mathbb{Z}$.

   (d) Supposons par l'absurde qu'il existe un nombre premier p tel que $\sqrt{p} \in \mathbb{Q}$. Alors, d'après la question précédente, il existe $m \in \mathbb{N}$ tel que $p = m^2$. Comme $p \geq 2$, alors cela impose $m \geq 2$, ce qui contredit la primalité de p.

Exercice 2.

1. Montrons que $(G, \star)$ est un groupe :
   - Pour tous $x, y \in G$, on a $x \star y = x \cdot a \cdot y \in G$, car $a \in G$ et l'opération $\cdot$ est interne à G puisque $(G, \cdot)$ est un groupe. Ainsi, l'opération $\star$ est bien interne à G.
   - Pour tous $x, y, z \in G$, par associativité de la loi $\cdot$ sur G, on a
   $$(x \star y) \star z = (x \cdot a \cdot y) \star z = (x \cdot a \cdot y) \cdot a \cdot z = x \cdot a \cdot y \cdot a \cdot z,$$
   $$x \star (y \star z) = x \star (y \cdot a \cdot z) = x \cdot a \cdot (y \cdot a \cdot z) = x \cdot a \cdot y \cdot a \cdot z.$$
   On a ainsi $(x \star y) \star z = x \star (y \star z)$, et donc l'opération $\star$ est bien associative.
   - Déterminons l'élément neutre e' pour l'opération $\star$. Pour tout $x \in G$, on a
   $$x \star e' = x \iff x \cdot a \cdot e' = x \iff a \cdot e' = e \iff e' = a^{-1} \in G.$$
   On a bien également $e' \star x = a^{-1} \star x = a^{-1} \cdot a \cdot x = x$.
   - Pour $x \in G$, déterminons l'inverse x' de x pour l'opération $\star$. On a
   $$x \star x' = e' \iff x \cdot a \cdot x' = a^{-1} \iff x' = a^{-1} \cdot x^{-1} \cdot a^{-1} \in G.$$
   On a bien également $x' \star x = (a^{-1} \cdot x^{-1} \cdot a^{-1}) \star x = (a^{-1} \cdot x^{-1} \cdot a^{-1}) \cdot a \cdot x = a^{-1} = e'$.

   Par conséquent, l'ensemble G muni de cette nouvelle opération $\star$ est bien un groupe. Son élément neutre est l'élément $e' = a^{-1}$, et tout $x \in G$ admet un symétrique x' défini par $x' = a^{-1} \cdot x^{-1} \cdot a^{-1}$.
2. (a) Pour tous $x, y \in G$, on a d'une part $f(x \cdot y) = x \cdot y \cdot a^{-1}$, et d'autre part
   $$f(x) \star f(y) = (x \cdot a^{-1}) \star (y \cdot a^{-1}) = x \cdot a^{-1} \cdot a \cdot y \cdot a^{-1} = x \cdot y \cdot a^{-1}.$$
   On a donc $f(x \cdot y) = f(x) \star f(y)$ pour tous $x, y \in G$, ce qui prouve que f est bien un morphisme du groupe $(G, \cdot)$ dans le groupe $(G, \star)$.

   (b) Ces deux propriétés sont des propriétés générales des morphismes de groupes. Vérifions-les dans ce cas particulier :
   - on a bien $f(e) = e \cdot a^{-1} = a^{-1} = e'$,
   - si $x \in G$, alors $f(x^{-1}) = x^{-1} \cdot a^{-1}$ et $(f(x))^{-1} = (x \cdot a^{-1})^{-1} = a \cdot x^{-1}$, et donc
   $$(f(x))' = a^{-1} \cdot (f(x))^{-1} \cdot a^{-1} = a^{-1} \cdot (a \cdot x^{-1}) \cdot a^{-1} = x^{-1} \cdot a^{-1} = f(x^{-1}).$$

   (c) Soient $x, y \in G$. On a
   $$y = f(x) \iff y = x \cdot a^{-1} \iff x = y \cdot a \iff x = g(y)$$
   en ayant défini l'application
   $$\begin{aligned} g : G &\longrightarrow G \\ y &\longmapsto y \cdot a. \end{aligned}$$
   Ainsi, g est l'application réciproque de l'application f, ce qui prouve en particulier que f est bijective.

   (d) C'est à nouveau une propriété générale des isomorphismes de groupes. Vérifions-la dans ce cas particulier : pour $x, y \in G$, on a
   $$g(x \star y) = g(x \cdot a \cdot y) = (x \cdot a \cdot y) \cdot a = (x \cdot a) \cdot (y \cdot a) = g(x) \cdot g(y).$$
   Ainsi, l'application g est bien un morphisme du groupe $(G, \star)$ dans le groupe $(G, \cdot)$.