Université Aix-Marseille 2021–2022

Licence – Mathématiques
Algèbre 2

Examen de seconde session
22 juin 2022

Il sera tenu compte de la présentation et de la clarté de la rédaction. Toute réponse devra être justifiée.
Les calculatrices, les téléphones portables et les documents sont strictement interdits.
Le barème n'est indiqué qu'à titre indicatif, et pourra être modifié.
L'épreuve dure deux heures.

Exercice 1. (5 points)

1. Sur l'ensemble $E = \{a, b, c\}$, on considère la loi de composition interne $\bullet$ définie par la table suivante :

$\bullet$	a	b	c
a	a	b	c
b	b	a	b
c	c	b	a

   (a) L'opération $\bullet$ admet-elle un élément neutre ?
   (b) Tout élément de E admet-il un inverse pour $\bullet$?
   (c) L'opération $\bullet$ est-elle commutative ?
   (d) L'opération $\bullet$ munit-elle E d'une structure de groupe ?
2. (a) Montrer que la relation de divisibilité est une relation d'ordre sur $\mathbb{N}^*$.
   (b) Soit G un groupe, H un sous-groupe de G, et N un sous-groupe distingué de G. Montrer que $H \cap N$ est un sous-groupe distingué de H.

Exercice 2. (4 points)

1. A l'aide de l'algorithme d'Euclide étendu, déterminer l'inverse de $\overline{127}$ dans $\mathbb{Z}/151\mathbb{Z}$.
2. Résoudre, dans $\mathbb{Z}/151\mathbb{Z}$, le système d'équations

$$\begin{cases} \overline{168}x + \overline{2}y + z = \overline{3} \\ \overline{110}x - \overline{2}y - z = \overline{1} \\ x - \overline{2}y = \overline{2} \end{cases}.$$

Exercice 3. (11 points)

1. (a) Rappeler le théorème de Lagrange et en déduire que, dans un groupe, l'ordre de tout élément divise l'ordre du groupe.
   (b) Soit p un nombre premier.
      i. On rappelle que, pour $k, n \in \mathbb{N}^*$, $\overline{k} \in \mathbb{Z}/n\mathbb{Z}$ est inversible si et seulement si k et n sont premiers entre eux. Montrer que $\left(\mathbb{Z}/p\mathbb{Z}\right)^\times$ est un groupe de cardinal $p-1$.
      ii. Montrer que, pour tout entier k premier avec p, on a $k^{p-1} \equiv 1 \mod p$.
2. On s'intèresse aux solutions dans $\mathbb{Z}$ de l'équation

$$y^2 = x^3 + 7. \tag{1}$$

   (a) Soit $(x_0, y_0) \in \mathbb{Z}^2$ une solution entière de l'équation (1).
      i. Montrer que 3 n'est pas un carré dans $\mathbb{Z}/4\mathbb{Z}$ et en déduire que x_0 n'est pas pair.

TSVP ⇒

ii. Montrer que $(x_0+2)\big((x_0-1)^2+3\big) = y_0^2+1$.

iii. Montrer que $(x_0-1)^2+3$ est congru à -1 modulo 4, et en déduire qu'au moins un des facteurs premier de $(x_0-1)^2+3$, que l'on notera p, est congru à -1 modulo 4.

iv. Montrer que $\frac{p-1}{2}$ est impair, et en déduire que $y_0^{p-1} \equiv -1 \mod p$.

(b) En déduire que l'équation (1) n'admet pas de solution dans $\mathbb{Z}$.