

Feuille d'exercices n° 3

3-1 – a) Rappeler la définition d'un nombre premier de \mathbb{Z} . Préciser les premiers termes de la suite croissante $(p_i)_{i \in \mathbb{N}^*}$ des nombres premiers > 0 . On rappelle que tout élément n de \mathbb{N}^* peut se décomposer de façon unique sous la forme $n = \prod_{i \geq 1} p_i^{a_i}$ où la suite $(a_i)_{i \in \mathbb{N}^*}$ est telle que les a_i de \mathbb{N} sont nuls sauf un nombre fini d'entre eux. Donner cette décomposition pour $n = 720$ et $n' = 300$.

b) Soit les éléments $n = \prod_{i \geq 1} p_i^{\alpha_i}$ et $n' = \prod_{i \geq 1} p_i^{\alpha'_i}$ de \mathbb{N} et leur décomposition en facteurs premiers. Rappeler les définitions de p.g.c.d (n, n') et de p.p.c.m (n, n') et donner leur décomposition en facteurs premiers. Retrouver la relation

$$\text{p.g.c.d}(n, n') \cdot \text{p.p.c.m}(n, n') = nn'.$$

3-2 – a) Soient $n \in \mathbb{N}^*$ et $H \neq \{\bar{0}\} \leq (\mathbb{Z}/n\mathbb{Z}, +)$. Soit α le plus petit entier > 0 tel que $\bar{\alpha} \in H$. Montrer que α divise n avec $n = k\alpha$ et que

$$H = \{\bar{0}, \bar{\alpha}, \bar{2\alpha}, \dots, \overline{(k-1)\alpha}\}.$$

b) Quels sont les sous-groupes de $(\mathbb{Z}/n\mathbb{Z}, +)$? Préciser le cas $n = 12$.

c) Soit $p \in \mathbb{Z}$ et $H_p = \{k\bar{p} = \underbrace{\bar{p} + \dots + \bar{p}}_{k \text{ fois}} \mid k \in \mathbb{N}\}$. Montrer que H_p est un sous-groupe de $(\mathbb{Z}/n\mathbb{Z}, +)$. Montrer que le plus petit entier $\alpha > 0$ tel que $\bar{\alpha} \in H_p$ est égal à p.g.c.d (p, n) . Préciser le cas particulier où $n = 12$ et $p = 8$ ou $p = 9$.

3-3 – On rappelle l'identité de Bezout : pour $a, b \in \mathbb{Z}^*$, a et b premiers entre eux, il existe $(u, v) \in \mathbb{Z} \times \mathbb{Z}$ tels que $au + bv = 1$.

a) En déduire que pour $a, b \in \mathbb{Z}^*$, il existe $(u, v) \in \mathbb{Z} \times \mathbb{Z}$ tels que $au + bv = \text{p.g.c.d}(|a|, |b|)$.

b) Déterminer le p.g.c.d d de 5940 et de 8712 à l'aide de l'algorithme d'Euclide puis par décomposition en facteurs premiers.

c) Trouver des entiers relatifs u_0 et v_0 tels que $d = 5940u_0 + 8712v_0$.

d) En déduire tous les couples (u, v) dans \mathbb{Z} tels que $d = 5940u + 8712v$.

3-4 – Vérifier que l'intersection de deux sous-groupes H_1 et H_2 d'un groupe G est un sous-groupe de G . Montrer qu'il en est de même de leur réunion si et seulement si on a $H_1 \subseteq H_2$ ou $H_2 \subseteq H_1$.

3-5 – On rappelle que les sous-groupes de $(\mathbb{Z}, +)$ sont de la forme $n\mathbb{N}$ ($n \in \mathbb{Z}$). Soient $a, b \in \mathbb{N}^*$. Que peut-on dire de $a\mathbb{Z} \cap b\mathbb{Z}$ et $a\mathbb{Z} + b\mathbb{Z}$?

3-6 – a) Soit E un ensemble de n éléments. Combien y-a-t-il de lois de composition (resp. de lois de composition commutatives) sur E ?

b) Combien a-t-on de lois de groupe (resp. de lois de groupe à isomorphisme près) sur E pour $n = 1, 2$ ou 3 ?

c) Donner les lois de groupe à isomorphisme près sur E pour $n = 4$.

3-7 – a) Soit un ensemble E . Montrer que l'ensemble (G, \circ) des bijections de E muni de la composition est un groupe non abélien dès que $\text{card } E \geq 3$.

b) On prend $E = \mathbb{Q}$. Montrer que les applications $f_{n,m} : a \mapsto na + m$, (avec $n \in \mathbb{Q}^*$ et $m \in \mathbb{Q}$) de \mathbb{Q} dans lui-même forment un sous-groupe de G .

3-8 – a) Rappeler pourquoi le module $z \rightarrow |z|$ définit un épimorphisme entre le groupe (\mathbb{C}^*, \times) et le groupe (\mathbb{R}_+^*, \times) . Quel est son noyau ?

b) Montrer, directement puis en utilisant ce qui précède, que l'ensemble S_1 des nombres complexes de module 1 est un sous-groupe du groupe multiplicatif (\mathbb{C}^*, \times) des nombres complexes non nuls.

c) Vérifier que pour $n \in \mathbb{N}$, l'application $z \rightarrow z^n$ définit un homomorphisme du groupe (\mathbb{C}^*, \times) .

d) Étant donné un entier $n > 0$, démontrer que l'ensemble U_n des racines n -ième de l'unité dans \mathbb{C} est un sous-groupe cyclique de S_1 . En considérant $\alpha = e^{\frac{2\pi i}{n}}$, en donner un générateur et montrer qu'il est isomorphe à $\mathbb{Z}/n\mathbb{Z}$.

3-9 – On note $GL_2(\mathbb{Z})$ l'ensemble des matrices inversibles à coefficients dans \mathbb{Z} ainsi que leur inverse. Montrer que c'est un sous-groupe de $GL_2(\mathbb{R})$. Montrer que pour qu'une matrice à coefficients entiers appartienne à $GL_2(\mathbb{Z})$, il faut et il suffit que son déterminant soit égal à ± 1 . Donner quelques exemples de telles matrices.

3-10 – Donner l'ordre de tous les éléments du groupe $(\mathbb{Z}/6\mathbb{Z}, +)$.

3-11 – Montrer, pour un groupe G , que l'application $x \mapsto x^{-1}$ (resp. l'application $x \mapsto x^2$) est un homomorphisme si et seulement si G est abélien.

3-12 – Soit $(G, *)$ un groupe fini. Montrer que, pour tout a et tout b de G :

a) a et a^{-1} ont même ordre.

b) a et $b * a * b^{-1}$ ont même ordre.

c) $a * b$ et $b * a$ ont même ordre.

d) Soit G un groupe possédant un seul élément d'ordre deux. On note a cet élément. Montrer que a est dans le centre de G .