Feuille d'exercices n° 2
Groupes, anneaux et idéaux

Groupes

Exercice 1. Lesquels de ces ensembles sont des groupes pour les lois de composition ?

$$(\mathbb{N},+) \qquad (\mathbb{Z},+) \qquad (\mathbb{Z},\times) \qquad (\mathbb{Z}\setminus\{0\},\times) \qquad (\mathbb{R}\setminus\{0\},\times)$$

Exercice 2.

i) Montrer que l'intersection de deux sous-groupes est un sous-groupe.

ii) Montrer que la réunion de deux sous-groupes de G est un sous-groupe si et seulement si l'un est contenu dans l'autre.

iii) Montrer que l'ensemble des entiers pairs est un sous-groupe de $(\mathbb{Z},+)$. L'ensemble des entiers impairs est-il un sous-groupe ?

Exercice 3. Soit $G = \{a + b\sqrt{2} | a \in \mathbb{Q}, b \in \mathbb{Q}\} \subset \mathbb{R}$.

i) Montrer que $(G,+)$ est un groupe.

ii) Montrer que l'ensemble des éléments non-nuls de G est un groupe pour la multiplication.

Exercice 4.

i) Soit H un sous-groupe de $\mathbb{Z}$. Montrer qu'il existe un unique $n \in \mathbb{Z}$ tel que $H = n\mathbb{Z}$.

ii) Déterminer les sous-groupes de $\mathbb{Z}$ contenant $48\mathbb{Z}$ et donner leurs relations d'inclusion.

Exercice 5. Soit $(G,\star)$ un groupe et $f : x \mapsto x^{-1}$ et $g : x \mapsto x^2$ deux applications de G dans G. Montrer que G est abélien si et seulement si f (resp. g) est un morphisme de groupe.

Exercice 6.

i) Montrer que l'application exponentielle $x \mapsto e^x$ est un isomorphisme entre les groupes $(\mathbb{R},+)$ et $(\mathbb{R},\times)$. Quel est l'isomorphisme réciproque ?

ii) Soit $\phi : \mathbb{Z} \to \mathbb{U}_n$ défini par $\phi(1) = e^{2i\pi/n}$. Montrer que c'est un morphisme de groupe. Identifier son noyau et en déduire un isomorphisme avec $\mathbb{U}_n$.

Exercice 7. Les groupes suivants sont-ils isomorphes ?

$$\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \text{ et } \mathbb{Z}/4\mathbb{Z} \qquad (\mathbb{Z}/2\mathbb{Z},+) \text{ et } (\mathbb{Z}/3\mathbb{Z}\setminus\{0\},\times) \qquad (\mathbb{Z}/4\mathbb{Z},+) \text{ et } (\mathbb{Z}/5\mathbb{Z}\setminus\{0\},\times).$$

Anneaux. Idéaux.

Exercice 8.

i) Soit A un anneau, I et J deux idéaux de A. Montrer que $I \cap J$ et $I + J = \{i + j | i \in I, j \in J\}$ sont des idéaux.

ii) Rappeler la forme générale des idéaux de $\mathbb{Z}$ et montrer que

$$n\mathbb{Z} + m\mathbb{Z} = pgcd(n,m)\mathbb{Z} \qquad n\mathbb{Z} \cap m\mathbb{Z} = ppcm(n,m)\mathbb{Z}$$

iii) Dans $\mathbb{Z}$, identifier l'idéal principal engendré par les éléments 2 et 5.

Benjamin Collas • *Email :* `collas@math.jussieu.fr`

Exercice 9. Écrire les tables de multiplication de $\mathbb{Z}/5\mathbb{Z}$ et $\mathbb{Z}/6\mathbb{Z}$. En déterminer les éléments inversibles.

Exercice 10.

i) Monter que A/I est intègre si et seulement si I est un idéal premier de A.

ii) Donner les idéaux premiers de $\mathbb{Z}$.

iii) Résoudre l'équation $3x = 0$ dans $\mathbb{Z}/12\mathbb{Z}$.

Exercice 11.

i) Montrer que $\mathbb{Z}[i] = \{a + ib, (a, b) \in \mathbb{Z}^2\}$ est un anneau intègre.

ii) Déterminer les inversibles de $\mathbb{Z}[i]^*$ et montrer que $\mathbb{Z}[i]^* \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.

Groupes finis. Ordres

Exercice 12.

i) Soit G un groupe et $g \in G$. Montrer que g est d'ordre n si et seulement si $g^n = e$ et $g^{n/p} \neq e$ pour tout p diviseur premier de n.

ii) *Un test de primalité :* pour $n \in \mathbb{N}$ fixé, en déduire que s'il existe $a \in \mathbb{Z}/n\mathbb{Z}$ tel que $a^{n-1} = 1 \mod n$ et $a^{(n-1)/p} \neq 1 \mod n$ pour tout p diviseur premier de n, alors n est premier.

Exercice 13. Soit G un groupe et $g \in G$ un élément d'ordre n non-nul.

i) Montrer que $ord(x^k) = n/pgcd(k, n)$.

ii) *Application* : donner l'ordre de 5 dans $(\mathbb{Z}/30\mathbb{Z}, +)$.

Exercice 14.

i) Montrer que tout sous-groupe d'un goupe cyclique est cyclique.

ii) Soit $G =< g >$ un groupe cyclique d'ordre n. Montrer que pour r diviseur positif de n, il existe un sous-groupe H de G d'ordre r. Donner un générateur de H.

iii) *Application* : écrire les tables d'addition de $\mathbb{Z}/5\mathbb{Z}$ et $\mathbb{Z}/6\mathbb{Z}$. Déterminer les sous-groupes de chacun de ces groupes.

Exercice 15.

i) Soit $n \in \mathbb{N}$. Montrer que, pour tout entier relatif $a \in \mathbb{Z}$, a est inversible dans $\mathbb{Z}/n\mathbb{Z}$ si et seulement si $pgcd(a, n) = 1$.

ii) En déduire que $\mathbb{Z}/n\mathbb{Z}$ est un corps si et seulement si n est premier.

iii) Montrer que 7 est inversible dans $\mathbb{Z}/24\mathbb{Z}$ et calculer son inverse.

Exercice 16. Vérifier que $(\mathbb{Z}/n\mathbb{Z})^*$ est cyclique pour $n \leqslant 7$. Vérifier que ce n'est pas le cas pour $\mathbb{Z}/8\mathbb{Z}$.

Exercice 17. Soient $G =< g >$ et $H =< h >$ deux groupes cycliques d'ordres respectifs n et m. Quel est l'ordre maximal d'un élément de $G \times H$? Montrer que $org((g, h)) = ppcm(n, m)$. En déduire que $G \times H$ est cyclique si et seulement si $pgcd(n, m) = 1$.