Groupes

Exercice 6. (∗∗) Soit H un sous-groupe de $(\mathbb{R},+)$ non réduit au singleton $\{0\}$.

1) Montrer que $H\cap\mathbb{R}_+^*$ admet une borne inférieure, que l'on note a.
2) Si a est le minimum de $H\cap\mathbb{R}_+^*$ montrer que H est le sous-groupe $a\mathbb{Z}$.
3) Si $H\cap\mathbb{R}_+^*$ n'admet pas de minimum, montrer par l'absurde que a est nul puis que H est dense dans $\mathbb{R}$.

Correction -

1) $H\cap\mathbb{R}_+^*$ est une partie de R, minorée par 0.
Reste à prouver qu'elle est non vide. Comme H n'est pas réduit au singleton $\{0\}$ posons $x\in H$ tel que $x\neq 0$.
Si $x>0$ alors $x\in H\cap\mathbb{R}_+^*$. Sinon, comme H est stable par opposé, $-x\in H$ et donc $-x\in H\cap\mathbb{R}_+^*$.
On a bien $H\cap\mathbb{R}_+^*$ non vide.
Enfin d'après le théorème de la borne supérieure, $H\cap\mathbb{R}_+^*$ admet une borne inférieure, notons la α.
2) Supposons $a=\min(H\cap\mathbb{R}_+^*)$. Montrons que $H=a\mathbb{Z}$.

   $\supset$: comme $a\in H$ et que H est un sous-groupe de R alors : $\forall n\in\mathbb{Z}$, $na\in H$. (détails laissés au lecteur, il faut distinguer $a<0$, $a>0$, $a=0$).
   On a donc bien $a\mathbb{Z}\subset H$.

   $\subset$: soit $x\in H$, posons $n=\lfloor\frac{x}{a}\rfloor$ alors $n\leqslant\frac{x}{a}<n+1$ donc $0\leqslant x-na<a$.
   Comme $x\in H$ et $a\in H$ alors par stabilité de H pour la somme et l'opposé : $x-na\in H$. Comme $0\leqslant x-na<a$ alors $x-na=0$ donc $x=na\in a\mathbb{Z}$.
   D'où la deuxième inclusion.

   Finalement, $\boxed{H=a\mathbb{Z}}$.
3) Supposons que $H\cap\mathbb{R}_+^*$ n'admet pas de minimum.
Par l'absurde supposons $a>0$. Par définition de la borne inférieur il existe alors $x\in H\cap\mathbb{R}_+^*$ tel que $a<x<2a$ puis $y\in H\cap\mathbb{R}_+^*$ tel que $a<y<x<2a$ et donc $0<x-y<a$ et $x-y\in H\cap\mathbb{R}_+^*$ ce qui est absurde. Donc $a=0$.
Montrons que H est dense dans $\mathbb{R}$. (Idée : la borne inférieure nulle traduit qu'il existe des éléments de H aussi petit que l'on veut).
Soit $(x,y)\in R^2$, posons $\varepsilon=y-x>0$. Par définition de la borne inférieure, il existe alors $h\in H$ tel que $0<h<\varepsilon$. On pose $n=\lfloor\frac{x}{h}\rfloor$, alors $n\leqslant\frac{x}{h}<n+1$ c'est-à-dire $nh\leqslant x<nh+h$, donc

$$x<nh+h\leqslant x+h<x+\varepsilon=y.$$

On a donc trouvé un élément $nh+h=(n+1)h\in H$ compris entre x et y.
Donc $\boxed{H \text{ dense dans } \mathbb{R}}$.

Exercice 10 Soit $(G,*)$ un groupe. On note $\mathrm{Aut}(G)$ l'ensemble des automorphismes de G.

1) Montrer que $(\mathrm{Aut}(G),\circ)$ est un groupe.
2) Pour $a\in G$, on note $f_a:G\to G$ l'application définie par $f_a(x)=a*x*a^{-1}$.
Montrer que pour tout $a\in G$, $f_a\in\mathrm{Aut}(G)$.
3) Montrer que l'application $\psi:G\to\mathrm{Aut}(G)$, définie par $\psi(a)=f_a$ est un morphisme de groupe. Déterminer son noyau.

Correction -

1) Vérification facile de la définition de groupe:
   - lci : la composée d'automorphismes est un automorphisme (démontré en cours)
   - $\circ$ associative sur $\mathrm{Aut}(G)$ car restreint à $\mathrm{Aut}(G)$ et l'est sur G^G
   - Id_G, le neutre de $\circ$ dans G^G, appartient bien à $\mathrm{Aut}(G)$ (c'est un morphisme bijectif)
   - Tout $f\in\mathrm{Aut}(G)$ admet un inverse dans G^G c'est la réciproque f^{-1}. Et f^{-1} est bien morphisme bijectif (démontré en cours).

   Donc $\boxed{(\mathrm{Aut}(G),\circ) \text{ est un groupe}}$.
2) Soit $a\in G$.
   - f_a morphisme : soit $(x,y)\in G$, on insère le neutre $e=a^{-1}*a$ de G dans le calcul suivant

$$f_a(x*y)=a*x*y*a^{-1}=a*x*a^{-1}*a*y*a^{-1}=f_a(x)*f_a(y).$$

- f_a bijective : soit $(x,y) \in G^2$,

$$y = f_a(x) \Leftrightarrow y = a*x*a^{-1} \Leftrightarrow a^{-1}*y*a = x \quad \text{d'où l'unicité de la solution.}$$

On a étoilé par a^{-1} à gauche et a à droite.
Donc $\boxed{f_a \text{ est bijective et } (f_a)^{-1} = f_{a^{-1}}}$.

Bilan : on a bien $\boxed{f_a \in \mathrm{Aut}(G)}$.

3) Soit $(a,b) \in G$, montrons que $\psi(a*b) = \psi(a) \circ \psi(b)$.
On a $\psi(a*b) = f_{a*b}$. Puis pour tout $x \in G$,

$$\psi(a*b)(x) = f_{a*b}(x) = a*b*x*(a*b)^{-1} = a*b*x*b^{-1}*a^{-1} = f_a(b*x*b^{-1}) = f_a(f_b(x)) = (f_a \circ f_b)(x).$$

Donc $\psi(a*b) = \psi(a) \circ \psi(b)$.
Donc $\boxed{\psi \text{ est un morphisme de groupes}}$.

$$\mathrm{Ker}\,\psi = \{a \in G \,/\, \psi(a) = \mathrm{Id}_G\} = \{a \in G \,/\, f_a = \mathrm{Id}_G\} = \{a \in G \,/\, \forall x \in G,\ a*x*a^{-1} = x\} = \{a \in G \,/\, \forall x \in G,\ a*x = x*a\}$$

Donc $\boxed{\mathrm{Ker}\,\psi = Z(G) \text{ (l'ensemble des éléments qui commutent avec tous les autres éléments de } G)}$.

Exercice 11. $(*)$ Soient deux entiers non nuls a et b.

1) Montrer que : $\delta = a \wedge b \Leftrightarrow \delta\mathbb{Z} = a\mathbb{Z} + b\mathbb{Z}$.

2) Montrer que : $\mu = a \vee b \Leftrightarrow \mu\mathbb{Z} = a\mathbb{Z} \cap b\mathbb{Z}$.

Correction - Je ne donne que des indications

1) Par double implication.
$\Rightarrow$: supposons $\delta = a \wedge b$.
Par double inclusion. Pour $\subset$: utiliser la relation de Bezout. Pour $\supset$: utiliser que δ divise a et b.
$\Leftarrow$: supposons $\delta\mathbb{Z} = a\mathbb{Z} + b\mathbb{Z}$.
Tout d'abord comme a et b appartiennent à $a\mathbb{Z} + b\mathbb{Z}$ alors par hypothèse $a = k\delta$ et $b = k'\delta$, où k, k' sont deux entiers, donc δ est un diviseur commun de a et b.
Soit maintenant d est un diviseur commun de a et b. Comme $\delta \in \delta\mathbb{Z}$ alors par hypothèse $\delta = au + bv$, où u et v sont deux entiers, alors par somme produit, d divise δ.
On a donc prouvé que δ est le plus grand diviseur commun positif de a et b pour la relation de divisibilité et donc $\delta = a \wedge b$.

2) Découle immédiatement du fait que le PPCM est le plus petit commun mutiple de a et b pour la relation de divisibilité.

Exercice 12. $(**)$Théorème de Wilson Soit un entier naturel $p \geqslant 3$.

1) On suppose que $(p-1)! \equiv -1\ [p]$. Montrer que p est premier.

2) On suppose p premier. On pose $G = [\![1, p-1]\!]$ et pour tout $(x,y) \in G^2$, $x*y$ est le reste de la division euclidienne de xy par p.

-a- Montrer que $(G,*)$ est un groupe.

-b- Résoudre l'équation $x*x = e$ dans G.

-c- Démontrer que $(p-1)! \equiv -1\ [p]$.

3) Énoncer le théorème démontré (théorème de Wilson).

Correction -

1) Supposons $(p-1)! \equiv -1\ [p]$ càd $p|(p-1)! + 1$.
Soit d un diviseur positif de p autre que p alors d'une part par hypothèse et transitivité de la relation de divisibilité $d|(p-1)! + 1$.
D'autre part d étant parmi les entiers $1, \ldots, p-1$, $d|(p-1)!$.
Donc par différence $d|1$ donc $d = 1$.
Conclusion : $\boxed{p \text{ premier}}$.

2) Tout d'abord notons que comme $x*y$ est le reste de la division euclidienne de xy par p alors $x*$ est caractérisé par les conditions :

$$xy \equiv x*\ [p] \quad \text{et} \quad x*y \in [\![0, p-1]\!].$$

-a- On vérifie la définition d'un groupe.

- Soit $(x,y) \in G^2$, on a déjà $x*y \in [\![0, p-1]\!]$. Montrer que $x*y \neq 0$. Par l'absurde supposons $x*y = 0$ alors $p|xy$. Et comme $x \in [\![1, p-1]\!]$ et que 1 est premier alors $x \wedge p = 1$ donc d'après le théorème de Gauss, $p|y$. Absurde.
Donc $x*y \in G$ et donc $*$ est une loi de composition interne.

- Associativité: (démo faite avec les congruences pour faire différemment de la correction de TD de cette année). $(x,y,z) \in G^3$, on sait que

$$xy = x*y\ [p] \qquad \text{et} \qquad (x*y)z = (x*y)*z\ [p] \qquad \text{donc en combinant les deux} \qquad xyz = (x*y)*z\ [p].$$

  De même, $xyz = x*(y*z)\ [p]$, et donc $x*(y*z) = (x*y)*z\ [p]$.
  Et comme ces deux entiers appartiennent à $[\![0, p-1]\!]$, ils sont égaux : $x*(y*z) = (x*y)*z$.
- La commutativité est évidente car $xy = yx$.
- Pour tout $x \in G$, $1x = x \equiv x\ [p]$ et $x \in [\![1, p-1]\!]$ ce qui caractérise $x*1 = x$. De même par commutativité $1*x = x$. Et donc 1 est le neutre de $*$.
- Soit $x \in G$. Comme $x[\![1, p-1]\!]$ et p premier alors $x \wedge p = 1$ donc d'après le théorème de Bezout posons u, v dans Z tel que $xu + pv = 1$ donc $xu \equiv 1\ [p]$. Posons maintenant x' le reste de la division euclidienne de u par p, alors $u \equiv x'\ [p]$ et donc injectant dans la congruence précédente, $xx' \equiv 1\ [p]$. Par l'absurde, on montre facilement que $x' \neq 0$ on a donc bien $x' \in G$ et $x*x' = 1$. Par commutativité, $x'*x = 1$.

Donc $(G, *)$ est bien un groupe.

-b- Tout d'abord, on remarque que $1*1 = 1$ et $(p-1)*(p-1) = 1$ car $(p-1)^1 = p^2 + 2p + 1 \equiv 1\ [p]$.
Soit alors $x \in G$, $x \neq 1$ et $x \neq p-1$ tel que $x*x = 1$ càd $x^2 \equiv 1\ [p]$ donc $p|(x-1)(x+1)$. Alors $1 \leqslant x-1 \leqslant p-3$ et comme p est premier $p \wedge x-1 = 1$ donc d'après le théorème de Gauss $p|x+1$, ce qui est absurde car $3 \leqslant x+1 \leqslant p-1$.
Bilan : $\mathcal{S} = \{1, p-1\}$.

-c- La question 2)-b- montre que les éléments de $[\![2, p-2]\!]$ ont leur inverse dans $[\![2, p-2]\!]$ autres que eux-même. On regroupe alors dans $2 \times \cdots \times p-2$ les éléments par pair avec leur inverse et l'on obtient :

$$2 \times \cdots \times p-2 \equiv 1\ [p].$$

Par conséquent

$$1 \times 2 \times \cdots \times p-2 \times p-1 \equiv p-1 \equiv -1\ [p].$$

Donc $\boxed{(p-1)! \equiv -1\ [p]}$.

3) On a donc démontré le théorème de Wilson :

$$\boxed{p \text{ premier } \Leftrightarrow (p-1)! \equiv -1\ [p]}.$$

Exercice 14 Soit $(A, +, \times)$ un anneau non nul, on note 1 le neutre de $\times$. On pose l'application $\varphi : \begin{array}{ccc} \mathbb{Z} & \to & A \\ n & \mapsto & n \times 1 = 1 + \cdots + 1 \end{array}$.

1) Montrer que φ est le seul morphisme d'anneaux de $\mathbb{Z}$ dans A.

2) Dans le cas où φ n'est pas injectif, montrer qu'il existe un unique $c \in \mathbb{N}^*$, tel que $\operatorname{Ker}\varphi = c\mathbb{Z}$.
On se place désormais dans ce cas de figure, c est appelé la caractéristique de l'anneau A.

3) Montrer que si A est intègre alors c est un nombre premier.

4) Montrer que si A est commutatif alors $x \mapsto x^c$ est un endomorphisme de l'anneau A.

Correction -

1) On vérifie tout d'abord que φ est bien un morphisme d'anneaux (pas de difficulté, laissé au lecteur).
Puis que c'est le seul. Soit ψ un morphisme d'anneaux de $\mathbb{Z}$ dans A. Alors, comme ψ est additive on prouve que pour tout $n \in \mathbb{Z}$, $\psi(n1) = n\psi(1)$ (pour $n \in \mathbb{N}$ c'est une récurrence, et pour $n \in \mathbb{Z}_-$ on se ramène à $n \in \mathbb{N}$ et on utilise le transport de l'opposé). Et comme $\psi(1) = 1$ (définition du morphisme d'anneaux) alors $\psi(n1) = n \times 1$ ce pour tout $n \in \mathbb{Z}$.
Donc $\psi = \phi$.

2) Supposons φ non injectif.
D'après le cours, $\operatorname{Ker}\varphi$ est un sous-groupe de l'ensemble de départ, ici $\mathbb{Z}$ et donc il est de la forme $c\mathbb{Z}$. Comme φ n'est pas injectif, $\operatorname{Ker}\varphi \neq \{0\}$ donc $c \neq 0$.

3) Supposons A intègre. Par l'absurde supposons, $c = ab$ où $2 \leqslant a, b \leqslant c-1$.
Comme φ est un morphisme $\varphi(c) = \varphi(a)\varphi(b)$ or $c \in \operatorname{Ker}\varphi$ donc $\varphi(c) = 0$.
Comme A est intègre $\varphi(a) = 0$ ou $\varphi(b) = 0$ càd a ou b appartient à $\operatorname{Ker}\varphi = c\mathbb{Z}$. Donc a ou b est un multiple de c. Ce qui est absurde car ils sont compris entre 2 et $c-1$.
Donc c est premier.

4) Supposons A commutatif. Posons $\psi : x \mapsto x^c$.

- On a bien $\psi : A \to A$ car pour tout $x \in A$, $x^c \in A$ (stabilité de A pour $\times$).
- $\psi(1) = 1^c = 1$
- Soit $(x, y) \in A^2$, $\psi(xy) = (xy)^c = x^c y^c$ car $\times$ commutative donc $\psi(xy) = \psi(x)\psi(y)$.
- Soit $(x, y) \in A^2$, $\psi(x+y) = (x+y)^c$. Puis on montre $(x+y)^c = x^c + y^c$ comme dans le lemme qui a servi à démontrer le petit théorème de Fermat en utilisant la formule du binôme de Newton qui s'applique bien ici car $x$et y commutent. Donc $\psi(x+y) = \psi(x) + \psi(y)$.

Bilan : $\boxed{\psi \text{ est un endomorphisme de l'anneau } A}$.

Exercice 15. (♡) Montrer que l'ensemble $\{a+b\sqrt{3} \,/\, (a,b) \in \mathbb{Q}^2\}$ est un corps.

Correction - Que des vérifications des différents points de la définition, aucune difficulté par rapport aux exemples déjà traités.

Exercice 16. (∗) On note $Z[i] = \{a+\mathrm{i}\,b \,/\, (a,b) \in \mathbb{Z}^2\}$ et $Z(i) = \{a+\mathrm{i}\,b \,/\, (a,b) \in \mathbb{Q}^2\}$.

1) Montrer que $(\mathbb{Z}[i], +, \times)$ est un anneau intègre qui n'est pas un corps.
2) Montrer que $(\mathbb{Z}(i), +, \times)$ est un corps.
3) Montrer que toute fraction $\dfrac{A}{B}$ avec $(A,B) \in (\mathbb{Z}[i])^2$ appartient à $\mathbb{Z}(i)$. Et réciproquement que tout élément de $\mathbb{Z}(i)$ s'écrit $\dfrac{A}{B}$ avec $(A,B) \in (\mathbb{Z}[i])^2$.

Correction - Pour 1) et 2) que des vérifications des différents points de la définition, aucune difficulté par rapport aux exemples déjà traités.
Pour 1) et montrer que ce n'est pas un corps, on prouve par exemple que $1+\mathrm{i}$ (qui est non nul) bien qu'inversible dans $\mathbb{C}$, d'inverse $\frac{1}{2}(1-\mathrm{i})$ ne l'est pas dans $\mathbb{Z}[i]$ l'inverse n'appartient pas à $\mathbb{Z}[i]$.
3) Soient $A = a+\mathrm{i}\,b$ et $B = c+\mathrm{i}\,d$ dans $Z[i]$ alors

$$\frac{A}{B} = \frac{a+\mathrm{i}\,b}{c+\mathrm{i}\,d} = \frac{1}{c^2+d^2}(a+\mathrm{i}\,b)(c-\mathrm{i}\,d) \in \mathbb{Z}(i).$$

Réciproquement, soit $\alpha \in \mathbb{Z}(i)$, $\alpha = \frac{a}{b} + \frac{c}{d}\,\mathrm{i} = \frac{ad+bc\,\mathrm{i}}{bd} = \frac{A}{B}$ où $A = ad+bc\,\mathrm{i}$ et $B = bd$ appartiennentn à $\mathbb{Z}[i]$.