Relations d'équivalence, quotients, premières propriétés des groupes.

1 Exercice 1.

1. *Donner un isomorphisme $f : \mathbb{R}/\mathbb{Z} \to \mathbb{S}^1$, où $\mathbb{S}^1$ est le cercle unité de $\mathbb{R}^2$ et $\mathbb{R}/\mathbb{Z}$ est le groupe quotient de $\mathbb{R}$ par son sous-groupe distingué $\mathbb{Z}$.*

Soient E et F deux ensembles et soit $f : E \to F$ une application.

2. **a)** *Montrer que la relation binaire sur E définie par*

$$x \sim y \iff f(x) = f(y)$$

est une relation d'équivalence.

b) *On pose $X := E/\sim$. Soit $\pi : E \to X$ l'application canonique. Montrer qu'il existe une unique application $\bar{f} : X \to F$ telle que $f = \bar{f} \circ \pi$.*

c) *Montrer que $\bar{f}$ est une bijection sur son image.*

1. On commence par considérer l'application

$$\begin{aligned} g : \mathbb{R}/\mathbb{Z} &\longrightarrow u^{-1}(\mathbb{S}^1) \\ x\mathbb{Z} &\longmapsto \mathrm{e}^{2\pi \mathrm{i} x}, \end{aligned}$$

où $u : \mathbb{C} \to \mathbb{R}^2$ est l'isomorphisme canonique de $\mathbb{R}^2$ et $\mathbb{C}$. Montrons trois propriétés.

- ▷ C'est bien défini. En effet, si $k \in \mathbb{Z}$, alors $\mathrm{e}^{2\mathrm{i}\pi(x+k)} = \mathrm{e}^{2\mathrm{i}\pi x}$ par a 2π-périodicité de cos et sin.
- ▷ C'est bien un morphisme. En effet, si $x\mathbb{Z}, y\mathbb{Z} \in \mathbb{R}/\mathbb{Z}$, alors on a

$$\begin{aligned} g(x\mathbb{Z} + y\mathbb{Z}) = g((x+y)\mathbb{Z}) &= \exp(2\mathrm{i}\pi(x+y)) \\ &= \exp(2\mathrm{i}\pi x) \cdot \exp(2\mathrm{i}\pi y) \\ &= g(x\mathbb{Z}) \cdot g(y\mathbb{Z}). \end{aligned}$$

- ▷ C'est une bijection. En effet, l'application réciproque est l'application $u^{-1}(\mathbb{S}^1) \ni z \mapsto (\arg z)\mathbb{Z}$.

On en conclut en posant l'isomorphisme $f := u \circ g : \mathbb{R}/\mathbb{Z} \to \mathbb{S}^1$.

2. **a)** On a trois propriétés à vérifier.

- ▷ Comme $f(x) = f(x)$, on a $x \sim x$ quel que soit $x \in E$.
- ▷ Si $x \sim y$, alors $f(x) = f(y)$ et donc $f(y) = f(x)$ et on en déduit $y \sim x$.
- ▷ Si $x \sim y$ et $y \sim z$, alors $f(x) = f(y) = f(z)$, et on a donc $x \sim z$.

b) La fonction f est constante sur chaque classe d'équivalence de E par $\sim$. On procède par analyse synthèse.

- ▷ *Analyse.* Si $\bar{f} : X \to F$ existe, alors $\bar{f}(\bar{x}) = f(x)$ quel que soit $x \in E$, où $\bar{x}$ est la classe d'équivalence de x. L'application $\bar{f}$ est donc unique, car déterminée uniquement par les valeurs de f sur les classes d'équivalences de x.
- ▷ *Synthèse.* On pose $\bar{f}(\bar{x}) := f(x)$, qui est bien définie car f est constante sur les classes d'équivalences de $\sim$.

c) Montrons que $\bar{f} : X \to \operatorname{im} \bar{f}$ est injective et surjective.

- ▷ Soient $\bar{x}$ et $\bar{y}$ dans X tels que $\bar{f}(\bar{x}) = \bar{f}(\bar{y})$. Alors, on a $f(x) = f(y)$ et donc $x \sim y$ d'où $\bar{x} = \bar{y}$.
- ▷ On a, par définition, $\operatorname{im} \bar{f} = \bar{f}(X)$.

D'où, $\bar{f}$ est une bijection sur son image.

2 Exercice 2. *Parties génératrices*

1. *Soit X une partie non vide d'un groupe G. Montrer que $\langle X\rangle$, le sous-groupe de G engendré par X, est exactement l'ensemble des produits finis d'éléments de $X \cup X^{-1}$, où X^{-1} est l'ensemble défini par $X^{-1} := \{x^{-1} \mid x \in X\}$.*
2. *Montrer que le groupe $(\mathbb{Q}, +)$ n'admet pas de partie génératrice finie.*
3. *Montrer que $(\mathbb{Q}^\times, \times) = \langle -1, p \in \mathbb{P}\rangle$, où $\mathbb{P}$ est l'ensemble des nombres premiers.*

1. Soit H l'ensemble des produits finis d'éléments de $X \cup X^{-1}$.
   - ▷ L'ensemble H contient X. De plus, H est un groupe. En effet, on a $H \neq \emptyset$ car $e = xx^{-1} \in H$ où $x \in X$. Puis, pour deux produits $x = x_1 \cdots x_n \in H$ et $y = y_1 \cdots y_m \in H$ (où les x_i et les y_j sont des éléments de $X \cup X^{-1}$) on a
   $$xy^{-1} = x_1 \cdots x_n y_m^{-1} \cdots y_1^{-1},$$
   qui est un produit fini d'éléments de $X \cup X^{-1}$, c'est donc un élément de H. On en conclut que H est un sous-groupe de G contenant H. D'où $H \geq \langle X\rangle$.
   - ▷ Soit K un sous-groupe de G contenant X. D'une part, on sait que $X \cup X^{-1} \subseteq K$. D'autre part, si $x = x_1 \cdots x_n$ où l'on a $x_i \in X \cup X^{-1} \subseteq K$, alors $x \in K$ car K est un groupe. On en déduit que $H \leq K$.

   Ainsi, H est le plus petit sous-groupe de G contenant X, il est donc égal à $\langle X\rangle$.
2. Supposons, par l'absurde, que $(\mathbb{Q}, +) = \left\langle \frac{p_1}{q_1}, \frac{p_2}{q_2} \ldots, \frac{p_n}{q_n}\right\rangle$. On pose $Q := \prod_{i=1}^n q_i$, puis on considère $\frac{1}{Q+1} \in \mathbb{Q}$.

   Montrons que l'on peut écrire tout élément de $\left\langle \frac{p_1}{q_1}, \ldots, \frac{p_n}{q_n}\right\rangle$ sous la forme $\frac{p}{Q}$. En effet, par la question 1, on considère
   $$x := \sum_{i\in I} \varepsilon_i \frac{p_i}{q_i} \quad \text{avec} \quad \varepsilon_i \in \{-1, 1\} \quad \text{et} \quad I \text{ fini},$$

un élément quelconque du sous-groupe engendré. Et, en mettant au même dénominateur, on obtient $p'/\prod_{i\in I} q_i = x$. On obtient donc bien

$$x = \frac{p' \times \prod_{i\notin I} p_i}{Q},$$

où le produit au numérateur contient un nombre fini de termes.

Or, $\frac{1}{Q+1} \in \mathbb{Q}$ ne peut pas être écrit sous la forme p/Q car $Q+1$ et Q sont premiers entre eux. C'est donc absurde ! On en conclut que $(\mathbb{Q}, +)$ n'admet pas de partie génératrice finie.

3. Notons $E := \langle -1, p \in \mathbb{P}\rangle$. Soit $\frac{a}{b}$ un rationnel strictement positif. On suppose a et b positifs. On décompose a et b en produit de nombre premiers :

$$a = \prod_{i\in I} p_i \qquad \text{et} \qquad b = \prod_{j\in J} p_j.$$

On a donc $a \in E$ et $b \in E$. On en conclut que $\frac{a}{b} \in E$.

Si $\frac{a}{b} \in \mathbb{Q}^\times$ est un rationnel tel que $a, b < 0$, on a $\frac{a}{b} = \frac{|a|}{|b|} \in E$ d'après ce qui précède.

Si $\frac{a}{b} \in \mathbb{Q}^\times$ est un rationnel négatif, alors on a $\left|\frac{a}{b}\right| \in E$, mais on a donc également $\frac{a}{b} = (-1) \times \left|\frac{a}{b}\right| \in E$.

On en conclut que $\mathbb{Q}^\times \subseteq E$ et on a égalité car $E \subseteq \mathbb{Q}^\times$ par définition de E comme sous-groupe de $\mathbb{Q}^\times$.

3 Exercice 3. *Ordre des éléments d'un groupe*

Soient g et h deux éléments d'un groupe G.

1. **a)** *Montrer que g est d'ordre fini si et seulement s'il existe $n \in \mathbb{N}^*$ tel que $g^n = e$.*

b) *Montrer que si g est d'ordre fini, alors son ordre est le plus petit entier $n \in \mathbb{N}^*$ tel que $g^n = e$. Montrer, de plus, que pour $m \in \mathbb{Z}$, $g^m = e$ si et seulement si l'ordre de g divise m.*

2. *Montrer que les éléments g, g^{-1} et hgh^{-1} ont même ordre.*

3. *Montrer que gh et hg ont même ordre.*

4. *Soit $n \in \mathbb{N}$. Exprimer l'ordre de g^n en fonction de celui de g.*

5. *On suppose que g et h commutent et sont d'ordre fini m et n respectivement.*

   a) *Exprimer l'ordre de gh lorsque $\langle g \rangle \cap \langle h \rangle = \{e\}$.*

   b) *Même question lorsque m et n sont premiers entre eux.*

   c) *(Plus difficile) On prend m et n quelconques. Soient $a := \min\{\ell \in \mathbb{N}^* \mid g^\ell \in \langle h \rangle\}$ et $b \in \mathbb{N}$ tel que $g^a = h^b$. Démontrer que l'ordre de gh est $an/\operatorname{pgcd}(n, (a+b))$.*

6. *En considérant*

$$A := \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \qquad \textit{et} \qquad B := \begin{pmatrix} 0 & 1 \\ -1 & 1 \end{pmatrix},$$

montrer que le produit de deux éléments d'ordre fini ne l'est pas forcément.

1. On rappelle que l'ordre de g est défini comme $\#\langle g \rangle$. On le note naturellement $\operatorname{ord} g$.

   a) On procède par double implication.

   ▷ Si g est d'ordre fini, alors $\langle g \rangle$ est fini et donc l'application

$$\begin{aligned} \varphi : \mathbb{Z} &\longrightarrow \langle g \rangle \\ n &\longmapsto g^n \end{aligned}$$

   est un morphisme non injectif. Il existe donc un entier non nul $n \in \mathbb{Z} \setminus \{0\}$ tel que $n \in \ker \varphi$, *i.e.* $g^n = e$.

   ▷ Si $g^n = e$ alors $\langle g \rangle = \{g^i \mid i \in [\![0, n-1]\!]\}$, qui est fini. Ainsi g est d'ordre fini.

   b) Si g est d'ordre fini, alors le morphisme φ (défini ci-avant) est surjectif et non injectif. Soit $p = \min(\ker \varphi \cap \mathbb{N}^\star)$. Alors les g^i pour $i \in [\![0, p-1]\!]$ sont distincts et constituent $\langle g \rangle$.

   Si $n \in \mathbb{Z}$ est tel que $g^n = e$. On écrit $n = q \times (\operatorname{ord} g) + r$ la division euclidienne de n par $\operatorname{ord} g$, avec $0 \leq r < \operatorname{ord} g$. Et,

$$e = g^n = (g^{\operatorname{ord} g})^q g^r = g^r,$$

d'où $g^r = e$. On en déduit que $r = 0$ et donc $\operatorname{ord} g$ divise n.

2. D'une part, $\langle g \rangle = \langle g^{-1} \rangle$, d'où $\operatorname{ord} g = \operatorname{ord} g^{-1}$. D'autre part, pour $n \in \mathbb{N}$, on a $(hgh^{-1})^n = hg^nh^{-1}$, et donc l'équivalence
$$g^n = e \iff (hgh^{-1})^n = e,$$
d'où $\operatorname{ord} g = \operatorname{ord}(hgh^{-1})$.
3. On a $hg = h(gh)h^{-1}$ et par la question précédente, on a que $\operatorname{ord}(hg) = \operatorname{ord}(gh)$.
4. On a
$$\begin{aligned}\operatorname{ord} g^n &= \min\{k \in \mathbb{N}^* \mid g^{nk} = e\}\\ &= \frac{1}{n} \min\big((\operatorname{ord} g)\mathbb{Z} \cap n\mathbb{Z} \cap \mathbb{N}^*\big)\\ &= \frac{\operatorname{ppcm}(\operatorname{ord} g, n)}{n}\\ &= \frac{\operatorname{ord} g}{\operatorname{pgcd}(\operatorname{ord} g, n)}.\end{aligned}$$
5. a) Si $\langle g \rangle \cap \langle h \rangle = \{e\}$ et $(gh)^k = e$ alors $g^k = h^{-k} \in \langle g \rangle \cap \langle h \rangle$. D'où, $g^k = h^{-k} = e$.

4 Exercice 4.

Soit G un groupe.

1. *On suppose que tout élément g de G est d'ordre au plus 2. Montrer que G est commutatif.*
2. *Montrer que G est commutatif si et seulement si l'application $g \mapsto g^{-1}$ est un morphisme de groupes.*

1. Pour tout $g \in G$, on a $g^2 = e$. Ainsi, pour tout $g \in G$, on a g est son propre inverse. Ceci permet de calculer
$$gh = g^{-1}h = g^{-1}h^{-1} = (hg)^{-1} = hg,$$
d'où G est commutatif.

2. On note $\phi : g \mapsto g^{-1}$, et on procède par équivalence.

$$\begin{aligned} G \text{ est commutatif} &\iff \forall g,h \in G, \quad gh = hg \\ &\iff \forall g,h \in G, \quad (gh)^{-1} = (hg)^{-1} \\ &\iff \forall g,h \in G, \quad (gh)^{-1} = g^{-1}h^{-1} \\ &\iff \forall g,h \in G, \quad \phi(gh) = \phi(g)\,\phi(h) \\ &\iff \phi \text{ est un morphisme.} \end{aligned}$$

5 Exercice 5.

Soit $\phi : G_1 \to G_2$ un morphisme de groupes, et soit $g \in G_1$ d'ordre fini. Montrer que $\phi(g)$ est d'ordre fini et que son ordre divise l'ordre de g.

On utilise habilement l'exercice 3 : pour tout $h \in G$, $h^m = e$ si et seulement si l'ordre de h divise m. Soit n l'ordre de g (qui est fini car G_1 d'ordre fini). Ainsi,

$$(\phi(g))^n = \phi(g^n) = \phi(e_1) = e_2.$$

On en déduit donc que $\phi(g)$ est d'ordre fini et qu'il divise $n = \operatorname{ord} g$.

6 Exercice 6.

Soient G_1 et G_2 des groupes, et $\phi : G_1 \to G_2$ un morphisme de groupes.

1. *Soient H_1 (resp. H_2) un sous-groupe de G_1 (resp. G_2). Montrer que $\phi(H_1)$ (resp. $\phi^{-1}(H_2)$) est un sous-groupe de G_2 (resp. G_1).*
2. *Montrer que H_2 est un sous-groupe distingué de G_2, alors $\phi^{-1}(H_2)$ est un sous-groupe distingué de G_1.*
3. *Montrer que si ϕ est surjective, l'image d'un sous-groupe distingué de G_1 par ϕ est un sous-groupe distingué de G_2.*
4. *Donner un exemple d'un morphisme de groupes $\phi : G_1 \to G_2$ et de sous-groupe distingué $H_1 \lhd G_1$ tel que $\phi(H_1)$ n'est pas distingué dans G_2.*

1. Remarquons que $e_2 \in \phi(H_1) \neq \emptyset$ et que $e_1 \in \phi^{-1}(H_2) \neq \emptyset$ car on a $\phi(e_1) = e_2$. Pour $a, b \in \phi(H_1)$, on sait qu'il existe $x, y \in H_1$ tels que $\phi(x) = a$ et $\phi(y) = b$. Alors,
$$ab^{-1} = \phi(x)\,\phi(y)^{-1} = \phi(\underbrace{xy^{-1}}_{\in H_1}) \in \phi(H_1),$$
d'où $\phi(H_1)$ est un sous-groupe de G_2. Pour $a, b \in \phi^{-1}(H_2)$, on sait que $\phi(a), \phi(b) \in H_2$ Alors, on a
$$\phi(ab^{-1}) = \underbrace{\phi(a)}_{\in H_2}\,\underbrace{\phi(b)^{-1}}_{\in H_2} \in H_2,$$
d'où $ab^{-1} \in \phi^{-1}(H_2)$ et donc $\phi(H_1)$ est un sous-groupe de G_2.
2. Supposons $H_2 \triangleleft G_2$ et montrons que $\phi^{-1}(H_2) \triangleleft G_2$. Soit un élément $g \in G_1$ quelconque, et soit $h \in \phi^{-1}(H_2)$. Alors,
$$\phi(ghg^{-1}) = \phi(g)\,\phi(h)\,\phi(g)^{-1} \in H_2,$$
car $\phi(h) \in H_2$ et que $H_2 \triangleleft G_2$. Ainsi, $ghg^{-1} \in \phi^{-1}(H_2)$. On a donc $g\,\phi^{-1}(H_2)\,g^{-1} \subseteq \phi^{-1}(H_2)$, quel que soit $g \in G_1$. On en déduit que $\phi^{-1}(H_2)$ est distingué dans G_1.
3. Suppsons ϕ surjective, on a donc l'égalité $\phi(G_1) = G_2$. Supposons de plus que $H_1 \triangleleft G_1$. Montrons que $\phi(H_1)$ est un sous-groupe distingué de G_2. Soit $g \in G_2 = \phi(G_1)$ quelconque, et soit un élément $h \in \phi(H_1)$. Il existe donc $x \in G_1$ et $y \in H_1$ deux éléments tels que $\phi(y) = h$ et $\phi(x) = g$. Ainsi
$$ghg^{-1} = \phi(x)\,\phi(y)\,\phi(x)^{-1} = \phi(xyx^{-1}) \in \phi(H_1)$$
car H_1 distingué dans G_1 et donc $xyx^{-1} \in H_1$. Ainsi $\phi(H_1) \triangleleft G_2$.
4. On considère le morphisme
$$\begin{aligned} f : (\mathbb{R}, +) &\longrightarrow (\mathrm{GL}_2(\mathbb{R}), \cdot) \\ x &\longmapsto \begin{pmatrix} 1 & x \\ 0 & 1 \end{pmatrix}, \end{aligned}$$

et le sous-groupe distingué $\mathbb{R} \lhd \mathbb{R}$. On a

$$\forall x \in \mathbb{R} \setminus \{0\},\ \underbrace{\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}}_{M \in \mathrm{GL}_2(\mathbb{R})} \underbrace{\begin{pmatrix} 1 & x \\ 0 & 1 \end{pmatrix}}_{f(x)} \underbrace{\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}}_{M^{-1} \in \mathrm{GL}_2(\mathbb{R})} = \begin{pmatrix} 1 & 0 \\ x & 1 \end{pmatrix} \notin f(\mathbb{R}).$$

Ainsi, $f(\mathbb{R}) \ntriangleleft \mathrm{GL}_2(\mathbb{R})$.

7 Exercice 7.

Soit G un groupe et soient H, K deux sous-groupes de G. Montrer que $H \cup K$ est un sous-groupe de G si et seulement si on a $H \subseteq K$ ou $K \subseteq H$.

On procède par double implications.

- « $\implies$ ». Supposons que $H \cup K$ soit un sous-groupe de G. Par l'absurde, supposons que $H \not\subseteq K$ et $K \not\subseteq H$. Il existe donc deux éléments $h \in H \setminus K$ et $k \in K \setminus H$. Considérons $hk \in H \cup K$.
  - Si $hk \in H$, alors $h^{-1}(hk) \in H$ et donc $k \in H$, *absurde* !
  - Si $hk \in K$, alors $(hk)k^{-1} \in K$ et donc $h \in K$, *absurde* !

  On en déduit que $H \subseteq K$ ou $K \subseteq H$.
- « $\impliedby$ ». Sans perte de généralité, supposons $H \subseteq K$. Ainsi, on a $H \cup K = K$ qui est un sous-groupe de G.

8 Exercice 8. *Classes à gauche et classes à droite*

Soit H un sous-groupe d'un groupe G. Montrer que l'on a une bijection canonique $G/H \to H\backslash G$.

On note $S^{-1} = \{s^{-1} \mid s \in S\}$ pour un sous-ensemble S de G. Alors nous avons l'égalité $(aH)^{-1} = Ha^{-1}$ et $(Ha)^{-1} = a^{-1}H$. En effet,

$$\begin{aligned}(aH)^{-1} &= \{ah \mid h \in H\}^{-1} \\ &= \{(ah)^{-1} \mid h \in H\} \\ &= \{h^{-1}a^{-1} \mid h \in H\} \\ &= \{ha^{-1} \mid h \in H\} \\ &= Ha^{-1}\end{aligned} \qquad \begin{aligned}(Ha)^{-1} &= \{ha \mid h \in H\}^{-1} \\ &= \{(ha)^{-1} \mid h \in H\} \\ &= \{a^{-1}h^{-1} \mid h \in H\} \\ &= \{a^{-1}h \mid h \in H\} \\ &= a^{-1}H.\end{aligned}$$

Il existe donc une bijection canonique

$$\begin{aligned} f : G/H &\longrightarrow H\backslash G \\ aH &\longmapsto (aH)^{-1} = Ha^{-1}. \end{aligned}$$

9 Exercice 9. *Normalisateur*

Soit $H \leq G$ un sous-groupe d'un groupe G. On dit que x normalise si $xHx^{-1} = H$. On note $\mathrm{N}_G(H)$ l'ensemble des éléments de G qui normalisent H. C'est le normalisateur de H dans G.

1. *Montrer que $\mathrm{N}_G(H)$ est le plus grand sous-groupe de G contenant H et dans lequel H est distingué.*
2. *En déduire que H est distingué dans G si et seulement si on a l'égalité $G = \mathrm{N}_G(H)$.*

1. Commençons par montrer que $\mathrm{N}_G(H)$ est un sous-groupe de G contenant H.
   - ▷ L'élément neutre normalise H, car $eHe^{-1} = H$. D'où, le normalisateur de H est non vide.
   - ▷ Soient x et y deux éléments qui normalisent H. Alors, xy normalise H :
   $$(xy)H(xy)^{-1} = xyHy^{-1}x^{-1} = xHx^{-1} = H.$$
   - ▷ Soit $x \in G$ qui normalise H. Alors x^{-1} normalise H :
   $$x^{-1}Hx = H \iff Hx = xH \iff H = xHx^{-1},$$
   et cette dernière condition est vérifiée car x normalise H.

- ▷ Soit $h \in H$. Alors h normalise H. En effet,

$$hHh^{-1} = Hh^{-1} = H,$$

car $h^{-1} \in H$ et puis car $h \in H$.

On en conclut que $\mathrm{N}_G(H)$ est un sous-groupe de G contenant H.

Par définition de $\mathrm{N}_G(H)$, on a que $H \triangleleft \mathrm{N}_G(H)$: quel que soit x qui normalise H, on a (par définition) $xHx^{-1} = H$.

Il ne reste plus qu'à montrer que tout sous-groupe $N \supseteq H$ tel que $H \triangleleft N$ vérifie $N \subseteq \mathrm{N}_G(H)$. Soit N un tel sous-groupe, et un élément $x \in N$. Ainsi $xHx^{-1} = H$, d'où x normalise H. On a donc bien l'inclusion $N \subseteq \mathrm{N}_G(H)$.

Ceci démontre bien que $\mathrm{N}_G(H)$ est le plus grand sous-groupe de G contenant H et dans lequel H y est distingué.

2. D'une part, si H est distingué dans G, alors le plus grand sous-groupe de G contenant H et dans lequel H est distingué est G.

   D'autre part, si $G = \mathrm{N}_G(H)$, alors tout élément $x \in G$ vérifie l'égalité $xHx^{-1} = H$ et donc $H \triangleleft G$.

10 Exercice 10. *Construction de* $\mathbb{Q}$

Soit $E := \mathbb{Z} \times (\mathbb{Z} \setminus \{0\})$. On définit $\sim$ sur E par $(a, b) \sim (a', b')$ dès lors que $ab' = a'b$.

1. *Montrer que $\sim$ est un relation d'équivalence sur E. Si $(a, b) \in E$, on note $\frac{a}{b}$ son image dans $E/\sim$.*
2. *Munir $E/\sim$ d'une structure de corps telle que $\mathbb{Z}$ s'injecte dans le corps $E/\sim$.*
3. *Similairement, pour un corps $\Bbbk$, construire $\Bbbk(X)$ à partir de l'ensemble $\Bbbk[X]$.*
4. *Construire $\mathbb{Z}$ à partir de $\mathbb{N}$.*

1. On a trois propriétés à vérifier.
   - ▷ Si $(a, b) \in E$, alors $ab = ab$ donc $(a, b) \sim (a, b)$.
   - ▷ Si $(a, b) \sim (a', b')$, alors $ab' = a'b$ et donc $(a', b') \sim (a, b)$.

- ▷ Si $(a, b) \sim (a', b')$ et $(a', b') \sim (a'', b'')$, alors

$$a'ab'b'' = a'a'bb'' = a'ba'b'' = a'ba''b',$$

et donc $a'b'(ab'' - a''b) = 0$. Par anneau intègre, on a une disjonction de cas :

  - si $a' = 0$, alors $a = a'' = 0$;
  - si $b' = 0$, alors ***absurde*** car $b' \in \mathbb{Z} \setminus \{0\}$;
  - si $ab'' - a''b = 0$, alors on a $ab'' = a''b$.

Dans les deux cas, on obtient bien $(a, b) \sim (a'', b'')$.

2. On munit $E/\sim$ de deux opérations « $\oplus$ » et « $\otimes$ ».

- ▷ On pose l'opération $\frac{a}{b} \oplus \frac{c}{d} := \frac{ad+bc}{bd}$ qui est bien définie car, si l'on a $(a, b) \sim (a', b')$, alors

$$\begin{aligned}(ad + bc, bd) \sim (a'd + b'c, b'd) &\iff (ad + bc)b'd = (a'd + b'c)bd \\ &\iff ab'd^2 = a'bd^2,\end{aligned}$$

ce qui est vrai car $(a, b) \sim (a', b')$. On peut procéder symétriquement pour $(c', d') \sim (c, d)$.

- ▷ On pose l'opération $\frac{a}{b} \otimes \frac{c}{d} := \frac{ac}{bd}$ qui est bien définie car, si l'on a $(a, b) \sim (a', b')$, alors

$$(ac, bd) \sim (a'c, b'd) \iff acb'd = a'cbd,$$

ce qui est vrai car $(a, b) \sim (a', b')$. On peut procéder symétriquement pour $(c', d') \sim (c, d)$.

Montrons que $(E/\sim, \oplus, \otimes)$ est un corps.

- ▷ La loi $\oplus$ est associative : on a

$$\tfrac{a}{b} \oplus \left(\tfrac{c}{d} \oplus \tfrac{e}{f}\right) = \left(\tfrac{a}{b} \oplus \tfrac{c}{d}\right) \oplus \tfrac{e}{f} = \tfrac{adf+cbf+ebd}{bdf},$$

par associativité de $+$.

- ▷ La loi $\oplus$ est commutative par commutativité de $+$.
- ▷ La loi $\oplus$ possède un élément neutre $\frac{0}{1} \in E/\sim$.
- ▷ Tout élément $\frac{a}{b}$ possède un symétrique $(\frac{-a}{b})$ pour $\oplus$ par rapport à $\frac{0}{1}$.

- La loi $\otimes$ est associative : on a

$$\tfrac{a}{b} \otimes \left(\tfrac{c}{d} \otimes \tfrac{e}{f}\right) = \left(\tfrac{a}{b} \otimes \tfrac{c}{d}\right) \otimes \tfrac{e}{f} = \tfrac{ace}{bdf},$$

  par associativité de $\times$.
- La loi $\otimes$ est distributive par rapport à $\oplus$, par distributivité de $\times$ par rapport à $+$.
- La loi $\otimes$ possède un élément neutre $\frac{1}{1} \in E/{\sim}$ pour $\otimes$.
- Tout élément non nul $\frac{a}{b}$ possède un inverse $\frac{b}{a}$ par rapport à $\frac{1}{1}$.

On en conclut que $(E/{\sim}, \oplus, \otimes)$ est un corps.

Finalement, on considère l'injection

$$\begin{aligned} f : \mathbb{Z} &\longhookrightarrow E/{\sim} \\ k &\longmapsto \tfrac{k}{1}. \end{aligned}$$

C'est bien une injection car, si $\frac{k}{1} = \frac{k'}{1}$, alors $k \times 1 = k' \times 1$ et donc $k = k'$. On a, de plus, que f est un morphisme de groupes $(\mathbb{Z}, +) \to (E/{\sim}, \oplus)$:

$$f(k) \oplus f(k') = \tfrac{k}{1} \oplus \tfrac{k'}{1} = \tfrac{k+k'}{1} = f(k+k').$$

3. On pose $F := \Bbbk[X] \times (\Bbbk[X] \setminus \{0_{\Bbbk[X]}\})$, et la relation

$$(P, Q) \sim (P', Q') \iff PQ' = P'Q.$$

   Cette relation est une relation d'équivalences (comme pour la question précédente, et car $\Bbbk$ est un anneau intègre). On pose ensuite $\Bbbk(X) := F/{\sim}$. Comme dans la question précédente, on peut donner une structure de corps avec les mêmes définitions (en replaçant les entiers par des polynômes de $\Bbbk$). Les propriétés découlent toutes du fait que $(\Bbbk, +, \times)$ est un corps.
4. On pose $Z := \mathbb{N}^2/{\sim}$, où la relation d'équivalence $\sim$ est définie par

$$(a, b) \sim (a', b') \iff a + b' = b + a'.$$

11 Exercice 11.

Soit $E := \mathbb{C}[X]$ le $\mathbb{C}$-espace vectoriel des polynômes à coefficients dans $\mathbb{C}$ et $P \in \mathbb{C}[X]$ un polynôme de degré $d \in \mathbb{N}^*$.

1. *Montrer que l'ensemble $(P) := \{QP \mid Q \in \mathbb{C}[X]\}$ est un sous-$\mathbb{C}$-espace vectoriel de $\mathbb{C}[X]$.*
2. *Déterminer un isomorphisme entre $\mathbb{C}[X]/(P)$ et le $\mathbb{C}$-espace vectoriel $\mathbb{C}_{d-1}[X]$ des polynômes de degrés inférieurs à $d-1$ de $\mathbb{C}[X]$.*
3. *Montrer que la multiplication dans $\mathbb{C}[X]$ induit une structure de $\mathbb{C}$-algèbre sur $\mathbb{C}[X]/(P)$.*

12 Exercice 12.

Soit G un groupe et H un sous-groupe strict de G. Montrer que l'on a l'égalité $\langle G \setminus H \rangle = G$.

13 Exercice 13.

Soit G un groupe fini. Montrer que G contient un élément d'ordre 2 si et seulement si son cardinal est pair. Montrer de plus que, dans ce cas là, il en contient un nombre impair.

14 Exercice 14.

Soit G un groupe et $\sim$ une relation d'équivalence sur G. On suppose que $G/\sim$ est un groupe, et que la projection canonique $\pi : G \to G/\sim$ est un morphisme de groupes.

Montrer qu'il existe un sous-groupe distingué $H \lhd G$ tel que pour tous éléments $x, y \in G$, $x \sim y$ si et seulement si $xy^{-1} \in H$.

15 Exercice 15.

Soit G un groupe et S_G l'ensemble des sous-groupes de G.

1. *Démontrer que si G est fini, alors S_G est fini.*
2. *Supposons S_G fini. Démontrer que tous les éléments de G sont d'ordre fini, en déduire que G est fini.*
3. *On ne suppose plus que S_G est fini. Si tous les éléments de G sont d'ordre fini, est-ce que G est fini ?*

Table des matières