Généralités sur les groupes

Travaux dirigés du 16 et du 19 septembre 2025

Exercice 1. Quelques cas où l'existence des inverses est automatique

1. *Quand les monoïdes sont des groupes.* On rappelle qu'un *monoïde* est un ensemble M muni d'une loi de composition interne associative $*$ et d'un élément neutre e (e est nécessairement unique).

   (a) Montrer qu'un monoïde M dont tout élément possède un inverse à gauche est un groupe.
   Soit $x \in M$, soit y un inverse à gauche de x (c'est-à-dire que $y * x = e$). Il s'agit de montrer que $x * y = e$. En multipliant la relation $y * x = e$ par x à gauche et par y à droite, on obtient $x * (y * x) * y = x * y$, soit (par associativité) $(x * y) * (x * y) = x * y$. On conclut que $x * y = e$ en multipliant à gauche par un inverse à gauche de l'élément $x * y$.

   (b) On dit qu'un monoïde M est *simplifiable à gauche* si pour tous $x, y, z \in M$, on a

   $$x * y = x * z \Longrightarrow y = z\,.$$

   Montrer que l'on ne peut pas généraliser le résultat du (a) aux monoïdes simplifiables à gauche.
   On parle de généralisation car à la fin de la solution de la question précédente, on a simplifié à gauche en multipliant par un inverse à gauche de ce par quoi on voulait simplifier. Néanmoins, quand on n'a plus d'inverse à gauche explicite à exhiber, ça ne marche plus : regarder par exemple $(\mathbb{N}, +)$, $(\mathbb{N}^*, \times)$, les suites finies munies de la concaténation ou encore $(A - \{0\}, \times)$ pour tout anneau A intègre (voir le 2) qui n'est pas un corps (exemple : $A = K[X]$, K un corps).

   (c) Montrer que c'est quand même possible si on suppose ces monoïdes finis.
   Soit $x \in M$, on regarde l'ensemble des x^k pour $k \in \mathbb{N}$. Cet ensemble est fini car inclus dans M. On trouve donc $k, l \in \mathbb{N}$ avec $k < l$ tels que $x^k = x^l = x^k x^{l-k}$. En simplifiant à gauche par x^k, on obtient

   $$e = x^{l-k} = x * x^{l-k-1} = x^{l-k-1} * x$$

   donc x est inversible d'inverse x^{l-k-1}.

   (d) Que se passe-t-il à droite ?
   La même chose !

2. *Quand les anneaux sont des corps gauches.* On rappelle qu'un anneau A est dit *intègre* si pour tous $a, b \in A$ on a

   $$ab = 0 \Longrightarrow (a = 0 \text{ ou } b = 0)\,.$$

   Montrer qu'un anneau intègre fini est un corps gauche.
   Il suffit de remarquer que le monoïde $(A^*, \times)$ est simplifiable à gauche et fini.

3. *Quand les sous-ensembles sont des sous-groupes.* Montrer que si G est un groupe, et si H est une partie finie non vide de G stable par la loi de G, alors H est un sous-groupe de G. Montrer que l'hypothèse de finitude de H est nécessaire.
   On regarde $(H, \times_G)$, c'est un monoïde fini et simplifiable à gauche (car il vit dans un groupe), donc c'est un groupe et H est un sous-groupe de G. Si H est infini, ce n'est plus vrai : regarder $G = (\mathbb{Z}, +)$ et $H = \mathbb{N}$.

Exercice 2. Monoïdes monogènes

Soient $n \geq 1$ un entier et $F(n)$ le monoïde des fonctions de $[\![0, n-1]\!]$ dans lui-même pour la composition $\circ$. Pour $0 \leq i < n$, on note $f_i \in F(n)$ la fonction définie par $f_i(j) = j + 1$ pour $0 \leq j < n - 1$ et $f_i(n-1) = i$.

1. On pose $M_i = \langle f_i \rangle$. Montrer $|M_i| = n$.
   Observons que f_i est un cycle de longueur $n-i$ sur $\{i, i+1, \ldots, n-1\}$, et que l'on a $f_i(\{0, 1, \ldots, n-1\}) \subseteq \{i, i+1, \ldots, n-1\}$. On en déduit $f_i^n = f_i^{n-i} f_i^i = f_i^i$, puis $M_i = \{f_i^k \mid 0 \leq k < n\}$. De plus, les éléments f_i^k avec $k = 0, \ldots, n-1$ sont distincts, car on a $f_i^k(0) = k$. On a montré $|M_i| = n$.

2. (suite) Montrer $M_i \simeq M_j \Longleftrightarrow i = j$.
   Si M est un monoïde, posons $M(n) = \{m^k \mid m \in M - \{1\}, k \geq n\}$. On constate que l'on a $M_i(n) = \{f_i^k \mid k \geq i\}$, et donc $|M_i(n)| = n - i$. Mais tout isomorphisme $M \xrightarrow{\sim} N$ induit une bijection $M(n) \simeq N(n)$. Ainsi, si on a $M_i \simeq M_j$, on a $n - i = n - j$, puis $i = j$.

3. Montrer qu'à isomorphisme près, il existe exactement n monoïdes monogènes de cardinal n.
   Supposons $M = \langle x \rangle$ et $|M| = n$. Les éléments $1, x, x^2, \dots, x^{n-1}$ sont distincts. En effet, si on a $x^j = x^i$ avec $0 \leq i < j \leq n-1$, une récurrence montre que pour tout entier $a \geq i$, l'élément x^a est de la forme x^b avec $i \leq b < j$. En particulier, on a $|M| \leq i + j - i \leq j < n$, une contradiction. On a donc $M = \{x_i \mid 0 \leq i < n\}$. Ainsi, il existe un unique entier $0 \leq i < n$ avec $x^n = x^i$. On peut vérifier à la main qu'il existe un (unique) isomorphisme $M \to M_i$ envoyant x sur f_i. On peut aussi procéder comme suit. Pour tout monoïde M, on dispose d'un morphisme naturel à la Cayley de M dans $(M^M, \circ)$, à savoir $m \mapsto L_m$ avec $L_m(n) = mn$. Il est injectif, car on a $L_m(1) = m$. Il identifie donc M à un sous-monoïde de M^M. Revenons à $M = \langle x \rangle$ comme ci-dessus et identifions l'ensemble M à $\{0, 1, \dots, n-1\}$ via $j \mapsto x^j$, de sorte que M^M s'identifie à l'ensemble $F(n)$ des applications de $\{0, 1, \dots, n-1\}$ dans lui-même. On constate que L_x n'est rien d'autre que la fonction f_i. Ainsi, on a construit un morphisme injectif $M \to F(n)$ d'image M_i, donc un isomorphisme $M \simeq M_i$. À isomorphisme près, les n monoïdes monogènes sont donc les M_i, $0 \leq i < n$.

Exercice 3. Monoïdes de cardinal ≤ 3

1. Montrer qu'à isomorphisme près, il existe exactement 2 monoïdes de cardinal 2, à savoir $(\mathbb{Z}/2\mathbb{Z}, +)$ et $(\mathbb{Z}/2\mathbb{Z}, \times)$.
   Soit M un monoïde de cardinal 2. On a $M = \{1, x\}$ avec $x \neq 1$. Si $x^2 = 1$, alors M est un groupe d'ordre 2, isomorphe à $(\mathbb{Z}/2\mathbb{Z}, +)$. Si $x^2 = x$, on constate que la bijection $(\mathbb{Z}/2\mathbb{Z}, \times) \to M$ envoyant 1 sur 1 et 0 sur x est un morphisme de monoïdes. Enfin, on sait que $(\mathbb{Z}/2\mathbb{Z}, +)$ et $(\mathbb{Z}/2\mathbb{Z}, \times)$ ne sont pas isomorphes car $(\mathbb{Z}/2\mathbb{Z}, \times)$ n'est pas un groupe.
2. Soit M un monoïde à 3 éléments. Montrer que soit M est monogène, soit on a $M \simeq (\mathbb{Z}/3\mathbb{Z}, \times)$, soit on a $x^2 = x$ pour tout $x \in M$.
   Soit M de cardinal 3 non monogène. Soit $x \in M$ avec $x \neq 1$. On a $x^2 \in \{1, x\}$. Soit y l'unique élément tel que l'on ait $M = \{1, x, y\}$. Supposons d'abord $x^2 = 1$, i.e. x inversible d'inverse x. Vérifions $xy = y = yx$. En effet, $xy = 1$ implique $y = x$ (absurde), de même pour $yx = 1$, $xy = x$ implique $y = 1$ (absurde) et de même pour $yx = x$. On constate alors que la bijection $(\mathbb{Z}/3\mathbb{Z}, \times) \to M$ envoyant 1 sur 1, -1 sur x, et 0 sur y est un morphisme de monoïdes. Cela montre aussi qu'un tel M existe, car $M = (\mathbb{Z}/3\mathbb{Z}, \times)$ a les propriétés requises. Dans le dernier cas, on a donc $x^2 = x$ pour tout $x \neq 1$, et même $x^2 = x$ pour tout x.
3. En déduire qu'à isomorphisme près, il existe exactement 7 monoïdes de cardinal 3.
   Supposons donc $M = \{1, x, y\}$ de cardinal 3 avec $x^2 = x$ et $y^2 = y$. On a $xy \neq 1$, car $xy = 1$ implique par exemple $x = x^2y = xy = 1$. On a donc $\{xy, yx\} \subseteq \{x, y\}$, et il y a au plus 4 cas. Soit $xy = x$ et $yx = y$. Dans ce cas, on constate que l'on a $ab = a$ pour tout $a, b \in M$ avec $a, b \neq 1$. Soit $xy = y$ et $yx = x$. Dans ce cas, on constate que l'on a $ab = b$ pour tout $a, b \in M$ avec $a, b \neq 1$. Soit $xy = x$ et $yx = x$, ou $xy = y$ et $yx = y$. Ces deux cas sont isomorphes comme on le voit en échangeant x et y. Les 3 cas ci-dessus ne sont pas isomorphes entre eux s'ils existent, par les constatations. Il y a donc au plus 3 tels monoïdes. Pour voir que ces 3 cas existent, on peut continuer l'analyse-synthèse et voir que par le morphisme de Cayley $M \to (M^M, \circ)$, $m \mapsto L_m$, ces trois monoïdes se plongent dans $F(3)$ (exercice précédent) s'ils existent. On va donc regarder l'image de $\{1, x, y\}$ dans $F(3)$ en identifiant (pour fixer les idées) 1 à 0, x à 1 et y à 2.
   - Dans le cas $xy = x$ et $yx = y$, c'est $\{\mathrm{id}, 1, 2\}$ qui est bien un monoïde
   - Dans le cas $xy = y$ et $yx = x$, c'est $\{\mathrm{id}, f, g\}$ avec d'une part f qui envoie 0 sur 1 et les autres sur eux-mêmes et d'autre part g qui envoie 0 sur 2 et les autres sur eux-mêmes ; c'est bien un monoïde.
   - Dans le cas $xy = x$ et $yx = x$, c'est $\{\mathrm{id}, 1, h\}$ où h est l'application qui envoie 0 sur 2 et les autres sur eux-mêmes ; c'est bien un monoïde.

   Donc les monoïdes hypothétiques sont en bijection avec des monoïdes concrets, d'une manière compatible avec les lois de composition : ils existent.

Exercice 4. L'argument de Eckmann-Hilton

Soit X un ensemble muni de deux lois unitaires $\circ$ et $\star$ avec $(x \circ y) \star (z \circ t) = (x \star z) \circ (y \star t)$ pour tout $x, y, z, t \in X$.

Montrer $\circ = \star$, et que ces lois sont associatives et commutatives.

Soient $1_\star$ et $1_\circ$ les neutres de $(X, \star)$ et $(X, \circ)$. On a $1_\star = 1_\star \star 1_\star = (1_\star \star 1_\circ) \star (1_\circ \circ 1_\star) = (1_\star \star 1_\circ) \circ (1_\circ \star 1_\star) = 1_\circ \circ 1_\circ = 1_\circ$. On pose $1 = 1_\star = 1_\circ$. Pour $x, y \in X$ on a $x \star y = (x \circ 1) \star (1 \circ y) = (x \star 1) \circ (1 \star y) = x \circ y$: les deux lois sont égales, on les note $xy = x \star y = x \circ y$. On a donc $(xy)(zt) = (xz)(yt)$ pour tout $x, y, z, t \in X$. Pour $z = 1$, c'est l'associativité. Pour $x = t = 1$, c'est la commutativité. (Ce lemme est moins futile qu'il n'en a l'air, et sert par exemple en topologie algébrique !)

Exercice 5. Un cas où la commutativité est automatique

On dit que l'*exposant* d'un groupe G est le plus petit entier $n \geq 1$ tel que pour tout $x \in G$, on ait $x^n = 1$. Montrer qu'un groupe d'exposant 2 est abélien.

Soit G un groupe d'exposant 2, soit $x, y \in G$, montrons que $xy = yx$. On a $xyxy = (xy)^2 = e$, donc en multipliant à gauche par x et à droite par y, on obtient ce qu'on voulait.

Exercice 6. Des exemples concrets

1. Décrire les sous-groupes non denses de $\mathbb{R}$.
   Soit G un sous-groupe non dense de $\mathbb{R}$. Supposons G non trivial et regardons $\alpha = \inf(G \cap \mathbb{R}_+^*)$. On va utiliser le fait que si $x \in \mathbb{R}$ et $\beta \in \mathbb{R}_+^*$, on a $0 \leq x - \lfloor \frac{x}{\beta} \rfloor \beta < \beta$. Si $\alpha = 0$, on trouve une suite (β_n) d'éléments de $G \cap \mathbb{R}_+^*$ qui tend vers 0, et pour tout $x \in \mathbb{R}$, la suite $(\lfloor \frac{x}{\beta_n} \rfloor \beta_n)$ d'éléments de G tend vers x, ce qui contredit la non-densité de G. Donc on a $\alpha > 0$. Si $\alpha \notin G$, on trouve des suites (γ_n) et (γ'_n) de $G \cap \mathbb{R}_+^*$ qui tendent vers α par valeurs supérieures et telles que pour tout n, $\gamma'_n < \gamma_n$ (construire d'abord (γ_n), puis (γ'_n)). Alors la suite $(\gamma_n - \gamma'_n)$ d'éléments de $G \cap \mathbb{R}_+^*$ tend vers 0 et on conclut comme dans le cas $\alpha = 0$ que G est dense : absurde. Donc $\alpha \in G \cap \mathbb{R}_+^*$. Maintenant, pour tout élément x de G on peut écrire $x = \lfloor \frac{x}{\alpha} \rfloor \alpha + \eta$ avec $0 \leq \eta < \alpha$, mais comme $x \in G$, on a $\eta \in G$ et donc $\eta = 0$. On a donc $G \subseteq \alpha\mathbb{Z}$. Comme l'inclusion réciproque est vraie, on a $G = \alpha\mathbb{Z}$. En rajoutant le cas trivial, on conclut que les sous-groupes non denses de $\mathbb{R}$ sont les $\alpha\mathbb{Z}$, $\alpha \in \mathbb{R}$.
2. Décrire les morphismes de groupes surjectifs de $(\mathbb{Q}, +)$ dans $(\mathbb{Q}^*, \times)$.
   Soit f un tel morphisme. Soit $\alpha \in \mathbb{Q}$ un antécédent de -1 par f. On a $0 \leq f(\alpha/2)^2 = f(\alpha) = -1$: contradiction (on aurait aussi pu regarder, par exemple, un antécédent de 2). Il n'y a donc aucun morphisme de groupes surjectif de $(\mathbb{Q}, +)$ dans $(\mathbb{Q}^*, \times)$. Remarque : on a utilisé le fait que $(\mathbb{Q}, +)$ était un groupe *divisible*, contrairement à $(\mathbb{Q}^*, \times)$.

Exercice 7. Produit de sous-groupes

Soient G un groupe et H, K deux sous-groupes de G. On considère l'application

$$f : H \times K \to G, \quad (h, k) \mapsto hk.$$

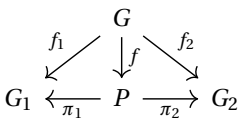
On note $\mathrm{Im} f = HK$.

1. Donner une condition nécessaire et suffisante portant sur H et K pour que f soit respectivement : un morphisme de groupes ; injective ; un isomorphisme de groupes.
   Par définition de la loi du groupe produit $H \times K$, f est un morphisme de groupes si et seulement si pour tout $h, h' \in H$ et tout $k, k' \in K$ on a $hh'kk' = hkh'k'$. Il est équivalent de demander que pour tout $h \in H$ et tout $k \in K$ on ait $hk = kh$, autrement dit tout élément de H commute avec tout élément de K. Supposons maintenant l'application f injective et soit $h \in H$, $k \in K$. On remarque que $f(h, 1) = h$ et $f(1, k) = k$, donc l'injectivité de f implique que si $h = k$, alors $h (= k) = 1$. On a montré que si f est injective alors $H \cap K = \{1\}$. Réciproquement, si $H \cap K = 1$ et il existe $h, h' \in H$ et $k, k' \in K$ tels que $hk = h'k'$, on a $h^{-1}h' = k(k')^{-1} \in H \cap K$, donc $h^{-1}h' = k(k')^{-1} = 1$ et $h = h'$, $k = k'$ d'où l'injectivité de f. Enfin, comme l'application f est surjective si et seulement si on a $G = HK$, f est un isomorphisme de groupes si et seulement si $hk = kh$ pour tout $(h, k) \in H \times K$, $H \cap K = \{1\}$ et $G = HK$.
2. On suppose H et K finis. Montrer $|HK| = \frac{|H||K|}{|H \cap K|}$.
   Comme $HK = \mathrm{Im} f$, les $f^{-1}(g)$ pour $g \in HK$ forment une partition de $H \times K$ et on a $|H||K| = |H \times K| = \sum_{g \in HK} |f^{-1}(g)|$. Il suffit pour conclure de montrer que toutes les fibres de f ont même cardinal $|H \cap K|$. Fixons $(h, k) \in H \times K$. Supposons que $(h', k') \in H \times K$ vérifie $h'k' = hk$. Alors l'élément $z := h^{-1}h' = k(k')^{-1}$ est dans $H \cap K$, et on a $(h', k') = (hz, z^{-1}k)$. Réciproquement, pour tout $z \in H \cap K$, l'élément $(h', k') = (hz, z^{-1}k)$ vérifie $h'k' = hzz^{-1}k = hk$. Ainsi, la fibre de f au dessus de $f(h, k) = hk$ est constituée des $|H \cap K|$ éléments de la forme $(hz, z^{-1}k)$ avec $z \in H \cap K$, ce qui conclut.

Exercice 8. Propriété universelle du produit

Soit G_1 et G_2 des groupes. Pour tout groupe P muni de morphismes $\pi_1 : P \to G_1$ et $\pi_2 : P \to G_2$, on peut considérer la propriété suivante, que l'on notera $\mathscr{P}(P; \pi_1, \pi_2)$:

≪ Pour tout groupe G et tous morphismes $f_1 : G \to G_1$ et $f_2 : G \to G_2$, il existe un unique morphisme $f : G \to P$ tel que le diagramme

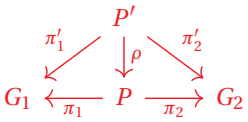


commute. ≫

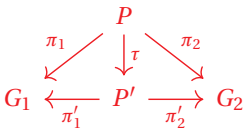
1. Se convaincre que pour $i \in \{1, 2\}$, la projection canonique $\mathrm{pr}_i : G_1 \times G_2 \to G_i$, $(g_1, g_2) \mapsto g_i$ est un morphisme de groupes, puis que $\mathscr{P}(G_1 \times G_2; \mathrm{pr}_1, \mathrm{pr}_2)$ est vraie.

2. Soit P (resp. P') un groupe muni de morphismes $\pi_i : P \to G_i$ (resp. $\pi'_i : P' \to G_i$) pour $i \in \{1,2\}$. On suppose que $\mathscr{P}(P;\pi_1,\pi_2)$ et $\mathscr{P}(P';\pi'_1,\pi'_2)$ sont vraies. Montrer qu'il existe un unique isomorphisme $\rho : P' \to P$ compatible avec les projections, c'est-à-dire tel que $\pi'_i = \pi_i \circ \rho$ pour $i \in \{1,2\}$.

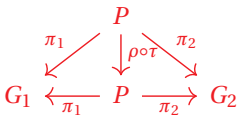
   La propriété $\mathscr{P}(P;\pi_1,\pi_2)$ appliquée avec $G = P'$ et $f_i = \pi'_i$ fournit l'existence d'un unique morphisme $\rho : P' \to P$ compatible avec les projections :



   De même, on a l'existence d'un morphisme τ faisant commuter le diagramme suivant :



   On a donc le diagramme commutatif suivant :



   Mais le morphisme identité fait également commuter ce dernier diagramme. On en conclut par unicité que $\rho \circ \tau = \mathrm{id}$. De même, on trouve $\tau \circ \rho = \mathrm{id}$, et donc ρ est un isomorphisme d'inverse τ.