Corrigé de la Série 3

1.4. Nombres rationnels

1. Montrez que pour $m, n \in \mathbb{Z}$,

$$mn = 0 \quad \Leftrightarrow \quad n = 0 \text{ ou } m = 0.$$

(Indication: observer que pour $(a, b) \in \mathbb{N}^2$, alors $(a, b) \sim (d, 0)$ ou $(a, b) \sim (0, d)$ avec $d \in \mathbb{N}$.)

$m, n \in \mathbb{Z}$ signifie que $m = [(a_m, b_m)]$ et $n = [(a_n, b_n)]$. Pour tout couple $(a, b) \in \mathbb{N}^2$, on a soit $(a, b) \sim (d, 0)$ si $a = b + d$, soit $(a, b) \sim (0, d)$ si $b = a + d$. Ainsi,

$$m \times n = [(a_m, b_m)] \times [(a_n, b_n)] = \begin{cases} [(d_m d_n, 0)] & \text{si } (a_m, b_m) \sim (d_m, 0) \text{ et } (a_n, b_n) \sim (d_n, 0), \\ [(0, d_m d_n)] & \text{si } (a_m, b_m) \sim (d_m, 0) \text{ et } (a_n, b_n) \sim (0, d_n), \\ [(d_m d_n, 0)] & \text{si } (a_m, b_m) \sim (0, d_m) \text{ et } (a_n, b_n) \sim (0, d_n), \\ [(0, d_m d_n)] & \text{si } (a_m, b_m) \sim (0, d_m) \text{ et } (a_n, b_n) \sim (d_n, 0). \end{cases}$$

Dans tous les cas on a

$$m \times n = [(0, 0)] \quad \Leftrightarrow \quad (a_m, b_m) \sim (0, 0) \text{ ou } (a_n, b_n) \sim (0, 0),$$

i.e. $m \times n = 0 \Leftrightarrow m = 0$ ou $n = 0$.

2. Vérifier que $\sim'$ est une relation d'équivalence sur $\mathbb{Z} \times \mathbb{Z}^*$.

(a) $\sim'$ est réflexif. En effet, Pour $(m, n) \in \mathbb{Z} \times \mathbb{Z}^*$ on a $mn = nm$ par la commutativité du produit sur $\mathbb{Z}$. Ainsi, $(m, n) \sim' (m, n)$.

(b) $\sim'$ est symétrique. En effet, pour $(m, n), (k, l) \in \mathbb{Z} \times \mathbb{Z}^*$, on a

$$(m, n) \sim' (k, l) \Leftrightarrow ml = kn \Leftrightarrow kn = ml \Leftrightarrow (k, l) \sim' (m, n).$$

(c) $\sim'$ est transitif. En effet, pour $(m, n), (k, l), (a, b) \in \mathbb{Z} \times \mathbb{Z}^*$, on a

$$\begin{gathered} (m, n) \sim' (k, l) \text{ et } (k, l) \sim' (a, b) \\ \Leftrightarrow \quad ml = kn \text{ et } kb = al \\ \Leftrightarrow \quad mlb = knb \text{ et } kb = al \ (\times \text{ sur } \mathbb{Z} \text{ possède la propriété de simplification}) \\ \Leftrightarrow \quad mlb = anl \text{ et } kb = al \\ \Leftrightarrow \quad mb = an \text{ et } kb = al \ (\times \text{ sur } \mathbb{Z} \text{ possède la propriété de simplification}) \\ \Rightarrow \quad (m, n) \sim' (a, b). \end{gathered}$$

3. Montrer que

$$\forall (a, b), (c, d) \in \mathbb{Z} \times \mathbb{Z}^*, \quad [(a, b)] = [(c, d)] \Leftrightarrow (a, b) \sim' (c, d).$$

Supposons que $(a,b) \sim' (c,d)$. Soit $(k,l) \in [(a,b)]$. Par définition, on a donc que $(k,l) \sim' (a,b)$. Par transitivité, on a donc que $(k,l) \sim' (c,d)$, c'est-à-dire que $(k,l) \in [(c,d)]$. On en conclut que $[(a,b)] \subset [(c,d)]$.
Soit $(k,l) \in [(c,d)]$. Par définition, on a donc que $(k,l) \sim' (c,d)$. Puisque $\sim'$ est symétrique et qu'on a supposé $(a,b) \sim' (c,d)$, on a aussi $(c,d) \sim' (a,b)$. Par transitivité, on a donc que $(k,l) \sim' (a,b)$, c'est-à-dire que $(k,l) \in [(a,b)]$. On en conclut que $[(c,d)] = [(a,b)]$.
Supposons maintenant que que $[(c,d)] = [(a,b)]$. Comme $\sim'$ est réflexive, on a $(a,b) \sim' (a,b)$, ou encore que $(a,b) \in [(a,b)]$. L'égalité des deux classes d'équivalence nous conduit alors à $(a,b) \sim' (c,d)$.

4. Vérifier que les opérations $+$ et $\times$ font de $\mathbb{Q}$ un corps commutatif.

Pour $p,q,r \in \mathbb{Q}$ on pose $p = [(m_p,n_p)]$, $q = [(m_q,n_q)]$ et $p = [(m_r,n_r)]$.

(a) L'opération $+$ fait de $\mathbb{Q}$ un groupe abélien.

i.

$$\begin{aligned} p+q &= [(m_p,n_p)] + [(m_q,n_q)] = [(m_pn_q + m_qn_p, n_pn_q)] \\ &= [(m_qn_p + m_pn_q, n_qn_p)] = [(m_q,n_q)] + [(m_p,n_p)] = q+p, \end{aligned}$$

où nous avons utilisé la commutativité de la somme et du produit sur $\mathbb{Z}$.

ii.

$$\begin{aligned} (p+q)+r &= \big([(m_p,n_p)] + [(m_q,n_q)]\big) + [(m_r,n_r)] \\ &= [(m_pn_q + m_qn_p, n_pn_q)] + [(m_r,n_r)] \\ &= [\big((m_pn_q + m_qn_p)n_r + m_rn_pn_q, n_pn_qn_r\big)] \\ &= [\big(m_pn_qn_r + n_p(m_qn_r + n_qm_r), n_pn_qn_r\big)] \\ &= [(m_p,n_p)] + [(m_qn_r + m_qn_r, n_qn_r)] \\ &= [(m_p,n_p)] + \big([(m_q,n_q)] + [(m_r,n_r)]\big) = p + (q+r), \end{aligned}$$

où nous avons utilisé la commutativité de la somme et du produit sur $\mathbb{Z}$, ainsi que la distributivité de ce dernier sur la première.

iii. En identifiant 0 à la classe $[(0,1)]$ on trouve

$$p + 0 = [(m_p,n_p)] + [(0,1)] = [(m_p,n_p)] = p,$$

et la commutativité de la somme, déjà vérifiée, nous conduit aussi à $0+p = p$. Ainsi 0 est l'élément neutre pour l'addition.

iv. En identifiant $-p$ à la classe $[(-m_p,n_p)]$, (avec $-m_p = [(b_{m_p}, a_{m_p})]$ si $m_p = [(a_{m_p}, b_{m_p})]$ dans $\mathbb{Z}$) on trouve

$$\begin{aligned} p + (-p) &= [(m_p,n_p)] + [(-m_p,n_p)] \\ &= [(m_pn_p + (-m_p)n_p, n_p^2)] = [(n_p(m_p + (-m_p))n_p^2)] \\ &= [(0,n_p^2)] = [(0,1)] = 0, \end{aligned}$$

où nous avons utilisé la commutativité du produit et la distributivité de ce dernier sur la somme dans $\mathbb{Z}$, ainsi que $(0,n) \sim' (0,1)$ pour tout $n \in \mathbb{Z}$. Ainsi, $-p$ est l'opposé de p dans $\mathbb{Q}$.

(b) L'opération $\times$ fait de $\mathbb{Q}^*$ un groupe abélien.

i.

$$\begin{aligned} p \times q &= [(m_p, n_p)] \times [(m_q, n_q)] = [(m_p m_q, n_p n_q)] \\ &= [(m_q m_p, n_q n_p)] = [(m_q, n_q)] \times [(m_p, n_p)] = q \times p, \end{aligned}$$

où nous avons utiliser la commutativité du produit sur $\mathbb{Z}$.

ii.

$$\begin{aligned} p \times \big(q \times r\big) &= [(m_p, n_p)] \times \big([(m_q, n_q)] \times [(m_r, n_r)]\big) \\ &= [(m_p, n_p)] \times [(m_q m_r, n_q n_r)] = [(m_p m_q m_r, n_p n_q n_r)] \\ &= [(m_p m_q, n_p n_q)] \times [(m_r, n_r)] \\ &= \big([m_p, m_p)] \times [(m_q, n_q)]\big) \times [(m_r, n_r)] = \big(p \times q\big) \times r, \end{aligned}$$

où nous avons utiliser la commutativité et l'associativité du produit sur $\mathbb{Z}$.

iii. En identifiant 1 à la classe $[(1,1)]$ on trouve

$$p \times 1 = [(m_p, n_p)] \times [(1,1)] = [(m_p, n_p)] = p,$$

et la commutativité du produit, déjà vérifiée, nous conduit aussi à $1 \times p = p$. Ainsi 1 est l'élément neutre pour le produit.

iv. En identifiant p^{-1} à la classe $[(n_p, m_p)]$ pour $p \in \mathbb{Q}^*$, (remarquer que $p \neq 0 \Leftrightarrow m_p \neq 0$, d'où $(n_p, m_p) \in \mathbb{Z} \times \mathbb{Z}^*$) on trouve

$$\begin{aligned} p \times p^{-1} &= [(m_p, n_p)] \times [(n_p, m_p)] \\ &= [(m_p n_p, n_p m_p)] = [(n_p m_p, n_p m_p)] = [(1,1)] = 1, \end{aligned}$$

où nous avons utilisé la commutativité du produit de $\mathbb{Z}$, le fait que $n_p \neq 0 \neq m_p$ dans $\mathbb{Z}$ implique $m_p n_p \neq 0$, ainsi que $(m,m) \sim' (1,1)$ pour tout $m \in \mathbb{Z}^*$. Ainsi, p^{-1} est l'inverse de $p \in \mathbb{Q}^*$.

(c) Le produit se distribue sur l'addition dans $\mathbb{Q}$. En effet,

$$\begin{aligned} p \times (q + r) &= [(m_p, n_p)] \times \big([(m_q, n_q)] + [(m_r, n_r)]\big) \\ &= [(m_p, n_p)] \times [(m_q n_r + m_r n_q, n_q n_r)] \\ &= [(m_p(m_q n_r + m_r n_q), n_p n_q n_r)] \\ &= [(m_p m_q n_r, n_p n_q n_r)] + [(m_p m_r n_q, n_p n_q n_r)] \\ &= [(m_p m_q, n_p n_q)] + [(m_p m_r, n_p n_r)] = (q \times q) + (p \times r), \end{aligned}$$

où nous avons utilisé la distributivité du produit sur l'addition dans $\mathbb{Z}$ et le fait que pour $n \in \mathbb{Z}$ et $m, a \in \mathbb{Z}^*$, $(na, ma) \sim' (n, m)$, grâce à la propriété de simplification du produit dans $\mathbb{Z}$.

5. Montrer les affirmations suivantes:

(a) $\mathbb{Q} = \mathbb{Q}_-^* \cup \{0\} \cup \mathbb{Q}_+^*$ et cette union est disjointe.

(b) Si $p, q \in \mathbb{Q}$, alors $pq = 0 \in \mathbb{Q}$ ssi $p = 0$ ou $q = 0$.

(c) Le produit $\times$ sur $\mathbb{Q}$ est compatible avec la prise de l'opposé de $+$, i.e. $-(pq) = (-p)q$.

(d) Le produit $\times$ sur $\mathbb{Q}^*$ est compatible avec la prise de l'inverse de $\times$, i.e. $(pq)^{-1} = p^{-1}q^{-1}$.

(e) L'ordre $<$ sur $\mathbb{Q}$ defini par $p < q \Leftrightarrow q - p \in \mathbb{Q}_+^*$ est total.

(a) Un élément de $\mathbb{Q}$ est donc une classe d'équivalence $[(a, b)]$ avec $(a, b) \in \mathbb{Z} \times \mathbb{Z}^*$. Le nombre $ab \in \mathbb{Z} = \mathbb{Z}_-^* \cup \{0\} \cup \mathbb{Z}_+^*$ et cette union est disjointe, comme on l'a vu au cours. Ainsi, $[(a, b)]$ est soit élément de $\mathbb{Q}_-^*$ (quand $ab \in \mathbb{Z}_-^*$), soit égale à 0 (quand $ab = 0$), soit élément de $\mathbb{Q}_+^*$(quand $ab \in \mathbb{Z}_+^*$).

(b) Posons $p = [(a_p, b_p)]$, $q = [(a_q, b_q)]$ avec $(a_p, b_p), (a_q, b_q) \in \mathbb{Z} \times \mathbb{Z}^*$. Alors,

$$\begin{aligned} pq = 0 \quad &\Leftrightarrow \quad [(a_p, b_p)] \times [(a_q, b_q)] = [(0, 1)] \\ \Leftrightarrow \quad [(a_pa_q, b_pb_q)] = [(0, 1)] \quad &\Leftrightarrow \quad (a_pa_q, b_pb_q) \sim' (0, 1) \\ \Leftrightarrow \quad a_pa_q = 0 \quad &\Leftrightarrow \quad a_p = 0 \text{ ou } a_q = 0 \text{ (intégrité de } \mathbb{Z}) \\ \Leftrightarrow \quad (a_p, b_p) \sim' (0, 1) \text{ ou } (a_q, b_q) \sim' (0, 1) \quad &\Leftrightarrow \quad p = 0 \text{ ou } q = 0. \end{aligned}$$

(c)

$$\begin{aligned} -(pq) &= 0 + (-(pq)) = 0 \times q + (-(pq)) = (p - p)q + (-(pq)) \\ &= pq + (-p)q + (-(pq)) = pq + (-pq) + (-p)q = 0 + (-p)q = (-p)q. \end{aligned}$$

(Remarquons qu'on ajuste utilisé les règles générales d'un corps commutatif, sans utiliser la structure spécifique des nombres rationnels.)

(d) Pour $p, q \in \mathbb{Q}^*$ on a

$$(pq)^{-1} = 1 \times (pq)^{-1} = pp^{-1}qq^{-1} \times (pq)^{-1} = p^{-1}q^{-1}pq(pq)^{-1} = p^{-1}q^{-1}.$$

(Remarquons qu'on ajuste utilisé les règles générales d'un corps commutatif, sans utiliser la structure spécifique des nombres rationnels.)

(e) Comme $p - q \in \mathbb{Q}_-^* \cup \{0\} \cup \mathbb{Q}_+^*$ et que cette union est disjointe, on a soit $p - q \in \mathbb{Q}_+^* \Leftrightarrow p > q$, soit $p - q = 0 \Leftrightarrow p = q$, soit $p - q \in \mathbb{Q}_-^*$. Mais comme $p - q = -(q - p) = (-1)(q - p)$, on a alors $q - p \in \mathbb{Q}_+^* \Leftrightarrow q > p$.

6. On rappelle ici que si $>$ est un ordre sur un ensemble X, alors $E \subset X$ est dit **minoré** si il existe $m \in X$ tel que $\forall x \in E$, $m \leq x$. Est-ce que les affirmations suivantes sont vraies (si c'est le cas, montrez-le, sinon, trouvez un contre-exemple)?

(a) Tout sous-ensemble $E \subset \mathbb{Z}$ non vide et minoré possède un élément minimal pour l'ordre $<$ dans $\mathbb{Z}$.

(b) Tout sous-ensemble $E \subset \mathbb{Q}$ non vide et minoré possède un élément minimal pour l'ordre $<$ dans $\mathbb{Q}$.

(a) Vrai. Si $E \subset \mathbb{Z}$ est minoré, cela implique l'existence d'un $m \in \mathbb{Z}$, tel que $\forall x \in E$, $m \leq x$. La compatibilité de l'ordre dans $\mathbb{Z}$ avec l'addition nous permet alors de dire, que $\forall x \in E$, $0 \leq x - m$, ou encore que $E' := \{x - m : x \in E\} \subset \mathbb{Z}_+$. Mais comme $\mathbb{Z}^+$ peut être identifié à $\mathbb{N}$, on peut identifier E' à un sous-ensemble non-vide de $\mathbb{N}$, qui lui aura un élément minimal, disons m'. Cet élément m' peut être identifié à un élément de $m'' \in E'$ et comme cette identification entre $\mathbb{Z}_+$ et $\mathbb{N}$ conserve l'ordre, on aura que m'' est minimal dans E'. Ainsi, $\forall x - m \in E'$, $m'' \leq x - m$, i.e. $\forall x \in E$, $m'' + m \leq x$ et clairement, $m'' + m \in E$.

(b) Faux. On peut par exemple considérer l'ensemble $E := \{n^{-1} : n \in \mathbb{N}^*\}$ (où on a de nouveau procédé à l'identification de $n \in \mathbb{N}^*$ avec l'élément $[(n, 1)] \in \mathbb{Q}_+$). Clairement, E est minoré par $0 \in \mathbb{Q}$, mais E ne possède pas d'élément minimal.

7. Pour cet exercice, on identifie $1, 2, 3, \ldots \in \mathbb{N}$ avec $[(1, 0)], [(2, 0)] \ldots \in \mathbb{Z}$ et $m \in \mathbb{Z}$ avec $[(m, 1)] \in \mathbb{Q}$.

(a) Trouver deux nombres rationnels $0 < p, q < 1$, tels que $pq = \frac{3}{4}(= 3 \times 4^{-1})$.

(b) Trouver deux nombres rationnels $0 < p < 4$ et $0 < q < 5$ tels que $p \times q = 19$.

(c) Soient $x, y, r \in \mathbb{Q}_+^*$ tels que $r < xy$. Trouver deux nombres rationnels $0 < q < x$ et $0 < p < y$, tels que $pq = r$.

(a) Clairement, $[(3, 4)] = [(6, 8)]$ et $[(6, 7)] \times [(7, 8)] = [(42, 56)] = [(3, 4)]$. On a bien $[(0, 1)] < [(6, 7)], [(7, 8)] < [(1, 1)]$.

(b) En posant $p' = p \times 4^{-1}$, $q' = q \times 5^{-1}$, on est ramené à trouver deux nombres rationnels $0 < p', q' < 1$, tels que $p'q' = 19 \times 20^{-1} = 38 \times 40^{-1}$. On trouve par exemple $p' = [(38, 39)]$ et $q' = [(39, 40)]$. On a donc par exemple, $p = [(152, 39)]$ et $q = [(195, 40)]$.

(c) On pose $q' = q \times x^{-1}$, $p' = p \times y^{-1}$ et on se ramène à trouver deux rationnels $0 < q', p' < 1$ avec $p'q' = r \times (xy)^{-1} = [(a_r b_x b_y, b_r a_x a_y)] = [(2a_r b_x b_y, 2b_r a_x a_y)]$, où $r = [(a_r, b_r)]$, $x = [(a_x, b_x)]$ et $y = [(a_y, b_y)]$. On prend alors par exemple $p' = [(2a_r b_x b_y, 2a_r b_x b_y + 1)]$ et $q' = [(2a_r b_x b_y + 1, 2b_r a_x a_y)]$, ce qui nous donne livre les solutions $p = [(2a_r b_x a_y, 2a_r b_x b_y + 1)]$ et $q = [(2a_r b_x b_y + 1, 2b_r b_x a_y)]$.

Problèmes supplémentaires

(PS1) On considère un ensemble E non vide muni d'une opération $\star : E \times E \to E$ commutative, associative et qui possède la propriété de simplification. Montrer que

$$(x, x') \sim (y, y') \quad \Leftrightarrow \quad x \star y' = x' \star y$$

est une relation d'équivalence sur $E \times E$.

(a) $\sim$ est réflexif: pour $(a, b) \in E^2$, on a $a \star b = b \star a$ par commutativité de $\star$. Donc $(a, b) \sim (a, b)$.

(b) $\sim$ est symétrique: pour $(a, b), (c, d) \in E^2$, on a $a \star d = b \star c$ implique $c \star b = d \star a$ par commutativité de $\star$. Donc $(a, b) \sim (c, d)$ implique $(c, d) \sim (a, b)$.

(c) $\sim$ est transitive: pour $(a, b), (c, d), (k, l) \in E^2$, on a $a \star d = b \star c$ et $c \star l = d \star k$ impliquent $(a \star d) \star l = (b \star c) \star l$, et par associativité de $\star$, on a $a \star (d \star l) = b \star (c \star l)$ et donc $a \star (d \star l) = b \star (d \star k)$. Par commutativité et associativité de $\star$, on a alors $(a \star l) \star d = (b \star k) \star d$. Par la propriété de simplification on a donc $a \star l = b \star k$, et donc $(a, b) \sim (k, l)$.

(PS2) On reprend les notations de l'exercice précédent et on pose $E^2/\sim \, := \{[(x, y)] : (x, y) \in E^2\}$. Montrer que l'opération

$$[(a, b)] * [(c, d)] := [(a \star c, b \star d)]$$

est bien définie sur $E^2/\sim$ et qu'elle en fait un goupe abélien.

Comme vu au cours, ou de manière similaire à l'exercice 3), on trouve que pour $(a, b), (c, d) \in E^2$,

$$[(a, b)] = [(c, d)] \quad \Leftrightarrow \quad (a, b) \sim (c, d).$$

Pour montrer que l'opération sur les classes d'équivalences est bien définie, il faut montrer que $(k, l) \in [(a, b)]$ et $(k', l') \in [(c, d)]$ impliquent $(k \star k', l \star l') \in [(a \star c, b \star d)]$. Or, $(k, l) \in [(a, b)]$ et $(k', l') \in [(c, d)]$ ssi $(k, l) \sim (a, b)$ et $(k', l') \sim (c, d)$. Mais alors,

$$\begin{gathered}
(k \star k') \star (b \star d) = k \star \big(k' \star (b \star d)\big) \quad (\text{ par associativité de } \star) \\
= k \star \big((k' \star b) \star d\big) = k \star \big((b \star k') \star d\big) \quad (\text{ par commutativité de } \star) \\
= k \star \big(b \star (k' \star d)\big) = (k \star b) \star (k' \star d) \quad (\text{ par associativité de } \star) \\
= (l \star a) \star (l' \star c) \quad (\text{ car } (k, l) \sim (a, b) \text{ et } (k', l') \sim (c, d)) \\
= l \star \big(a \star (l' \star c)\big) = l \star \big((a \star l') \star c\big) \quad (\text{ par associativité de } \star) \\
= l \star \big((l' \star a) \star c\big) = l \star \big(l' \star (a \star c)\big) \quad (\text{ par commutativité de } \star) \\
= (l \star l') \star (a \star c) \quad (\text{ par associativité de } \star).
\end{gathered}$$

Ainsi, $(k \star k', l \star l') \sim (a \star c, b \star d)$ et $(k \star k', l \star l') \in [(a \star c, b \star d)]$.
$*$ fait de $E^2/\sim$ un groupe abélien:

(a) $*$ est commutative: $[(a,b)]*[(c,d)] = [(a\star c, b\star d)] = [(c\star a, d\star b)] = [(c,d)]*[(a,b)]$ (par commutativité de $\star$).

(b) $*$ est associative:

$$\begin{aligned}
&[(a,b)] * \big([(c,d)] * [(k,l)]\big) = [(a,b)] * [(c\star k, d\star l)] \\
&= [\big(a\star(c\star k), b\star(d\star l)\big)] = [\big((a\star c)\star k, (b\star d)\star l\big)] \\
&= [(a\star c, b\star d)] * [(k,l)] = \big([(a,b)] * [(c,d)]\big) * [(k,l)],
\end{aligned}$$

où nous avons utilisé l'associativité de $\star$.

(c) $[(a,a)]$ est l'élément neutre pour $*$: $[(a,a)] * [(c,d)] = [(a\star c, a\star d)] = [(c,d)]$, puisque $(a\star c, a\star d) \sim (c,d)$ par l'associativité et la commutativité de $\star$.

(d) $[(a,b)]$ est l'élément opposé de $[(b,a)]$ pour $*$: $[(a,b)] * [(b,a)] = [(a\star b, b\star a)] = [(a,a)]$, puisque $(a\star b, b\star a) \sim (a,a)$ par l'associativité et la commutativité de $\star$.

(PS3) On reprend les notations de l'exercice précédent et on suppose ici, que le lecteur est familier avec la notion de morphisme de semi-groupes.
Soit G un ensemble non-vide, muni d'une opérations $+ : G\times G \to G$ qui en fait un groupe abélien. Soit $f : E \to G$ un morphisme de semi-groupes et $\imath : E \to E^2/\!\sim$, $a \mapsto [(a\star a, a)]$.
Montrer qu'il existe un unique morphisme de groupe $[f] : E^2/\!\sim\, \to G$, tel que $[f]\circ\imath = f$.

On pose

$$[f] : [(a,b)] \mapsto f(a) - f(b),$$

où $-f(b)$ est l'opposé de $f(b)$ dans G et où nous avons abrégé $f(a) + (-f(b))$ par $f(a) - f(b)$.
$[f]$ est bien définie: si $(c,d) \in [(a,b)]$ alors $(c,d) \sim (a,b)$ et $f(c) - f(d) = f(a) + f(c) - f(d) - f(a) = f(a\star c) - f(d\star a) = f(a\star c) - f(c\star b) = f(a) + f(c) - f(c) - f(b) = f(a) - f(b)$.
$[f]$ est un morphisme de groupes: $[f]\big([(a,b)] * [(c,d)]\big) = f\big([(a\star c, b\star d)]\big) = f(a\star c) - f(b\star d) = f(a) + f(c) - f(b) - f(d) = \big(f(a) - f(b)\big) + \big(f(c) - f(d)\big) = [f]\big([(a,b)]\big) + f\big([(c,d)]\big)$.
$f = [f]\circ\imath$: $[f]\circ\imath(a) = [f]([(a\star a, a)]) = f(a\star a) - f(a) = f(a) + f(a) - f(a) = f(a)$.
Si $f = g\circ\imath$, alors $f(a) = g([(a\star a, a)])$, et donc $[f]([(a,b)]) = f(a) - f(b) = g([(a\star a, a)]) - g([(b\star b, b)]) = g([(a\star a, a)]) + g([(b, b\star b)]) = g([(a\star a\star b, a\star b\star b)]) = g([(a,b)])$, car $(a\star a\star b, a\star b\star b) \sim (a,b)$. donc, $g = [f]$.