Exercices du chapitre 2

Exercice 2.1. (i) Soit M régulier et $x \in M$. Par hypothèse, l'application $M \to M, m \mapsto xm$, est injective. Si M est fini, elle est donc aussi surjective. En particulier, pour tout $x \in M$ il existe $y \in M$ tel que $xy = 1$ (*tout $x \in M$ admet un inverse à droite*). Il reste à voir que ce y vérifie aussi $yx = 1$. On constate que l'élément $e = yx$ vérifie $e^2 = yxyx = y1x = e$ (*idempotent*). Mais si f désigne un inverse à droite de e, on a alors $e = e^2f = ef = 1$, et donc $yx = 1$.

Le (ii) est une conséquence du (i) appliqué à $M = A^\times$ (l'argument est même un peu plus simple, car la régularité vaut des deux côtés dans ce cas particulier). Montrons le (iii). Il faut voir que si H est non vide et stable par produits, alors c'est un sous-groupe. Il existe $h \in H$. Comme G est fini, on a $h^n = 1$ pour un certain entier $n > 0$, et donc $h^{-1} = h^{n-1}$ est dans H, puis $h^n = 1$ est dans H.

Exercice 2.2. (i) Observons que f_i est un cycle de longueur $n-i$ sur $\{i, i+1, \dots, n-1\}$, et que l'on a $f_i^i(\{0, 1, \dots, n\}) \subset \{i, i+1, \dots, n-1\}$. On en déduit $f_i^n = f_i^{n-i}f_i^i = f_i^i$, puis $M_i = \{f_i^k \,|\, 0 \leq k < n\}$. De plus, les éléments f_i^k avec $k = 0, \dots, n-1$ sont distincts, car on a $f_i^k(0) = k$. On a montré $|M_i| = n$.

(ii) Si M est un monoide, posons $M(n) = \{m^k | \, m \in M \smallsetminus \{1\}, k \geq n\}$. 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 $M \to N$ induit une bijection $M(n) \sim N(n)$. Ainsi, si on a $M_i \simeq M_j$, on a $n - i = n - j$, puis $i = j$.

(iii) 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 immédiate montre que pour tout entier $n \geq i$, l'élément x^n est de la forme x^m avec $i \leq m < j$. En particulier, on a $|M| \leq i + j - i \leq j < n$, une contradiction. On a donc $M = \{x^i \,|\, 0 \leq i < n\}$. Ainsi, il existe un unique entier $0 \leq i < n$ avec $x^n = x^i$. Il ne serait pas difficile de 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 $m \mapsto \mathrm{L}_m$ avec $\mathrm{L}_m(n) = mn$. Il est injectif, car on a $\mathrm{L}_m(1) = m$. Il identifie donc M à un sous-monoide 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 $\mathrm{F}(n)$. On constate que L_x n'est rien d'autre que la fonction f_i. Ainsi, on a construit un morphisme injectif $M \to \mathrm{F}(n)$ 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 2.3. (i) 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 monoïde.

(ii) 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 monoïde ! 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.

(iii) 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 $\{xy, yx\} \subset \{x, y\}$, 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 $M \to (M^M, \circ), m \mapsto \mathrm{L}_m$, ces trois monoïdes se plongent dans F(3) (exercice précédent) s'ils existent. On a tout fait pour qu'il soit aisé de les réaliser concrètement dans F(3) : nous laissons cette vérification au lecteur.

Exercice 2.4. Soient $1_\star$ et $1_\circ$ les neutres de $(X, \star)$ et $(X, \circ)$. On a $1_\star = 1_\star \star 1_\star = (1_\star \circ 1_\circ) \star (1_\circ \circ 1_\star) = (1_\star \star 1_\circ) \circ (1_\circ \star 1_\star) = 1_\circ \circ 1_\circ = 1_\circ$. 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 2.5. (i) Fixons $r \in \mathbb{Z}$. Par Bezout, il existe $(a, b) \in \mathbb{Z}^2$ avec $r = am + bn$. On peut toujours ajouter ou soustraire à (a, b) le couple $(n, -m)$ et préserver cette égalité, de sorte que l'on peut supposer $0 \leq b < m$. Si on a une autre écriture $am + bn = a'm + b'n$ on a $(a' - a)m = (b - b')n$ et donc, comme m et n sont premiers entre eux, $a \equiv a' \bmod n$ et $b \equiv b' \bmod m$. Si on a $0 \leq b, b' < m$, cela force $b = b'$, puis $a = a'$.

Montrons le (ii). Si on a $r = am + bn$ avec $a, b \geq 0$, observons que quitte à ajouter $(n, -m)$ à (a, b) on peut supposer $0 \leq b < m$. Autrement dit, $\mathbb{N}n + \mathbb{N}m$ est l'ensemble des $am + bn$ avec $a \geq 0$ et $0 \leq b < m$. Par le (i), les entiers non de cette forme sont les $am + bn$ avec $a < 0$ et $0 \leq b < m$. Le plus grand d'entre eux s'obtient pour $a = -1$ et $b = m - 1$: c'est $-m + (m - 1)n = mn - n - m$.

Pour le (iii), notons d_i le pgcd de $(m_1, \ldots, m_i)$, pour $1 \leq i \leq n$. On a $d_{i+1} = \mathrm{pgcd}(d_i, m_{i+1})$ pour $i < n$, et $d_n = 1$. Observons que pour $a, b \in \mathbb{N}$, de pgcd d, alors on a $a\mathbb{N} + b\mathbb{N} = d(a'\mathbb{N} + b'\mathbb{N})$ avec $a = a'd$ et $b = b'd$, et donc $a\mathbb{N} + b\mathbb{N}$ contient tous les multiples de d assez grands par le (ii). Ainsi, $m_1\mathbb{N} + m_2\mathbb{N}$ contient un entier de la forme $d_2 s_2$ avec s_2 premier avec m_3. Le pgcd de $d_2 s_2$ et m_3 est d_3. Ensuite, $d_2 s_2 \mathbb{N} + m_3\mathbb{N}$ contient un entier de la forme $d_3 s_3$ avec s_3 premier à m_4, etc... À la $n-1$-ème étape, on a construit un sous-monoïde $d_{n-1}s_{n-1}\mathbb{N} + m_n\mathbb{N} \subset m_1\mathbb{N} + m_2\mathbb{N} + \cdots + m_n\mathbb{N}$, avec s_{n-1} premier à m_n, et donc $\mathrm{pgcd}(d_{n-1}s_{n-1}, m_n) = d_n = 1$, ce qui conclut.

Montron le (iv). Notons $F(z) \in \mathbb{C}(z)$ la fraction rationnelle de l'énoncé. On a $F(z) = \sum_{k \geq 0} f_k z^k$ pour $|z| < 1$ et on veut montrer $f_k \neq 0$ pour tout k assez grand. Le complexe $z = 1$ est un pôle d'ordre n de $F(z)$, et les autres pôles sont des racines de l'unité $\neq 1$, et sont (en tant que pôle) d'ordre $\leq n$. On constate que comme les m_i sont premiers entre eux, ces pôles $\neq 1$ sont d'ordre $< n$. Mais pour $n \geq 1$ on a $1/(1 - z)^n = \sum_{k \geq 0} p_k(n)\, z^k$ avec $p_k(n) = (k + 1)(k + 2) \cdots (k + n - 1)$ (et $p_k(1) = 1$). On a $p_k(n) = k^{n-1} + \mathrm{O}(k^{n-2})$ pour $k \to \infty$. Décomposons $F(z)$ en éléments simples. Il y a un terme en $c/(1 - z)^n$, avec $c = \lim_{z \to 1}(z - 1)^n F(z) = 1/(m_1 \cdots m_n)$. Les autres termes sont de la forme $d/(1 - \zeta z)^{n'}$ avec $n' < n$ et $|\zeta| = 1$. On en déduit $f_k = ck^{n-1} + \mathrm{O}(k^{n-2})$ où $c = 1/(m_1 \ldots m_n)$ (c'est vrai aussi pour $n = 1$, car on a alors $m_1 = 1$ et $f_k = 1$ pour tout $k \geq 0$).

Exercice 2.6. (i) Soit $M \subset \mathbb{N}$ un sous-monoïde. Si M contient r et $r + 1$ (premiers entre eux), alors il est primitif. Réciproquement, si le pgcd d'une famille infinie éléments $x_1, x_2, \ldots, x_n, \ldots$, (disons non nuls) vaut 1, c'est que le pgcd de $x_1, \ldots, x_n$ vaut 1 pour n assez grand. En effet, si on pose $d_i = \mathrm{pgcd}(x_1, \ldots, x_i)$, on a $d_{i+1} = \mathrm{pgcd}(d_i, x_{i+1})$ et donc $d_{i+1} \mid d_i$. Ainsi, la suite des entiers $d_i \geq 1$ est décroissante, et donc est constante égale à un certain entier d pour n assez grand. Par définition, d divise tous les x_i. On a donc $d = 1$, ce qui conclut. On conclut par le (i) par le point (iii) de l'exercice précédent.

(ii) Soit M un sous-monoïde de $\mathbb{N}$. On peut supposer $M \neq \{0\}$. Notons $d \geq 1$ le pgcd des éléments de M. On a $M \subset d\mathbb{N}$, et quitte à remplacer M par $\frac{1}{d}M$, on peut supposer

$d = 1$. Si $m_1, \dots, m_n$ sont dans M et premiers entre eux, on a vu que $\mathbb{N}m_1 + \mathbb{N}m_2 + \cdots + \mathbb{N}m_n \subset M$ contient tous les entiers plus grand qu'un certain entier r. Soient N l'ensemble fini des entiers qui sont à la fois dans M et $< r$. Il est clair que M est engendré par N et par les m_i (un nombre fini d'éléments).

(iii) Soient M_1 et M_2 deux sous-monoïdes de $\mathbb{N}$, ainsi que $f : M_1 \to M_2$ un morphisme de monoïdes. Si M_1 est primitif, le sous-groupe de $\mathbb{Z}$ engendré par M_1 est $\mathbb{Z}$. Tout $x \in \mathbb{Z}$ s'écrit donc $x = m - n$ avec $m, n \in M_1$. On constate que $f(m) - f(n) \in \mathbb{Z}$ ne dépend pas de l'écriture choisie de x. En effet, si on a $m - n = m' - n'$ avec m, m', n, n' dans M_1, alors on a $m + n' = m' + n$ dans M_1, puis $f(m) + f(n') = f(m') + f(n)$ car f morphisme, puis $f(m) - f(n) = f(m') - f(n')$. Il existe donc une unique application $f' : \mathbb{Z} \to \mathbb{Z}$ vérifiant $f'(m) = f(m)$ pour $m \in M_2$, et $f'(m - n) = f(m) - f(n)$ pour tout $m, n \in M_2$. Un tel f' est manifestement un morphisme de groupes. Posons $d = f'(1)$: on a alors $f'(n) = nd$ pour tout $n \in \mathbb{Z}$, et donc $f(M_1) \subset d\mathbb{Z}$. Supposant maintenant $f(M_1) = M_2$ et M_2 primitif, on a $d = \pm 1$, puis $d = 1$ car M_2 est dans $\mathbb{N}$. On a donc $f = \mathrm{id}$ et $M_1 = M_2$.

(iv) Les sous-monoïdes primitifs $M_n := n\mathbb{N} + (n+1)\mathbb{N}$ de $\mathbb{N}$ sont distincts car le plus petit élément non nul de M_n est n. Ces monoïdes sont donc non isomorphes par le (iii).

Exercice 2.7. (i) Soit $f : X \to X$ vue comme élément de M. Alors f est inversible à droite si, et seulement si, elle admet une section, et on a vu que c'est équivalent à f surjective. De même, f est inversible à gauche si, et seulement si, elle admet une retraction (Exercice 1.9 Chap. 1), ce qui est équivalent à f injective.

(ii) Si X est infini, on a $X \sim X \coprod \{0\} \sim X \coprod \mathbb{N}$, et donc il existe une surjection $f : X \to X$ possédant une fibre infinie en un point x_0. Une telle f admet une infinité de sections. De même, il existe une injection $f : X \to X$ avec $X \smallsetminus f(X)$ infini. Une telle f admet une infinité de rétractions.

(iii) Soit $m \in M$. Supposons que l'on a $x, y \in M$ avec $mx = 1$ et $ym = 1$. Alors par associativité on a $y = y(mx) = (ym)x = x$.

(iv) Soit $e : X \to X$. On a $e^2 = e$ si, et seulement si, $e(e(x)) = e(x)$ pour tout $x \in X$ (on dit alors que e est *idempotent*). Il est donc équivalent de demander que e vaut l'identité sur $\mathrm{Im}\, e$ (c'est l'analogue ensembliste des projecteurs). Supposons $e^2 = e$ et soit $f : X \to X$. On a $ef = f$ si, et seulement si, $\mathrm{Im}\, f \subset \mathrm{Im}\, e$. On a $fe = f$ si, et seulement si, f est constante sur les fibres de e.

(v) On a $emen = e(men)$ donc $eM \subset M$ est stable par produits. La loi induite est bien sûr associative car celle de M l'est. On a $e = e.1 \in eM$. Pour $x = em$ avec $m \in M$, on constate $ex = eem = em = x$. Réciproquement, si $x = ex$ on a $x \in eM$. On a donc $eM = \{m \in M \,|\, em = m\}$. Si eM a un élément neutre, il est donc nécessairement égal à e. De plus, e est neutre si, et seulement si on a $me = m$ pour tout $m \in eM$, *i.e.* si toute fonction $X \to \mathrm{Im}\, e$ est constante sur les fibres de e par le (iv). Si $|\mathrm{Im}e| = 1$, toute telle fonction est constante, donc convient. Si e est surjective, c'est l'identité par (iv), et les fibres de e sont des singletons, donc tout f convient. Dans le cas restant, il existe a, b, c distincts dans X avec $\{a, b\} \in \mathrm{Im}\, e$ et $c \notin \mathrm{Im}\, e$. On peut même supposer $b = e(c)$. Soit $f : X \to X$ la fonction définie par $f(c) = a$ et $f(x) = b$ pour $x \neq c$. On a bien $\mathrm{Im}\, f \subset \mathrm{Im}\, e$ mais f n'est pas constante sur $e^{-1}(b) \supset \{c, b\}$.

Exercice 2.8. (i) On a $(h, k)(h', k') = (hh', kk')$ dans le groupe $H \times K$ par définition de la loi de groupe produit. Ainsi, 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 a $hk = kh$. (Autrement dit tout élément de H commute avec tout élément de K. Attention, les sous-groupes H et K ne sont pas nécessairement commutatifs).

(ii) Vérifions que f est injective si, et seulement si, on a $H \cap K = \{1\}$. En effet, si $x \in H \cap K$ est non trivial, on a $(1,x) \neq (x,1)$ et $f(1,x) = f(x,1) = x$, donc f est non injective. Réciproquement, supposons $H \cap K = \{1\}$. Alors $hk = h'k'$ avec $h, h' \in H$ et $k, k' \in K$ implique $h^{-1}h' = k(k')^{-1} \in H \cap K = \{1\}$, et donc $h = h'$ et $k = k'$: f est injective.

(iii) L'application f est surjective si, et seulement si, on a $G = HK$.

(iv) C'est la concaténation des conditions (i), (ii), (iii) : $hk = kh$ pour tout $(h,k) \in H \times K$, $H \cap K = \{1\}$ et $G = HK$.

Exercice 2.9. (i) Comme dans l'exercice précédent, on regarde l'application $f : H \times K \to HK$, $(h,k) \mapsto hk$. Elle est surjective par construction, et il suffit pour conclure de montrer que toutes ses fibres 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 $(h',k') = (hz, z^{-1}k)$. Récipoquement, 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 constitué des $|H \cap K|$ éléments de la forme $(hz, z^{-1}k)$ avec $z \in H \cap K$, ce qui conclut.

(ii) Le groupe $H \cap K$ est un sous-groupe de H et de K, donc par Lagrange son cardinal divise $|H|$ et $|K|$, puis $|H \cap K| = 1$. On conclut par le (i).

Exercice 2.10. (i) Supposons que HK est un sous-groupe. Il est alors stable par la bijection $x \mapsto x^{-1}$, donc on a $HK = (HK)^{-1} = K^{-1}H^{-1} = KH$. Réciproquement, si $HK = KH$ le même calcul montre que HK est stable par inversion. Il contient $1 = 1.1$, et il est stable par produit car $HKHK = HHKK = HK$.

(ii) Supposons que dans le groupe G on a deux éléments s et t d'ordre 2 qui ne commutent pas. Par exemple, on peut prendre $G = \mathrm{O}(2)$ et deux reflexions d'axes distincts et non perpendiculaires. On pose $H = \langle s \rangle$ et $K = \langle t \rangle$. Alors on a $HK = \{1, s, t, st\} \neq KH = \{1, t, s, ts\}$.

(iii) Si H est distingué dans G on a $Hk = kH$ pour tout k dans K, et en particulier, $HK = KH$.

Exercice 2.11. Soient $h \in H$ et $k \in K$. On regarde l'élément

$$hkh^{-1}k^{-1} = (hkh^{-1})k^{-1} = k(hk^{-1}h^{-1}).$$

La première écriture montre qu'il est dans K (qui est distingué), et la seconde qu'il est dans H (idem). Il est donc dans $H \cap K = \{1\}$. On a donc $hkh^{-1}k^{-1} = 1$ puis $hk = kh$. On conclut par le (iv) de l'Exercice 2.8.

Exercice 2.12. (i) Vrai. On a $G = G^{-1} = (HK)^{-1} = K^{-1}H^{-1} = KH$.

(ii) Vrai. Rappelons que pour $g \in G$, on dispose d'un automorphisme $\mathrm{int}_g : G \to G, x \mapsto gxg^{-1}$. Il suffit de montrer que l'on a $G = gKg^{-1}H$ pour tout $g \in G$, par le (i). Mais tout $g \in G$ s'écrit $g = hk$ avec $h \in H$ et $k \in K$. Utilisant $kKk^{-1} = K$ et $hHh^{-1} = H$ on constate $gKg^{-1}H = hkKk^{-1}h^{-1}H = hKh^{-1}H = h(KH)h^{-1} = hGh^{-1} = G$.

(iii) Faux. Soit $G = \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$, $H = \langle (1,0) \rangle$, $K = \langle (0,1) \rangle$ et $L = \langle (1,1) \rangle$. On a $G = H + K = H + L$, $H \cap K = H \cap L = \{0\}$, mais $K \neq L$.

Exercice 2.13. Toutes les vérifications sont triviales.

Exercice 2.14. (i) Toute application $f : S \to H \times K$, s'écrit de manière unique sous la forme $f(x) = (a(x), b(x))$ avec $a : S \to H$ et $b : S \to K$ (quelconques). Par définition du groupe produit, f est un morphisme de groupes si, et seulement si, a et b en sont. Pour S fini on a donc $|\mathrm{Hom}(S, G \times H)| = |\mathrm{Hom}(S,G)||\mathrm{Hom}(S,H)|$, et de même$|\mathrm{Hom}(S, G \times K)| = |\mathrm{Hom}(S,G)||\mathrm{Hom}(S,K)|$. Mais on a aussi $|\mathrm{Hom}(S, G \times H)| = |\mathrm{Hom}(S, G \times K)|$ car on

a $G \times H \simeq G \times K$ par hypothèse. Comme $|\mathrm{Hom}(S,G)|$ est fini non nul (considérer le morphisme trivial !), cela montre le (i).

(ii) Par récurrence sur $|S|$. Tout morphisme $f : S \to H$ admet un noyau, qui est un sous-groupe distingué Q de S, et le morphisme f est injectif si et seulement si on a $Q = 1$. Le nombre de morphismes $S \to H$ de noyau Q est, par propriété universelle du groupe quotient, $|\mathrm{inj}(S/Q,H)|$. La même chose vaut pour les morphismes $S \to K$ de noyau Q. Mais on a $|\mathrm{inj}(S/Q,H)| = |\mathrm{inj}(S/Q,K)|$ par récurrence quand $Q \neq 1$, et $|\mathrm{Hom}(S,H)| = |\mathrm{Hom}(S,K)|$ d'après le (i). On a donc aussi $|\mathrm{inj}(S/Q,H)| = |\mathrm{inj}(S/Q,K)|$ pour $Q = 1$.

(iii) On a $|\mathrm{inj}(H,H)| \geq 1$ (l'identité !). Par le (ii) pour $S = H$ on en déduit l'existence d'un morphisme injectif $H \to K$. C'est un isomorphisme, car on a $|H| = |K|$.

(iv) Posons $G = (\mathbb{Z}/2\mathbb{Z})^{\mathbb{N}}$. On a $\mathbb{N} \coprod \{\bullet\} \sim \mathbb{N}$, et donc un isomorphisme $G \times \mathbb{Z}/2\mathbb{Z} \simeq (\mathbb{Z}/2\mathbb{Z})^{\mathbb{N}}$. On a même $\mathbb{N} \coprod \mathbb{N} \sim \mathbb{N}$, et donc $G \times G \simeq G$.

Exercice 2.15. On voit $(\mathbb{Z}/2\mathbb{Z})^X$ comme l'ensemble des fonctions $X \to \mathbb{Z}/2\mathbb{Z}$. C'est un anneau pour les lois $+$ et $\cdot$ évidentes, issues de l'anneau $(\mathbb{Z}/2\mathbb{Z}, +, \cdot)$. Pour $A \subset X$ on note $1_A \subset (\mathbb{Z}/2\mathbb{Z})^X$ la fonction caractéristique de A. On constate $1_A 1_B = 1_{A \cap B}$ et $1_A + 1_B = 1_{A \Delta B}$. Ainsi, $A \mapsto 1_A$ est une bijection $\mathrm{P}(X) \to (\mathbb{Z}/2\mathbb{Z})^X$ qui définit à la fois un morphisme $(\mathrm{P}(X), \Delta) \to ((\mathbb{Z}/2\mathbb{Z})^X, +)$ et un morphisme $(\mathrm{P}(X), \cap) \to ((\mathbb{Z}/2\mathbb{Z})^X, \cdot)$. On conclut par transport de structure que $(\mathrm{P}(X), \Delta, \cap)$ est un anneau isomorphe à $(\mathbb{Z}/2\mathbb{Z})^X$.

Exercice 2.16. Montrons le (i). Soient x et y deux points fixes distincts de f. On veut montrer que la droite (x,y) est constituée de point fixes de f. Comme la distance d de E est euclidienne, pour tout point z de cette droite, si on pose $a = \mathrm{d}(z,x)$ et $b = \mathrm{d}(z,y)$, alors z est l'unique point de E à distance a de x et à distance b de y (cas d'égalité de l'inégalité triangulaire). Mais on a $a = \mathrm{d}(x,z) = \mathrm{d}(f(x), f(z)) = \mathrm{d}(x, f(z))$ et $b = \mathrm{d}(y,z) = \mathrm{d}(f(y), f(z) = \mathrm{d}(y, f(z))$, et donc $z = f(z)$.

Montrons le (ii) par récurrence descendante sur l'entier p (qui est ≥ 0). On a $p = n$ si, et seulement si, $f = \mathrm{id}_E$, et on convient naturellement dans ce cas que f est produit de 0 reflexions. Si $p < n$, il existe $x \in E - 0$ avec $f(x) \neq x$. Soit H l'hyperplan médiateur du segment $[x, f(x)]$. On a $\mathrm{s}_H(f(x)) = x$ et H contient manifestement $\mathrm{Fix}(f)$: pour $z \in \mathrm{Fix}(f)$ on a $\mathrm{d}(z,x) = \mathrm{d}(f(z), f(x)) = \mathrm{d}(z, f(x))$. Mézalor l'isométrie $g = \mathrm{s}_H \circ f$ vérifie $\mathrm{Fix}(g) \supsetneq \mathrm{Fix}(f)$ et donc on a $p' = \dim \mathrm{Fix}(g) \geq p + 1$ (cela colle avec notre convention $p = -1$ si $\mathrm{Fix}(f)$ est vide). Par hypothèse de récurrence, g est produit d'au plus $n - p' \leq n - p - 1$ réflexions, et donc $f = \mathrm{s}_H^{-1} \circ g = \mathrm{s}_H \circ g$ est produit d'au plus $n - p$ réflexions. Cela termine la preuve du (ii). Le (iii) en découle car le fait d'être affine est stable par composition, et les réflexions sont affines.

Exercice 2.17. Par définition, les réflexions affines de $\mathbb{R}$ sont les $\mathrm{s}_a(x) = a - x$, où $a \in \mathbb{R}$, ce qui répond à (i). On sait que toute isométrie affine de $\mathbb{R}$ est produit de 0, 1 ou 2 réflexions affines. C'est donc respectivement soit $\mathrm{id}_{\mathbb{R}}$, soit s_a avec $a \in \mathbb{R}$, soit de la forme $\mathrm{s}_a \circ \mathrm{s}_b(x) = a - (b - x) = a - b + x$ avec $a, b \in \mathbb{R}$, *i.e.* une translation de vecteur $a - b$. On a montré le (ii). Pour $v \in \mathbb{R}$ on note τ_v la translation de vecteur v, *i.e.* $\tau_v(x) = x + v$. Les translations forment un sous-groupe $H \subset \mathrm{Iso}(1)$ isomorphe à $\mathbb{R}$: c'est l'image du morphisme injectif $\mathbb{R} \to \mathrm{Iso}(1), v \mapsto \tau_v$. Fixons arbitrairement $a \in \mathbb{R}$ et posons $K = \langle \mathrm{s}_a \rangle \simeq \mathbb{Z}/2\mathbb{Z}$. En fait, K coincide avec le sous-groupe K' des $f \in \mathrm{Iso}(1)$ vérifiant $f(a/2) = a/2$. Par exemple, K' ne contient aucune translation non triviale, et on a $s_b \in K'$ si et seulement si $b = a$. On a trivialement $K' \cap H = \{1\}$ et aussi $\mathrm{Iso}(1) = HK'$. En effet, pour $f \in \mathrm{Iso}(1)$, f envoit $a/2$ sur un réel b, et on a $\tau_v \circ f \in K'$ pour $v = a/2 - b$, et donc $f \in HK'$. Cela montre la première assertion du (iii). Pour la seconde c'est non, car $\mathrm{Iso}(1)$ n'est pas commutatif : on a $\mathrm{s}_0 \circ \tau_v = \tau_{-v} \circ \mathrm{s}_0$ pour tout $v \in \mathbb{R}$.

Exercice 2.18. Pour le (i), le sous-groupe μ de $\mathbb{C}^\times$ constitué des racines de l'unité d'ordre arbitraire, *i.e.* $\mu = \cup_{n\geq 1}\mu_n$, convient. Un autre exemple est $G = (\mathbb{Z}/2\mathbb{Z})^{\mathbb{N}}$, dont tous les éléments sont d'ordre 1 ou 2. Pour le (ii), on peut regarder les réflexions $\mathrm{s}_0(x) = -x$ et $\mathrm{s}_1(x) = 1 - x$ dans $\mathrm{Iso}(1)$ (exercice précédent). Elles sont d'ordre 2, mais $\mathrm{s}_0 \circ \mathrm{s}_1$ est la translation $x \mapsto x + 1$, qui est d'ordre infini. Un autre exemple du même type est obtenu en considérant deux réflexions orthogonales s et t du le plan euclidien. On a $s^2 = t^2 = 1$, et st est la rotation d'angle le double de l'angle $\pi\theta$ entre les deux axes. Ainsi, st est d'ordre fini si, et seulement si, $\theta \in \mathbb{Q}$.

Exercice 2.19. Pour le (i), on remarque que comme on a $d_i x_i = 0$ dans G pour $i = 1, \ldots, n$, on dispose d'un morphisme bien défini $f : \prod_{i=1}^n (\mathbb{Z}/d_i\mathbb{Z}) \to G, (\overline{m_i}) \mapsto \sum_{i=1}^n m_i x_i$. Il est surjectif car les x_i engendrent G. On a donc

$$d_1 d_2 \cdots d_n = |\prod_{i=1}^n (\mathbb{Z}/d_i\mathbb{Z})| = |\mathrm{Im}\, f|\,|\ker f| = |G||\ker f|,$$

et donc $|G|$ divise $d_1 d_2 \cdots d_n$. Pour le (ii), on constate que si p divise $|G|$, il divise l'un des d_i, disons $d_i = pm_i$, et donc $m_i x_i$ est d'ordre $d_i/m_i = p$.

Exercice 2.20. (i) Que A soit d'ordre a est clair. Pour le B, l'observation donnée montre que le polynôme caractéristique de B est $(X - \zeta_b)(X - \zeta_b^{-1})$. On a $\zeta_b \neq \zeta_b^{-1}$ car $b > 2$. Ainsi, B est diagonalisable de valeurs propres ζ_b et ζ_b^{-1}, et donc conjuguée à la matrice diagonale $\mathrm{diag}(\zeta_b, \zeta_b^{-1})$, manifestement d'ordre b.

(ii) Un calcul immédiat montre $\mathrm{trace}\, A\, B_t = (\zeta_a - \zeta_a^{-1})t + \zeta_a^{-1}\zeta_b + \zeta_a^{-1}\zeta_b^{-1}$.

(iii) La trace ci-dessus est de la forme $\alpha t + \beta$ avec $\alpha \neq 0$ (car $a > 2$). Pour t bien choisi elle vaut donc $\zeta_c + \zeta_c^{-1}$. Pour un tel t, la matrice $A\, B_t$ (de déterminant 1) est de trace $\zeta_c + \zeta_c^{-1}$, donc d'ordre c par l'observation et le même argument qu'au (i) (il utilise $c > 2$). Pour un t bien choisi, on a $|\mathrm{trace}\, A\, B_t| > 2$, et donc $A\, B_t$ est d'ordre infini (les valeurs propres d'un $M \in \mathrm{GL}_n(\mathbb{C})$ d'ordre fini sont des racines de l'unité).

(iv) En effet, si $p \equiv 1 \bmod abc$, le groupe cyclique $(\mathbb{Z}/p\mathbb{Z})^\times$, qui est d'ordre $p - 1$, contient des éléments d'ordre a, b et c, que l'on note encore ζ_a, ζ_b et ζ_c. L'argument précédent fonctionne alors verbatim dans $G = \mathrm{SL}_2(\mathbb{Z}/p\mathbb{Z})$.

(v) Soit m impair avec $h^m = 1$. On a $\det gh = \det g \det h$, $\det g = \pm 1$ et $(\det h)^m = 1$. Si $\det g = -1$, on en déduit que $\det gh$ est d'ordre pair, et donc gh est d'ordre pair. Si $\det g = 1$, comme g est diagonalisable de valeurs propres ± 1, la seule possibilité est $g = -1_2$. Mais dans ce cas g est central, et donc on a $(gh)^{2m} = 1_2$ et $(gh)^m = -1_2$, et gh est d'ordre pair. Cela montre que l'on ne peut pas d'affranchir des hypothèses $a, b, c \geq 3$ par cette méthode.

(vi) Observons que le seul élément d'ordre 2 de $\mathrm{SL}_2(k)$, quand k est un corps de caractéristique $\neq k$, est -1_2. En effet, si on a $g^2 = 1$ alors $X^2 - 1 = (X-1)(X+1)$ annule g et est à racines simples, donc g est conjugué dans $\mathrm{GL}_2(k)$ à $\mathrm{diag}(\pm 1, \pm 1)$. Mais $\det g = 1$ montre que ces deux signes sont les mêmes, et $g \neq 1$ conclut l'observation.

Fixons a, b, c des entiers ≥ 2. Supposons que l'on a un groupe G possédant un unique élément z d'ordre 2, que z est dans le centre de G (en fait, c'est automatique), et que l'on a $g, h \in G$ avec g d'ordre $2a$, h d'ordre $2b$ et gh d'ordre $2c$. Soit $Z = \langle z \rangle$. C'est un sous-groupe distingué de G car z est central. Notons g' et h' les images de g et h dans le groupe quotient $G' = G/Z$. On observe que l'on a $g^a = z$, $h^b = z$ et $(gh)^c = z$, car ces trois éléments sont d'ordre 2. On en déduit aisément que g', h' et $g'h'$ sont d'ordre respectifs a, b et c dans G' : ce que l'on cherchait à démontrer.

Exercice 2.21. (i) Deux morphismes $f, f' : G \to H$ qui coïncident sur le générateur g de G sont égaux, donc ev_g est injective. Soit $x \in H$, avec en outre $x^N = 1$ si g est

d'ordre $N \geq 1$. Montrons qu'il existe un morphisme $f : G \to H$ tel que $f(g^n) = x^n$ pour tout $n \in \mathbb{Z}$. Il est nécessairement unique s'il existe par ce que l'on vient de voir. Il est bien défini car si on a $g^n = g^m$ dans G alors on a $n = m$ si g est d'ordre infini (et donc $x^n = x^m$), et $n \equiv m \bmod N$ si g est d'ordre $N \geq 1$, et donc encore $x^n = x^m$ car $x^N = 1$.

(ii) Par définition, quand G et H sont des groupes quelconques avec H abélien la loi de groupes que l'on met sur $\mathrm{Hom}(G, H)$ est $(f, f') \mapsto ff'$ avec $(ff')(x) := f(x)f'(x)$. Noter que l'on a bien $ff' \in \mathrm{Hom}(G, H)$ car pour tout $x, y \in G$ on a $f(y)f'(x) = f'(x)f(y)$ puis

$$(ff')(xy) = f(xy)f'(xy) = f(x)f(y)f'(x)f'(y) = f(x)f'(x)f(y)f'(y) = (ff')(x)(ff')(y),$$

On conclut car pour G monogène engendré par g, et $f, f' \in \mathrm{Hom}(G, H)$, on a trivialement

$$\mathrm{ev}_g(ff') = (ff')(g) = f(g)f'(g) = \mathrm{ev}_g(f)\mathrm{ev}_g(f').$$

Exercice 2.37. Montrons le (i). Soit P le produit de tous les éléments de $(\mathbb{Z}/p\mathbb{Z})^\times$. On a $P \equiv (p-1)! \bmod p$. Regardons l'involution $f : x \mapsto a/x$ de $(\mathbb{Z}/p\mathbb{Z})^\times$ (noter $\overline{a} \in (\mathbb{Z}/p\mathbb{Z})^\times$). Pour $x \in (\mathbb{Z}/p\mathbb{Z})^\times$ tel que $\{x, a/x\}$ a deux éléments, on a $x \cdot a/x = a$. Sinon, on a $x^2 = a$. Si a n'est pas un carré, cela ne se produit pas, et donc en regroupant dans P les paires $\{x, a/x\}$ on a $P \equiv a^{\frac{p-1}{2}} \bmod p$. Si a est un carré, c'est le carré de deux éléments distincts u et $-u$ (car $p \neq 2$) et donc f a deux uniques points fixes, u et $-u$, et $\frac{p-3}{2}$ paires échangées. On a donc $P \equiv -u^2 a^{\frac{p-3}{2}} \equiv -a^{\frac{p-1}{2}}$. Dans tous les cas on a bien $(p-1)! \equiv P \equiv -(\frac{a}{p})a^{\frac{p-1}{2}}$. Pour $a = 1$, on retrouve $(p-1)! \equiv -1 \bmod p$. On en déduit alors $(\frac{a}{p}) \equiv a^{\frac{p-1}{2}}$, puis la multiplicativité est immédiate car $(ab)^{\frac{p-1}{2}} = a^{\frac{p-1}{2}} b^{\frac{p-1}{2}}$. On a montré le (ii).

Exercice 2.38. Montrons le (i). On a la congruence classique $(p-1)! \equiv -1 \bmod p$, vue par exemple à l'exercice précédent. On a aussi $(p-1)! = \prod_{i=1}^{(p-1)/2} i(p-i) \equiv x^2(-1)^{\frac{p-1}{2}} \bmod p$, où $x := (\frac{p-1}{2})!$. Pour $p \equiv 1 \bmod 4$, on a donc $x^2 \equiv -1 \bmod p$.

Montrons le (ii). On peut supposer $p > 3$. La relation de l'énoncé n'est autre que l'identité $4(X^2+X+1) = (2X+1)^2+3$. Ainsi, -3 est un carré dans $\mathbb{Z}/p\mathbb{Z}$ si, et seulement si, $X^2 + X + 1$ a une racine dans $\mathbb{Z}/p\mathbb{Z}$. Mais on a $X^3 - 1 = (X-1)(X^2+X+1)$ dans $(\mathbb{Z}/p\mathbb{Z})[X]$ et 1 n'est pas racine de $X^2 + X + 1$ dans $\mathbb{Z}/p\mathbb{Z}$ pour $p \neq 3$. On en déduit que $X^2 + X + 1$ a une racine dans $\mathbb{Z}/p\mathbb{Z}$ si, et seulement si, $(\mathbb{Z}/p\mathbb{Z})^\times$ a un élément d'ordre 3. Utilisant soit le fait que $(\mathbb{Z}/p\mathbb{Z})^\times$ est cyclique (Gauss), soit le lemme de Cauchy, c'est équivalent à $p \equiv 1 \bmod 3$.

Montrons le (iii). Par multiplicativité du symbole de Legendre, on a $(\frac{3}{p}) = (\frac{-3}{p})(\frac{-1}{p})$. Pour $p \equiv 1 \bmod 12$, ce signe vaut $1.1 = 1$, pour $p \equiv 5 \bmod 12$ il vaut $1 \cdot -1 = -1$, pour $p \equiv 7 \bmod 12$ il vaut $-1 \cdot 1 = -1$, et pour $p \equiv -1 \bmod 12$ il vaut $-1 \cdot -1 = 1$. On en déduit $(\frac{3}{p}) = 1$ si, et seulement si, $p \equiv \pm 1 \bmod 12$.

Montrons le (iv). Si $p \equiv 1 \bmod 8$, par Gauss il existe $\xi \in (\mathbb{Z}/p\mathbb{Z})^\times$ d'ordre 8. On a $\xi^8 = 1$ et $\xi^4 \neq 1$, donc $\xi^4 = -1$, puis $\xi^{-2} = -\xi^2$, et donc $(\xi + \xi^{-1})^2 = 2$. Ainsi, 2 est un carré dans $\mathbb{Z}/p\mathbb{Z}$.

Montrons le (v). Soit F un corps de cardinal p^2 contenant $\mathbb{Z}/p\mathbb{Z}$ comme dans l'énoncé. Par Gauss, le groupe $F^\times$ est cyclique d'ordre p^2-1. On a toujours $p^2 \equiv 1 \bmod 8$, et donc il existe un élément ξ d'ordre 8 dans $F^\times$. L'élément $u = \xi + \xi^{-1} \in F$ est de carré 2, car on a $\xi^2 = -\xi^{-2}$. Les deux racines de $X^2 - 2$ dans F sont donc $\pm u$. En particulier, 2 est un carré dans $\mathbb{Z}/p\mathbb{Z}$ si, et seulement si, on a $u \in \mathbb{Z}/p\mathbb{Z}$. Mais $\mathbb{Z}/p\mathbb{Z}$ est exactement l'ensemble des racines du polynôme $X^p - X$ dans F (une inclusion est évidente, et ce polynôme a au plus p racines). Il ne reste qu'à comparer $u^p = (\xi + \xi^{-1})^p = \xi^p + \xi^{-p}$ (car F est de carctéristique p) avec u. Si $p \equiv \pm 1 \bmod 8$, on a $\xi^p = \xi$ ou ξ^{-1}, et donc $u^p = u$, *i.e.* $u \in \mathbb{Z}/p\mathbb{Z}$, et donc 2 est un carré modulo p. Si $p \equiv \pm 3 \bmod 8$, on a $\xi^p = \xi^{\pm 3} = -\xi^{\pm 1}$, puis $u^p = -u \neq u$ et donc $u \notin \mathbb{Z}/p\mathbb{Z}$: 2 n'est pas un carré dans $\mathbb{Z}/p\mathbb{Z}$.

Exercice 2.22. Soit H un sous-groupe de G. Alors $I = \cap_{g\in G} gHg^{-1}$ est un sous-groupe distingué de G. Supposons H d'indice fini, disons $G = \coprod_{i=1}^{n} g_i H$ avec les g_i dans G. On constate alors $gHg^{-1} = g_i H g_i^{-1}$ pour $g \in g_i H$, et donc $I = \cap_{i=1}^{n} g_i H g_i^{-1}$. On conclut par le (iii) de l'exercice précédent.

Exercice 2.23. Appliquons le théorème de Lagrange dans le groupe G/H (de cardinal n). Pour tout $g \in G$ on a $H = (gH)^n = g^n H$, et donc $g^n \in H$.

Exercice2.36. (i) L'inversion $x \mapsto x^{-1}, G \to G$, étant bijective, on a $|T^{-1}| = |T|$. Soit $g \in G$. En utilisant la bijectivité des applications $x \mapsto x^{-1}$ et $x \mapsto gx$, de G dans G, on a $|gT^{-1}| = |T^{-1}| = |T|$. Comme $|S| + |T| > |G|$, les parties gT^{-1} et S ne sont pas disjointes dans G, donc il existe $s \in S$ et $t \in T$ avsc $gt^{-1} = s$, puis $g = st$.

(ii) On se place dans le groupe *additif* $G = \mathbb{Z}/p\mathbb{Z}$. On prend $S = \{ax^2 \mid x \in \mathbb{Z}/p\mathbb{Z}\}$ et $T = \{bx^2 \mid x \in \mathbb{Z}/p\mathbb{Z}\}$. Pour $p = 2$ on a $|S| = |T| = 2$ et pour $p > 2$ on a $|S| = |T| = 1 + \frac{p-1}{2} > p/2$ car il y a $\frac{p-1}{2}$ carrés non nuls dans $(\mathbb{Z}/p\mathbb{Z})^\times$.

(iii) On suppose que G possède un sous-groupe S (distingué) d'indice 2, par exemple $G = \mathbb{Z}/n\mathbb{Z}$ avec n pair. On a $SS = S \neq G$ et $|S| + |S| = |G|$.

Exercice 2.25. (i) Soit une famille $\{x_i\}_{i\in I}$ d'éléments de G telle que $G = \coprod_{i\in I} x_i B$. On a $I \sim G/B$. Soit de même une famille $\{y_j\}_{j\in J}$ d'éléments de B avec $B = \coprod_{j\in J} y_j A$. On a clairement $G = \bigcup_{(i,j)\in I\times J} x_i y_j A$. On vérifie immédiatement que cette réunion est disjointe, ce qui montre que l'on a des bijections $G/A \sim I \times J \sim G/B \times B/A$.

(ii) On regarde l'application $f : A \to AB/B, a \mapsto aB$. Elle est surjective par définition. Si on a deux éléments a, a' de A avec $a \sim_{A\cap B} a'$, *i.e.* $a' = ab$ avec $b \in A \cap B$, alors on a $f(a') = a'B = abB = aB = f(a)$. Ainsi, f se factorise en une application $f' : A/A \cap B \to AB/B, aA \cap B \mapsto aB$. Cette application f' est encore clairement surjective. Elle est aussi injective : si on a $aB = a'B$, alors $a' \in aB$, puis $a' = ab$ avec $b \in B$, et même $b = a'a^{-1} \in A \cap B$. On a donc $aA \cap B = a'A \cap B$. On a montré que f' est bijective.

(iii) Soit $C = A \cap B$. Par le (ii), on a $A/C \sim AB/B \hookrightarrow G/B$, donc C est d'indice fini dans A. On a alors $|G/C| = |G/A|\,|A/C|$ par le (i), donc C est d'indice fini dans G.

(iv) Posons $C = A \cap B$. Par (iii) et (i) on a $|G/C| = |G/A|\,|A/C| = |G/B|\,|B/C|$. Comme $|G/A|$ et $|G/B|$ sont premiers entre eux, $|G/B|$ divise $|A/C|$. Mais on a aussi $A/C \sim AB/B \hookrightarrow G/B$ par (ii), donc on a $AB/B = G/B$, ou ce qui revient au même, $G = AB$.

Exercice 2.27. Pour le (i) on suppose $G/\mathrm{Z}(G)$ monogène engendré par $x\mathrm{Z}(G)$. On en déduit que pour tout $g \in G$, alors $g\mathrm{Z}(G)$ est de la forme $x^n\mathrm{Z}(G)$ pour $n \in \mathbb{Z}$. En particulier, G est engendré par x et $\mathrm{Z}(G)$. Comme x commute avec $\mathrm{Z}(G)$ et lui-même, cela entraîne $x \in \mathrm{Z}(G)$, puis $G = \mathrm{Z}(G)$ est abélien.

Pour $G = \mathrm{H}_8$, on a $\mathrm{Z}(G) = \{\pm 1\}$, puis $G/\mathrm{Z}(G)$ est d'ordre 4 engendré par les images i et j de I et J, qui vérifient $i^2 = j^2 = 1$ et $ij = ji$. On a donc $G/\mathrm{Z}(G) \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ (bien non monogène).

Exercice 2.28. Si on a $\mathrm{Aut}(G) = 1$, les automorphismes intérieurs de G sont triviaux, *i.e* $gxg^{-1} = x$ pour tout $g \in G$ et $x \in G$. Ainsi, G est abélien. Dans ce cas, l'application $g \mapsto g^{-1}$ est aussi un automorphisme. On a donc $g = g^{-1}$ pour tour $g \in G$, *i.e.* $g^2 = 1$. Cela montre que G est un $\mathbb{Z}/2\mathbb{Z}$-espace vectoriel de manière naturelle (voir la discussion des p-groupes abéliens élémentaires au Chapitre 3), puis $G \simeq (\mathbb{Z}/2\mathbb{Z})^{(I)}$ en en considérant une base indexée par un certain ensemble I. Si on a $|I| \geq 2$, on peut écrire $G \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times H$. Mais l'application $(x, y, h) \mapsto (x + y, y, h)$ est un automorphisme non trivial de $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times H$ (de carré identité) : absurde. On a donc $|I| \leq 1$, *i.e.* $|G| \leq 2$.

Exercice 2.30. Pour $\lambda \in \mathbb{Q}$ on pose $u(\lambda) = \left[\begin{smallmatrix} 1 & \lambda \\ 0 & 1 \end{smallmatrix}\right] \in \mathrm{GL}_2(\mathbb{Q})$. On a $u(\lambda)u(\lambda') = u(\lambda+\lambda')$, donc l'application $\mathbb{Q} \to \mathrm{GL}_2(\mathbb{Q}), \lambda \mapsto u(\lambda)$, est donc un morphisme de groupes. Il est injectif, et induit donc un isomorphisme $\mathbb{Z} \xrightarrow{\sim} u(\mathbb{Z}) = H$. On a

$$g\,u(\lambda)\,g^{-1} \;=\; u(2\lambda), \text{ pour } \lambda \in \mathbb{Q},$$

et donc $gHg^{-1} = u(2\mathbb{Z}) \subsetneq u(\mathbb{Z}) = H$. On a montré le (i). On constate que H' est le sous-groupe constitué des $u(\lambda)$ avec λ de la forme $n/2^m$ pour $n \in \mathbb{Z}$ et $m \geq 0$. C'est le plus petit sous-groupe de $\mathrm{GL}_2(\mathbb{Q})$ contenant $H = u(\mathbb{Z})$ et stable par $x \mapsto g^{-1}xg$.

Exercice 2.31. Regardons l'application $f : \prod_i G_i \to \prod_i G_i/H_i, (g_i) \mapsto (g_iH_i)$, Elle est clairement surjective, et un morphisme de groupes. Son noyau est l'ensemble des $(g_i) \in \prod_i G_i$ vérifiant $g_iH_i = H_i$ pour tout i, c'est-à-dire $g_i \in H_i$. On a donc $\ker f = \prod_i H_i$. Ainsi, ce dernier est distingué (ce qui justifie le (i)) et on conclut le (ii) par $G/\ker f \simeq \mathrm{Im} f$.

Exercice 2.40. Si p et q sont premiers impairs, la relation d'Eisenstein montre $(\frac{p}{q})\,((\frac{q}{p}) = (-1)^s$ où s est le nombre de points à coordonnées entières à l'intérieur du rectangle OP'S'Q'. En effet, les seuls points à coordonnées entières sur la diagonale $y = qx/p$ du rectangle OPSQ sont O et S car p et q sont premiers entre eux. On conclut le (i) car on a $s = \frac{p-1}{2}\frac{q-1}{2}$.

Montrons la relation d'Eisenstein. Comme q est premier à p, la multiplication par q est injective dans $\mathbb{Z}/p\mathbb{Z}$; on a donc $|R| = |X| = \frac{p-1}{2}$. Pour montrer le (ii) il suffit alors de voir que l'application de l'énoncé est injective. Soient $r, r' \in R$ de parités différentes et avec $r + r' = p$. On écrit $r \equiv qx \bmod p$ et $r' \equiv qx' \bmod p$ pour $x, x' \in X$. Il vient $x + x' \equiv 0 \bmod p$ car q est premier à p, puis $x + x' = p$, ce qui est absurde modulo 2.

Le (ii) entraîne $\prod_{x\in X} x \equiv \prod_{r\in R}(-1)^r r \bmod p$. Le (iii) s'en déduit car on a $\prod_{r\in R} r \equiv q^{\frac{p-1}{2}} \prod_{x\in X} x \bmod p$ (le produit sur X est non nul car p est premier).

Le (iv) est immédiat car x est pair et p est impair. On a déjà observé que la droite $y = qx/p$ ne contient aucun point (x, y) avec $y \in \mathbb{Z}$ et $x \in X$ car q est premier à p, on a donc $f = \sum_{x\in X}[qx/p]$ en dénombrant abscisse par abscisse, ce qui prouve le (v) d'après le (iv).

Pour le (vi), on raisonne abscisse par abscisse en observant qu'il y a $q - 1$ entiers compris strictement entre 0 et q, et $q - 1 \equiv 0 \bmod 2$. La symétrie $(x, y) \mapsto (p - x, q - y)$ identifie les points à coordonnées entières et d'abscisse paire intérieurs au triangle S'SQ", aux points à coordonnées entières et d'abscisse impaire intérieurs au triangle OP'S'.

Le (vii) se déduit alors de (v) et (vi). Le premier point du (viii) découle du (v) pour $q = 2$. Si $n \in \mathbb{Z}$ est un entier impair, notons $f(n)$ le nombre d'entiers pairs compris entre $n/2$ et n. On a $f(1) = 0$, $f(3) = 1$, $f(5) = 1$ et $f(7) = 2$. On observe de plus $f(n + 8) = f(n) + 2$. A insi, on a $f(n) \equiv \frac{n^2-1}{8} \bmod 2$.