Exercices du chapitre 3

Exercice 3.1. Observons d'abord que pour une suite d'entiers a_1, a_2, …, a_n on a

$$a_1 \,|\, a_2 \,|\, \cdots \,|\, a_n \quad \Leftrightarrow \mathrm{v}_p(a_1) \leq \mathrm{v}_p(a_2) \leq \cdots \leq \mathrm{v}_p(a_n) \quad \text{pour tout } p \text{ premier},$$

où v_p désigne la valuation p-adique. Revenons au problème. On a $2025 = 3^4 5^2$. Les facteurs invariants possibles d'un groupe abélien d'ordre 5^2 sont $(5, 5)$ et (5^2). Les facteurs invariants possibles d'un groupe abélien d'ordre 3^4 sont $(3, 3, 3, 3)$, $(3, 3, 3^2)$, $(3, 3^3)$, $(3^2, 3^2)$ et (3^4). Les facteurs invariants possibles d'un groupe abélien d'ordre 2025 sont donc $(3, 3, 3 \cdot 5, 3 \cdot 5)$, $(3, 3 \cdot 5, 3^2 \cdot 5)$, $(3 \cdot 5, 3^3 \cdot 5)$, $(3^2 \cdot 5, 3^2 \cdot 5)$, $(5, 3^4 \cdot 5)$, $(3, 3, 3, 3 \cdot 5^2)$, $(3, 3, 3^2 \cdot 5^2)$, $(3, 3^3 \cdot 5^2)$, $(3^2, 3^2 \cdot 5^2)$ et $(3^4 \cdot 5^2)$. Autrement dit, ce sont exactement

$$(3, 3, 15, 15), (3, 15, 15), (3, 15, 45), (15, 135), (45, 45), (5, 405), (3, 3, 3, 75), (3, 3, 225), (3, 675), (2025).$$

En particulier, il y a exactement 10 groupes abéliens non isomorphes d'ordre 2025.

Exercice 3.2. Soit $G = \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$. Observons que les éléments d'ordre 4 de G sont $(0, \pm 1)$ et $(1, \pm 1)$. Les deux premiers (inverses l'un de l'autre) engendrent le même sous-groupe $H_1 = \{0\} \times \mathbb{Z}/4\mathbb{Z}$, et les deux second engendrent de même un même sous-groupe $\simeq \mathbb{Z}/4\mathbb{Z}$, à savoir $H_2 = \{(n \bmod 2, n \bmod 4) \,|\, n \in \mathbb{Z}\} \subset G$. Soit H un sous-groupe de G, que l'on peut supposer $\neq G$, donc d'ordre divisant 4. Si H contient un élément d'ordre 4, alors H contient le groupe cyclique engendré par cet élément, et coïncide donc avec H_1 ou H_2 pour des raisons de cardinalité. Sinon, tout élément h de H vérifie $2h = 0$, et donc H est inclus dans le sous-groupe $H_3 = \{(x, y) \,| x \in \mathbb{Z}/2\mathbb{Z}, y \in 2\mathbb{Z}/4\mathbb{Z}\} \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$. Mais H_2 est un 2-groupe abélien élémentaire, donc un $\mathbb{Z}/2\mathbb{Z}$-espace vectoriel de dimension 2, et ses sous-groupes sont ses sous-espaces. Il a donc H_2 lui-même, ses trois droites, engendrées respectivement par $(1, 0)$, $(0, 2)$ et $(1, 2)$, et le groupe trivial $\{0\}$. Le groupe G a donc exactement $1 + 3 + 4 = 8$ sous-groupes.

Exercice 3.3. Un tel groupe G est d'ordre 16. Comme on le suppose abélien, il est isomorphe à $(\mathbb{Z}/2\mathbb{Z})^4$, $(\mathbb{Z}/2\mathbb{Z})^2 \times \mathbb{Z}/4\mathbb{Z}$, $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/8\mathbb{Z}$, $\mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$ ou $\mathbb{Z}/16\mathbb{Z}$. Mais G n'a pas d'élément d'ordre 8. En effet, pour tout $g \in G$ on a $g^2 = 1$ dans G/H, donc $g^2 \in H$, puis $(g^2)^2 = g^4 = 1$ car $h^2 = 1$ pour tout $h \in H$. Cela élimine $G \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/8\mathbb{Z}$ et $G \simeq \mathbb{Z}/16\mathbb{Z}$. Les autres cas sont possibles : pour $G = (\mathbb{Z}/2\mathbb{Z})^4$ on peut prendre $H = \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \{0\} \times \{0\}$, pour $G = (\mathbb{Z}/2\mathbb{Z})^2 \times \mathbb{Z}/4\mathbb{Z}$ on peut prendre $H = \mathbb{Z}/2\mathbb{Z} \times \{0\} \times 2\mathbb{Z}/4\mathbb{Z}$, et pour $G = \mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$ on peut prendre $H = 2\mathbb{Z}/4\mathbb{Z} \times 2\mathbb{Z}/4\mathbb{Z}$.

Exercice 3.4. (i) On note G additivement. On a clairement $G[a] \subset G[b]$ si $a|b$. On a donc $G[n]$ et $G[m]$ inclus dans $G[mn]$. Par Bezout, on a u, v dans $\mathbb{Z}$ avec $1 = un + vm$. Supposons $x \in G$ avec $nx = 0$ et $mx = 0$. On en déduit $x = unx + vmx = 0$. On a donc $G[n] \cap G[m] = \{0\}$. De plus, pour tout x dans G on a $x = unx + vmx$. Si x est dans $G[mn]$, on a alors $nx \in G[m]$ et $mx \in G[n]$, puis $x \in G[m] + G[n]$. On a monté $G[mn] = G[m] \oplus G[n]$. Pour le (ii), imiter la démonstration de l'Exercice 3.1.

Exercice 3.5. Soient $a_1, \ldots, a_n$ les facteurs invariants de G. Soit d un diviseur de G. En utilisant la première observation de la solution de l'Exercice 3.1 il n'est pas difficile de voir que l'on peut trouver, pour tout $i = 1, \ldots, n$, un diviseur d_i de a_i, tels que $d = d_1 d_2 \cdots d_n$. On a $G \simeq \prod_i C_i$ avec C_i cyclique d'ordre a_i. On sait que C_i a un sous-groupe (cyclique) D_i d'ordre d_i. On en déduit que le sous-groupe $\prod_i D_i$ convient.

Exercice 3.6. Si G est abélien p-élémentaire, on a vu que G est un $\mathbb{Z}/p\mathbb{Z}$-espace vectoriel $G^\sharp$ de manière naturelle. Il est équivalent de se donner un automorphisme de G et un automorphisme de cet espace vectoriel $G^\sharp$. On a donc $\mathrm{Aut}(G) = \mathrm{GL}(G^\sharp) \simeq \mathrm{GL}_n(\mathbb{Z}/p\mathbb{Z})$. Les sous-groupes caractéristiques de G sont les sous-espaces vectoriels de $G^\sharp$ stables par toute application linéaire inversible : ce sont donc $\{0\}$ et $G^\sharp$.

Exercice 3.7. Supposons $g^2 = 1$ pour tout $g \in G$, *i.e.* $g^{-1} = g$ pour tout $g \in G$. Pour $g, h \in G$ on a $gh = g^{-1}h^{-1} = (hg)^{-1} = hg$. Donc G est commutatif : il est abélien 2-élémentaire. On conclut par le cours.

Exercice 3.8. (i) On sait que si k est un corps et $N \in \mathrm{M}_n(k)$ est nilpotente, on a $N^n = 0$. On en déduit que pour $p \geq n$ et $N \in \mathrm{M}_n(\mathbb{Z}/p\mathbb{Z})$ on a $(1+N)^p = 1 + N^p = 1$. Pour le (ii), on prend $G = \mathrm{U}_3(\mathbb{Z}/p\mathbb{Z})$ et $p \geq 3$. On a $|G| = p^3$, et même

$$|\mathrm{U}_n(\mathbb{Z}/p\mathbb{Z})| = p^{1+2+\cdots+n-1} = p^{\frac{n(n-1)}{2}}$$

pour tout $n \geq 1$. On a $g^p = 1$ pour tout $g \in G$ par le (i). Il est facile de voir que $\mathrm{U}_3(k)$ n'est jamais commutatif (pour k un corps), et même que le centre de $\mathrm{U}_n(k)$ est constitué des matrices $(m_{i,j}) \in \mathrm{U}_n(k)$ avec $m_{i,j} = 0$ pour tout $i \leq j$ vérifiant soit $i > 1$, soit $j < n$.

Exercice 3.9. (a) Faux : $\{2, 3\}$ est une famille génératrice minimale de $\mathbb{Z}$, mais elle n'est pas libre car on a $3 \cdot 2 - 2 \cdot 3 = 0$.

(b) Faux : $\{2\}$ est une famille libre maximale non génératrice de $\mathbb{Z}$. En effet, pour tout $a, b \in \mathbb{Z}$ on a $ba - ab = 0$, donc les familles libres de $\mathbb{Z}$ ont au plus un élément.

(c) Vrai. On a vu en cours qu'un groupe abélien de type fini sans torsion est libre.

(d) Vrai (plus difficile). Si $e_1, \ldots, e_n$ est une famille libre de G, regardons $H = \mathbb{Z}e_1 \oplus \mathbb{Z}e_2 \oplus \cdots \oplus \mathbb{Z}e_n$. Aucun élément non nul de H n'est d'ordre fini : on a donc $H \cap G_{\mathrm{tor}} = \{0\}$. On en déduit que les images des e_i dans G/G_{tor} forment encore une famille libre de G/G_{tor}. Mais on a $G/G_{\mathrm{tor}} \simeq \mathbb{Z}^m$ où m est le rang de G. Il ne reste qu'à montrer qu'une famille libre $f_1, \ldots, f_n$ de $\mathbb{Z}^m$ a au plus m éléments. Pour cela, on voit $\mathbb{Z}^m$ comme inclus dans $\mathbb{Q}^m$. On constate que les f_i sont $\mathbb{Q}$-linéairement indépendants. En effet, si on a $\sum_{i=1}^n \lambda_i f_i = 0$ avec $\lambda_i \in \mathbb{Q}$, on écrit $\lambda_i = p_i/q$ avec $q \geq 1$ et les p_i dans $\mathbb{Z}$, on en déduit en multipliant par q que l'on a $\sum_{i=1}^n p_i f_i = 0$. Par $\mathbb{Z}$-liberté des f_i on a donc $p_i = 0$ pour tout i, puis $\lambda_i = 0$ pour tout i. Mais dans le $\mathbb{Q}$-espace vectoriel $\mathbb{Q}^m$, les familles $\mathbb{Q}$-libres ont au plus m éléments. On a donc $n \leq m$.

(e) Faux. Soient $p_1, \ldots, p_n$ des nombres premiers distincts. On pose $q_i = \prod_{j \neq i} p_j$. Alors les q_i sont premiers entre eux dans leur ensemble, mais aucun sous-ensemble strict des q_i n'a cette propriété. Ainsi, $q_1, \ldots, q_n$ est une famille génératrice minimale de $\mathbb{Z}$.

(f) Faux : $\{1\}$ et $\{2, 3\}$ sont deux familles génératrices minimales de $\mathbb{Z}/6\mathbb{Z}$.

Exercice 3.10. Supposons que $h_1, \ldots, h_m$ engendrent H et que $x_1H, \ldots, x_nH$ engendrent G/H, avec $x_i \in G$. Alors $\{x_1, \ldots, x_n, h_1, \ldots, h_m\}$ engendre G. En effet, soit $\pi : G \to G/H$ la projection canonique. Pour $g \in G$, $\pi(g)$ est un certain mot en les x_iH et les $(x_iH)^{-1} = x_i^{-1}H$. Soit $g' \in \langle x_1, \ldots, x_n \rangle$ ce même mot, mais en les x_i et les $x_i^{\pm 1}$. On a donc $\pi(g') = \pi(g)$. Mais alors $(g')^{-1}g$ est dans $H = \langle h_1, \ldots, h_m \rangle$. On a donc montré $G \subset \langle x_1, \ldots, x_n \rangle \langle h_1, \ldots, h_m \rangle$.

Exercice 3.11. (i) C'est le cas $G = \mathbb{Z}g$ monogène (disons non nul). Considérons

$$\varphi : \mathbb{Z} \to G, m \mapsto mg.$$

C'est un morphisme surjectif. Si H est un sous-groupe de G, on a $H = \varphi(\varphi^{-1}(H))$ et $\varphi^{-1}(H)$ est un sous-groupe de $\mathbb{Z}$. On a donc $\varphi^{-1}(H) = d\mathbb{Z}$ pour un certain $d \geq 0$, puis $H = \varphi(d\mathbb{Z}) = \mathbb{Z}dg$ est monogène, et donc $\min(H) \leq 1 = \min(G)$.

(ii) Posons $n = \min(G)$ et choisissons $g_1, \ldots, g_n$ des générateurs de G. On pose $g = g_1$. Alors $G' = G/\langle g \rangle$ est engendré par les images $g_i\langle g \rangle$ des g_i dans G'. Mais comme celle de g_1 est triviale, G' est engendré par les $g_i\langle g \rangle$ avec $i > 1$. On a donc $\min(G') \leq n - 1 < \min(G)$.

(iii) On raisonne par récurrence sur $\min(G)$, le cas $\min(G) = 0$ étant évident. Supposons $\min(G) \geq 1$. Regardons le morphisme $H \to G'$ de l'énoncé. Soient H' son image et $H'' = H \cap \langle g \rangle$ son noyau. Par l'exercice précédent, on a $\min(H) \leq \min(H') + \min(H'')$.

Par le (i), on a $\min(H'') \leq 1$ car $H'' \subset \mathbb{Z}g$. Par récurrence et le (ii), on a $\min(H') \leq \min(G') < \min(G)$. On a donc $\min(H) \leq \min(G)$.

(iv) Un sous-groupe H de $\mathbb{Z}^n$ vérifie $\min(H) \leq n$ par ce que l'on a montré. Il est donc de type fini. Il est aussi sans torsion. Il est donc libre par le cours, *i.e.* $H \simeq \mathbb{Z}^m$. On conclut car $\min(\mathbb{Z}^m) = m$.

Exercice 3.12. Notons a et b les matrices respectives de l'énoncé, et $G = \langle a, b\rangle$. On a
$$a^{-n}ba^n = \begin{bmatrix} 1 & \frac{1}{2^n} \\ 0 & 1 \end{bmatrix}.$$
On en déduit que G contient toutes les matrices de la forme $\mathrm{m}(x) := \begin{bmatrix} 1 & x \\ 0 & 1 \end{bmatrix}$ avec x dans
$$\mathbb{Z}[1/2] = \{m/2^n \mid m \in \mathbb{Z},\ n \geq 0\}.$$
Mais ces matrices forment un sous-groupe de G isomorphe à $(\mathbb{Z}[1/2], +)$, via $x \mapsto \mathrm{m}(x)$, et ce dernier est un sous-groupe de $\mathbb{Q}$ qui n'est pas de type fini (*dénominateurs non bornés*).

Exercice 3.13. On sait que le groupe $H = (\mathbb{Z}/2\mathbb{Z})^3$ vérifie $\min(H) = 3$. Mais par Cayley, ce groupe est isomorphe à un sous-groupe de $G = \mathrm{S}_8$. Mais nous verrons bientôt que pour $n > 2$, le groupe S_n est non abélien et engendré par $(1\,2)$ et $(1\,2\,3\,\ldots\,n)$, donc $\min(\mathrm{S}_n) = 2$.

Exercice 3.15. (i) est une vérification immédiate. Montrons (ii). Posons $n = |G|$. On a $g^n = 1$ pour tout $g \in G$ par Lagrange. Comme $X^n - 1$ est à racines simples dans $\mathbb{C}[X]$, chaque endomorphisme $g \in G$ est diagonalisable (de valeurs propres des racines n-èmes de l'unité). Comme G est commutatif, ses éléments sont codiagonalisables. Soit $v \in V - \{0\}$ un vecteur propre commun : pour tout $g \in G$ il existe $\lambda_g \in \mathbb{C}^\times$ avec $gv = \lambda_g v$. On a d'une part $g'(gv) = g'(\lambda_g v) = \lambda_g g'v = \lambda_g \lambda'_g v$, et d'autre part $g'(gv) = (g'g)(v) = \lambda_{gg'} v$, donc $\lambda_{gg'} = \lambda_g \lambda'_g$ pour tout $g, g' \in G$ (comme $v \neq 0$). Ainsi, $\chi(g) := \lambda_g$ définit un élément χ de $\widehat{G}$, et on a $v \in V_\chi$. On a donc $V = \sum_\chi V_\chi$ par codiagonalisabilité. Reste à voir que la somme est directe. Supposons que l'on a $v_1 + \cdots + v_n = 0$ avec $v_i \neq 0$, $v_i \in V_{\chi_i}$, $\chi_i \neq \chi_j$ pour $i \neq j$, et n minimal. On a clairement $n > 1$. En appliquant $g \in G$ à $v_1 + \cdots + v_n = 0$ on a $\sum_i \chi_i(g) v_i = 0$, puis $\sum_i (\chi_i(g) - \chi_1(g)) v_i = 0$. Par minimalité de n, on a donc $\chi_i(g) = \chi_1(g)$ pour tout g, *i.e.* $\chi_i = \chi_1$, une contradiction.

Exercice 3.16. (i) Soit χ un caractère de $G_1 \times G_2$. On définit $\chi_1 : G_1 \to \mathbb{C}^\times$ et $\chi_2 : G_2 \to \mathbb{C}^\times$ par $\chi_1(g) = \chi(g, 1)$ et $\chi_2(g) = \chi(1, g)$. Ce sont deux caractères. On a donc défini une application $\widehat{G_1 \times G_2} \to \widehat{G_1} \times \widehat{G_2}$, $\chi \mapsto (\chi_1, \chi_2)$. C'est clairement un morphisme de groupes. La formule $\chi(g_1, g_2) = \chi((g_1, 1)(1, g_2)) = \chi(g_1, 1)\chi(1, g_2) = \chi_1(g_1)\chi_2(g_2)$ montre qu'il est injectif. Il est surjectif, car si $\psi_i : G_i \to \mathbb{C}^\times$ sont des caractères pour $i = 1, 2$, alors $\chi(g_1, g_2) := \psi_1(g_1)\psi_2(g_2)$ est un caractère de $G_1 \times G_2$ avec $\chi_i = \psi_i$ pour $i = 1, 2$.

(ii) Soit G un groupe abélien fini. On sait qu'il existe un isomorphisme $G \simeq \prod_{i=1}^n \mathbb{Z}/a_i\mathbb{Z}$ avec $a_1, \ldots, a_n$ des entiers ≥ 1. On a donc $\widehat{G} \simeq \prod_{i=1}^n \widehat{\mathbb{Z}/a_i\mathbb{Z}}$ par le (i). Mais on a vu en cours que pour $m \geq 1$ on a $\widehat{\mathbb{Z}/m\mathbb{Z}} \simeq \mu_m \simeq \mathbb{Z}/m\mathbb{Z}$. On a donc bien $\widehat{G} \simeq G$.

Exercice 3.17. (i) Dire que ι_G est injective signifie que pour tout $g \neq 1$, il existe $\chi \in \widehat{G}$ tel que $\chi(g) \neq 1$. Fixons donc $g \neq 1$. L'étude des caractères d'un groupe cyclique montre qu'il existe $\psi : \langle g\rangle \to \mathbb{C}^\times$ avec $\psi(g) \neq 1$. On conclut en considérant un prolongement χ de ψ à G tout entier. L'injectivité de ι_G entraîne sa bijectivité, car on a $|\widehat{\widehat{G}}| = |\widehat{G}| = |G|$.

(ii) La bijectivité de ι montre que les caractères de $\widehat{G}$ sont les $\chi \mapsto \chi(g)$ avec $g \in G$. Les relations d'orthogonalité s'écrivent donc $\frac{1}{|G|} \sum_{\chi \in \widehat{G}} \chi(g)\overline{\chi}(h) = 0$ pour $h \neq g$, 1 pour $h = g$.

Exercice 3.18. (i) G est un 2-groupe abélien élémentaire, ou ce qui revient au même, un $\mathbb{Z}/2\mathbb{Z}$-espace vectoriel de dimension 2. Pour tout $v \in G$ non nul, il existe une unique forme linéaire $v^* : G \to \mathbb{Z}/2\mathbb{Z}$ qui vaut 0 sur v et qui est non nulle. En effet, v^* vaut automatiquement 1 sur les deux autres vecteurs non nuls, qui sont de la forme w et $w + v$. On définit aussi 0^* comme étant la forme linéaire nulle sur G. On constate que $G \to \mathrm{Hom}(G, \mathbb{Z}/2\mathbb{Z}), v \mapsto v^*$ est un isomorphisme de $\mathbb{Z}/2\mathbb{Z}$-espace vectoriels. En effet, seule la linéarité est non évidente, mais pour $u, v \in G$ on a bien $(u + v)^\star = u^* + v^*$: c'est clair si $u = v$, et si $u \neq v$ c'est vrai aussi car on a $u^*(v) = v^*(u) = 1$ (!). Ainsi, l'application $G \to \widehat{G}, u \mapsto (-1)^{u^*}$ est un isomorphisme de groupes. Je le qualifierais de naturel car on n'a utilisé aucun choix particulier pour le définir.

(ii) L'existence de χ_g est du cours. Un φ comme dans l'énoncé est unique, car c'est un morphisme et qu'il est donné sur un générateur de G. Soit g un générateur du groupe cyclique G (d'ordre n). Pour tout $k \in (\mathbb{Z}/n\mathbb{Z})^*$, on sait que g^k est encore un générateur de G, on a donc d'une part $\varphi(g^k) = \chi_{g^k}$ et d'autre part $\varphi(g^k) = \varphi(g)^k = (\chi_g)^k$ (car φ est un morphisme). En évaluant ces égalités en l'élément g^k, on a donc $\varphi(g^k)(g^k) = \chi_{g^k}(g^k) = e^{2i\pi/n}$ et $\varphi(g^k)(g^k) = (\chi_g(g^k))^k = \chi_g(g)^{k^2} = e^{2i\pi k^2/n}$, ce qui conclut.

(iii) On a donc $k^2 \equiv 1 \bmod n$ pour tout k premier à n. Ainsi, $(\mathbb{Z}/n\mathbb{Z})^\times$ est un 2-groupe abélien élémentaire. En particulier, l'indicatrice d'Euler $\varphi(n)$ est une puissance de 2, ce qui force $n = 2^m$ ou $n = 3 \cdot 2^m$ avec $m \geq 0$. Mais alors 5 est premier à n, et $5^2 \equiv 1 \bmod n$, donc n divise $25 - 1 = 24$.

(iv) Supposons donc G cyclique d'ordre n avec $n \mid 24$. Fixons un générateur g de G. Pour $k, k' \in \mathbb{Z}$ on définit $\varphi(g^k) \in \widehat{G}$ par $\varphi(g^k)(g^{k'}) = e^{2i\pi kk'/n}$. On constate que c'est bien défini (le résultat ne dépend que de $k \bmod n$ et $k' \bmod n$). Par définition, on a $\varphi(g^k g^q) = \varphi(g^{k+q})$: φ est un morphisme $G \to \widehat{G}$. De plus, caractère le $\varphi(g^k)$ de G vaut $e^{2i\pi k^2/n}$ en g^k. On conclut car pour $n|24$, on a $k^2 \equiv 1 \bmod n$ pour tout k premier à n. (C'est la réciproque de l'observation du (ii), plus facile.)

Exercice 3.19 (i) (C'est assez tautologique mais on vérifie quand même les détails) Vérifions la bilinéarité de b_f. Fixons $g \in G$. L'application $h \mapsto \mathrm{b}_f(g, h) = f(g)(h), G \to \mathbb{C}^\times$ est un morphisme : c'est le caractère $f(g)$. L'application $h \mapsto \mathrm{b}_f(h, g) = f(h)(g)$ est aussi un morphisme car f est un morphisme de groupes. Donc $f \mapsto \mathrm{b}_f$ est bien définie (c'est même un morphisme de groupes si l'on munit $\mathrm{Bil}(G)$ de la loi évidente). Elle est trivialement injective. Elle est aussi surjective car pour $b \in \mathrm{Bil}(G)$, posant $f(g)(h) = b(g, h)$ alors $g \mapsto f(g)$ est un morphisme $G \to \widehat{G}$ vérifiant $b = \mathrm{b}_f$.

(ii) Il est équivalent de dire que f est injective, et que b_f est non dégénérée à droite. Comme $\widehat{G}$ et G ont même cardinal, f est injective si et seulement si f est bijective. Cela montre $(a) \iff (b)$. On dispose aussi du morphisme $f' : G \to \widehat{G}$, $g \mapsto (h \mapsto f(h)(g) = \mathrm{b}_f(h, g))$. Il est injectif si, et seulement si, b_f est non dégénéré à gauche. Le noyau de f' est l'ensemble des éléments $g \in G$ tels que $f(h)(g) = 1$ pour tout $h \in G$. S'il possède un élément non trivial g, cela veut dire que tout les caractères dans $f(G)$ sont triviaux sur h. Mais par prolongement des caractères il existe $\chi \in \widehat{G}$ tel que $\chi(h) \neq 1$, donc f n'est pas surjective. Cela montre $(a) \implies (c)$. Enfin, si f' est injective, elle est surjective, donc tout caractère de G est de la forme $h \mapsto f(h)(g)$ pour un certain $g \in G$. Comme tous ces caractères sont triviaux sur $\ker f$, cela entraîne que f est injective, donc bijective.

Exercice 3.20. (i) f est naturel si, et seulement si, pour tout $g \in G$ on a $f(\alpha(g)) = f(g) \circ \alpha^{-1}$, soit encore si pour tout g et h dans G on a $f(\alpha(g))(h) = f(g)(\alpha^{-1}(h))$, *i.e.* $\mathrm{b}_f(\alpha(g), h) = \mathrm{b}_f(g, \alpha^{-1}(h))$, et on conclut par la bijection $h \mapsto \alpha(h)$.

(ii) Pour le (iv), l'isomorphisme construit satisfait par définition $\mathrm{b}_f(g^a, g^b) = e^{2i\pi ab/n}$. Mais comme G est cyclique d'ordre n, on sait que $(\mathbb{Z}/n\mathbb{Z})^\times \to \mathrm{Aut}(G), k \mapsto (x \mapsto x^k)$, est un isomorphisme. On conclut car pour tout $k \in (\mathbb{Z}/n\mathbb{Z})^\times$ on a $k^2 \equiv 1 \bmod n$ et donc $\mathrm{b}_f(g^{ak}, g^{bk}) = e^{2i\pi k^2 ab/n} = \mathrm{b}_f(g^a, g^b)$. Considérons maintenant l'exemple du (i). On rappelle que l'on voit G comme un $\mathbb{Z}/2\mathbb{Z}$-espace vectoriel de dimension 2. On a $\mathrm{b}_f(u,v) = (-1)^{u^*(v)}$ par définition. On constate que la forme $\mathbb{Z}/2\mathbb{Z}$-bilinéaire $(u,v) \mapsto u^*(v) \in \mathbb{Z}/2\mathbb{Z}$ est alternée et non nulle. Comme on est sur $(\mathbb{Z}/2\mathbb{Z})^2$, il n'y a qu'une seule telle forme, qui coincide nécessairement avec le déterminant (dans n'importe quelle base) ! On a $\mathrm{Aut}(G) \simeq \mathrm{GL}_2(\mathbb{Z}/2\mathbb{Z}) = \mathrm{SL}_2(\mathbb{Z}/2\mathbb{Z})$, donc tout automorphisme α de G vérifie bien $\mathrm{b}_f(\alpha(g), \alpha(h)) = \det(\alpha)\mathrm{b}_f(g,h) = \mathrm{b}_f(g,h)$.

(iii) Supposons que f est un isomorphisme naturel entre G et son dual. Soit $k \in \mathbb{Z}$ premier à l'exposant e de G. Alors $x \mapsto kx$ est un automorphisme de G. On en déduit $k^2x = x$ pour tout x dans G. En effet, soit on applique directement la définition d'isomorphisme naturel $G \to \widehat{G}$ à cet automorphisme, soit on écrit $\mathrm{b}_f(kx, ky) = \mathrm{b}_f(x,y)$ pour tout $x, y \in G$, puis $\mathrm{b}_f(kx, y)^k = \mathrm{b}_f(k^2x, y) = \mathrm{b}_f(x,y)$ pour tout x, y dans G, et on conclut par non dégénérescence de b_f. On en déduit que l'exposant e de G vérifie $k^2 \equiv 1 \bmod e$ pour tout k premier à e, donc e divise 24.

(iv) On a $G = G[n] \oplus G[m]$ (voir l'Exercice 3.4). L'application naturelle $\widehat{G} \to \widehat{G[n]} \times \widehat{G[m]}, \chi \mapsto (\chi_{|G[n]}, \chi_{|G[m]})$, est bijective par l'argument de l'Exercice 3.16. De plus, on sait que si G' est un autre groupe abélien, tout (iso-)morphisme $G \to G'$ induit par restriction à $G[n]$ un (iso-)morphisme $G[n] \to G'[n]$ (idem avec n remplacé par m, bien entendu). Ainsi, l'application $\mathrm{Aut}(G) \to \mathrm{Aut}(G[n]) \times \mathrm{Aut}(G[m]), \varphi \mapsto (\varphi_{|G[n]}, \varphi_{|G[m]})$, est bijective. De même, l'application naturelle $\mathrm{Hom}(G, \widehat{G}) \to \mathrm{Hom}(G[n], \widehat{G[n]}) \times \mathrm{Hom}(G[m], \widehat{G[m]})$ est bijective. Le résultat en découle.

(v) Tout élément c de G s'écrit de manière unique $c = c_1 + \cdots + c_n$ avec $c_i \in C_i$. Fixons $1 \leq i \leq n$. L'application $\alpha_i : G \mapsto G$ envoyant $c \in G$ sur l'unique élément c' tel que $c'_i = -c_i$ et $c'_j = c_j$ pour $j \neq i$ est clairement un automorphisme de G (*inversion à la place* i). Pour $j \neq i$, on a donc $f(x_i, x_j) = f(\alpha_i(x_i), \alpha_i(x_j)) = f(-x_i, x_j) = f(x_i, x_j)^{-1}$, puis $f(x_i, x_j)^2 = 1$.

(vi) Comme $e_i \,|\, e_n$ pour $i < n$, il existe un morphisme de groupes $C_n \to C_i$ envoyant x_n sur x_i. Notons $\beta_i : G \to G$ l'application envoyant $c = \sum_{i=1}^n c_i$ sur l'unique élément c' vérifiant $c'_j = c_j$ pour $j < n$, et $c'_n = c_n + \varphi(c_n)$. C'est clairement un morphisme de groupes, manifestement injectif, donc bijectif : c'est un automorphisme (c'est une *transvection* !). Il vérifie $\beta_i(x_j) = x_j$ pour $j < n$ et $\beta_i(x_n) = x_n + x_i$. On a donc, toujours pour $j < n$,

$$f(x_j, x_n) = f(\beta_i(x_j), \beta_i(x_n)) = f(x_j, x_n + x_i) = f(x_j, x_n)f(x_j, x_i),$$

puis $f(x_j, x_i) = 1$.

(vii) Si $e_1 = 2$, on peut trouver un morphisme de groupes $C_1 \to C_n$ envoyant x_1 sur l'élément y (car $2y = 0$). En procédant comme au (vi), il existe donc un automorphisme γ de G envoyant x_1 sur $x_1 + y$, et x_i sur x_i pour $i > 1$. On a $f(x_1, x_n) = f(\gamma(x_1), \gamma(x_n)) = f(x_1 + y, x_n) = f(x_1, x_n)f(y, x_n)$ puis $f(y, x_n) = 1$.

(viii) Si b est non dégénérée, alors G est naturellement isomorphe à son dual par le (i) et l'Exercice 3.19, et donc l'exposant e_n de G divise 24 par le (iii).

(ix) Pour $i < n$, on a $f(x_i, x_j) = \pm 1$ pour tout j par les (v) et (vi). On a donc $1 = f(2x_i, x_j) = f(x_i, x_j)^2$ pour tout j, puis $f(2x_i, g) = 1$ pour tout g dans G, et donc $2x_i = 0$ car f est non dégénérée. Cela montre $e_i = 2$ pour $i < n$ (et donc e_n est pair.) Supposons $n > 2$. Alors l'un au moins des trois éléments $f(x_1, x_n), f(x_2, x_n)$ et $f(x_1 + x_2, x_n) = f(x_1, x_n)f(x_2, x_n)$ vaut 1, car $f(x_i, x_n) = \pm 1$ par (v). Soit $u \in \{x_1, x_2, x_1 + x_2\}$ avec $f(u, x_n) = 1$. Le (vi) montre alors $f(u, x_i) = 1$ pour tout i, puis $u = 0$ par non dégénérescence : absurde. Si on a $n \equiv 0 \bmod 4$, alors y est un carré dans C_n, et donc

$f(x_i, y) = 1$ pour $i < n$ par le (v). Mais on a aussi $f(x_n, y) = 1$ par le (vii), et donc $y = 0$ par non dégénérescence. Absurde.

(x) Supposons G isomorphe à son dual. Si G est cyclique, il est d'ordre divisant 24 par le (iii), et réciproquement on a vu que les groupes cycliques d'un tel ordre conviennent. Supposons G non cyclique. La question (ix) montre que ses facteurs invariants sont $(2, e)$ avec $e|24$ et e non multiple de 4. On a donc soit $e = 2$ et $G \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$, soit $e = 6$ et $G \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z}$. Autrement dit, on a $G[2] \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ et $G[3] \simeq \mathbb{Z}/3\mathbb{Z}$. Ces exemples conviennent par le (ii) et (iv).

Exercice 3.21. L'application de l'énoncé est un morphisme de groupes. Il suffit de voir que son noyau est trivial. Soit $g \in G$ non trivial. Si g est d'ordre fini, on peut trouver un caractère χ du groupe cyclique $\langle g \rangle$ avec $\chi(g) \neq 1$ par le cours. Si g est d'ordre infini, c'est aussi vrai, et même plus facile : pour n'importe quel $x \in \mathbb{C}^\times$, $\chi(g^k) := x^k$ définit un caractère de $\langle g \rangle$, avec $\chi(g) \neq 1$ dès que $x \neq 1$. Comme $\mathbb{C}^\times$ est divisible, on peut prolonger χ en un caractère de G : l'application de l'énoncé est injective. Cela prouve le (i). Pour le (ii), on observe que si D est divisible, il en va de même du groupe produit D^I pour tout ensemble I.

Exercice 3.22. Pour tout entier $n \geq 1$, le morphisme $x \mapsto nx$ est bijectif. Pour $\lambda \in \mathbb{Q}$ et $x \in G$, il y a alors un sens à considérer "λx" dans G. Pour le voir, observons que si on a $p/q = p'/q'$ dans $\mathbb{Q}$, avec p, p', q, q' dans $\mathbb{Z}$ et $q, q' \geq 1$, et si y et y' sont les uniques éléments de G vérifiant $qy = px$ et $q'y = p'x$, alors $y = y'$. En effet, on a $pq' = qp'$ puis

$$qq'y' = qp'x = q'px = q'qy,$$

et donc $y = y'$ par bijectivité de la multiplication par qq' dans G. Au final, pour tout $\lambda \in \mathbb{Q}$ et tout $x \in G$, il existe un unique élément que l'on notera $\lambda x \in G$ tel que pour toute écriture $\lambda = p/q$ avec $p, q \in \mathbb{Z}$ et $q \geq 1$ on ait $q\lambda x = px$. Il est alors trivial de vérifier que $\mathbb{Q} \times G \to G, (\lambda, x) \mapsto \lambda x$, est une structure de $\mathbb{Q}$-espace vectoriel sur G dont le groupe abélien sous-jacent est G. Le (i) s'en déduit en considérant une base de ce $\mathbb{Q}$-espace vectoriel. Pour le (ii), on applique l'Exercice 1.18 Chap. 1.

Exercice 3.23. (i) Montrons $A_{\text{tor}} = \prod'_p \mathbb{Z}/p\mathbb{Z}$ (produit restreint). Autrement dit, un élément $x = (x_p)$ avec $x_p \in \mathbb{Z}/p\mathbb{Z}$ est d'ordre fini si, et seulement si, on a $x_p = 0$ pour tout p assez grand. En effet, si $x_p = 0$ pour $p \geq N$, et si on pose $n = \prod_{p \leq N}$, on a $nx = (nx_p) = 0$. Réciproquement, si on a $n \geq 1$ et $nx = 0$, alors on a $nx_p = 0$ pour tout p. Comme n est inversible dans l'anneau $\mathbb{Z}/p\mathbb{Z}$ pour $p > n$, on a donc $x_p = 0$ pour $p > n$.

(ii) Soit n un entier ≥ 1. Vérifions que la multiplication par $n : A/A_{\text{tor}} \to A/A_{\text{tor}}, x + A_{\text{tor}} \mapsto nx + \mathrm{A}_{\text{tor}}$, est surjective. Soit $x \in A$. Comme la multiplication par n est surjective sur $\mathbb{Z}/p\mathbb{Z}$ pour tout $p > n$, il existe $y \in A$ tel que $y_p = nx_p$ pour $p > n$. Mézalor $y - nx$ a toutes ses p-coordonnées nulles pour $p > n$, et donc $y - nx \in A_{\text{tor}}$ par le (i).

(iii) Pout tout groupe abélien G, le groupe G/G_{tor} est sans torsion. En effet, soient $\pi : G \to G/G_{\text{tor}}$ la projection canonique et $x \in G/G_{\text{tor}}$ de torsion. Il existe $n \geq 1$ avec $x^n = 1$ dans G/G_{tor}. Soit $y \in G$ avec $\pi(y) = x$. On a $1 = x^n = \pi(y^n)$ donc $y^n \in \ker \pi = G_{\text{tor}}$. Ainsi, il existe $m \geq 1$ avec $(y^n)^m = 1$. Mais alors $y^{nm} = 1$ avec $nm \geq 1$ et donc $y \in G_{\text{tor}}$ et $x = \pi(y) = 1$. Ainsi, $G = A/A_{\text{tor}}$ est sans torsion, et divisible par le (ii). Autrement dit, il est uniquement divisible : les applications $G \to G, x \mapsto x^n$, sont bijectives pour $n \geq 1$. Par l'Exercice 3.22, on a donc $G \simeq \mathbb{Q}^{(I)}$ pour un certain ensemble I, avec en outre $I \sim G$ si G est indénombrable. La projection sur une coordonnée répond à la question.

(iv) On utilise les exercices sur la cardinalité du Chapitre 1. On a $\{0,1\}^{\mathbb{N}}$ qui s'injecte dans A, et A qui s'injecte dans $\mathbb{N}^{\mathbb{N}}$. Mais $\{0,1\}^{\mathbb{N}}$ et $\mathbb{N}^{\mathbb{N}}$ sont tous deux équipotents à $\mathbb{R}$ (Cantor, Exercice 1.11 Chap. 1.). On a donc $A \sim \mathbb{R}$ par Cantor-Bernstein. Mais

A_{tor} est dénombrable : c'est une réunion dénombrable d'ensemble finis (par exemple des $\prod_{p\leq n}\mathbb{Z}/p\mathbb{Z}\times\{0\}$ pour $n\geq 1$). Par Lagrange, on a aussi $A\sim A/A_{\text{tor}}\times A_{\text{tor}}$, et donc $\mathbb{R}\sim A/A_{\text{tor}}\times\mathbb{N}$. On en déduit d'abord que A/A_{tor} est infini, puis $A/A_{\text{tor}}\times\mathbb{N}\sim A/A_{\text{tor}}$, et donc $A/A_{\text{tor}}\sim\mathbb{R}$. Comme $\mathbb{R}$ est indénombrable, on a donc $A/A_{\text{tor}}\simeq\mathbb{Q}^{(I)}$ avec $I\sim\mathbb{R}$.

Exercice 3.24. (i) Le fait que $\mathbb{Z}_p$ est un sous-groupe découle de ce que l'application naturelle (bien définie) $f_n:\mathbb{Z}/p^{n+1}\mathbb{Z}\to\mathbb{Z}/p^n\mathbb{Z}$, $x \bmod p^{n+1}\mapsto x\bmod p^n$, est un morphisme de groupes. Le fait que $\mathbb{Z}_p\to\mathbb{Z}/p^n\mathbb{Z},(x_n)\mapsto x_n$, est un morphisme de groupes est évident (définition d'un groupe produit). Il est surjectif, car pour tout $y\in\mathbb{Z}$, l'élément (y_m) avec $y_m:=y\bmod p^m$ est dans $\mathbb{Z}_p$, et sa composante $y_n\in\mathbb{Z}/p^n\mathbb{Z}$ est arbitraire.

(ii) Comme au (iv) ci-dessus on a $\{0,1\}^n\hookrightarrow\mathbb{Z}_p\hookrightarrow\mathbb{N}^{\mathbb{N}}$ et donc $\mathbb{Z}_p$ est équipotent à $\mathbb{R}$ par Cantor-Bernstein.

(iii) Soit $(x_n)\in\mathbb{Z}_p$ non nul. Il existe $N\geq 1$ tel que $x_N\neq 0$. On peut donc écrire $x_N\in p^v(\mathbb{Z}/p^N\mathbb{Z})^\times$ avec $0\leq v<N$. Mais pour $M\geq N$, l'élément x_N est image de x_M par la projection naturelle $\mathbb{Z}/p^M\mathbb{Z}\to\mathbb{Z}/p^N\mathbb{Z}$. On a donc aussi $x_M\in p^v(\mathbb{Z}/p^M\mathbb{Z})^\times$. L'ordre de x_M dans $\mathbb{Z}/p^M\mathbb{Z}$ est donc p^{M-v}. Cet ordre tend vers l'infini avec M. Ainsi, il n'existe aucun entier $m\geq 1$ tel que $m(x_n)=(mx_n)=0$.

(iv) Soit χ un caractère de μ_{p^∞}. Sa restriction au groupe cyclique μ_{p^n} vérifie donc $\chi(e^{2i\pi/p^n})=e^{2i\pi k_n/p^n}$ pour un certain $k_n\in\mathbb{Z}$, uniquement déterminé modulo p^n. En appliquant χ à l'égalité $(e^{2i\pi/p^{n+1}})^p=e^{2i\pi/p^n}$ on déduit $e^{2i\pi k_{n+1}/p^n}=e^{2i\pi k_n/p^n}$, ou ce qui revient au même, $k_{n+1}\equiv k_n\bmod p^n$. Ainsi, $k(\chi):=(k_n)$ est dans $\mathbb{Z}_p$.

(v) On a défini ci-dessus une application $\widehat{\mu_{p^\infty}}\to\mathbb{Z}_p$, $\chi\mapsto k(\chi)$. C'est un morphisme de groupes : on a $k(\chi)+k(\psi)=k(\chi\psi)$. Il est clairement injectif puisqu'on a $\chi(e^{2i\pi/p^n})=1$ si, et seulement si, $k_n\equiv 0\bmod p^n$. Il ne reste donc qu'à justifier sa surjectivité. Soit $k=(k_n)$ un entier p-adique. On définit un caractère χ_n du groupe cyclique $\mu_{p^n}=\langle e^{2i\pi/p^n}\rangle$ en posant $\chi(e^{2i\pi/p^n})=e^{2i\pi k_n/p^n}$. Observons que l'on a $(\chi_m)_{|\mu_{p^n}}=\chi_n$ pour $m\geq n$. En effet :

$$\chi_m(e^{2i\pi/p^n})=\chi_m(e^{2i\pi/p^m})^{p^{m-n}}=e^{2i\pi k_m/p^n}=e^{2i\pi k_n/p^n},$$

la dernière égalité venant de $k_m\equiv k_n\bmod p^n$. Ainsi, pour $x\in\mu_{p^\infty}$, $\chi_n(x)$ est bien défini et indépendant de n dès que n est assez grand de sorte que $x\in\mu_{p^n}$: on le note $\chi(x)$. On a $\chi(xy)=\chi(x)\chi(y)$ car x,y et xy sont dans un même μ_{p^n} pour n assez grand, et l'égalité vaut alors pour χ remplacé par χ_n. Par définition, on a $\chi_{|\mu_{p^n}}=\chi_n$, et donc $k(\chi)=(k_n)$.

Exercice 3.26 (i) On a $\mathrm{J}(\chi,\chi^{-1})=\sum_{x\in\mathbb{Z}/p\mathbb{Z}\smallsetminus\{1\}}\chi(\frac{x}{1-x})$. Regardons l'application

$$\mathbb{Z}/p\mathbb{Z}\smallsetminus\{1\}\to\mathbb{Z}/p\mathbb{Z},\ x\mapsto x/(1-x).$$

Elle est injective, car c'est $x\mapsto -1+1/(1-x)$. Elle ne prend pas la valeur -1. Elle définit donc une bijection $\mathbb{Z}/p\mathbb{Z}\smallsetminus\{1\}\to\mathbb{Z}/p\mathbb{Z}\smallsetminus\{-1\}$. On a donc $\mathrm{J}(\chi,\chi^{-1})=-\chi(-1)+\sum_{x\in\mathbb{Z}/p\mathbb{Z}}\chi(x)=-\chi(-1)$, car on sait que la somme est nulle pour $\chi\neq 1$.

(ii) On a $|C|=\sum_{a+b=1}\mathrm{N}(x^2=a\alpha^{-1})\mathrm{N}(y^2=b\beta^{-1})$, puis par le cours

$$|C|=\sum_{a+b=1}(1+(\frac{a\alpha^{-1}}{p}))(1+(\frac{b\beta^{-1}}{p}))=\sum_{a+b=1}(1+(\frac{\alpha}{p})(\frac{a}{p})+(\frac{\beta}{p})(\frac{b}{p})+(\frac{\alpha\beta}{p})(\frac{a}{p})(\frac{b}{p})).$$

Mais on a $\sum_{a+b}1=p$ et $\sum_a(\frac{a}{p})=0$, puis $|S|=p+(\frac{\alpha\beta}{p})\mathrm{J}(\lambda,\lambda)$, et on conclut par le (i).

(iii) On fixe u non carré dans $(\mathbb{Z}/p\mathbb{Z})^\times$. Un élément de $\mathbb{Z}/p\mathbb{Z}$ est non carré si, et seulement si, il est de la forme uy^2 avec $y\neq 0$. On regarde donc l'équation $x^2+1=uy^2$, soit $x^2-uy^2=1$. Cette équation a $p-(\frac{u}{p})=p+1$ solutions (x,y) dans $(\mathbb{Z}/p\mathbb{Z})^2$ par le (ii). L'application associant à une solution (x,y) l'élément $x^2\in(\mathbb{Z}/p\mathbb{Z})^\times$ se surjecte sur l'ensemble à dénombrer. Ses fibres ont 4 éléments, sauf pour $x^2=-1$, auquel cas les deux antécédents sont $(\pm x, 0)$. Le nombre cherché est donc $(p+1)/4$, sauf si -1 est un carré dans $\mathbb{Z}/p\mathbb{Z}$, auquel cas c'est $(p-1)/4$.

Exercice 3.27. On a vu en cours $|\mathrm{S}_p| \equiv 1 \bmod 2$ et $|\mathrm{S}_p| \equiv -1 \bmod 3$, autrement dit $|\mathrm{S}_p| \equiv -1 \bmod 6$ (Bezout). Il s'agit donc de montrer $|\mathrm{S}_p| \equiv -1 \bmod 4$, et aussi que $|\mathrm{S}_p| \equiv -1 \bmod 8$ implique $p \equiv 1 \bmod 4$. Mais d'après le théorème de Gauss vu en cours on a aussi $|\mathrm{S}_p| = p + 2A$ avec $p = A^2 + 3B^2$. En regardant modulo 4 et en se rappelant $p \neq 2$, on constate que l'on a soit A pair, B impair et $p \equiv -1 \bmod 4$, soit A impair, B pair et $p \equiv 1 \bmod 4$. Dans les deux cas on constate $p + 2A \equiv -1 \bmod 4$, et donc $|\mathrm{S}_p| \equiv -1 \bmod 4$. Enfin, si on a $p + 2A \equiv -1 \bmod 8$, on en déduit $A^2 + 3B^2 + 2A + 1 \equiv 0 \bmod 8$, puis $(A+1)^2 \equiv -3B^2 \bmod 8$. Si B est impair, on a $(A+1)^2 \equiv -3 \bmod 8$, ce qui est absurde, donc B est pair, *i.e.* $p \equiv 1 \bmod 4$.

Exercice 3.28. Pour tout entier $n \geq 1$, le nombre u_n de solutions dans $(\mathbb{Z}/p\mathbb{Z})^2$ de $y^2 = x^n + 1$ s'ecrit $u_n = \sum_{x \in \mathbb{Z}/p\mathbb{Z}} \mathrm{N}(y^2 = x^n + 1) = \sum_{x \in \mathbb{Z}/p\mathbb{Z}} (1 + (\frac{x^n+1}{p})) = p + v_n$ où $v_n = \sum_{x \in \mathbb{Z}/p\mathbb{Z}} (\frac{x^n+1}{p})$ est la somme de l'énoncé. On a $u_2 = p - 1$ par l'Exercice 3.26 (ii), donc $v_2 = u_2 - p = -1$, ce qui répond à la question (i). On a $u_3 = p + 2A$ comme dans le Théorème de Gauss vu en cours, donc $v_3 = 2A$, ce qui répond à la question (ii). Enfin, pour répondre à la question (iii) on écrit par le cours

$$u_n = \sum_{a+b=1} \mathrm{N}(y^2 = a)\mathrm{N}(x^n = -b) = \sum_{a+b=1} (1 + \lambda(a))(\sum_{\chi} \chi(-b)),$$

la somme portant sur les m caractères de $(\mathbb{Z}/p\mathbb{Z})^\times$ vérifiant $\chi^m = 1$. Mais on a $\mathrm{J}(1, \chi) = \mathrm{J}(\chi, 1) = 0$ pour $\chi \neq 1$. On a donc $v_n = u_n - p = \sum_{\chi \neq 1 \,|\, \chi^m = 1} \chi(-1)\mathrm{J}(\lambda, \chi)$. Si m est impair, aucun des $m - 1$ caractères $\chi \neq 1$ vérifiant $\chi^m = 1$ n'est l'inverse de λ (*i.e.* égal à λ), de sorte que l'on a $\lambda\chi \neq 1$ et $|\mathrm{J}(c, \chi)| = \sqrt{p}$ par le cours. Si m est pair, un seul des $m - 1$ caractères $\chi \neq 1$ vérifiant $\chi^m = 1$ est égal à $\lambda^{-1} = \lambda$, et pour $\chi = \lambda$ on a $\mathrm{J}(\chi, \lambda) = \mathrm{J}(\lambda, \lambda^{-1}) = \pm 1$ par l'Exercice 3.26 (i). Cela conclut la démonstration.

Exercice 3.29. (i) On a $G^2 = \mathrm{J}(c, c)\mathrm{G}(c^2)$ car $c^2 \neq 1$. Par la Formule (17) Chap. 3, et $c^2 = c^{-1} = \overline{c}$, on a aussi $\mathrm{G}(c^2) = c(-1)\overline{G}$. Mais on a $c(-1) = c((-1)^3) = c(-1)^3 = 1$, donc $\mathrm{G}(c^2) = \overline{G}$. On conclut par la relation $\overline{G}G = p$.

(ii) On a $J = a + bj$ avec $a, b \in \mathbb{Z}$ et $j = e^{2i\pi/3}$, donc $J + \overline{J} = a + a - b = 2a - b$. On a aussi par le cours $p = |J|^2 = a^2 - ab + b^2$, donc $4p = (2a - b)^2 + 3b^2$.

(iii) En utilisant $\sum_{x \in (\mathbb{Z}/p\mathbb{Z})^\star} \zeta^x = -1$, ainsi qu'un changement de variable $x \mapsto -x$ dans $\overline{G}$, et encore $c(-1) = 1$, on trouve $-1 + G + \overline{G} = \sum_{x \in (\mathbb{Z}/p\mathbb{Z})^\times} (c(x) + \overline{c(x)} + 1)\, \zeta^x$. Si x n'est pas un cube, on a $c(x) + \overline{c(x)} + 1 = 0$ car $c(x) = j$ ou j^2. Si x est un cube, on a $c(x) + \overline{c(x)} + 1 = 3$, et comme x est le cube d'exactement 3 éléments on a aussi $-1 + G + \overline{G} = \sum_{x \in (\mathbb{Z}/p\mathbb{Z})^\times} \zeta^{x^3}$. Le terme de droite étant réel, on peut y remplacer ζ^{x^3} par sa partie réelle $\cos(2\pi x^3/p)$, et on conclut.

(iv) On a $(G + \overline{G})^3 = G^3 + \overline{G^3} + 3G\overline{G}(G + \overline{G})$, avec $G^3 + \overline{G^3} = p(J + \overline{J}) = pA$ par le (i) et (ii), et aussi $G\overline{G} = p$, de sorte que $x = G + \overline{G}$ vérifie $x^3 = pA + 3px$. Le polynôme $X^3 - 3pX - pA$ a trois racines réelles car son discriminant $-4(-3p)^3 - 27p^2A^2 = 27p^2(4p - A^2) = 3^4p^2B^2$ est > 0 (c'est même un carré !).

Exercice 3.30. (i) Soit $\mathrm{C}_p \subset (\mathbb{Z}/p\mathbb{Z})^\times$ le sous-groupe des carrés. On suppose $p \equiv 3 \bmod 4$, et donc $-1 \notin \mathrm{C}_p$. Le morphisme $\mathrm{C}_p \to \mathrm{C}_p, x \mapsto x^2$, est alors de noyau trivial : il est donc bijectif. Ainsi, on a $\mathrm{T}_p \sim \{(x, y) \in (\mathbb{Z}/p\mathbb{Z})^2 \,|\, y^2 + x^2 = 1\}$. On est dans le cas $\alpha = \beta = 1$ de l'Exercice 3.26. On a donc $|\mathrm{T}_p| = p + 1$ car $(\frac{-1}{p}) = -1$.

(ii) On suppose $p \equiv 1 \bmod 4$. On sait qu'il existe un élément $i \in \mathbb{Z}/p\mathbb{Z}$ avec $i^2 = -1$. L'idée est d'exploiter le fait que les deux bijections $\alpha(x, y) = (x, -y)$ et $\beta(x, y) = (ix, y)$ de

$(\mathbb{Z}/p\mathbb{Z})^2$ préservent T_p. En anticipant un peu sur la suite du cours on peut procéder comme suit. Soit G le sous-groupe de $\mathrm{S}_{(\mathbb{Z}/p\mathbb{Z})^2}$ engendré par α et β. On vérifie aisément que ce groupe est d'ordre 8 (en fait, isomorphe à D_8). Son action naturelle sur $(\mathbb{Z}/p\mathbb{Z})^2$ préserve le sous-ensemble T_p. L'orbite d'une solution $(x, y) \in \mathrm{T}_p$ est l'ensemble des $(ux, \pm y)$ avec $u = \pm 1$ ou $\pm i$. Pour $(x, y) \neq 0$, cette orbite a 8 éléments. Pour $y = 0$, la seule possibilité est $x = \pm 1$, et $\{(1, 0), (-1, 0)\}$ est une orbite à 2 éléments. Enfin, pour $x = 0$, la seule possibilité est $y = \pm 1, \pm i$, et $\{(0, \pm 1), (0, \pm i)\}$ est une orbite à 4 éléments. Écrivant T_p comme réunion disjointe de ses G-orbites on a $|\mathrm{T}_p| \equiv 2 + 4 \bmod 8$.

(iii) On fixe g un générateur du groupe cyclique $(\mathbb{Z}/p\mathbb{Z})^\times$. Comme $p \equiv 1 \bmod 4$, on sait par le cours qu'il existe exactement 4 caractères $\chi : (\mathbb{Z}/p\mathbb{Z})^\times \to \mu_4$ avec $\chi^4 = 1$, uniquement déterminés par l'élément $\chi(g) \in \mu_4$. On note c le tel que χ vérifiant $\chi(g) = i$ (il dépend du choix de g). Les 4 caractères précédents sont donc $1, c, c^2 = \lambda$ (le symbole de Legendre) et $c^3 = c^{-1}$. Par la méthode de Weil, on trouve en procédant comme dans le cours $|\mathrm{T}_p| = p + \mathrm{J}(\lambda, c) + \mathrm{J}(\lambda, \lambda) + \overline{\mathrm{J}(\lambda, c)}$. On a $\mathrm{J}(\lambda, \lambda) = -1$ par l'Exercice 3.26 (i). On constate aussi que $\mathrm{J}(\Lambda, c)$ est de la forme $a + bi$ avec $a, b \in \mathbb{Z}$. Et donc $|\mathrm{T}_p = p - 1 + 2a$. La congruence du (ii) donne $p - 1 + 2a \equiv 6 \bmod 8$, puis $a \equiv -\frac{p+1}{2} \bmod 4$. En particulier, a est impair car $p \equiv 1 \bmod 4$. Comme on a $\lambda c = c^3 \neq 1$, le cours donne $a^2 + b^2 = |\mathrm{J}(\lambda, c)|^2 = p$. Comme a est impair, on a b pair.

Exercice 3.31. (i) Fixons $a \leq k \leq b - 1$ un entier. On applique le théorème de convergence de Dirichlet (en analyse de Fourier) à la fonction 1-périodique nulle aux entiers et coïncidant avec f sur $]k, k+1[$, et en un point dans $\mathbb{Z}$. On en déduit

$$\frac{1}{2}(f(k) + f(k+1)) = \lim_{A\to\infty} \sum_{n=-A}^{A} \int_k^{k+1} f(t) e^{2i\pi nt} dt =: \sum_{n\in\mathbb{Z}} \int_k^{k+1} f(t) e^{2i\pi nt} dt.$$

On conclut en sommant cette identité pour $k = a, \ldots, b-1$. Bien noter que la sommation dans l'énoncé (et donc la somme sur $\mathbb{Z}$ de droite) est à prendre au sens de la limite ci-dessus. Pour le (ii), on applique le (i) à la fonction $f(t) = e^{2i\pi t^2/N}$ sur le segment $[0, N]$. Le terme de gauche est G_N. Par changement de variables $u = t + \frac{nN}{2}$, on a aussi

$$\int_0^N f(t) e^{2i\pi nt} dt \;=\; i^{-n^2 N} \int_{\frac{nN}{2}}^{\frac{(n+2)N}{2}} e^{\frac{2i\pi u^2}{N}} du \;=\; i^{-n^2 N} N^{1/2} \int_{\frac{n}{2}}^{\frac{n}{2}+1} e^{2i\pi u^2} du.$$

Le (ii) s'en déduit en séparant les n pairs et impairs. Pour le (iii), On en déduit d'abord $I = (1-i)^{-1} = \frac{1+i}{2}$ en prenant $N = 1$, car dans ce cas on a $\mathrm{G}_1 = 1$, et on conclut par le (ii).

Exercice 3.32. (i) On suppose ici plus généralement que p, q sont des entiers ≥ 1 premiers entre eux. Posons $\zeta = e^{\frac{2i\pi}{pq}}$. En développant, $\mathrm{G}_{p,q}\mathrm{G}_{q,p}$ est la somme, sur tous les couples $(\overline{a}, \overline{b}) \in \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/q\mathbb{Z}$, des $\zeta^{a^2q^2 + b^2p^2}$. Mais on constate $a^2q^2 + b^2p^2 \equiv (aq + bp)^2 \equiv 0 \bmod pq$. Il suffit donc de voir que l'application $\mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/q\mathbb{Z} \to \mathbb{Z}/pq\mathbb{Z}, (\overline{a}, \overline{b}) \mapsto aq + bp$, qui est bien définie et un morphisme, est bijective. Il suffit de voir qu'elle est injective, mais si on a $aq + bp \equiv 0 \mod pq$, on a $aq \equiv 0 \bmod p$ et $bp \equiv 0 \bmod q$, et comme p et q sont premiers entre eux, on a bien$a \equiv 0 \bmod p$ et $b \equiv 0 \bmod q$.

(ii) Si p divise a, on a $\mathrm{G}_{p,a} = 0$ et $(\frac{a}{p}) = 0$. On suppose a premier à p. Si $a \equiv u^2 \bmod p$, le changement de variable bijectif $\overline{k} \mapsto \overline{ku}$ dans $\mathbb{Z}/p\mathbb{Z}$ montre $\mathrm{G}_{p,a} = \mathrm{G}_{p,1} = \mathrm{G}_p$. Posons $\zeta = e^{2i\pi/p}$ et notons C_p l'ensemble des carrés de $(\mathbb{Z}/p\mathbb{Z})^\times$. Si a n'est pas un carré, l'ensemble N_p des non carrés dans $(\mathbb{Z}/p\mathbb{Z})^\times$ est $\mathrm{N}_p = a\mathrm{C}_p$. Comme tout carré non nul est le carré d'exactement 2 éléments, on a $-1 = \sum_{k\in(\mathbb{Z}/p\mathbb{Z})^\times} \zeta^k = \sum_{k\in\mathrm{C}_p} \zeta^k + \zeta^{ak} = \frac{1}{2}(\mathrm{G}_p - 1) + \frac{1}{2}(\mathrm{G}_{p,a} - 1)$, puis $\mathrm{G}_{p,a} = -\mathrm{G}_p$. On a bien montré $\mathrm{G}_{p,a} = (\frac{a}{p})\,\mathrm{G}_p$.

(iii) Par le (i) et le (ii) on a $G_{pq} = (\frac{p}{q})(\frac{q}{p})G_pG_q$. Mais pour $N \geq 1$ impair, on a vu à l'exercice précédent que l'on a $G_N = \epsilon_N N^{1/2}$, avec $\epsilon_N = 1$ pour $N \equiv 1 \bmod 4$ et $\epsilon_N = i$ pour $N \equiv 3 \bmod 4$. On en déduit

$$(\frac{p}{q})(\frac{q}{p}) = \epsilon_p\epsilon_q/\epsilon_{pq}.$$

Pour $p \equiv 1 \bmod 4$, on a $q \equiv pq \equiv 3 \bmod 4$ et donc $\epsilon_p\epsilon_q/\epsilon_{pq} = 1$, mais on a aussi $(-1)^{\frac{p-1}{2}\frac{q-1}{2}} = (-1)^{\text{pair}} = 1$. De même bien sûr pour $q \equiv 1 \bmod 4$. Enfin, pour $p \equiv q \equiv 3 \bmod 4$, et donc $pq \equiv 1 \bmod 4$, on a $\epsilon_p\epsilon_q/\epsilon_{pq} = i \cdot i/1 = -1$, et aussi $(-1)^{\frac{p-1}{2}\frac{q-1}{2}} = (-1)^{\text{impair}} = -1$. On a montré $(\frac{p}{q})(\frac{q}{p}) = (-1)^{\frac{p-1}{2}\frac{q-1}{2}}$ dans tous les cas.

(iv) Le premier point du est un cas particulier du (i) tel qu'on l'a rédigé. Pour le second , posons $\zeta = e^{2i\pi/8}$. Pour $k \in \mathbb{Z}/8\mathbb{Z}$, on a $k^2 \equiv 1 \bmod 8$ si k est impair, $k^2 \equiv 4 \bmod 8$ si $k \equiv \pm 2 \bmod 8$, et $k^2 \equiv 0 \bmod 8$ pour $k \equiv 0 \bmod 4$. On a donc $G_{8,p} = 4\zeta^p + 2(-1)^p + 2 = 4\zeta^p$.

(v) Le (ii) pour $a = 8$ montre $G_{p,8} = (\frac{8}{p})G_p$. Mais on a $(\frac{8}{p}) = (\frac{2}{p})^3 = (\frac{2}{p})$, et donc $G_{p,8} = (\frac{2}{p})G_p$. On a vu à l'exercice précédent que l'on a $G_p = \epsilon_p p^{1/2}$ et $G_{8p} = (1+i)(8p)^{1/2} = 4\zeta\sqrt{p}$. La formule $G_{8,p}G_{p,8} = G_{8p}$ s'écrit donc $4\,\zeta^p\,(\frac{2}{p})\,\epsilon_p = 4\,\zeta$, puis $(\frac{2}{p}) = \zeta^{1-p}/\epsilon_p$. Pour $p \equiv 1, 3, -3, -1 \bmod 8$, ce symbole de Legendre vaut donc respectivement $1, -1, -1$ et 1, et coïncide avec $(-1)^{\frac{p^2-1}{8}}$.

Exercice 3.33. (i) Évident. (ii) Soit $f \in L^2(G)$. On a $\widehat{f}(\chi) = \sum_{g\in G} f(g)\overline{\chi(g)}$. Notons $\mathrm{ev}_g : \widehat{G} \to \mathbb{C}^\times$ le caractère $\chi \mapsto \chi(g)$. On a donc, pour tout $g \in G$,

$$\widehat{(\widehat{f})} \circ \iota_G(g) = \widehat{(\widehat{f})}(\mathrm{ev}_g) = \sum_{\psi\in\widehat{G}} \widehat{f}(\psi)\overline{\psi(g)} = \sum_{h\in G, \psi\in\widehat{G}} f(h)\psi(h^{-1})\overline{\psi(g)} = f(g^{-1})$$

où on a utilisé $\overline{\psi(h)} = \psi(h^{-1})$ et le (ii) de l'Exercice 3.17.

Exercice 3.34. (i) Tout est immédiat sauf l'associativité de $\star$. Mais on a

$$(f \star f'') \star f''(g) = \sum_{a,b|ab=g} (f \star f')(a)f''(b) = \sum_{a,b,c|abc=g} f(a)f'(b)f''(c) = f \star (f'' \star f'')(g).$$

Pour le (ii) on observe $f \star \chi(g) = \sum_{a\in G} f(a)\chi(a^{-1}g) = \chi(g)\widehat{f}(\chi)$. Par associativité et (ii), on en déduit le (iii) : $\widehat{f \star f'}(\chi)\,\chi = f \star f' \star \chi = f \star (\widehat{f'}(\chi)\chi) = \widehat{f'}(\chi) f \star \chi = \widehat{f'}(\chi)\widehat{f}(\chi)\chi$.