8. Exercices

On commence par quelques exercices sur la structure des groupes abéliens finis.

EXERCICE 3.1. *Déterminer, à isomorphisme près, les groupes abéliens d'ordre* 2025*, et préciser dans chacun des cas leurs facteurs invariants.*

EXERCICE 3.2. *Déterminer tous les sous-groupes de* $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$.

EXERCICE 3.3. *Déterminer, à isomorphisme près, tous les groupes abéliens* G *possédant un sous-groupe* H *vérifiant* $H \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \simeq G/H$.

EXERCICE 3.4. *Soient* G *un groupe abélien.*

(i) Soient $m, n \in \mathbb{Z}$ *premiers entre eux. Montrer* $G[mn] = G[n] \oplus G[m]$.

(ii) En déduire qu'il aurait suffit de montrer le Théorème 3.1 pour les groupes abéliens finis d'ordre une puissance d'un nombre premier.

EXERCICE 3.5. *Soit* G *un groupe abélien fini. Montrer que pour tout diviseur* d *de* $|G|$ *il existe un sous-groupe de* G *d'ordre* d.

Un sous-groupe H d'un groupe G est dit *caractéristique* si on a $\alpha(H) = H$ pour tout $\alpha \in \mathrm{Aut}(G)$.

EXERCICE 3.6. *Soient* p *un nombre premier,* $n \geq 1$ *et* $G = (\mathbb{Z}/p\mathbb{Z})^n$.

(i) Monter $\mathrm{Aut}(G) \simeq \mathrm{GL}_n(\mathbb{Z}/p\mathbb{Z})$.

(ii) En déduire les sous-groupes caractéristiques de G.

EXERCICE 3.7. *Soit* G *un groupe fini tel que* $g^2 = 1$ *pour tout* $g \in G$*. Montrer que* G *est abélien, puis* $G \simeq (\mathbb{Z}/2\mathbb{Z})^n$ *pour un certain entier* $n \geq 0$.

L'exercice suivant montre que l'on ne peut pas remplacer 2 par p premier dans l'exercice ci-dessus, ou encore que la condition *abélien* est nécessaire dans la définition des groupes abéliens p-élémentaires. Si k est un corps et $n \geq 1$ est un entier, on note $\mathrm{U}_n(k)$ le sous-ensemble de $\mathrm{M}_n(k)$ constitué des matrices de la forme $\mathrm{I}_n + N$ avec $N_{ij} = 0$ pour $i \geq j$ (autrement dit, N est triangulaire supérieure nilpotente). C'est un sous-groupe de $\mathrm{GL}_n(k)$ (justifier).

EXERCICE 3.8. *Soit* p *un nombre premier.*

(i) On suppose $p \geq n$*. Montrer* $g^p = 1$ *pour tout* $g \in \mathrm{U}_n(\mathbb{Z}/p\mathbb{Z})$.

(ii) En déduire que pour $p \geq 3$*, il existe un groupe non abélien* G *d'ordre* p^3 *tel que* $g^p = 1$ *pour tout* $g \in G$.

On continue par des exercices sur les groupes abéliens de type fini. On commence par un Vrai ou Faux sur les notions de familles libres et génératrices. Dans cet exercice, la notion de maximalité/minimalité est sous-entendue relativement à la relation d'inclusion.

EXERCICE 3.9. *Soit G un groupe abélien de type fini. Deux seulement des assertions suivantes sont exactes : lesquelles ? (justifier !)*

(a) *Si G est sans torsion, une famille génératrice minimale de G est libre.*
(b) *Si G est sans torsion, une famille libre maximale de G est génératrice.*
(c) *Si G est sans torsion, il existe une famille génératrice et libre de G.*
(d) *Le cardinal des familles libres de G est uniformément borné.*
(e) *Le cardinal des familles génératrices minimales de G est uniformément borné.*
(f) *Si G est fini, les familles génératrices minimales de G ont même cardinal.*

EXERCICE 3.10. *Montrer que si H est un sous-groupe distingué d'un groupe G, et si les groupes H et G/H sont de type fini, alors G est de type fini et on a*

$$\min(G) \leq \min(H) + \min(G/H).$$

EXERCICE 3.11. *On se propose de montrer que si G est abélien de type fini, et si H est un sous-groupe de G, alors on a $\min(H) \leq \min(G)$.*

(i) Traiter le cas $\min(G) = 1$.
(ii) On suppose $\min(G) > 1$. Montrer que l'on peut trouver $g \in G$ tel que $\min(G') < \min(G)$, où l'on a posé $G' = G/\langle g \rangle$.
(iii) Conclure en considérant le morphisme $H \to G'$, $h \mapsto h\langle g \rangle$.
(iv) (Application) En déduire une démonstration du fait qu'un sous-groupe de $\mathbb{Z}^n$ est isomorphe à $\mathbb{Z}^m$ pour $m \leq n$.

L'exercice suivant montre que l'hypothèse « G est abélien » dans l'exercice ci-dessus est nécessaire.

EXERCICE 3.12. *Montrer que le sous-groupe de $\mathrm{GL}_2(\mathbb{Q})$ engendré par $\begin{bmatrix} 2 & 0 \\ 0 & 1 \end{bmatrix}$ et $\begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}$ possède un sous-groupe (abélien) qui n'est pas de type fini.*

On peut montrer qu'un sous-groupe H *d'indice fini* d'un groupe de type fini G est encore de type fini (Schreier), mais il n'est pas vrai en général qu'on a $\min(H) \leq \min(G)$ si G n'est pas abélien :

EXERCICE 3.13. *Donner un exemple de groupe fini G avec $\min(G) = 2$, ayant un sous-groupe abélien H avec $\min(H) = 3$.*

On donne maintenant quelques exercices sur les caractères.

EXERCICE 3.14. *(i) Montrer $\mathrm{H}_8/\langle -1 \rangle \simeq \mu_2 \times \mu_2$.*
(ii) En déduire les caractères de H_8.
(iii) Donner un exemple de caractère d'un sous-groupe de H_8 qui ne se prolonge pas à H_8.

EXERCICE 3.15. *Soient V un $\mathbb{C}$-espace vectoriel de dimension finie et G un sous-groupe abélien fini de $\mathrm{GL}(V)$. Pour tout $\chi \in \widehat{G}$ on pose*

$$V_\chi = \{v \in V \mid g(v) = \chi(g)v \ \forall g \in G\}.$$

(i) Montrer que V_χ est un sous-espace vectoriel de V.
(ii) Montrer $V = \bigoplus_{\chi\in\widehat{G}} V_\chi$.

EXERCICE 3.16. *(i) Montrer que si G_1 et G_2 sont deux groupes, on a un isomorphisme naturel $\widehat{G_1 \times G_2} \xrightarrow{\sim} \widehat{G_1} \times \widehat{G_2}$.*
(ii) En déduire que si G est un groupe abélien fini, alors $\widehat{G}$ est isomorphe à G.

Le (i) de l'exercice qui suit montre qu'un groupe abélien fini est canoniquement isomorphe à son bidual.

EXERCICE 3.17. (Bidualité) *Soit G un groupe abélien fini.*
(i) Montrer que l'application $\iota_G : G \to \widehat{\widehat{G}},\ g \mapsto (\chi \mapsto \chi(g))$, est un morphisme injectif, puis bijectif.
(ii) Énoncer les relations d'orthogonalité des caractères pour $\widehat{G}$ en terme de l'isomorphisme du (i).

Dans la série d'exercices suivants, on répond à la question suivante : est-ce qu'un groupe abélien fini G est *naturellement* isomorphe à son dual $\widehat{G}$? Bien entendu, il s'agira entre autres de préciser ce qu'on entend par « naturellement ».

EXERCICE 3.18. *(Groupes abéliens finis naturellement isomorphes à leur dual I)*
(i) Soit G un groupe abélien isomorphe à $(\mathbb{Z}/2\mathbb{Z})^2$ (mais on ne fixe pas de tel isomorphisme). Construire un isomorphisme $G \to \widehat{G}$ qui vous semble naturel.

On suppose désormais G cyclique d'ordre n. Pour tout générateur g de G, on note $\chi_g \in \widehat{G}$ l'unique caractère vérifiant $\chi_g(g) = e^{2i\pi/n}$ (justifier).

(ii) Supposons qu'il existe $\varphi \in \mathrm{Hom}(G, \widehat{G})$ avec $\varphi(g) = \chi_g$ pour tout générateur g de G. Montrer que φ est unique et que l'on a $k^2 \equiv 1 \bmod n$ pour tout $k \in (\mathbb{Z}/n\mathbb{Z})^\times$.
(iii) (suite) En déduire que l'entier n divise 24.
(iv) Réciproquement, montrer que si n divise 24, il existe un isomorphisme $G \to \widehat{G}$ envoyant tout générateur g de G sur χ_g.

EXERCICE 3.19. *(Dualité et formes bilinéaires) Soit $(G, +)$ un groupe abélien. On note $\mathrm{Bil}(G)$ l'ensemble des applications $b : G \times G \to \mathbb{C}^\times$ qui vérifient*

$$b(g + g', h) = b(g, h)b(g', h) \quad \text{et} \quad b(h, g + g') = b(h, g)b(h, g'), \quad \forall g, g', h \in G.$$

On dira qu'une telle application est bilinéaire. *Pour tout morphisme $f \in \mathrm{Hom}(G, \widehat{G})$, on définit $\mathrm{b}_f : G \times G \to \mathbb{C}^\times$ par $\mathrm{b}_f(g, g') = f(g)(g')$.*

(i) Montrer que $f \mapsto \mathrm{b}_f$ est une bijection $\mathrm{Hom}(G, \widehat{G}) \to \mathrm{Bil}(G)$.

Une application bilinéaire $b : G \times G \to \mathbb{C}^\times$ est dite non dégénérée à droite (resp. à gauche) si l'unique élément $g \in G$ tel que $b(h, g) = 1$ (resp. $b(g, h) = 1$) pour tout $h \in G$ est $g = 1$.

(ii) Soit $f \in \mathrm{Hom}(G, \widehat{G})$. *Montrer qu'il y a équivalence entre : (a)* f *est un isomorphisme, (b)* b_f *est non dégénérée à droite, (c)* b_f *est non dégénérée à gauche.*

Pour tout morphisme de groupes $\alpha : G \to G'$, on dispose d'un morphisme évident $\widehat{\alpha} : \widehat{G'} \to \widehat{G}, \chi \mapsto \chi \circ \alpha$ (noter l'échange de G et G'). On dira qu'un isomorphisme $f : G \to \widehat{G}$ est *naturel* si pour tout $\alpha \in \mathrm{Aut}(G)$ on a $f \circ \alpha = \widehat{\alpha}^{-1} \circ f$. Si un tel isomorphisme f existe on dira alors que G est *naturellement isomorphe à son dual.*

EXERCICE 3.20. *(Groupes abéliens finis naturellement isomorphes à leur dual II) On se propose de démontrer qu'un groupe abélien fini* G *est* naturellement isomorphe à son dual *(au sens ci-dessus) si, et seulement si, soit* $|G|$ *divise* 12, *soit* $G \simeq \mathbb{Z}/24\mathbb{Z}$.

(i) Vérifier qu'un isomorphisme $f : G \to \widehat{G}$ *est* naturel *si, et seulement si, pour tout* $\alpha \in \mathrm{Aut}(G)$ *et tout* $g, h \in G$, *on a* $\mathrm{b}_f(\alpha(g), \alpha(h)) = \mathrm{b}_f(g, h)$.

(ii) Montrer que les isomorphismes $f : G \to \widehat{G}$ *construits dans l'Exercice 3.19 (i) et (iv) sont bien* naturels *et expliciter* b_f *dans les deux cas.*

(iii) Montrer que si G *est* naturellement isomorphe à son dual, *alors l'exposant de* G *divise* 24.

(iv) Soit G *un groupe abélien d'ordre* mn *avec* $(m, n) = 1$. *Montrer que* G *est* naturellement isomorphe à son dual *si, et seulement si,* $G[m]$ *et* $G[n]$ *le sont.*

Soit $b : G \times G \to \mathbb{C}^\times$ *bilinéaire vérifiant* $b(\alpha(g), \alpha(h)) = b(g, h)$ *pour tout* g, h *dans* G, *et tout* $\alpha \in \mathrm{Aut}(G)$. *On suppose* $G = C_1 \oplus C_2 \oplus \cdots \oplus C_n$ *avec* $n \geq 2$, C_i *cyclique d'ordre* e_i, *disons engendré par l'élément* $x_i \in C_i$, *et enfin* $e_1 \,|\, e_2 \,|\, \ldots \,|\, e_n$.

(v) Montrer $f(x_i, x_j) = \pm 1$ *pour* $i \neq j$.

(vi) Montrer $f(x_i, x_j) = 1$ *pour tout* $1 \leq i, j < n$.

(vii) On suppose $e_1 = 2$ *(et donc* e_n *pair). Montrer* $f(x_n, y) = 1$ *avec* $y = x_n^{e_n/2}$.

On suppose désormais b *non dégénérée (voir l'Exercice 3.19).*

(viii) Montrer $e_n \,|\, 24$.

(ix) Montrer $e_i = 2$ *pour* $i < n$, $n = 2$, *puis* $e_n \not\equiv 0 \bmod 4$.

(x) Conclure.

On poursuit par quelques exercices sur les groupes abéliens généraux.

EXERCICE 3.21. *Soit* G *un groupe abélien.*

(i) Montrer que l'application $G \to (\mathbb{C}^\times)^{\widehat{G}}, g \mapsto (\chi(g))_\chi$, *est injective.*

(ii) En déduire que G *se plonge dans un groupe divisible (de manière naturelle !).*

EXERCICE 3.22. *Soit* G *un groupe abélien supposé divisible et sans torsion.*

(i) Montrer qu'il existe un ensemble I *tel que* G *est isomorphe à* $\mathbb{Q}^{(I)}$.

(ii) (suite) On suppose G *indénombrable. Montrer* $I \sim G$.

EXERCICE 3.23. *Soit* A *le groupe abélien* $\prod_p \mathbb{Z}/p\mathbb{Z}$, *le produit portant sur tous les nombres premiers* p. *On va montrer qu'il existe un morphisme surjectif* $A \to \mathbb{Q}$,

(i) Déterminer A_{tor}.
(ii) Montrer que A/A_{tor} *est divisible.*
(iii) Conclure.
(iv) Montrer qu'on a en fait $A/A_{\mathrm{tor}} \simeq \mathbb{Q}^{(\mathbb{R})}$.

EXERCICE 3.24. (Le groupe des entiers p-adiques) *Soit p un nombre premier. On note $\mathbb{Z}_p$ le sous-ensemble du produit $\prod_{n\geq 1}\mathbb{Z}/p^n\mathbb{Z}$ constitué des suites (x_n) telles que $x_{n+1} \bmod p^n = x_n$ pour tout $n \geq 1$. Une telle suite est appelée* entier p-adique.

(i) Montrer que $\mathbb{Z}_p$ est un sous-groupe du groupe produit $\prod_{n\geq 1}\mathbb{Z}/p^n\mathbb{Z}$, et que l'application $\mathbb{Z}_p \to \mathbb{Z}/p^n\mathbb{Z}, (x_n) \mapsto x_n$, est un morphisme surjectif.
(ii) Montrer que $\mathbb{Z}_p$ est en bijection avec $\mathbb{R}$.
(iii) Montrer que $\mathbb{Z}_p$ n'a aucun élément non trivial d'ordre fini.

On note $\mu_{p^\infty} = \cup_{n\geq 1}\mu_{p^n}$ le sous-groupe de $\mathbb{C}^\times$ constitué des racines de l'unité d'ordre une puissance de p.

(iv) Montrer que pour tout caractère $\chi \in \widehat{\mu_{p^\infty}}$ il existe un unique entier p-adique $(\overline{k_n}) \in \mathbb{Z}_p$ vérifiant $\chi(e^{2i\pi/p^n}) = e^{2i\pi k_n/p^n}$ pour tout $n \geq 1$.
(v) Montrer $\widehat{\mu_{p^\infty}} \simeq \mathbb{Z}_p$.

EXERCICE 3.25. (Propriété universelle des sommes directes de groupes abéliens) *Soient $\{G_i\}_{i\in I}$ une famille de groupes abéliens, et $S = \oplus_{i\in I}G_i$ leur somme directe externe. Pour $j \in I$, on note $\iota_j \in \mathrm{Hom}(G_j, S)$ l'inclusion canonique (justifier). Montrer que pour tout groupe abélien G, l'application $\mathrm{Hom}(S, G) \to \prod_{i\in I}\mathrm{Hom}(G_i, G)$, $f \mapsto (f \circ \iota_i)_i$, est bijective.*

On donne maintenant quelques exercices concernant la Section 1.

EXERCICE 3.26. (Coniques sur $\mathbb{Z}/p\mathbb{Z}$) *Soit p un nombre premier impair.*

(i) Montrer $\mathrm{J}(\chi, \chi^{-1}) = -\chi(-1)$ pour tout $\chi \in \widehat{(\mathbb{Z}/p\mathbb{Z})^\times} \smallsetminus \{1\}$.
(ii) En déduire[11] *que si l'on pose $C = \{(x, y) \in (\mathbb{Z}/p\mathbb{Z})^2 \mid \alpha\, x^2 + \beta\, y^2 = 1\}$ avec $\alpha, \beta \in (\mathbb{Z}/p\mathbb{Z})^\times$, on a l'égalité $|C| = p - (\frac{-\alpha\beta}{p})$.*
(iii) Montrer qu'il existe $\frac{p\pm 1}{4}$ carrés $x \in \mathbb{Z}/p\mathbb{Z}$ tels que $x + 1$ n'est pas un carré.

EXERCICE 3.27. *En examinant la Table 1, on constate pour $p \equiv 1 \bmod 3$:*

(i) $|\mathrm{S}_p| \equiv -1 \bmod 12$,
(ii) $|\mathrm{S}_p| \equiv -1 \bmod 24 \;\Rightarrow\; p \equiv 1 \bmod 4$.

Démontrer ces congruences.

EXERCICE 3.28. *Soit p un nombre premier impair.*

(i) Déterminer $\sum_{x\in\mathbb{Z}/p\mathbb{Z}} (\frac{x^2+1}{p})$.

11. Une autre démonstration consisterait à dire qu'il y a $\frac{p+1}{2}$ carrés dans $\mathbb{Z}/p\mathbb{Z}$, et donc aussi $\frac{p+1}{2}$ éléments de la forme $\beta^{-1}(1 - \alpha x^2)$, de sorte qu'il y a au moins un point P sur la conique C. Les autres points sont obtenus en paramétrant les cordes (ou tangente) de C passant par P.

(ii) Déterminer $\sum_{x\in\mathbb{Z}/p\mathbb{Z}} (\frac{x^3+1}{p})$.

(iii) Soient $n \geq 1$ *un entier et* $m = \mathrm{pgcd}\,(p-1,\, n)$. *Montrer*

$$\Big|\sum_{x\in\mathbb{Z}/p\mathbb{Z}} (\frac{x^n+1}{p})\Big| \leq \begin{cases} (m-1)\sqrt{p} & \text{pour } m \text{ impair,} \\ (m-2)\sqrt{p}+1 & \text{pour } m \text{ pair.} \end{cases}$$

EXERCICE 3.29. (Somme de Gauss cubique) *Soient* p *premier* $\equiv 1 \bmod 3$, c *un caractère d'ordre* 3 *de* $(\mathbb{Z}/p\mathbb{Z})^\times$, $G = \mathrm{G}(c)$ *la somme de Gauss associée et* $J = \mathrm{J}(c,c)$.

(i) Montrer $G^3 = J\,p$.

(ii) Soit $A = J + \overline{J}$. *Montrer* $A \in \mathbb{Z}$ *et qu'il existe* $B \in \mathbb{Z}$ *avec* $4p = A^2 + 3B^2$.

(iii) Soit $x = \sum_{k=0}^{p-1} \cos(\frac{2\pi k^3}{p})$. *Montrer* $x = G + \overline{G}$.

(iv) (suite) En déduire que x *est l'une des trois racines réelles du polynôme à coefficients entiers* $X^3 - 3pX - Ap$.

EXERCICE 3.30. (Un théorème de Gauss) *Soit* p *un nombre premier. On considère*

$$\mathrm{T}_p = \{(x,y) \in (\mathbb{Z}/p\mathbb{Z})^2 \mid x^4 + y^2 = 1\}.$$

(i) En utilisant l'Exercice 3.26 (ii), montrer $|\mathrm{T}_p| = p+1$ *pour* $p \equiv 3 \bmod 4$.

On suppose désormais $p \equiv 1 \bmod 4$.

(ii) Montrer $|\mathrm{T}_p| \equiv 6 \bmod 8$.

(iii) Montrer qu'il existe des uniques $A, B \in \mathbb{Z}$ *avec* $A \equiv -\frac{p+1}{2} \bmod 4$ *et* $B > 0$ *tels que* $p = A^2 + 4B^2$, *et que l'on a en outre* $|\mathrm{T}_p| = p + 2A - 1$.

EXERCICE 3.31. (Le signe de la somme de Gauss, d'après Dirichlet) *Soient* $N \geq 1$ *et* $\mathrm{G}_N = \sum_{a=0}^{N-1} e^{\frac{2i\pi a^2}{N}}$.

(i) Soient $a < b$ *deux entiers et* $f : [a,b] \to \mathbb{C}$ *une fonction continue et* $\mathscr{C}^1$ *par morceaux. Montrer* $\frac{f(a)+f(b)}{2} + \sum_{k=a+1}^{b-1} f(k) = \sum_{n\in\mathbb{Z}} \int_a^b f(t)e^{2i\pi nt}dt$.

(ii) En déduire $\mathrm{G}_N = (1+i^{-N})N^{\frac{1}{2}}I$ *où* $I = \int_{-\infty}^{+\infty} e^{2i\pi t^2}dt$.

(iii) Montrer $I = \frac{1+i}{2}$ *(intégrale de Gauss) et*

$$\mathrm{G}_N = \begin{cases} (1+i)N^{\frac{1}{2}} & \text{si } N \equiv 0 \bmod 4, \\ N^{\frac{1}{2}} & \text{si } N \equiv 1 \bmod 4, \\ 0 & \text{si } N \equiv 2 \bmod 4, \\ iN^{\frac{1}{2}} & \text{si } N \equiv 3 \bmod 4. \end{cases}$$

Dans l'exercice suivant, on utilise le résultat ci-dessus pour démontrer, suivant Gauss, la *loi de réciprocité quadratique*.

EXERCICE 3.32. *Pour* $N, M \geq 1$, *on pose* $\mathrm{G}_{N,M} = \sum_{k=0}^{N-1} e^{\frac{2i\pi Mk^2}{N}}$ *et* $\mathrm{G}_N = \mathrm{G}_{N,1}$. *On se donne* p *et* q *deux nombres premiers impairs distincts.*

(i) Montrer $\mathrm{G}_{p,q}\,\mathrm{G}_{q,p} = \mathrm{G}_{pq}$.

(ii) Montrer $\mathrm{G}_{p,a} = (\frac{a}{p})\,\mathrm{G}_p$ *pour tout* $a \in \mathbb{Z}$.

(iii) En déduire $(\frac{p}{q}) = (\frac{q}{p})\ (-1)^{\frac{(p-1)(q-1)}{2}}$ *(« la loi de réciprocité quadratique »).*

(iv) Montrer $\mathrm{G}_{p,8}\,\mathrm{G}_{8,p} = \mathrm{G}_{8p}$ *et vérifier* $\mathrm{G}_{8,p} = 4\,e^{\frac{2i\pi\,p}{8}}$.

(v) En déduire $(\frac{2}{p}) = (-1)^{\frac{p^2-1}{8}}$ *(« loi complémentaire »).*

La série d'exercices suivante revient sur l'analyse de Fourier sur un groupe abélien fini. Le premier fait notamment suite à l'Exercice 3.17. Le dernier donne un point de vue plus éclairant sur certains calculs de la section 1 (dans l'esprit de l'Exemple 2.4).

Exercice 3.33. (Inversion de Fourier)

(i) Vérifier que l'application $\mathrm{j}_G : \mathrm{L}^2(G) \to \mathrm{L}^2(\widehat{\widehat{G}}), f \mapsto (x \mapsto f(\iota_G^{-1}(x^{-1})))$, *est* $\mathbb{C}$*-linéaire bijective.*

(ii) Soit $\mathscr{F}_G : \mathrm{L}^2(G) \to \mathrm{L}^2(\widehat{G}), f \mapsto \frac{1}{\sqrt{|G|}}\widehat{f}$. *Montrer* $\mathscr{F}_{\widehat{G}} \circ \mathscr{F}_G = \mathrm{j}_G$.

Exercice 3.34. (Convolution) *Soit* G *un groupe fini. Le produit de convolution de* $f, f' \in \mathrm{L}^2(G)$ *est défini par* $f \star f'(g) = \sum f(a)f'(b)$, *la somme portant sur tous les couples* $(a, b) \in G \times G$ *tels que* $ab = g$.

(i) Montrer que $(\mathrm{L}^2(G), +, \star)$ *est un anneau, de neutre le dirac en* 1.

(ii) Soient $\chi \in \widehat{G}$ *et* $f \in \mathrm{L}^2(G)$. *Vérifier* $f \star \chi = \widehat{f}(\chi)\,\chi$.

(iii) En déduire $\widehat{f \star f'}(\chi) = \widehat{f}(\chi)\,\widehat{f'}(\chi)$, *pour tout* $f, f' \in \mathrm{L}^2(G)$ *et* $\chi \in \widehat{G}$.

L'exercice suivant fait suite au précédent (cas $G = \mathbb{Z}/p\mathbb{Z}$) et donne un point de vue plus conceptuel sur certaines des formules démontrées en Section 1. Comme dans cette section, on étend tout caractère c de $(\mathbb{Z}/p\mathbb{Z})^\times$ en une fonction $\mathbb{Z}/p\mathbb{Z} \to \mathbb{C}$ en posant $c(0) = 0$ pour $c \neq 1$, et $c(0) = 1$ pour $c = 1$.

Exercice 3.35. (Convolution et sommes de Gauss et de Jacobi) *Soit* p *un nombre premier. On identifie* μ_p *à* $\widehat{\mathbb{Z}/p\mathbb{Z}}$ *comme dans la Proposition 1.3, en faisant correspondre à* $\zeta \in \mu_p$ *le caractère* $\overline{k} \mapsto \zeta^k$ *de* $\mathbb{Z}/p\mathbb{Z}$. *Soient* $c, c' \in (\widehat{\mathbb{Z}/p\mathbb{Z}})^\times$.

(i) Vérifier que pour tout $\zeta \in \mu_p$ *on a* $\widehat{c}(\zeta) = \sum_{x \in \mathbb{Z}/p\mathbb{Z}} c(x)\zeta^{-x}$.

(ii) Si $cc' \neq 1$, *montrer* $c * c' = \mathrm{J}(c, c')cc'$ *et retrouver* $\mathrm{G}(c)\mathrm{G}(c') = \mathrm{J}(c, c')\mathrm{G}(cc')$.

(iii) On suppose $c \neq 1$. *En utilisant l'Exercice 3.26 (i), montrer que l'on a la relation* $c * c^{-1} = -c(-1) + p\,c(-1)\delta$, *où* δ *désigne le Dirac en* 0.

(iv) (suite) Retrouver $|\mathrm{G}(c)|^2 = p$.