Mais d'un autre côté, on sait que le morphisme

$$(\mathbb{Z}/p\mathbb{Z})^\times \to (\mathbb{Z}/p\mathbb{Z})^\times, x \mapsto x^n,$$

a pour image les $(p-1)/m$ puissances n-èmes de $(\mathbb{Z}/p\mathbb{Z})^\times$, et que ses fibres sont donc de cardinal 0 ou m. Il ne reste qu'à observer que g^k est une puissance n-ème dans $(\mathbb{Z}/p\mathbb{Z})^\times$ si, et seulement si, on a $k \equiv 0 \bmod m$. Mais on a vu que c'est équivalent à $g^{k\frac{p-1}{m}} = 1$ (Corollaire 5.7 Chap. 2 (ii)), et donc à $k\frac{p-1}{m} \equiv 0 \bmod p-1$, ce qui est bien équivalent à $k \equiv 0 \bmod m$. □

REMARQUE 1.16. (Culturelle) La même méthode s'applique plus généralement aux équations *diagonales*, *i.e.* de la forme $ax^n+by^m = c$ avec $a, b, c \in \mathbb{Z}/p\mathbb{Z}$ et $n, m \geq 1$, et même plus généralement à celles de la forme $a_1x_1^{n_1} + a_2x_2^{n_2} + \cdots + a_mx_m^{n_m} = b$ (*hypersurfaces diagonales*). Nous renvoyons à l'article sus-cité de Weil et au chapitre 8 du livre de Ireland et Rosen pour de nombreux exemples détaillés. Ces résultats sont à l'origine des fameuses *conjectures de Weil*, qui s'appliquent à toutes les variétés algébriques sur $\mathbb{Z}/p\mathbb{Z}$, et dont la résolution par Grothendieck et Deligne a modifié le paysage de la géométrie algébrique.

2. Décomposition de Fourier finie

L'analyse de Fourier classique affirme notamment que l'espace de Hilbert $\mathrm{L}^2(\mathbb{R}/\mathbb{Z})$ des fonctions 1-périodique de carré intégrable sur le cercle $\mathbb{R}/\mathbb{Z}$[4] admet pour base Hilbertienne les fonctions $x \mapsto e^{2i\pi nx}$ pour $n \in \mathbb{Z}$ ("décomposition de Fourier"). La propriété particulière de ces fonctions est que ce sont des caractères continus du groupe abélien (topologique compact) $\mathbb{R}/\mathbb{Z}$. C'est même un exercice de voir que tout morphisme continu $\mathbb{R}/\mathbb{Z} \to \mathbb{C}^\times$ est de la forme $x \mapsto e^{2i\pi nx}$ (Exercice 2.34 Chap. 2). Cette théorie admet un analogue plus simple, mais utile et instructif, dans le cadre des groupes finis. C'est aussi l'un des chemins qui mène à la théorie des représentations des groupes finis, qui sera étudiée à la fin du cours.

Pour G un groupe *fini*, on note $\mathrm{L}^2(G)$ le $\mathbb{C}$-espace vectoriel des fonctions $G \to \mathbb{C}$, muni du produit scalaire hermitien $\langle f, f'\rangle = \frac{1}{|G|}\sum_{g\in G} f(g)\overline{f'(g)}$. C'est un espace de dimension finie $|G|$.

THÉORÈME 2.1. *Soit G un groupe fini.*

(i) L'ensemble $\widehat{G}$ est une famille libre et orthonormée de $\mathrm{L}^2(G)$,

(ii) si G est abélien, alors $\widehat{G}$ est une base de $\mathrm{L}^2(G)$.

On appelle souvent le (i) la propriété d'*orthogonalité des caractères*.

Avant d'entamer la démonstration, observons que pour tout $g \in G$ on dispose d'un endomorphisme R_g de $\mathrm{L}^2(G)$ défini par $f \mapsto \mathrm{R}_g(f)$, $h \mapsto f(hg)$ (translation par g). Cet endomorphisme est unitaire : si $f, f' \in \mathrm{L}^2(G)$, et si $g \in G$, alors $\langle \mathrm{R}_g(f), \mathrm{R}_g(f')\rangle = \langle f, f'\rangle$. De plus, on a $\mathrm{R}_1 = \mathrm{id}$ et $\mathrm{R}_{gh} = \mathrm{R}_g \circ \mathrm{R}_h$ pour tout $g, h \in G$. Autrement dit, $g \mapsto \mathrm{R}_g$ défini un morphisme de groupes $G \to \mathrm{GL}(V)$ avec $V = \mathrm{L}^2(G)$. Ce morphisme est appelé *représentation régulière de G*. Observons

4. C'est à dire les fonctions 1-périodiques Lebesgue mesurables $f : \mathbb{R} \to \mathbb{C}$ telles que $\int_0^1 |f(t)|^2 dt < \infty$.

déjà que tout $\chi \in \widehat{G}$ vérifie $\mathrm{R}_g\chi = \chi(g)\chi$. Autrement dit, χ est vecteur propre de (chaque) R_g, de valeur propre $\chi(g)$.

Démonstration — Montrons le (i). Pour $\chi \in \widehat{G}$ on a déjà vu que $|\chi(g)| = 1$ pour tout $g \in G$. On en déduit $\langle \chi, \chi\rangle = \frac{1}{|G|} \cdot |G| = 1$. Pour voir qu'ils sont orthogonaux, il suffit de dire que pour $\chi \neq \chi'$, il existe $g \in G$ tel que $\chi(g) \neq \chi'(g)$, et donc χ et χ' sont dans des espaces propres pour des valeurs propres distinctes de l'endomorphisme unitaire R_g. Ils sont donc orthogonaux : on a $\langle \chi, \chi'\rangle = \langle \mathrm{R}_g\chi, \mathrm{R}_g\chi'\rangle = \langle \chi(g)\chi, \chi'(g)\chi'\rangle = \chi(g)\overline{\chi'(g)}\,\langle \chi, \chi'\rangle$, et donc $\langle \chi, \chi'\rangle = 0$ car $\chi(g)\overline{\chi'(g)} = \chi(g)\chi'(g)^{-1} \neq 1$. Prouvons enfin que les caractères sont linéairements indépendants. Si on a $0 = \sum_{\psi\in\widehat{G}} \mu_\psi \psi$ avec $\mu_\psi \in \mathbb{C}$ pour tout ψ, en faisant $\langle -, \chi\rangle$ on en déduit $\mu_\chi = 0$.

Montrons le (ii). Si G est abélien, les endomorphismes R_g avec $g \in G$ commutent. Comme un endomorphisme unitaire est diagonalisable, les R_g sont diagonalisables.[5] Ils sont donc co-diagonalisables : $\mathrm{L}^2(G)$ possède une base constituée de vecteurs propres communs à tous les R_g. Si f est un tel vecteur propre, on a $\mathrm{R}_g f = \lambda_g f$ pour tout $g \in G$, avec $\lambda_g \in \mathbb{C}^\times$ (car R_g est inversible, d'inverse $\mathrm{R}_{g^{-1}}$, ou encore car R_g est unitaire). La relation $\mathrm{R}_{gh} = \mathrm{R}_g \circ \mathrm{R}_h$ entraîne $\lambda_{gh} = \lambda_g\lambda_h$ pour $g, h \in G$. Autrement dit, la fonction $g \mapsto \lambda_g$ est dans $\widehat{G}$. Enfin, on a par définition $(\mathrm{R}_g f)(h) = f(hg)$, donc $f(hg) = \lambda_g f(h)$ pour tout $g, h \in G$, puis $f(g) = \lambda_g f(1)$. Comme $f \neq 0$, on a $f(1) \neq 0$, et quitte à remplacer f par $f/f(1)$ on peut supposer $f(1) = 1$, *i.e.* f est dans $\widehat{G}$. □

Corollaire 2.2. *Soit G un groupe abélien fini.*

(i) On a $|\widehat{G}| = |G|$.
(ii) Pour toute fonction $f : G \to \mathbb{C}$, on a $f = \sum_{\chi\in\widehat{G}} \langle f, \chi\rangle\, \chi$.

Les $\langle f, \chi\rangle$ sont appelés *coefficients de Fourier* de f, et la fonction $\widehat{f} \in \mathrm{L}^2(\widehat{G})$ définie par $\widehat{f}(\chi) = |G|\,\langle f, \chi\rangle$ est appelée *transformée de Fourier* de f. On constate alors que $f \mapsto \frac{1}{\sqrt{|G|}}\,\widehat{f}$ est une isométrie linéaire $\mathrm{L}^2(G) \to \mathrm{L}^2(\widehat{G})$, par le point (ii).

Démonstration — On a clairement $|G| = \dim \mathrm{L}^2(G)$, et aussi $\dim \mathrm{L}^2(G) = |\widehat{G}|$ par le (ii) du théorème. Cela montre le (i). Pour le (ii), on écrit $f = \sum_{\chi\in\widehat{G}} \lambda_\chi \chi$ pour certains $\lambda_\chi \in \mathbb{C}$ par le (ii) du théorème. Par le (i), on a $\langle f, \chi\rangle = \lambda_\chi$. □

Exemple 2.3. Dans le cas $G = \mathbb{Z}/n\mathbb{Z}$ on a déjà vu que les caractères de G sont les $\overline{k} \mapsto \zeta^k$ avec $\zeta^n = 1$. Le théorème montre donc que toute fonction $\mathbb{Z}/n\mathbb{Z} \to \mathbb{C}$ est combinaison linéaire unique de ces fonctions. C'est le point de départ de la théorie de la *transformée de Fourier discrète*, utile en traitement du signal, et un outil important dans la *combinatoire additive*. Nous ne nous aventurerons pas ici dans ces directions !

Exemple 2.4. Supposons $G = \mathbb{Z}/p\mathbb{Z}$ avec p premier. Soit c un caractère non trivial du groupe multiplicatif $(\mathbb{Z}/p\mathbb{Z})^\times$. On peut voir c comme une fonction $\mathbb{Z}/p\mathbb{Z} \to \mathbb{C}$ en le prolongeant par 0 en 0 comme au §1. Attention, ce prolongement n'est pas du

5. On peut dire aussi ici que pour $n = |G|$ on a $g^n = 1$ par Lagrange, et donc $(\mathrm{R}_g)^n = \mathrm{id}$ de sorte que R_g est annulé par le polynôme $X^n - 1$, scindé à racines distinctes.

tout un caractère de $\mathbb{Z}/p\mathbb{Z}$, et de fait ses coefficients de Fourier sont intéressants ! En effet, si $\chi : \mathbb{Z}/p\mathbb{Z} \to \mathbb{C}^\times$ désigne le caractère $\overline{k} \mapsto \zeta^{-k}$ avec $\zeta = e^{2i\pi/p}$, on constate $\widehat{c}(\chi) = \mathrm{G}(c)$ (la somme de Gauss de c). Certaines des formules de la Proposition 1.13 prennent un peu plus de sens avec ce point de vue (sans toutefois simplifier substantiellement leur démonstration). Par exemple, la formule (ii) pourrait être déduite de l'Exercice 3.14 sur la convolution et du fait que $c \star c'(1)$ coïncide avec la somme de Jacobi $\mathrm{J}(c, c')$.

Une application du Théorème 2.1 due à Dedekind, qui est d'apparence anecdotique mais historiquement importante dans le développement par Frobenius de la théorie des représentations, est la question du calcul du *déterminant* d'un groupe fini G : nous renvoyons au court Complément 5 pour une discussion de cette anecdote, sur laquelle nous reviendrons également dans le dernier chapitre. Terminons ce paragraphe par un énoncé important de *prolongement des caractères.*

PROPOSITION 2.5. *Soit G un groupe abélien fini et $H \subset G$ un sous-groupe. Pour tout caractère χ de H, il existe un caractère $\widetilde{\chi}$ de G vérifiant $\widetilde{\chi}_{|H} = \chi$.*

DÉMONSTRATION — En effet, considérons l'application de restriction $r : \widehat{G} \to \widehat{H}$, $\chi \mapsto \chi_{|H}$. C'est clairement un morphisme de groupes. Son noyau est le sous-groupe des caractères de G triviaux sur H. Par la propriété universelle du groupe quotient G/H, si $\pi : G \to G/H$ désigne la projection canonique, alors l'application $\psi \mapsto \psi \circ G$ définit une bijection entre $\widehat{G/H}$ et $\ker r$. D'après le Corollaire 2.2, on a

$$|\widehat{G}| = |G|, \ \ |\widehat{H}| = |H| \text{ et } |\ker r| = |\widehat{G/H}| = |G/H| = |G|/|H|.$$

On en déduit $|\mathrm{Im}\, r| = |\widehat{G}|/|\ker r| = |H| = |\widehat{H}|$, et donc r est surjective. □

Étant donné l'importance de ce résultat pour la section suivante, nous en donnons une seconde démonstration, à la fois plus directe et plus générale. Dans cet énoncé, les groupes en question ne sont plus nécessairement finis. Un groupe abélien D est dit *divisible* si pour tout entier $n \geq 1$, le morphisme de groupes $D \to D, x \mapsto x^n$, est surjectif. Par exemple, le groupe multiplicatif $\mathbb{C}^\times$, et les groupes additifs $\mathbb{Q}$ et $\mathbb{Q}/\mathbb{Z}$, sont des groupes abéliens divisibles, mais pas $\mathbb{Z}$ ou $\mathbb{Z}/m\mathbb{Z}$.

PROPOSITION 2.6. (Prolongement des morphismes) *Soient G, H, D des groupes* abéliens *avec $H \subset G$, D divisible, et $f : H \to D$ un morphisme de groupes. Alors il existe un morphisme de groupes $\widetilde{f} : G \to D$ tel que $\widetilde{f}_{|H} = f$.*

DÉMONSTRATION — Supposons d'abord que G est engendré par H et un élément $g \in G$. Tout élément de G s'écrit donc sous la forme hg^n pour certains $h \in H$ et $n \in \mathbb{Z}$, par commutativité de G. Cette écriture n'est pas nécessairement unique. En effet, considérons $K = \{n \in \mathbb{Z} \,|\, g^n \in H\}$; c'est un sous-groupe de $\mathbb{Z}$, donc de la forme $d\mathbb{Z}$ avec $d \geq 0$. Ainsi, si on a $hg^n = h'g^m$ avec $h, h' \in H$ et $n, m \in \mathbb{Z}$, on a $h^{-1}h' = g^{n-m}$ puis $n \equiv m \bmod d$ et $h' = h\,(g^d)^{\frac{n-m}{d}}$ avec $g^d \in H$. Comme g^d est dans H, il y a un sens à considérer $f(g^d) \in D$, et par divisibilité de G on peut choisir un élément $x \in D$ tel que $x^d = f(g^d)$ (si $d = 0$ on a $f(g^d) = f(1) = 1$ et on peut prendre $x = 1$). On a tout fait pour que l'application

$$\widetilde{f} : G \to D, \ \ hg^n \mapsto f(h)x^n,$$

soit bien définie : si on a $hg^n = h'g^m$ avec $h, h' \in H$ et $n, m \in \mathbb{Z}$, on a vu $n \equiv m \bmod d$ et $h' = h.(g^d)^{\frac{n-m}{d}}$ avec $g^d \in H$, de sorte qu'en appliquant f à cette dernière égalité on trouve $f(h') = f(h)(x^d)^{\frac{n-m}{d}}$ puis $f(h)x^n = f(h')x^m$. Enfin, il est clair que $\widetilde{f}$ ainsi définie est un morphisme de groupes tel que $\widetilde{f}_{|H} = f$.

Quand G est fini, ou plus généralement de type fini, disons $G = \langle b_1\rangle \langle b_2\rangle \cdots \langle b_r\rangle$ (car G est commutatif), on conclut en prolongeant f successivement à chaque sous-groupe $H_i := H\langle b_1\rangle \langle b_2\rangle \cdots \langle b_i\rangle$ pour $i = 1, \ldots, r$.

Pour un G général, on peut encore conclure par le lemme de Zorn. En effet, soit X l'ensemble des couples (H', f') avec H' un sous-groupe de G contenant H et $f' : H' \to D$ un morphisme prolongeant f. On munit X d'une relation d'ordre en posant $(H', f') \leq (H'', f'')$ si on a $H' \subset H''$ et $f''_{|H'} = f'$. On constate que $(X, \leq)$ est inductif. Si (H', f') est maximal, alors on a $H' = G$. En effet, sinon il existe $g \in G - H'$ et on peut prolonger f' à $H'\langle b\rangle$ par le premier cas étudié plus haut, ce qui contredit la maximalité de (H', f'). □

Remarque 2.7. L'énoncé est bien sûr très faux si D n'est pas divisible. Par exemple, si on prend $G = \mathbb{Z}/4\mathbb{Z}$ et $H = D = \mathbb{Z}/2\mathbb{Z}$, alors pour tout morphisme $\varphi : G \to D$ on a $\varphi(\overline{2}) = \varphi(2.\overline{1}) = 2\varphi(\overline{1}) = 0$. Ainsi, l'identité $f : H \to D, x \mapsto x$, ne se prolonge pas à G.

3. Structure des groupes abéliens finis

On se propose de classifier à isomorphismes près les groupes abéliens finis.

Théorème 3.1. *Soit G un groupe abélien fini. Il existe un unique entier*[6] *n, et des uniques entiers $a_i > 1$ pour $i = 1, \ldots, n$, vérifiant $a_1 \mid a_2 \mid \cdots \mid a_n$ et*

$$G \simeq \prod_{i=1}^{n} \mathbb{Z}/a_i\mathbb{Z}.$$

En particulier, tout groupe fini est isomorphe à un produit de groupes cycliques. Bien sûr, nous pouvons remplacer chaque $\mathbb{Z}/a_i\mathbb{Z}$ dans le produit ci-dessus par n'importe quel groupe cyclique d'ordre a_i, par exemple par μ_i.

Les entiers a_i de l'énoncé s'appellent les *facteurs invariants* de G. Ils vérifient bien sûr $|G| = a_1 a_2 \cdots a_n$. Les a_i sont donc des diviseurs (ou *facteurs*) canoniques de $|G|$, au sens où ils sont uniquement déterminés par la structure de G.

Exemple 3.2. *D'après le Théorème 3.1, les groupes* abéliens *de cardinal* 8 *sont, à isomorphisme près, les groupes $\mathbb{Z}/8\mathbb{Z}$, $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$ et $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$. Bien noter qu'il existe aussi des groupes non abéliens d'ordre* 8*, comme le groupe* H_8*, sur lesquels le théorème ne dit rien et que nous étudierons plus tard.*

Attention aussi à bien comprendre l'énoncé : dans le cas du groupe abélien $G = \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$ on a nécessairement $n = 1$ et $a_1 = 6$, et donc $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z} \simeq \mathbb{Z}/6\mathbb{Z}$. L'existence d'un tel isomorphisme est aussi conséquence directe de l'isomorphisme chinois des restes (Corollaire 3.11). En guise d'autre exemple, les facteurs invariants

6. On convient qu'un produit vide de groupes vaut 1, de sorte que l'on a $G = \{1\}$ si, et seulement si, $n = 0$.

de $G = \mathbb{Z}/6\mathbb{Z} \times \mathbb{Z}/10\mathbb{Z}$ sont 2 et 30, car on a $2|30$. C'est bien cohérent avec la suite d'isomorphismes chinois suivante :

$$\mathbb{Z}/6\mathbb{Z} \times \mathbb{Z}/10\mathbb{Z} \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/10\mathbb{Z} \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/30\mathbb{Z}.$$

3.1. Démonstration de l'existence. Le principe de la démonstration va consister à caractériser d'abord le facteur invariant a_n comme étant l'*exposant* de G.

Définition 3.3. *L'*exposant *d'un groupe fini G est le plus petit entier $e \geq 1$ vérifiant $g^e = 1$ pour tout $g \in G$. On le note* $\exp G$.

Par définition, $\exp G$ est aussi le ppcm des ordres des éléments de G. En effet, pour $e \in \mathbb{Z}$ on a $g^e = 1$ pour tout $g \in G$ si, et seulement si, $\operatorname{ord} g, \mid e$ pour pour $g \in G$. On constate aussi que si on a $G = \prod_{i=1}^n \mathbb{Z}/a_i\mathbb{Z}$ alors l'exposant de G est le ppcm des a_i, c'est donc a_n si on suppose en outre $a_1 \,|\, a_2 \,|\, \cdots \,|\, a_n$.

Lemme 3.4. *Si G est un groupe abélien fini, il existe un élément $g \in G$ d'ordre l'exposant de G.*

Démonstration — Soient $e = \exp G$, de décomposition en facteurs premiers $e = \prod_i p_i^{\alpha_i}$. Comme e est le ppcm des ordres des éléments de G, pour tout i il existe un élément $g_i \in G$ d'ordre de la forme $p_i^{\alpha_i} m_i$. En particulier, $g_i^{m_i}$ est d'ordre exactement $p_i^{\alpha_i}$ (Lemme 3.6 Chap. 2). Le produit g des $g_i^{m_i}$ convient (Lemme 5.3 Chap. 2). □

Le dévissage en produit se fera ensuite grâce à l'énoncé suivant.

Proposition 3.5. *Soient G un groupe et H et K deux sous-groupes de G. On suppose $H \cap K = 1$, $G = HK$ et enfin $hk = kh$ pour tout $h \in H$ et tout $k \in K$. Alors l'application $(h, k) \mapsto hk$ définit un isomorphisme de groupes $H \times K \xrightarrow{\sim} G$.*

Sous les hypothèses de l'énoncé, on dit que G est *produit direct interne* de H et K. Noter que les groupes H et K ne sont pas supposés ici commutatifs (même s'ils le seront dans l'application ci-après).

Démonstration — Soit φ l'application de l'énoncé. Elle est surjective car $G = HK$. C'est un morphisme de groupes car on a $\varphi((h,k)(h',k')) = \varphi(hh', kk') = hh'kk' = hkh'k'$ puisque $h'k = kh'$ pour tout $h' \in H$ et $k' \in K$. Elle est injective car $hk = 1$ entraîne $h = k^{-1} \in H \cap K = \{1\}$. □

Démonstration — (partie existence du théorème) Soient G un groupe abélien fini, a l'exposant de G et $x \in G$ d'ordre a (Lemme 3.4). Le groupe cyclique $\langle x \rangle$ est d'ordre a. On peut donc trouver un caractère $\chi : \langle x \rangle \to \mathbb{C}^\times$ envoyant x sur $e^{2i\pi/a}$ (Proposition 1.3). Par prolongement des caractères, on peut trouver un caractère $\widetilde{\chi} : G \to \mathbb{C}^\times$ prolongeant χ (Proposition 2.5 ou 2.6).

Soit $g \in G$. On a $g^a = 1$ car a est l'exposant de G, donc $\widetilde{\chi}(g)^a = 1$, puis $\widetilde{\chi}(g) \in \mu_a$. Il existe donc $k \in \mathbb{Z}$ tel que $\widetilde{\chi}(g) = \widetilde{\chi}(x^k)$, puis $gx^{-k} \in \ker \widetilde{\chi}$. On a montré $G = \langle x \rangle \ker \widetilde{\chi}$. Comme d'autre part on a $\langle x \rangle \cap \ker \widetilde{\chi} = \{1\}$ car on a

$$\widetilde{\chi}(x^k) = 1 \iff \chi(x^k) = 1 \iff e^{2ik\pi/a} = 1 \iff k \equiv 0 \bmod a \iff x^k = 1,$$

c'est une situation de produit direct interne : la Proposition 3.5 montre $G \simeq \langle x \rangle \times \ker \widetilde{\chi}$. On conclut par récurrence sur $|G|$ car on a $\langle x \rangle \simeq \mathbb{Z}/a\mathbb{Z}$ et car l'exposant