Chapitre 3

Groupes abéliens de type fini

Le premier but de ce chapitre est de classifier à isomorphisme près les groupes abéliens de type fini. C'est le cas par exemple du sous-groupe d'un groupe donné quelconque engendré par une famille finie d'éléments qui commutent 2 à 2. Le cas crucial est celui des groupes abéliens finis.

La méthode suivie passe par l'étude des caractères d'un tel groupe G, c'est à dire des morphismes $G \to \mathbb{C}^\times$. C'est pourquoi nous commençons par illustrer l'intérêt de ces derniers en expliquant, suivant Gauss et Weil, comment utiliser les caractères du groupe $(\mathbb{Z}/p\mathbb{Z})^\times$ (comme le symbole de Legendre) pour déterminer le nombre de solutions dans $\mathbb{Z}/p\mathbb{Z}$ de l'équation $y^2 = x^3 + 1$.

Nous montrons ensuite comment les caractères de G, pour G abélien fini, permettent de décomposer à la Fourier l'espace des fonctions $G \to \mathbb{C}$. C'est l'un des points de départ de la théorie des *représentations des groupes finis*, qui fera l'objet du dernier chapitre du cours, et dont on donne une première application ici aux *déterminants de groupes*, suivant Dedekind. Le lemme technique clé est le lemme de *prolongement des caractères*, dont on donne deux démonstrations différentes. L'analogie à avoir en tête ici est que les caractères sont aux groupes abéliens finis ce que les formes linéaires sont aux espaces vectoriels.

Le lemme de prolongement permet de montrer simplement que tout groupe abélien fini est produit de groupes cycliques. La question de l'unicité d'une telle décomposition, plus délicate, est aussi étudiée. Une méthode assez similaire permet de donner la structure des groupes abéliens de type fini généraux. Le cas particulier des réseaux de $\mathbb{R}^n$ est important. On conclut par une discussion culturelle du groupe des points d'une courbe elliptique.

1. Caractères et $y^2 = x^3 + 1$ sur $\mathbb{Z}/p\mathbb{Z}$

Définition 1.1. *Un* caractère *(ou caractère linéaire) d'un groupe G est un morphisme de groupes $G \to \mathbb{C}^\times$. On note $\widehat{G}$ l'ensemble des caractères de G.*

Le groupe $\mathbb{C}^\times$ étant commutatif, rappelons que $\widehat{G} = \mathrm{Hom}(G, \mathbb{C}^\times)$ est muni d'une loi de groupe abélien naturelle : le produit de deux caractères $\chi, \psi \in \widehat{G}$ est la fonction $\chi\psi : G \to \mathbb{C}^\times$, $g \mapsto \chi(g)\psi(g)$. Son élément neutre est le caractère trivial 1 (envoyant tout $g \in G$ sur 1) et l'inverse d'un caractère χ est le caractère $\chi^{-1} : g \mapsto \chi(g)^{-1}$. Pour cette loi, $\widehat{G}$ est appelé *groupe des caractères*, ou *groupe dual*, du groupe G. Comme nous le verrons, l'étude de $\widehat{G}$ s'avèrera particulièrement pertinente quand G est abélien fini.

Remarque 1.2. *Si G est fini d'ordre n, et si $\chi \in \widehat{G}$, on a $\chi(G) \subset \mu_n$. En effet, la relation $g^n = 1$ dans G (Lagrange) entraîne $\chi(g)^n = 1$ dans $\mathbb{C}^\times$ pour tout $\chi \in \widehat{G}$. En particulier, $\widehat{G}$ est un groupe abélien fini, et on a aussi $\chi^{-1} = \overline{\chi}$.*

Il est aisé de déterminer les caractères d'un groupe cyclique :

PROPOSITION 1.3. *Soit G un groupe cyclique d'ordre n engendré par $g \in G$. Pour tout $\zeta \in \mu_n$ il existe un unique caractère χ_ζ de G tel que $\chi_\zeta(g) = \zeta$. De plus, l'application $\zeta \mapsto \chi_\zeta$ est un isomorphisme de groupes $\mu_n \xrightarrow{\sim} \widehat{G}$.*

DÉMONSTRATION — Soit $\zeta \in \mu_n$. L'unicité de χ_ζ est claire car on a nécessairement $\chi_\zeta(g^k) = \zeta^k$ pour $k \in \mathbb{Z}$. Pour l'existence, on constate que l'application $\chi_\zeta : G \to \mathbb{C}^\times, g^k \mapsto \zeta^k$, est bien définie, car pour $k, k' \in \mathbb{Z}$ on a $g^k = g^{k'} \implies k \equiv k' \bmod n \implies \zeta^k = \zeta^{k'}$. C'est clairement un morphisme de groupes, *i.e.* un caractère de G, vérifiant $\chi_\zeta(g) = \zeta$. On a donc défini une application $\mu_n \to \widehat{G}, \zeta \mapsto \chi_\zeta$, injective (car $\chi_\zeta(g) = \zeta$) et surjective par la Remarque précédente. C'est trivialement un morphisme de groupes car on a $\chi_\zeta \chi_{\zeta'} = \chi_{\zeta\zeta'}$, c'est donc un isomorphisme. □

Les caractères du groupe $(\mathbb{Z}/n\mathbb{Z})^\times$, appelés *caractères de Dirichlet*, ont un côté plus mystérieux. Un exemple typique est donné par le *caractère de Legendre*

$$\lambda : (\mathbb{Z}/p\mathbb{Z})^\times \to \{\pm 1\}, \quad x \mapsto (\frac{x}{p}),$$

déjà rencontré, qui est défini pour p premier impair et encode la répartition des carrés de $(\mathbb{Z}/p\mathbb{Z})^\times$. C'est l'unique caractère d'ordre 2 de $(\mathbb{Z}/p\mathbb{Z})^\times$. En effet, un tel caractère doit envoyer un générateur g de $(\mathbb{Z}/p\mathbb{Z})^\times$ sur -1, et donc un carré g^{2k} sur 1, et un non carré g^{2k+1} sur -1 : c'est λ. Donnons un autre exemple.

EXEMPLE 1.4. (*Cubes de $(\mathbb{Z}/p\mathbb{Z})^\times$ et caractères cubiques*) Considérons le morphisme $f : (\mathbb{Z}/p\mathbb{Z})^\times \to (\mathbb{Z}/p\mathbb{Z})^\times, x \mapsto x^3$, d'image le sous-groupe Cubes_p des cubes de $(\mathbb{Z}/p\mathbb{Z})^\times$ (aussi noté $(\mathbb{Z}/p\mathbb{Z})^{\times,(3)}$ au §5 Chap. 2). Pour fixer les idées, choisissons un générateur g du groupe $(\mathbb{Z}/p\mathbb{Z})^\times$ (Gauss), de sorte que Cubes_p est engendré par g^3, et donc d'indice $\mathrm{pgcd}(p-1, 3)$. Il y a deux cas très différents :

(Cas a) $p \not\equiv 1 \bmod 3$. On a $\mathrm{Cubes}_p = (\mathbb{Z}/p\mathbb{Z})^\times$, donc tout élément est un cube. C'est même le cube d'un unique élément. En effet, f est surjective et est donc bijective pour des raisons de cardinal. Alternativement, on peut dire aussi que $\ker f$ est trivial car un élément non trivial de $\ker f$ serait d'ordre 3 dans $(\mathbb{Z}/p\mathbb{Z})^\times$, mais 3 ne divise pas $p-1$.

(Cas b) $p \equiv 1 \bmod 3$. Dans ce cas, le plus intéressant !, Cubes_p est un sous-groupe d'indice 3 de $(\mathbb{Z}/p\mathbb{Z})^\times$. On a donc trois classes

$$(\mathbb{Z}/p\mathbb{Z})^\times/\mathrm{Cubes}_p = \{\mathrm{Cubes}_p,\ g\,\mathrm{Cubes}_p,\ g^2\,\mathrm{Cubes}_p\} \simeq \mathbb{Z}/3\mathbb{Z}.$$

Posons $j = e^{2i\pi/3}$. D'après la Proposition 1.3, il existe exactement 2 caractères non triviaux $c : (\mathbb{Z}/p\mathbb{Z})^\times \to \mathbb{C}^\times$ tels que $c^3 = 1$, à savoir les caractères χ_j et $\chi_{j^2} = \chi_j^2$, avec $\chi_j(g) = j$. On pose $c = \chi_j$. Il faut bien noter qu'il dépend du choix du générateur g, mais que l'ensemble $\{c, c^2\}$ ne dépend pas de ce choix : c'est l'ensemble des deux caractères d'ordre 3 de $(\mathbb{Z}/p\mathbb{Z})^\times$. Observons que c prend l'unique valeur 1 sur Cubes_p, j sur $g\mathrm{Cubes}_p$ et j^2 sur $g^2\mathrm{Cubes}_p$. En particulier, on a encore $c(x) = 1$ si, et seulement si, x est un cube, mais il y a deux types de non cubes : les x tels que $c(x) = j$, et ceux tels que $c(x) = j^2$.

Les caractère de Dirichlet sont particulièrement importants en théorie des nombres, notamment car ils interviennent de manière cruciale dans la démonstration du théorème de la progression arithmétique (Dirichlet). Cette démonstration, de nature

analytique, sort du cadre de ce cours. [1] À la place, en guise de motivation, nous allons voir comment les caractères de $(\mathbb{Z}/p\mathbb{Z})^\times$, avec p premier, permettent aussi d'étudier le nombre de solutions de certaines équation polynomiales sur $\mathbb{Z}/p\mathbb{Z}$, en considérant précisément le cas de l'équation

$$y^2 = x^3 + 1, \text{ avec } x, y \in \mathbb{Z}/p\mathbb{Z}.$$

Nous suivrons pour cela la méthode introduite par Weil dans son article fameux *Numbers of solutions of equations in finite fields.* [2] On pose donc

$$\mathrm{S}_p = \{(x, y) \in (\mathbb{Z}/p\mathbb{Z})^2 \mid y^2 = x^3 + 1\}.$$

En général, on a $|\mathrm{S}_p| \leq 2p$ car pour chaque x, l'élément x^3+1 a au plus deux racines carrés (opposées) y dans $\mathbb{Z}/p\mathbb{Z}$. Par exemple, pour $p = 2$ on a $\mathrm{S}_2 = \{(1, 0), (0, 1)\}$, puis $|\mathrm{S}_2| = 2$. Plus généralement :

LEMME 1.5. *Pour $p \not\equiv 1 \bmod 3$ on a $|\mathrm{S}_p| = p$.*

DÉMONSTRATION — En effet, pour un tel p l'application $\mathbb{Z}/p\mathbb{Z} \to \mathbb{Z}/p\mathbb{Z}, x \mapsto x^3$, est bijective par le cas (a) de la Remarque 1.4, de sorte que l'application $\mathrm{S}_p \to \mathbb{Z}/p\mathbb{Z}, (x, y) \mapsto y$, est aussi bijective. □

Le cas $p \equiv 1 \bmod 3$ est sensiblement plus fin ! Supposons par exemple $p = 7$. Les carrés de $\mathbb{Z}/7\mathbb{Z}$ sont $\{\overline{0}, \overline{1}, \overline{2}, \overline{4}\}$, et les cubes $\{\overline{0}, \overline{1}, \overline{-1}\}$, donc les seules solutions sont celles associées aux identités $1 \equiv 0 + 1$ ($1 \cdot 2$ solutions), $2 \equiv 1 + 1$ ($3 \cdot 2$ solutions) et $0 \equiv -1 + 1$ ($3 \cdot 1$ solutions), et on a donc $|\mathrm{S}_7| = 2 + 6 + 3 = 11$. On a aussi l'observation élémentaire :

LEMME 1.6. *Pour $p \equiv 1 \bmod 3$ on a $|\mathrm{S}_p| \equiv 2 \bmod 3$ et $|\mathrm{S}_p| \equiv 1 \bmod 2$.*

DÉMONSTRATION — Pour $p \equiv 1 \bmod 3$, les fibres de $(\mathbb{Z}/p\mathbb{Z})^\times \to (\mathbb{Z}/p\mathbb{Z})^\times, x \mapsto x^3$ ont 3 éléments. En particulier, $(\mathbb{Z}/p\mathbb{Z})^\times$ contient un élément d'ordre 3, disons ω. L'application $\varphi : (x, y) \mapsto (\omega x, y)$ est alors une bijection de S_p vérifiant $\varphi^3 = \mathrm{id}$. Comme ses uniques points fixes sont les deux éléments $(0, \pm 1)$, on a $|\mathrm{S}_p| \equiv 2 \bmod 3$ par le Corollaire 1.9 Chap. 1. La seconde congruence se démontre de même en considérant l'involution $(x, y) \mapsto (x, -y)$, qui a pour points fixes les $(x, 0)$ avec $x^3 = -1$, *i.e.* $x = -1, -\omega, -\omega^2$ (on a utilisé $p \neq 2$). □

On suppose désormais $p \equiv 1 \bmod 3$. Nous allons voir d'une part que p s'écrit de manière unique sous la forme $A^2 + 3B^2$ avec $A, B \in \mathbb{N}$, et d'autre part qu'il existe un lien surprenant cette écriture et $|\mathrm{S}_p|$. Nous attribuerons cet énoncé à Gauss, car c'est une variante de la célèbre *last entry* de son journal mathématique (1814). À ce stade il sera plus clair de faire l'observation élémentaire suivante :

LEMME 1.7. *Soient $d \geq 1$ entier et p un nombre premier. Il existe au plus un couple d'entiers $(a, b) \in \mathbb{N}^2$, ou deux pour $d = 1$, avec $p = a^2 + db^2$.*

Reportons la démonstration de ce lemme à la fin de la section. Le résultat de Gauss est le suivant :

1. Voir le *cours d'Arthmétique* de J.-P. Serre, ou *Multiplicative number theory* de H. Davenport.
2. Bull. Amer. Math. Soc. 55(5), 497–508 (1949). Cette méthode est elle-même inspirée de travaux de Gauss, Jacobi, Hasse et Davenport : nous renvoyons à l'article de Weil pour plus de références historiques.

THÉORÈME 1.8. (Gauss) *Soit p un nombre premier $\equiv 1 \bmod 3$. Alors p s'écrit de manière unique sous la forme $p = A^2+3B^2$ avec $A, B \in \mathbb{Z}$, $B \geq 0$ et $A \equiv -1 \bmod 3$. De plus, on a la relation $|\mathrm{S}_p| = p + 2A$.*

Par exemple pour $p = 7$, on a $7 = 2^2 + 3 \cdot 1^2$ donc $A = 2$, et on retrouve $|\mathrm{S}_7| = 7+4 = 11$. Voir la Table 1 pour plus d'exemples. En pratique, A est beaucoup

p	7	13	19	31	37	43	61	67	73	79	97	103	109
$\lvert\mathrm{S}_p\rvert$	11	11	11	35	47	35	47	83	83	83	83	83	107
A	2	-1	-4	2	5	-4	-7	8	5	2	-7	-10	-1
B	1	2	1	3	2	3	2	3	2	5	4	1	6

TABLE 1. Quelques valeurs de $|\mathrm{S}_p|$, A et B.

plus simple à déterminer que $|\mathrm{S}_p|$! Bien noter que la congruence sur A détermine le signe à choisir pour A. L'inégalité évidente $A^2 < p$ entraîne l'inégalité suivante, qui confirme et précise l'heuristique naturelle [3] selon laquelle on pourrait avoir $|\mathrm{S}_p| \approx p$.

COROLLAIRE 1.9. *Pour tout premier p on a $||\mathrm{S}_p| - p| < 2\sqrt{p}$.*

La démonstration du Théorème 1.8 va nous occuper jusqu'à la fin de cette section. Nous allons faire grand usage des caractères de $(\mathbb{Z}/p\mathbb{Z})^\times$, et ce dès la proposition suivante. Pour $a \in \mathbb{Z}/p\mathbb{Z}$ et $n \geq 1$ on pose

$$\mathrm{N}(x^n = a) = |\{x \in \mathbb{Z}/p\mathbb{Z} \mid x^n = a\}|.$$

Si χ est un caractère de $(\mathbb{Z}/p\mathbb{Z})^\times$, on le prolongera toujours en une fonction $\mathbb{Z}/p\mathbb{Z} \to \mathbb{C}$ en posant $\chi(0) = 0$, sauf si $\chi = 1$ auquel cas on pose $\chi(0) = 1$. Cette convention d'apparence curieuse assurera l'élégance des énoncés (comme le suivant). Noter qu'on a encore $\chi(ab) = \chi(a)\chi(b)$ pour tout $a, b \in \mathbb{Z}/p\mathbb{Z}$ (car $ab = 0 \Leftrightarrow a = 0$ ou $b = 0\}$).

PROPOSITION 1.10. *Pour tout $a \in \mathbb{Z}/p\mathbb{Z}$ on a $\mathrm{N}(x^n = a) = \sum_\chi \chi(a)$, la somme portant sur les m caractères χ de $(\mathbb{Z}/p\mathbb{Z})^\times$ vérifiant $\chi^m = 1$, avec $m = (n, p-1)$.*

Démontrons d'abord seulement les deux cas particuliers $n = 2$ et 3 de cette proposition, les seuls nécessaires à la démonstration du le Théorème 1.8. Dans le cas $n = 2$ et $p > 2$, la Proposition s'écrit :

$$\mathrm{N}(x^2 = a) = 1 + (\frac{a}{p}). \tag{11}$$

C'est vrai, comme on le voit en distinguant les 3 cas $a = 0$ (les deux termes valent 1), a carré non nul (les deux termes valent 2) et a non carré (les deux termes valent 0) ! Pour $n = 3$ et $p \equiv 1 \bmod 3$, l'Exemple 1.4 montre que la Proposition s'écrit :

$$\mathrm{N}(x^3 = a) = 1 + c(a) + c^2(a). \tag{12}$$

Là encore, on constate que les deux termes valent 1 si $a = 0$. Si $a = b^3 \neq 0$ est un cube, alors $x^3 = a$ a pour trois solutions $b, b\omega$ et $b\omega^2$ et on a par définition $a \in \ker c$:

3. En effet, il y a environ $p/2$ carrés et $p/3$ cubes dans $\mathbb{Z}/p\mathbb{Z}$, de sorte que s'il sont "bien répartis" on s'attend à ce qu'environ $p/6$ carrés soient des cubes plus 1. Comme un carré (resp. un cube) non nul est le carré de 2 (resp. 3) éléments, on s'attend donc à avoir $|\mathrm{S}_p| \simeq 6 \cdot p/6 = p$.

ça marche encore. Enfin, si a n'est pas un cube on a $c(a) = j$ ou j^2, et on conclut car $0 = 1 + j + j^2$. La démonstration de la Proposition 1.10 est similaire en général, et reportée à la fin de la section. □

On a $\mathrm{S}_p \sim \{(x, y) \in (\mathbb{Z}/p\mathbb{Z})^2 \mid y^2 + x^3 = 1\}$ par changement de variable $x \mapsto -x$. Le point de départ de la méthode de Weil est la formule évidente :

$$|\mathrm{S}_p| = \sum_{a+b=1} \mathrm{N}(y^2 = a)\,\mathrm{N}(x^3 = b), \tag{13}$$

la somme portant sur les couples $(a, b) \in (\mathbb{Z}/p\mathbb{Z})^2$ avec $a + b = 1$. En appliquant les Formules (11) et (12), la Formule (13) s'écrit alors :

$$|\mathrm{S}_p| = \sum_{a+b=1} (1 + \lambda(a))(1 + c(b) + c^2(b)). \tag{14}$$

Cela conduit à introduire, pour deux caractères χ, ψ de $(\mathbb{Z}/p\mathbb{Z})^\times$ la *somme de Jacobi*

$$\mathrm{J}(\chi, \psi) = \sum_{a+b=1} \chi(a)\psi(b),$$

la somme portant sur les $(a, b) \in (\mathbb{Z}/p\mathbb{Z})^2$ avec $a + b = 1$. C'est un nombre complexe qui est somme finie de racines $p - 1$-èmes de l'unités. La Formule (14) se ré-écrit $|\mathrm{S}_p| = \mathrm{J}(1, 1) + \mathrm{J}(1, c) + \mathrm{J}(1, c^2) + \mathrm{J}(\lambda, 1) + \mathrm{J}(\lambda, c) + \mathrm{J}(\lambda, c^2)$.

Lemme 1.11. *On a* $\mathrm{J}(1, \chi) = \mathrm{J}(1, \chi) = 0$ *pour* $\chi \neq 1$, *et* $\mathrm{J}(1, 1) = p$.

Démonstration — On a $\mathrm{J}(1, \chi) = \mathrm{J}(1, \chi) = \sum_{a \in \mathbb{Z}/p\mathbb{Z}} \chi(a)$. L'égalité $\mathrm{J}(1, 1) = p$ est donc évidente. L'annulation $\mathrm{J}(1, \lambda) = 0$ résulte alors par exemple de ce qu'il y a autant de carrés que de non carrés dans $(\mathbb{Z}/p\mathbb{Z})^\times$. Pour χ général et $x \in (\mathbb{Z}/p\mathbb{Z})^\times$, on a $\chi(x)\mathrm{J}(1, \chi) = \mathrm{J}(1, \chi)$ par le changement de variable bijectif $a \mapsto ax$ dans $\mathbb{Z}/p\mathbb{Z}$. On en déduit $\mathrm{J}(1, \chi) = 0$ pour $\chi \neq 1$ en choisissant x tel que $\chi(x) \neq 1$. □

En utilisant $\mathrm{J}(\lambda, c^2) = \overline{\mathrm{J}(\lambda, c)}$ (car $\overline{\lambda} = \lambda$ et $\overline{c} = c^2$) on obtient finalement

$$|\mathrm{S}_p| = p + \mathrm{J}(\lambda, c) + \overline{\mathrm{J}(\lambda, c)}. \tag{15}$$

L'information finale cruciale sur les $\mathrm{J}(\lambda, c)$ est donnée par la proposition suivante :

Proposition 1.12. *Pour* $\chi, \psi, \chi\psi$ *non triviaux, on a* $|\mathrm{J}(\chi, \psi)|^2 = p$.

Expliquons d'abord comment elle entraîne le Théorème.

Démonstration — (du Théorème 1.8) Par définition, $\mathrm{J}(\lambda, c)$ est une somme d'éléments de la forme $\pm 1, \pm j$ et $\pm j^2$, avec $j = e^{2i\pi/3}$. Comme $j^2 = -1 - j$, on a $\mathrm{J}(\lambda, c) = a + bj$ avec $a, b \in \mathbb{Z}$. La Proposition 1.12 entraîne $p = |a + bj|^2 = a^2 - ab + b^2$. On a aussi $\mathrm{J}(\lambda, c) + \overline{\mathrm{J}(\lambda, c)} = 2a - b$. La formule (15) montre donc

$$|\mathrm{S}_p| = p + 2a - b.$$

Mais $|\mathrm{S}_p|$ est impair par le Lemme 1.6, et on a $p \neq 2$, donc b est pair. On pose $A = a - b/2$ et $B = |b/2|$. On a donc $|\mathrm{S}_p| = p + 2A$ et $p = a^2 - ab + b^2 = (a - b/2)^2 + 3b^2/4 = A^2 + 3B^2$. Enfin, le Lemme 1.6 montre $A \equiv -1 \bmod 3$. □

La Proposition 1.12 va résulter de l'étude des *sommes de Gauss*. Pour un caractère χ de $(\mathbb{Z}/p\mathbb{Z})^\times$ donné, c'est la somme $\mathrm{G}(\chi) = \sum_{a\in\mathbb{Z}/p\mathbb{Z}} \chi(a)\zeta^a$, avec $\zeta = e^{2i\pi/p}$.

PROPOSITION 1.13. *Soient $\chi, \psi \in \widehat{(\mathbb{Z}/p\mathbb{Z})^\times}$ des caractères non triviaux. On a :*

(i) $|\mathrm{G}(\chi)|^2 = p$,

(ii) $\mathrm{G}(\chi)\mathrm{G}(\psi) = \mathrm{J}(\chi,\psi)\mathrm{G}(\chi\psi)$ *si* $\chi\psi \neq 1$.

Le côté très surprenant de l'égalité (i) est qu'une somme de $p-1$ racines de l'unité soit de module $\sqrt{p}$. Noter que (i) et (ii) entraînent la Proposition 1.12, et terminent donc la démonstration du théorème de Gauss.

DÉMONSTRATION — Montrons le (i). On a $\overline{\mathrm{G}(\chi)} = \sum_{a\in\mathbb{Z}/p\mathbb{Z}} \chi^{-1}(a)\zeta^{-a}$, et donc

$$|\mathrm{G}(\chi)|^2 = \mathrm{G}(\chi)\overline{\mathrm{G}(\chi)} = \sum_{a,b\in\,\mathbb{Z}/p\mathbb{Z}} \chi(a)\chi^{-1}(b)\zeta^{a-b}$$

par un développement brutal. La convention $\chi(0) = \chi^{-1}(0) = 0$ montre que l'on peut supposer $a, b \in (\mathbb{Z}/p\mathbb{Z})^\times$ dans la somme ci-dessus. Le changement de variable $b = at$ avec $t \in (\mathbb{Z}/p\mathbb{Z})^\times$ permet alors de ré-écrire :

$$|\mathrm{G}(\chi)|^2 = \sum_{a,t\in(\mathbb{Z}/p\mathbb{Z})^\times} \chi^{-1}(t)\zeta^{a(1-t)} = \sum_{t\in(\mathbb{Z}/p\mathbb{Z})^\times} \chi^{-1}(t) \sum_{a\in(\mathbb{Z}/p\mathbb{Z})^\times} \zeta^{a(1-t)}.$$

Mais $\sum_{a\in(\mathbb{Z}/p\mathbb{Z})^\times} \zeta^{a(1-t)}$ vaut -1 pour $t \neq 1$, et $p-1$ pour $t = 1$. On en déduit

$$|\mathrm{G}(\chi)|^2 = -\sum_{t\in(\mathbb{Z}/p\mathbb{Z})^\times} \chi^{-1}(t) + \chi^{-1}(1) + p - 1 = 0 + 1 + p - 1 = p.$$

Montrons le (ii). On a encore $\mathrm{G}(\chi)\mathrm{G}(\psi) = \sum_{a,b\in\mathbb{Z}/p\mathbb{Z}} \chi(a)\psi(b)\zeta^{a+b}$, puis

$$\mathrm{G}(\chi)\mathrm{G}(\psi) = \sum_{k\in\mathbb{Z}/p\mathbb{Z}} \Big(\sum_{a+b=k} \chi(a)\psi(b)\Big)\,\zeta^k.$$

Pour $k = 0$, la somme entre parenthèses vaut $\sum_{a\in\mathbb{Z}/p\mathbb{Z}} \chi(a)\psi(-a) = \mathrm{J}(1,\chi\psi)\psi(-1) = 0$ car $\chi\psi \neq 1$. Pour $k \neq 0$, le changement de variables $a = ka'$ et $b = kb'$ montre qu'elle vaut $\sum_{a'+b'=1} \chi(a'k)\psi(b'k) = \chi(k)\psi(k)\mathrm{J}(\chi,\psi)$. On a donc

$$\mathrm{G}(\chi)\mathrm{G}(\psi) = \sum_{k\in(\mathbb{Z}/p\mathbb{Z})^\times} \chi(k)\psi(k)\mathrm{J}(\chi,\psi)\zeta^k = \mathrm{J}(\chi,\psi)\mathrm{G}(\chi\psi).$$

□

Il nous reste encore à démontrer le Lemme 1.7, laissé de côté.

DÉMONSTRATION — (du Lemme 1.7) Supposons $p = a^2 + db^2$ avec $a, b \in \mathbb{N}$. On peut supposer $p \nmid d$, sinon on a $d = p$ et une unique solution $(a,b) = (0,1)$, puis $a, b \geq 1$. On a alors les inégalités $1 \leq a < \sqrt{p}$ et $1 \leq b < \sqrt{p/d}$. On a aussi $\mathrm{pgcd}(a,b) = 1$, et $p \nmid b$, sinon on aurait $p \mid a$ et $p^2 \mid p$, une contradiction. On a donc $(a/b)^2 \equiv -d \bmod p$.

Supposons enfin $p = a^2 + db^2 = (a')^2 + d(b')^2$ avec $a, a', b, b' \in \mathbb{N}$. L'analyse ci-dessus montre $(a/b)^2 \equiv -d \equiv (a'/b')^2 \bmod p$, puis $a/b \equiv \pm a'/b' \bmod p$ car p est premier. Ceci et les inégalités ci-dessus montrent donc

$$ab' \equiv \pm a'b \bmod p \quad \text{et} \quad 1 \leq ab', a'b < p/d. \tag{16}$$

Pour $d \geq 2$ cela entraîne $ab' = a'b$. Mais on a $\mathrm{pgcd}(a,b) = \mathrm{pgcd}(a',b') = 1$, donc $a \mid a'$, $a' \mid a$, $a = a'$ et $b = b'$. Dans le cas $d = 1$, la relation (16) entraîne soit $ab' = a'b$, et donc $(a,b) = (a',b)$ comme ci-dessus, soit $ab' + a'b = p$. Mais dans ce cas, les vecteurs $u = (a,b)$ et $v = (b',a')$ de $\mathbb{R}^2$ vérifient $u.u = v.v = u.v = p$ et on a $u = v$ par Cauchy-Schwarz : les deux solutions sont (of course !) (a,b) et (b,a). □

Remarque 1.14. (Retour sur les premiers 1 mod 4) La Proposition 1.12 entraîne aussi qu'un nombre premier $p \equiv 1 \bmod 4$ est somme de deux carrés. En effet, pour $p \equiv 1 \bmod 4$ on peut trouver un caractère χ d'ordre 4 de $(\mathbb{Z}/p\mathbb{Z})^\times$ (pourquoi ?). D'après la proposition, on a $|\mathrm{J}(\chi,\chi)|^2 = p$, ou encore $|\mathrm{J}(\chi,\lambda)|^2 = p$. Ces deux sommes de Jacobi sont de la forme $a + bi$ avec $a, b \in \mathbb{Z}$, et donc $p = a^2 + b^2$. Voir l'Exercice 3.5 pour une suite !

Remarque 1.15. (Somme de Gauss quadratique) Pour $p \neq 2$, c'est la somme $\mathrm{G}_p := \mathrm{G}(\lambda) = \sum_{k \in \mathbb{Z}/p\mathbb{Z}} \left(\frac{k}{p}\right) e^{\frac{2ik\pi}{p}}$. En utilisant $\sum_{k=0}^{p-1} e^{\frac{2ik\pi}{p}} = 0$, on constate aussi

$$\mathrm{G}_p = \sum_{k=0}^{p-1} e^{\frac{2i\pi k^2}{p}}.$$

Pour tout caractère χ, on a aussi $\chi(-1) = \pm 1$, et par la bijection $x \mapsto -x$,

$$\overline{\mathrm{G}(\chi)} = \sum_{x \in \mathbb{Z}/p\mathbb{Z}} \overline{\chi(x)} \zeta^{-x} = \chi(-1)\mathrm{G}(\overline{\chi}). \tag{17}$$

Comme $\lambda = \overline{\lambda}$, on a $\overline{\mathrm{G}_p} = (\frac{-1}{p})\mathrm{G}_p$, mais aussi $|\mathrm{G}_p|^2 = p$ par la proposition, puis

$$\mathrm{G}_p^2 = \left(\frac{-1}{p}\right) p = (-1)^{\frac{p-1}{2}} p.$$

On a donc $\mathrm{G}_p = \pm\sqrt{p}$ pour $p \equiv 1 \bmod 4$ et $\mathrm{G}_p \equiv \pm i\sqrt{p}$ pour $p \equiv 3 \bmod 4$. Gauss a démontré (de son aveu, avec difficulté !) que ces signes sont toujours $+$. Nous renvoyons aux exercices pour une démonstration due à Dirichlet de ce résultat, et pour une preuve simple de la loi de réciprocité quadratique qui s'en déduit. Pour $\chi \neq \lambda$, il n'y a pas de formule simple connue pour $\mathrm{G}(\chi)$ (ni même pour la *somme de Gauss cubique* $\mathrm{G}(c)$, qui a fait l'objet de nombreux travaux initiés par Kummer : voir l'Exercice 3.4).

Terminons cette section par une démonstration de la Proposition 1.10.

Démonstration — (de la Proposition 1.10, omise en classe) Dans le cas $a = 0$, le terme de gauche vaut 1 (0 est seule solution) et celui de droite vaut aussi 1 par la convention $\chi(0) = 0$ pour $\chi \neq 1$, et $\chi(0) = 1$ pour $\chi = 1$. On suppose donc $a \neq 0$.

Fixons g un générateur de $(\mathbb{Z}/p\mathbb{Z})^\times$. D'après la Proposition 1.3, les caractères de $(\mathbb{Z}/p\mathbb{Z})^\times$ sont les $g^k \mapsto \zeta^k$ avec $\zeta^{p-1} = 1$. Un tel caractère χ vérifie $\chi^m = 1$ si, et seulement si, $\zeta^m = 1$. Noter $\mu_m \subset \mu_{p-1}$. Écrivons $a = g^k$ pour $k \in \mathbb{Z}$. On a donc

$$\sum_{\{\chi \,|\, \chi^m = 1\}} \chi(a) = \sum_{\zeta \in \mu_m} \zeta^k.$$

Cette somme qui vaut m si $k \equiv 0 \bmod m$, et 0 sinon. Il suffit donc de montrer

$$\mathrm{N}(x^n = g^k) = m \text{ si } k \equiv 0 \bmod m, \ 0 \text{ sinon.} \tag{18}$$