

**Exercice 1**

Pour tout  $a$  premier à  $p$ , notons  $\lambda(a)$  la signature de la multiplication par  $a$ .

**Première preuve.** Les applications  $a \mapsto \left(\frac{a}{p}\right)$  et  $a \mapsto \lambda(a)$  sont deux morphismes de groupes de  $(\mathbb{Z}/p\mathbb{Z})^\times$  vers  $\{-1, 1\}$ ; comme leur valeur en un élément donné ne peut être égale qu'à 1 ou  $(-1)$  il suffit, pour montrer qu'ils coïncident, de vérifier qu'ils prennent la valeur 1 exactement sur les mêmes éléments, c'est-à-dire qu'ils ont même noyau.

Or  $(\mathbb{Z}/p\mathbb{Z})^\times$  est cyclique de cardinal pair, et possède dès lors un unique sous-groupe  $G$  d'indice 2, et tout morphisme surjectif de  $(\mathbb{Z}/p\mathbb{Z})^\times$  vers  $\{-1, 1\}$  a nécessairement  $G$  pour noyau. C'est en particulier le cas de  $a \mapsto \left(\frac{a}{p}\right)$ , et il suffit donc pour conclure de démontrer que  $\lambda$  est lui aussi surjectif. Autrement dit, il suffit d'exhiber un élément  $a$  de  $(\mathbb{Z}/p\mathbb{Z})^\times$  tel que  $\lambda(a) = -1$ . Prenons pour  $a$  un générateur du groupe cyclique  $(\mathbb{Z}/p\mathbb{Z})^\times$ . L'orbite de 1 sous l'action de  $\langle a \rangle$  est  $\{a^i\}_{i \in \mathbb{Z}}$  et c'est donc  $(\mathbb{Z}/p\mathbb{Z})^\times$  tout entier. La permutation de  $(\mathbb{Z}/p\mathbb{Z})^\times$  induite par  $a$  est par conséquent un  $(p-1)$ -cycle; puisque  $p-1$  est pair, cette permutation est impaire, et  $\lambda(a) = -1$ .

**Seconde preuve, proposée par l'un d'entre-vous.** Soit  $a$  un élément de  $(\mathbb{Z}/p\mathbb{Z})^\times$  et soit  $\sigma$  la permutation de  $(\mathbb{Z}/p\mathbb{Z})^\times$  induite par la multiplication par  $a$ . Si l'on identifie  $(\mathbb{Z}/p\mathbb{Z})^\times$  à  $\{1, \dots, p-1\}$  on a

$$\varepsilon(\sigma) = \prod_{1 \leq i < j \leq p-1} \frac{\sigma(j) - \sigma(i)}{j - i}.$$

C'est une égalité qu'on peut réduire modulo  $p$  car si  $i$  et  $j$  sont deux entiers tels que  $1 \leq i < j \leq p-1$  alors  $1 \leq j-i \leq p-2$  et  $j-i$  est en particulier inversible modulo  $p$ .

Il vient

$$\lambda(a) = \prod_{1 \leq i < j \leq p-1} \frac{a(j-i)}{j-i},$$

puisque  $\sigma(i)$  est par définition pour tout  $i$  la classe de  $ai$  modulo  $p$ . Comme il y a  $(p-1)(p-2)/2$  paires d'éléments de  $\{1, \dots, p-1\}$  on voit que

$$\lambda(a) = \prod_{1 \leq i < j \leq p-1} a = a^{(p-1)(p-2)/2} = a^{(p-1)/2} = \left(\frac{a}{p}\right),$$

où l'avant-dernière égalité provient du fait que  $a^{(p-1)/2} \in \{-1, 1\}$  (c'est un symbole de Legendre) et que  $p-2$  est impair.

## Exercice 2

Commençons par une remarque : l'exercice introduit une matrice  $S$ , carrée de taille  $p$  (mais indexée par  $\{0, \dots, p-1\}^2$  et non par  $\{1, \dots, p\}^2$ ). On a par définition

$$\text{Tr}(S) = \sum_{x=0}^{p-1} \xi^{x^2} = G_p;$$

le nombre complexe qu'on se propose de calculer est donc la trace de  $S$ .

**Question (1).** Le terme d'indice  $(i, j)$  de  $S^2$  est

$$\begin{aligned} \sum_{k=0}^{p-1} \xi^{ik} \xi^{kj} &= \sum_{k=0}^{p-1} \xi^{k(i+j)} \\ &= \sum_{k=0}^{p-1} (\xi^{i+j})^k. \end{aligned}$$

On distingue maintenant deux cas. Si  $i+j$  est non nul modulo  $p$ , c'est-à-dire ici si  $i+j \neq 0$  et  $i+j \neq p$ , alors  $\xi^{i+j} \neq 1$  et la somme calculée vaut

$$\frac{1 - (\xi^{i+j})^p}{1 - \xi^{i+j}} = 0.$$

Et si  $i+j$  est nul modulo  $p$  alors  $\xi^{i+j} = 1$  et la somme calculée vaut  $p$ .

On voit donc que tous les coefficients de  $S^2$  sont nuls, hormis les coefficients d'indice  $(0, 0)$  et  $(i, p-i)$  pour  $i$  variant entre 1 et  $p-1$ . La matrice  $S^2$  est donc égale à  $\text{Diag}(p, B)$  où  $B$  est le bloc de taille  $(p-1, p-1)$ , paramétré par  $(\{1, \dots, p-1\}^2)$ , et dont tous les termes sont nuls sauf ceux de l'antidiagonale qui valent  $p$ .

La suite de l'exercice va requérir de bien comprendre les valeurs propres de  $S^2$  et leurs multiplicités. Pour cela, il va être commode de faire la remarque suivante. Identifions  $B$  à l'endomorphisme de  $\mathbb{C}^{p-1}$  dont elle est la matrice dans la base canonique  $(e_1, \dots, e_{p-1})$ . On a alors  $Be_i = pe^{p-i}$  pour tout  $i$ , si bien que dans la base  $(e_1, e_{p-1}, e_2, e_{p-2}, \dots, e_{p-1/2}, e_{p+1/2})$ , l'endomorphisme  $B$  a pour matrice  $\text{Diag}(\underbrace{C, \dots, C}_{(p-1)/2 \text{ blocs}})$  où

$$C = \begin{pmatrix} 0 & p \\ p & 0 \end{pmatrix}.$$

La matrice  $C$  a pour polynôme caractéristique  $X^2 - p^2 = (X+p)(X-p)$ . Elle est donc diagonalisable, avec deux valeurs propres distinctes  $p$  et  $(-p)$ .

Il s'ensuit que  $S^2$  est diagonalisable avec pour valeurs propres  $p$ , qui apparaît avec multiplicité  $1 + \frac{p-1}{2} = \frac{p+1}{2}$  et  $(-p)$  qui apparaît avec multiplicité  $\frac{p-1}{2}$ . En particulier  $\det S^2 = (-1)^{(p-1)/2} p^p$ , que l'on peut récrire  $(-1)^{p(p-1)/2} p^p$  puisque  $p$  est impair.

**Question (2).** On remarque que la matrice  $S$  est la matrice de Vandermonde associée à  $(1, \xi, \xi^2, \dots, \xi^{p-1})$ . Il vient, en posant  $\omega = \exp(i\pi/p)$  :

$$\begin{aligned}
\det S &= \prod_{0 \leq i < j \leq p-1} \xi^j - \xi^i \\
&= \prod_{0 \leq i < j \leq p-1} \omega^{i+j} (\omega^{j-i} - \omega^{i-j}) \\
&= \prod_{0 \leq i < j \leq p-1} \omega^{i+j} \\
&= \omega^{\sum_{0 \leq i < j \leq p-1} i+j} (2i)^{p(p-1)/2} \prod_{0 \leq i < j \leq p-1} \sin(\pi(j-i)/p).
\end{aligned}$$

Nous savons que  $\det S^2 = (-1)^{p(p-1)/2} p^p$ , si bien que  $|\det S| = p^{p/2}$ . Pour déterminer complètement  $\det S$ , il suffit de déterminer son argument. Comme  $\sin(\pi(j-i)/p) > 0$  pour tous les couples  $(i, j)$  avec  $0 \leq i < j \leq p-1$ , cet argument est celui de  $i^{p(p-1)/2} \omega^N$ , où l'on a posé  $N = \sum_{0 \leq i < j \leq p-1} i+j$ .

Il reste donc à calculer  $N$ . On a

$$\begin{aligned}
N &= \sum_{0 \leq i < j \leq p-1} i+j \\
&= \sum_{1 \leq j \leq p-1} \sum_{0 \leq i \leq j-1} j+i \\
&= \sum_{1 \leq j \leq p-1} j^2 + \frac{j(j-1)}{2} \\
&= \frac{1}{2} \sum_{1 \leq j \leq p-1} 3j^2 - j \\
&= \frac{1}{2} \left( \frac{(p-1)p(2p-1)}{2} - \frac{(p-1)p}{2} \right) \\
&= \frac{1}{2} \frac{p(p-1)(2p-2)}{2} \\
&= \frac{p(p-1)^2}{2}.
\end{aligned}$$

Or comme  $(p-1)$  est pair,  $(p-1)^2$  est multiple de 4 et  $(p-1)^2/2$  est donc pair. Par conséquent  $N$  est multiple de  $2p$ , si bien que  $\omega^N = 1$ . L'argument de  $S$  est dès lors égal à celui de  $i^{p(p-1)/2}$  et il vient

$$\det S = i^{p(p-1)/2} p^{p/2},$$

ce qu'on souhaitait établir.

**Question (3).** En considérant une base de trigonalisation de l'endomorphisme de matrice  $S$  (dans la base canonique) on voit que si  $\lambda_1, \dots, \lambda_n$  désigne la liste des valeurs propres de  $S$  (chacune étant répétée autant de fois qu'il convient) alors  $\lambda_1^2, \dots, \lambda_n^2$  est la liste des valeurs propres de  $S^2$ , que nous connaissons : il y a  $p$  avec multiplicité  $(p+1)/2$ , et  $(-p)$  avec multiplicité  $(p-1)/2$ . Il s'ensuit que toute valeur propre de  $S$  est de carré  $p$  ou  $-p$ , donc de la forme  $\pm\sqrt{p}$  ou  $\pm i\sqrt{p}$ .

Les valeurs propres de  $S$  égales à  $\pm\sqrt{p}$  sont celles de carré  $p$ , si bien que  $u+v$  doit être égal à la multiplicité de  $p$  comme valeur propre de  $S$ , c'est-à-dire  $p+1/2$ . De même, les propres de  $S$  égales à  $\pm i\sqrt{p}$  sont celles de carré  $-p$ , si bien que  $r+s$  doit être égal à la multiplicité de  $p$  comme valeur propre de  $S$ , c'est-à-dire  $p+1/2$ .

Enfin le déterminant de  $S$  est égal à  $(-1)^v i^r (-i)^s p^{p/2}$ , c'est-à-dire à  $i^{2v+r-s} p^{p/2}$  (puisque  $(-1) = i^2$  et  $-i = i^{-1}$  et on sait par ailleurs qu'il vaut  $(i)^{p(p-1)/2} p^{p/2}$ ). Il vient  $i^{p(p-1)/2} = i^{2v+r-s}$ , ce qui revient à dire que  $2v+r-s = p(p-1)/2$  modulo 4 puisque  $i$  est d'ordre 4.

**Question (4).** La trace de  $S$  est égale  $\sum_{x \in \mathbb{F}_p} \xi^{x^2}$ . Or si  $k$  est un élément de  $\mathbb{F}_p$ , on est dans l'un des trois cas suivants (exclusifs l'un de l'autre) :

- (a) On a  $k = 0$  ; dans ce cas  $k$  est égal à  $x^2$  pour un unique  $x$  de  $\mathbb{F}_p$ , à savoir 0 ;
- (b) Si  $k \in (\mathbb{F}_p^\times)^2$  alors  $k$  est égal à  $x^2$  pour exactement deux éléments  $x$  de  $F_p$  ;
- (c) Si  $k \notin (\mathbb{F}_p^\times)^2$  alors  $k$  n'est égal à  $x^2$  pour aucun élément  $x$  de  $F_p$ .

La somme  $\sum_{x \in \mathbb{F}_p} \xi^{x^2}$  peut donc se récrire  $\sum_{k \in F_p} \lambda(k) \xi^k$  où  $\lambda(k)$  vaut 1 si  $k = 0$ , 2 si  $k \in (\mathbb{F}_p^\times)^2$ , et 0 sinon. Petit miracle : si l'on a une bonne vue, on remarque que  $\lambda(k)$  peut s'écrire uniformément (sans disjonction de cas) comme  $1 + \left(\frac{k}{p}\right)$ .

On a donc

$$\text{Tr}(S) = \sum_{k=0}^{p-1} \left(1 + \left(\frac{k}{p}\right)\right) \xi^k.$$

Mais comme  $\sum_{k=0}^{p-1} \xi^k = (1 - \xi^p)/(1 - \xi) = 0$ , on a finalement

$$\text{Tr}(S) = \sum_{k=0}^{p-1} \left(\frac{k}{p}\right) \xi^k,$$

ce qu'il fallait démontrer.

**Question (6).** Pour conclure, nous allons commencer par étudier le module et l'argument de  $\text{Tr}(S)$ . On commence par remarquer que

$$\begin{aligned} \overline{\text{Tr}(S)} &= \sum_{k=0}^{p-1} \left(\frac{k}{p}\right) \xi^{-k} \\ &= \sum_{k \in \mathbb{F}_p} \left(\frac{k}{p}\right) \xi^{-k} \\ &= \sum_{k \in \mathbb{F}_p} \left(\frac{-k}{p}\right) \xi^k \\ &= \left(\frac{-1}{p}\right) \sum_{k \in \mathbb{F}_p} \left(\frac{k}{p}\right) \xi^k \\ &= \left(\frac{-1}{p}\right) \text{Tr}(S). \end{aligned}$$

Par conséquent  $\text{Tr}(S)$  est réel si  $p$  vaut 1 modulo 4, et imaginaire pur si  $p$  vaut  $(-1)$  modulo 4.

Calculons maintenant  $|\text{Tr}(S)|$ . On a

$$\begin{aligned}\text{Tr}(S)\overline{\text{Tr}(S)} &= \left( \sum_{k \in \mathbb{F}_p} \left( \frac{k}{p} \right) \xi^k \right) \left( \sum_{k \in \mathbb{F}_p} \left( \frac{k}{p} \right) \xi^{-k} \right) \\ &= \sum_{k, \ell \in \mathbb{F}_p} \left( \frac{k}{p} \right) \left( \frac{\ell}{p} \right) \xi^{k-\ell} \\ &= \sum_{k \in \mathbb{F}_p, i \in \mathbb{F}_p} \left( \frac{k}{p} \right) \left( \frac{k-i}{p} \right) \xi^i\end{aligned}$$

(la dernière s'obtient en faisant le changement de variable  $(k, \ell) = (k, k - \ell)$ ).

Fixons  $i$  et calculons  $\sum_{k \in \mathbb{F}_p} \left( \frac{k}{p} \right) \left( \frac{k-i}{p} \right)$ . Supposons tout d'abord que  $i = 0$ .

On trouve alors  $\sum_{k \in \mathbb{F}_p} \left( \frac{k}{p} \right)^2$ , ce qui fait  $p - 1$  car  $\left( \frac{k}{p} \right)$  est égal à  $\pm 1$  si  $k$  est non nul et à 0 sinon. Supposons maintenant que  $i \neq 0$ . On a

$$\begin{aligned}\sum_{k \in \mathbb{F}_p} \left( \frac{k}{p} \right) \left( \frac{k-i}{p} \right) &= \sum_{k \in \mathbb{F}_p^\times} \left( \frac{k}{p} \right) \left( \frac{k-i}{p} \right) \\ &= \sum_{k \in \mathbb{F}_p^\times} \left( \frac{k}{p} \right) \left( \frac{k}{p} \right) \left( \frac{1 - ik^{-1}}{p} \right) \\ &= \sum_{k \in \mathbb{F}_p^\times} \left( \frac{1 - ik^{-1}}{p} \right).\end{aligned}$$

Or comme  $i$  est non nul l'application  $a \mapsto 1 - ia$  est une bijection de  $\mathbb{F}_p$  sur lui-même. L'application  $k \mapsto k^{-1}$  est une bijection de  $\mathbb{F}_p^\times$  sur lui-même et comme  $i$  est non nul l'application  $a \mapsto 1 - ia$  est une bijection de  $\mathbb{F}_p^\times$  sur lui-même, qui en induit une de  $\mathbb{F}_p^\times$  sur  $\mathbb{F}_p - \{1\}$ . Il s'ensuit que  $k \mapsto 1 - ik^{-1}$  induit une bijection de  $\mathbb{F}_p^\times$  sur  $\mathbb{F}_p^\times \setminus \{1\}$ .

La somme étudiée se réécrit donc  $\sum_{a \in \mathbb{F}_p, a \neq 1} \left( \frac{a}{p} \right)$ . Or on sait que  $\sum_{a \in \mathbb{F}_p} \left( \frac{a}{p} \right) = 0$  (cela découle du fait que  $\left( \frac{0}{p} \right) = 0$  et que  $a \mapsto \left( \frac{a}{p} \right)$  définit un caractère non trivial de  $\mathbb{F}_p^\times$ ). Il vient

$$\sum_{a \in \mathbb{F}_p, a \neq 1} \left( \frac{a}{p} \right) = - \left( \frac{1}{p} \right) = (-1).$$

Il découle de tout ce qui précède que

$$\text{Tr}(S)\overline{\text{Tr}(S)} = (p - 1) - \sum_{i \in \mathbb{F}_p^\times} \xi^i.$$

Mais comme  $\sum_{i \in \mathbb{F}_p} \xi^i = \sum_{0 \leq i \leq p-1} \xi^i = (1 - \xi^p)/(1 - \xi) = 0$ ,  $\sum_{i \in \mathbb{F}_p^\times} \xi^i = -1$ . On en conclut que  $\text{Tr}(S)\overline{\text{Tr}(S)} = p$ . Par conséquent,  $|\text{Tr}(S)| = \sqrt{p}$ .

Nous allons maintenant pouvoir déterminer entièrement  $\text{Tr}(S)$ . Remarquons déjà que par définition même de  $u, v, r$  et  $s$  on a  $\text{Tr}(S) = (u-v)\sqrt{p} + i(r-s)\sqrt{p}$ . On distingue maintenant deux cas.

Supposons que  $p \equiv 1 \pmod{4}$ . On sait alors que  $\text{Tr}(S)$  est réelle, ce qui entraîne  $r = s = (p-1)/4$  puisque  $r+s = (p-1)/2$ . Et comme  $|\text{Tr}(S)| = \sqrt{p}$  on a  $u-v = 1$  ou  $u-v = -1$ ; comme on sait par ailleurs que  $u+v = (p+1)/2$ , cela signifie qu'on a  $u = (p+3)/4$  et  $v = (p-1)/4$  ou  $u = (p-1)/4$  et  $v = (p+3)/4$ . Mais on sait aussi que  $2v+r-s$  est égal à  $p(p-1)/2$  modulo 4, c'est-à-dire encore à  $(p-1)/2$  modulo 4 puisque  $p$  vaut 1 modulo 4. Cela exclut le cas où  $v = (p+3)/4$  car  $(p+3)/2 - (p-1)/2 = 2 \not\equiv 0 \pmod{4}$ . Par conséquent  $v = (p-1)/4$ ,  $u = (p+3)/4$  et  $\text{Tr}(S) = \sqrt{p}$ .

Supposons que  $p \equiv -1 \pmod{4}$ . On sait alors que  $\text{Tr}(S)$  est imaginaire pure, ce qui entraîne  $u = v(p+1)/4$  puisque  $u+v = (p+1)/2$ . Et comme  $|\text{Tr}(S)| = \sqrt{p}$  on a  $r-s = 1$  ou  $r-s = -1$ ; comme on sait par ailleurs que  $r+s = (p-1)/2$ , cela signifie qu'on a  $r = (p+1)/4$  et  $s = (p-3)/4$  ou  $r = (p-3)/4$  et  $s = (p+1)/4$ . Mais on sait aussi que  $2v+r-s$  est égal à  $p(p-1)/2$  modulo 4, c'est-à-dire encore à  $-(p-1)/2$  modulo 4 puisque  $p$  vaut  $-1$  modulo 4. Cela exclut le cas où  $r-s = -1$  car  $(p+1)/2 - 1 = (p-1)/2$  qui est différent de  $-(p-1)/2$  modulo 4 puisque  $(p-1)/2$  est impair (car  $p \not\equiv 1 \pmod{4}$ ), donc inversible modulo 4. Par conséquent  $r-s = 1$  et  $\text{Tr}(S) = i\sqrt{p}$ .

## Exercice 4

Avant d'entamer la correction de l'exercice proprement dit, nous allons rappeler quelques faits généraux de théorie des groupes, qui doivent être bien connus, et dont l'utilisation doit être un réflexe.

### Préliminaires (P1) : Morphismes depuis un groupe cyclique.

Commençons par rappeler quelques faits généraux sur les morphismes de groupes, et les caractères en particulier.

Soit  $H$  un groupe et soit  $n$  un entier. L'application  $\varphi \mapsto \varphi(\bar{1})$  établit une bijection de  $\text{Hom}(\mathbb{Z}/n\mathbb{Z}, H)$  sur  $\{h \in H, h^n = e\}$ . Sa réciproque envoie un élément  $h$  de  $H$  tel que  $h^n = e$  sur le morphisme  $\bar{a} \mapsto h^a$  de  $\mathbb{Z}/n\mathbb{Z}$  vers  $H$ , qui est bien défini car comme  $h^n = e$ , l'élément  $h^a$  de  $G$  ne dépend bien que de la classe  $\bar{a}$  de  $a$  modulo  $n$ .

Supposons de plus que  $H$  est abélien. Dans ce cas  $\text{Hom}(G, H)$  a pour tout groupe  $G$  une structure naturelle de groupe abélien : sa loi interne envoie un couple  $(\varphi, \psi)$  de morphismes sur  $\varphi\psi: G \rightarrow H, g \mapsto \varphi(g)\psi(g)$  (exercice : vérifiez que  $\varphi\psi$  est bien un morphisme ; c'est là que le caractère abélien de  $H$  intervient). Et  $\{h \in H, h^n = e\}$  est un sous-groupe de  $H$  (c'est le noyau de  $h \mapsto h^n$  qui est un morphisme de groupes de  $H$  dans  $H$  car  $H$  est abélien). La bijection entre  $\text{Hom}(\mathbb{Z}/n\mathbb{Z}, H)$  et  $\{h \in H, h^n = e\}$  construite ci-dessus est alors un *isomorphisme de groupes*.

Soit maintenant  $G$  un groupe cyclique, soit  $n$  son cardinal et soit  $g$  un générateur de  $G$ . Il existe un isomorphisme entre  $\mathbb{Z}/n\mathbb{Z}$  et  $G$  envoyant  $\bar{1}$  sur  $g$ , et l'on déduit alors de ce qui précède que pour tout groupe  $H$ , l'application  $\varphi \mapsto \varphi(g)$  établit une bijection de  $\text{Hom}(G, H)$  sur  $\{h \in H, h^n = e\}$ , dont la réciproque envoie un élément  $h$  de  $H$  tel que  $h^n = e$  sur le morphisme  $g^a \mapsto h^a$  de  $G$  vers  $H$ , qui est bien défini ; et cette bijection est un isomorphisme de groupes lorsque  $H$  est abélien.

**Préliminaires (P2) : morphismes depuis un produit.** Soient  $G$  et  $H$  deux groupes, et soit  $K$  un groupe *abélien*. On dispose alors d'un isomorphisme de groupes

$$\mathrm{Hom}(G \times H, K) \simeq \mathrm{Hom}(G, K) \times \mathrm{Hom}(H, K).$$

Il est donné par la formule

$$\chi \mapsto (g \mapsto \chi(g, 1), h \mapsto \chi(1, h))$$

et sa réciproque est

$$(\varphi, \psi) \mapsto ((g, h) \mapsto \varphi(g)\psi(h))$$

(que  $(g, h) \mapsto \varphi(g)\psi(h)$  soit un morphisme résulte du fait que  $K$  est abélien, vérifiez-le en exercice).

**Question (1).** Le groupe  $(\mathbb{Z}/4\mathbb{Z})^\times$  est égal à  $\{-1, 1\}$  et est cyclique d'ordre 2, de générateur  $(-1)$ . Il résulte alors du paragraphe (P1) que  $\varphi \mapsto \varphi(-1)$  établit un isomorphisme entre le groupe des caractères de Dirichlet modulo 4 et  $\{z \in \mathbb{C}^\times, z^2 = 1\} = \{-1, 1\}$ . Il y a par conséquent deux caractères de Dirichlet modulo 4 : le caractère trivial qui envoie 1 et  $(-1)$  sur 1, et le caractère qui envoie 1 sur 1 et  $(-1)$  sur  $(-1)$ .

Le groupe  $(\mathbb{Z}/8\mathbb{Z})^\times$  est égal à  $\{-1, 1, 3, -3\}$ , avec  $3^2 = (-3)^2 = 9 = 1$  (on travaille modulo 8). Les sous-ensembles  $\{1, -1\}$  et  $\{1, 3\}$  de  $(\mathbb{Z}/8\mathbb{Z})^\times$  en sont deux sous-groupes, tous deux cycliques d'ordre 2, et l'application du produit  $\{1, -1\} \times \{1, 3\}$  vers  $(\mathbb{Z}/8\mathbb{Z})^\times$  qui envoie  $(a, b)$  sur  $ab$  est clairement un isomorphisme de groupes. On en déduit à l'aide du paragraphe (P2) que se donner un caractère sur  $(\mathbb{Z}/8\mathbb{Z})^\times$  revient à se donner un caractère sur  $\{1, -1\}$ , c'est-à-dire par le paragraphe (P1) un élément de carré 1 de  $\mathbb{C}^\times$  (l'image de  $(-1)$ ), et un caractère sur  $\{1, 3\}$ , c'est-à-dire par le paragraphe (P1) un élément de carré 1 de  $\mathbb{C}^\times$  (l'image de  $(3)$ ). On a en conséquence quatre caractères sur  $(\mathbb{Z}/8\mathbb{Z})^\times$ , donnés par les quatre tableaux de valeurs

$$\begin{pmatrix} 1 & -1 & 3 & -3 \\ 1 & 1 & 1 & 1 \end{pmatrix} \begin{pmatrix} 1 & -1 & 3 & -3 \\ 1 & 1 & -1 & -1 \end{pmatrix} \\ \begin{pmatrix} 1 & -1 & 3 & -3 \\ 1 & -1 & 1 & -1 \end{pmatrix} \begin{pmatrix} 1 & -1 & 3 & -3 \\ 1 & -1 & -1 & 1 \end{pmatrix}.$$

**Question (2).** On sait que le groupe  $(\mathbb{Z}/7\mathbb{Z})^\times = \{-3, -2, -1, 1, 2, 3\}$  est cyclique; commençons par en trouver un générateur. Modulo 7 on a  $2^3 = 1$  donc 2 est d'ordre 3; on a  $3^2 = 2$  et  $3^3 = -1$  donc l'ordre de 3 n'est ni 1, ni 2, ni 3 et 3 est par conséquent d'ordre 6 : c'est un générateur de  $(\mathbb{Z}/7\mathbb{Z})^\times$ . On sait alors d'après le paragraphe (P1) que  $\varphi \mapsto \varphi(3)$  établit une bijection entre l'ensemble des caractères d'ordre 3 de  $(\mathbb{Z}/7\mathbb{Z})^\times$  et l'ensemble des éléments d'ordre 3 de  $\mathbb{C}^\times$ , qui n'est autre que  $\{j, j^2\}$  où  $j = \exp(2i\pi/3)$ . On a donc deux tels caractères. Pour les décrire explicitement, commençons par exprimer tous les éléments de  $(\mathbb{Z}/7\mathbb{Z})^\times$  comme des puissances de 3 :

$$3^0 = 1, 3^1 = 3, 3^2 = 2, 3^3 = (-1), 3^4 = (3^2)^2 = -3, 3^5 = 3 \cdot 3^4 = (-2).$$

On peut alors donner les deux caractères par leur tableau de valeurs ; sur la première ligne on met les éléments de  $(\mathbb{Z}/7\mathbb{Z})^\times$ , sur la seconde on rappelle (en

rouge) leur écriture comme puissance de 3, et sur la troisième on met (en bleu) la valeur du caractère, obtenue par la formule  $\varphi(3^n) = \varphi(3)^n$ .

$$\begin{pmatrix} -3 & -2 & -1 & 1 & 2 & 3 \\ \textcolor{red}{3^4} & \textcolor{red}{3^5} & \textcolor{red}{3^3} & \textcolor{red}{3^0} & \textcolor{red}{3^2} & \textcolor{red}{3^1} \\ \textcolor{blue}{j} & \textcolor{blue}{j^2} & 1 & 1 & \textcolor{blue}{j^2} & \textcolor{blue}{j} \end{pmatrix} \begin{pmatrix} -3 & -2 & -1 & 1 & 2 & 3 \\ \textcolor{red}{3^4} & \textcolor{red}{3^5} & \textcolor{red}{3^3} & \textcolor{red}{3^0} & \textcolor{red}{3^2} & \textcolor{red}{3^1} \\ \textcolor{blue}{j^2} & \textcolor{blue}{j} & 1 & 1 & \textcolor{blue}{j} & \textcolor{blue}{j^2} \end{pmatrix}.$$

### Exercice 5.

Soit  $\varphi$  un caractère de  $G$ . On a alors

$$\begin{aligned} \langle \varphi, \varphi \rangle &= \frac{1}{|G|} \sum_{g \in G} \varphi(g) \overline{\varphi(g)} \\ &= \frac{1}{|G|} \sum_{g \in G} 1 \\ &= \frac{|G|}{|G|} \\ &= 1, \end{aligned}$$

(la deuxième égalité provient du fait que  $\varphi(g)$  est une racine de l'unité, et en particulier un nombre complexe de module 1, pour tout  $g \in G$ ).

Soit maintenant  $\chi$  un caractère distinct de  $\varphi$ . On a alors

$$\begin{aligned} \langle \varphi, \chi \rangle &= \frac{1}{|G|} \sum_{g \in G} \varphi(g) \overline{\chi(g)} \\ &= \frac{1}{|G|} \sum_{g \in G} \varphi(g) \chi(g)^{-1} \\ &= \frac{1}{|G|} \sum_{g \in G} (\varphi \chi^{-1})(g) \\ &= 0, \end{aligned}$$

où la deuxième égalité provient encore du fait que  $\chi(g)$  est de module 1 pour tout  $g \in G$ , et la dernière du fait que le caractère  $\psi := \varphi \chi^{-1}$  est non trivial (car  $\varphi \neq \chi$  par hypothèse), ce qui entraîne d'après le cours que  $\sum_{g \in G} \psi(g) = 0$ .

Les caractères de  $G$  forment donc une famille orthonormée de l'espace  $E$  des applications de  $G$  dans  $\mathbb{C}$ ; cette famille est en particulier libre, et pour montrer que c'est une base il suffit de s'assurer que son cardinal est égal à la dimension de  $E$ . Or  $E$  est de dimension  $|G|$  : si l'on note  $\delta_g$  l'application  $h \mapsto \delta_{gh}$  de  $G$  dans  $\{0, 1\} \subset \mathbb{C}$ , la famille  $(\delta_g)_{g \in G}$  est en effet une base de  $E$  (si  $f \in E$  on a  $f = \sum_g f(g) \delta_g$  et si  $\sum a_g \delta_g = 0$ , en appliquant cette fonction à un élément quelconque  $h$  de  $G$  on voit que  $a_h = 0$ ). Et on sait d'après le cours que  $|\widehat{G}| = |G|$ ; les caractères de  $\widehat{G}$  forment donc bien une base orthonormée de  $E$ .

### Exercice 6

**Questions (1) et (2).** Fixons une racine primitive  $m$ -ième de l'unité  $\zeta$ . On utilise le paragraphe (P1) de la correction de l'exercice (4) : comme  $\zeta^m = 1$ , il existe un unique morphisme  $\chi$  de  $H$  dans  $\mathbb{C}^\times$  tel que  $\chi(\zeta) = \zeta$ , et le théorème de



prolongement des caractères assure que  $\chi$  peut être prolongé en un caractère de  $G$  tout entier, que nous noterons encore  $\chi$ . L'image  $\chi(H)$  est le groupe engendré par  $\zeta$  (car  $H$  est engendré par  $h$ ), qui est le groupe  $\mu_m$  des racines  $m$ -ièmes de l'unité puisque  $\zeta$  est primitive. Par conséquent  $\chi(G) \supset \mu_m$ . D'autre part si  $g \in G$  son ordre divise  $m$  par choix de  $m$ , si bien que  $g^m = e$  et donc que  $\chi(g)^m = 1$ ; ainsi  $\chi(g) \in \mu_m$ , d'où l'inclusion  $\chi(G) \subset \mu_m$  et finalement l'égalité  $\chi(G) = \mu_m$ .

**Question (3).** Si  $n$  est un entier on a

$$\chi(h^n) = 0 \iff \zeta^n = 0 \iff n = 0 \bmod m \iff h^n = e.$$

Par conséquent,  $\chi|_H$  est injective. Or  $K \cap H$  est le noyau de  $\chi|_H$ ; il s'ensuit que  $K \cap H = \{e\}$ .

Soit  $\mu: H \times K \rightarrow G$  le morphisme  $(h, k) \mapsto hk$ . Montrons que  $\mu$  est injectif. Soit  $(h, k) \in H \times K$  tel que  $hk = e$ . On a alors  $h = k^{-1}$ , si bien que  $h$  et  $k$  appartiennent tous deux à  $H \cap K$ , lequel est trivial. Il vient  $h = k = e$ , c'est-à-dire  $(h, k) = (e, e)$  et  $\mu$  est injective. Montrons que  $\mu$  est surjective. Soit  $g \in G$ . On a vu plus haut que  $\chi(G) = \chi(H) = \mu_m$ . Il existe donc  $h \in H$  tel que  $\chi(h) = \chi(g)$ . On a  $g = h(h^{-1}g)$ , et  $\chi(h^{-1}g) = \chi(h)^{-1}\chi(g) = 1$ ; ainsi  $h^{-1}g \in K$  et  $g = \mu(h, h^{-1}g)$ . Par conséquent  $\mu$  est surjective et est finalement un isomorphisme.

## Exercice 7

La question (1) a été traitée au paragraphe préliminaire (P2) de la correction de l'exercice 4.

**Question (2).** Montrons le résultat par récurrence sur  $|G|$ . Si  $|G|$  est égal à 1 le résultat est vrai car  $G \simeq \mathbb{Z}/1\mathbb{Z}$  ou, de manière plus satisfaisante conceptuellement, car  $G$  s'identifie au *produit vide* de groupes cycliques. Supposons  $|G| > 1$  et le résultat vrai pour tout groupe abélien fini de cardinal strictement inférieur à  $|G|$ . Soit  $m$  le PPCM des ordres des éléments de  $G$ . C'est un entier  $> 1$  car  $|G| > 1$  (et n'importe quel élément non trivial de  $G$  est d'ordre strictement supérieur à 1). D'après le cours, il existe un élément  $h$  d'ordre  $m$  dans  $G$ . Si  $H$  désigne le sous-groupe de  $G$  engendré par  $h$ , l'exercice 6 fournit un sous-groupe  $K$  de  $G$  et un isomorphisme entre  $H \times K$  et  $G$ . L'existence de cet isomorphisme assure que  $|G| = |H| \times |K|$ . Comme  $|H| = m > 1$ , le cardinal de  $K$  est strictement inférieur à celui de  $G$ . L'hypothèse de récurrence garantit alors que  $K$  est isomorphe à un produit fini de groupes cycliques. Comme  $H$  est lui-même cyclique par construction,  $G$  est isomorphe à un produit fini de groupes cycliques, ce qui achève la démonstration.

**Question (3).** Par la question précédente  $G$  est isomorphe à un produit

$$H_1 \times H_2 \times \dots \times H_r$$

avec les  $H_i$  cycliques. Par conséquent  $\widehat{G}$  est isomorphe au groupe des caractères de  $H_1 \times H_2 \times \dots \times H_r$ , qui est lui-même d'après la question (1) (et une récurrence immédiate sur  $r$ ) isomorphe à  $\widehat{H}_1 \times \widehat{H}_2 \times \dots \times \widehat{H}_r$ . Il suffit dès lors pour conclure

de montrer que pour tout  $i$  le groupe  $\widehat{H}_i$  est isomorphe à  $H_i$ . Fixons donc  $i$ , et soit  $n_i$  le cardinal du groupe cyclique  $H_i$ . Une fois fixé un générateur de  $H_i$ , le paragraphe préliminaire (P1) du corrigé de l'exercice 4 fournit un isomorphisme entre  $\widehat{H}_i$  et  $\{z \in \mathbb{C}^\times, z^{n_i} = 1\}$ ; or ce dernier groupe est lui-même cyclique de cardinal  $n_i$ , donc isomorphe à  $H_i$ , ce qui achève la démonstration.