Devoir maison n^o 4

(corrigé)

Table des matières

1 Commentaires

Je sais que le théorème de structure des groupes commutatifs finis, démontré à l'aide des caractères, fut déjà l'objet de problèmes de concours, mais je n'ai pas retrouvé de référence. Le sujet proposé est donc inédit mais sans originalité.

Il vous fait étudier les caractères de différents groupes, finis ou infinis, commutatifs ou non. La structure du groupe $\widehat{G}$ des caractères est un peu imprévisible lorsqu'il s'agit de caractères d'un groupe G infini ou non commutatif (cf. le groupe des caractères de $\mathbb{Z}$ qui est « beaucoup plus gros que $\mathbb{Z}$ » et celui de S_n qui est « beaucoup plus petit que S_n »), mais on démontre en fin de deuxième partie que lorsque le groupe G est fini et commutatif, il y a autant de caractères de G que d'éléments de G. On a même un peu mieux en fin de problème : l'ensemble des caractères est un groupe isomorphe à G (il y a encore mieux en un certain sens : G est canoniquement isomorphe au groupe $\widehat{\widehat{G}}$ appelé le « bidual » de G, ce qui est essentiel pour l'analyse de Fourier : c'est un théorème dû à Pontryagin). L'intérêt de procéder ainsi est que les caractères étant à valeurs dans $\mathbb{C}$, on peut y faire de l'analyse. Ainsi il y a toute une analogie de l'analyse de Fourier qui s'étend aux groupes finis commutatifs.

Que viennent faire les caractères dans une telle analogie ? L'idée, pour imiter la transformée de Fourier d'une fonction réelle :

$$\forall x \in \mathbb{R}, \quad f(x) = \int_{\mathbb{R}} f(t)e^{-itx}\mathrm{d}t,$$

est de se demander ce qui joue le rôle des exponentielles et de l'intégrale dans le cas d'un groupe. Pour l'intégrale, c'est facile, son analogue dans un groupe fini commutatif G est une somme indexée par tous les éléments de G. Et pour e^{-itx} ? Il s'agit de remarquer que les morphismes *continus* de $\mathbb{R}$ dans $\mathbb{U}$ sont exactement les applications de la forme $t \mapsto e^{itx}$ avec $x \in \mathbb{R}$. Il en est de même lorsqu'on parle des coefficients de Fourier d'une fonction périodique, comme vous l'avez déjà peut-être vu en Physique (la formule suivante est, encore une fois, à normalisation près, pour que les exponentielles forment une famille orthonormée) :

$$\forall n \in \mathbb{Z}, \quad c_n(f) = \int_0^{2\pi} f(t)e^{-int}\mathrm{d}t,$$

où les applications de la forme $t \mapsto e^{int}$ avec $n \in \mathbb{Z}$ sont exactement les morphismes continus de $\mathbb{R}/2\pi\mathbb{Z}$ dans $\mathbb{U}$.

Par conséquent, pour définir la transformée de Fourier d'une fonction définie sur G, on remplace ces morphismes continus de $\mathbb{R}$ dans $\mathbb{U}$, ou de $\mathbb{R}/2\pi\mathbb{Z}$ dans $\mathbb{U}$, par des morphismes de G dans $\mathbb{U}$ (on ne parle pas de continuité pour une fonction définie sur un ensemble fini). On obtient la définition suivante de la transformée de Fourier d'une fonction $f : G \to \mathbb{C}$:

$$\forall \chi \in \widehat{G}, \quad f(\chi) = \sum_{g \in G} f(g)\overline{\chi}(g).$$

Pour des raisons de normalisation, encore une fois, on trouve parfois un terme devant la somme ($\frac{1}{\mathrm{card}(G)}$). On peut de la même manière définir un produit de convolution, démontrer un théorème de Parseval, une formule d'inversion, etc.

De la même manière que la famille $(t \mapsto e^{int})_{n\in\mathbb{Z}}$ est orthonormale pour le produit scalaire $(f,g) \mapsto \dfrac{1}{2\pi}\displaystyle\int_0^{2\pi} f\overline{g}$, les caractères d'un groupe commutatif fini vérifient des formules d'orthogonalité, auxquelles je fais parfois référence :

$$\forall(\chi,\chi') \in \widehat{G}^2,\ \frac{1}{\mathrm{card}(G)}\sum_{g\in G}\chi(g)\overline{\chi'}(g) = \delta_{\chi,\chi'}, \quad \forall(g,g') \in G^2,\ \frac{1}{\mathrm{card}(G)}\sum_{\chi\in\widehat{G}}\chi(g)\overline{\chi}(g') = \delta_{g,g'},$$

et c'est la raison pour laquelle l'analyse de Fourier s'étend si bien au cas des groupes. Ces formules ont d'autres intérêts : je vous ai fait utiliser l'orthogonalité des caractères de $\mathbb{Z}/n\mathbb{Z}$ pour simplifier des sommes indexées par des classes de congruence (cela marche parce qu'à chaque classe de congruence modulo n correspond exactement un caractère de $\mathbb{Z}/n\mathbb{Z}$). La deuxième formule ci-dessus permet en effet d'écrire, dans le cas particulier $G = \mathbb{Z}/n\mathbb{Z}$:

$$\forall(a,b) \in \mathbb{Z}^2, \quad \frac{1}{n}\sum_{\chi\in\widehat{\mathbb{Z}/n\mathbb{Z}}}\chi(\bar{a})\overline{\chi}(\bar{b}) = \delta_{\bar{a},\bar{b}} = \mathbb{1}_{b+n\mathbb{Z}}(a).$$

Or, comme on le démontre dans le devoir, les caractères de $\mathbb{Z}/n\mathbb{Z}$ sont exactement les morphismes de la forme $\bar{x} \mapsto e^{\frac{2i\pi kx}{n}}$ avec $k \in [\![0, n-1]\!]$. Cette formule peut donc se réécrire :

$$\forall(a,b) \in \mathbb{Z}^2, \quad \frac{1}{n}\sum_{k=0}^{n-1} e^{\frac{2i\pi k(a-b)}{n}} = \mathbb{1}_{b+n\mathbb{Z}}(a).$$

On retrouve la formule d'orthogonalité dont je vous ai déjà parlé. Cependant, avoir des caractères additifs $(\mathbb{Z}/n\mathbb{Z},+) \to \mathbb{C}^*$ n'est pas toujours le plus commode en arithmétique, où les fonctions sont en général multiplicatives (les relations de divisibilité, etc., font plutôt intervenir des produits). Dans ce cas, on privilégie les caractères de $((\mathbb{Z}/n\mathbb{Z})^\times, \times)$, et c'est ce qui apparaît systématiquement lorsqu'on étudie des fonctions L de Dirichlet à des fins arithmétiques. C'est implicitement ce que je fis dans votre devoir des vacances : je vous fis utiliser la formule d'orthogonalité avec $(\mathbb{Z}/4\mathbb{Z})^\times$, $(\mathbb{Z}/3\mathbb{Z})^\times$ et $(\mathbb{Z}/6\mathbb{Z})^\times$ afin d'avoir des sommes indexées par les classes de congruence ±1 mod 4, ±1 mod 3 et ±1 mod 6, ce qui est facile à faire à la main (sans même remarquer qu'on manipule des caractères) puisqu'il n'y a à chaque fois qu'un seul caractère non trivial, et qui doit d'ailleurs être à valeurs dans $\{1,-1\}$. C'est d'ailleurs ainsi que j'ai choisi ces groupes : ce sont les seuls à être de cardinal $\varphi(n) = 2$.

Une autre formule d'orthogonalité, donnant la fonction indicatrice des carrés de $(\mathbb{Z}/p\mathbb{Z})^\times$ (exprimée en fonction du symbole de Legendre), apparaît dans *Méthodes* du chapitre IV et en travaux dirigés.

Trêves de digressions. Ce devoir n'aborde rien de tout cela, et démontre modestement d'autres résultats malgré tout classiques, valables dans les groupes finis commutatifs :

— le fait que **les caractères d'un sous-groupe se prolongent** à tout le groupe ;

— le fait que **le groupe des caractères soit isomorphe au groupe initial** (avec explicitation du groupe des caractères dans des cas particuliers importants, comme $\mathbb{Z}/n\mathbb{Z}$) ;

— le fait que **tout groupe commutatif fini soit produit de groupes cycliques**, de manière unique si l'on impose une condition de divisibilité sur leurs cardinaux.

Tout cela nécessite en passant de démontrer certains résultats très utiles et fréquemment rencontrés en théorie des groupes :

— l'ordre d'un élément d'un groupe fini commutatif **divise l'ordre maximal du groupe** (appelé *exposant* du groupe) ;

— les **commutateurs** de S_n, c'est-à-dire les éléments de la forme $\sigma\tau\sigma^{-1}\tau^{-1}$, et qui mesurent en quelque sorte le défaut de commutativité du groupe, **engendrent le groupe alterné** A_n ;

— ce n'est pas tant un résultat qu'une stratégie : **les groupes quotients**, entre autres choses, **permettent aussi certains raisonnements par récurrence** ; ayant un résultat sur H et G/H (par hypothèse de récurrence ou un autre argument), on espère l'étendre à G.

Ce qu'on retiendra en bref. Image d'un caractère. Généralisation d'un résultat sur l'ordre d'un produit d'éléments d'un groupe commutatif. L'exposant d'un groupe commutatif est divisible par tous les ordres. Structure de groupe de l'ensemble des caractères. Caractères d'un groupe cyclique. Prolongement des caractères. Théorème chinois.

Questions faciles ou classiques à retravailler

— PRÉLIMINAIRES : questions 1 et 3 ;

— PREMIÈRE PARTIE : questions 4 à 6 ;

— DEUXIÈME PARTIE : questions 9 et 10 ;

— TROISIÈME PARTIE : questions 13 à 15, question 19.

2 Corrigé

Préliminaires

1. Soit χ un caractère d'un groupe fini G de cardinal n. Par le théorème de Lagrange, on a : $\forall g \in G$, $g^n = 1_G$. Comme χ est un morphisme, prendre l'image par χ dans cette égalité donne : $\forall g \in G$, $\chi(g)^n = 1$, donc : $\forall g \in G$, $\chi(g) \in \mathbb{U}_n$, ce qu'il fallait démontrer.

   Questions à se poser, réflexes à acquérir. Reconnaître, dans cette démonstration, une n^{e} illustration du fait qu'un morphisme préserve la structure (de manière parfaite si c'est un isomorphisme). Comment aurait-on pu reformuler la résolution proposée en raisonnant uniquement en termes d'ordres ?

2. Démontrons d'abord le résultat de l'indication de l'énoncé. Soit $g \in G$. On veut montrer : $g^d = 1_G$, ce qui revient exactement à démontrer que l'ordre de g divise d. Pour cela : soit $h \in G$ un élément d'ordre d (il en existe, par définition de l'exposant d'un groupe). Admettons *provisoirement* le résultat suivant :

   (H) Pour tous éléments x et y de G, dont on note s et t les ordres, il existe un élément de G qui soit d'ordre $\text{ppcm}(s,t)$.

   Si **(H)** est vrai, alors ce qu'on veut démontrer en résulte aisément : notons m l'ordre de g. D'après **(H)**, il existe un élément d'ordre $\text{ppcm}(m,d)$; or $\text{ppcm}(m,d) \geqslant d$ puisque d divise ce ppcm, et $\text{ppcm}(m,d) \leqslant d$ puisque d est supposément l'ordre *maximal* d'un élément de G. On a donc : $\text{ppcm}(m,d) = d$, ce qui est vrai si et seulement si m divise d. Comme m est l'ordre de g, on a donc : $g^d = 1_G$. Partant de là, il suffit d'imiter le raisonnement de la question précédente pour avoir : $\forall g \in G$, $\chi(g)^d = 1$, si bien que χ est à valeurs dans $\mathbb{U}_d$.

   Démontrons ce qui fut admis provisoirement, à savoir l'hypothèse **(H)**. Si s et t sont premiers entre eux, le raisonnement est classique, et un élément qui convient est xy. Soit ℓ l'ordre de xy. Comme G est commutatif, on a $(xy)^k = x^k y^k$ pour tout $k \in \mathbb{Z}$. Or $x^{st} = 1_G$ car x est d'ordre s, et de même $y^{st} = 1_G$, donc : $(xy)^{st} = 1_G$. On en déduit que ℓ divise st.

   De plus, $(xy)^\ell = x^\ell y^\ell = 1_G$, donc : $x^\ell = y^{-\ell}$, puis : $x^{\ell t} = y^{-\ell t} = 1_G$, donc l'ordre de x divise ℓt, c'est-à-dire : s divise ℓt. Or s et t sont premiers entre eux, donc par le théorème de Gauß s divise ℓ. On montre de même que t divise ℓ et donc, comme s et t sont premiers entre eux : st divise ℓ.

   Puisque ℓ et st sont associés et positifs, on en déduit : $\ell = st$. Ainsi xy est bien d'ordre st.

   À présent, si s et t ne sont pas premiers entre eux, on se ramène au cas précédent comme suit : on décompose s et t en nombres premiers (ci-dessous $\mathbb{P}$ désigne l'ensemble des nombres premiers) :

$$s = \prod_{p \in \mathbb{P}} p^{v_p(s)}, \quad t = \prod_{p \in \mathbb{P}} p^{v_p(t)}.$$

Avec ces notations, on a :

$$\mathrm{ppcm}(s,t) = \prod_{p\in\mathbb{P}} p^{\max(v_p(s),v_p(t))} = \prod_{\substack{p\in\mathbb{P}\\ v_p(s)>v_p(t)}} p^{v_p(s)} \times \prod_{\substack{p\in\mathbb{P}\\ v_p(s)\leqslant v_p(t)}} p^{v_p(t)}.$$

Donc, si l'on pose :

$$s' = \prod_{\substack{p\in\mathbb{P}\\ v_p(s)>v_p(t)}} p^{v_p(s)}, \text{ et : } t' = \prod_{\substack{p\in\mathbb{P}\\ v_p(s)\leqslant v_p(t)}} p^{v_p(t)},$$

alors :

— s' divise s ;
— t' divise t ;
— $s't' = \mathrm{ppcm}(s,t)$;
— s' et t' sont premiers entre eux parce qu'ils n'ont pas de diviseur premier en commun.

De plus, il est facile de vérifier que $x^{\frac{s}{s'}}$ est d'ordre s' et $y^{\frac{t}{t'}}$ d'ordre t'. D'après la question précédente, le produit $z = x^{\frac{s}{s'}} y^{\frac{t}{t'}}$ est d'ordre $s't' = \mathrm{ppcm}(s,t)$: d'où **(H)**, ce qui achève la résolution de cette question.

Questions à se poser, réflexes à acquérir.
— Où intervient la commutativité ? Trouver des contre-exemples à **(H)** dans le cas non commutatif.
— Se convaincre de l'équivalence entre : $\mathrm{ppcm}(m,d) = d$, et : m divise d. A-t-on une équivalence analogue avec le pgcd ? Laquelle ?
— Démonstration de l'hypothèse **(H)** : traiter le cas où s et t sont premiers entre eux avec une relation de Bézout. Pourrait-on aussi recourir à cette relation dans le cas où s et t ont un pgcd différent de 1 ?
— Comprendre la stratégie du cas où s et t ne sont pas premiers entre eux. Pourquoi avoir raisonné sur la décomposition en facteurs premiers ? Était-il important que s' soit défini à l'aide des valuations vérifiant $v_p(s) > v_p(t)$? Pouvait-on inverser les inégalités ? Qu'est-ce qui était vraiment important pour définir s' et t' ?
— Vérifier ce qui est affirmé sans détailler, à savoir : que $x^{\frac{s}{s'}}$ et $y^{\frac{t}{t'}}$ sont respectivement d'ordre s' et t'. Cela revient souvent en théorie des groupes.

3. Tout d'abord, montrons que pour tout $(\chi,\chi') \in \widehat{G}^2$, on a bien : $\chi\times\chi' \in \widehat{G}$. Soit $(\chi,\chi') \in \widehat{G}^2$. Alors $\chi\times\chi'$ est bien une application de G dans $\mathbb{C}^*$ (parce que χ et χ' sont à valeurs dans $\mathbb{C}^*$ et $\mathbb{C}$ est intègre), et c'est un morphisme parce que pour tout $(g_1,g_2)\in G^2$ on a :

$$\begin{aligned}(\chi\times\chi')(g_1g_2) = \chi(g_1g_2)\chi'(g_1g_2) = \chi(g_1)\chi(g_2)\chi'(g_1)\chi'(g_2) &= \chi(g_1)\chi'(g_1)\chi(g_2)\chi'(g_2)\\ &= (\chi\times\chi')(g_1)(\chi\times\chi')(g_2).\end{aligned}$$

La commutativité de $\mathbb{C}^*$ est essentielle comme on l'observe. Ainsi la loi de composition $\times$ est interne, associative par associativité de la multiplication dans $\mathbb{C}^*$, et elle admet pour élément neutre le caractère $\chi_0 : g\mapsto 1$ (vérification triviale). Il reste donc à démontrer que tout élément dans $\widehat{G}$ admet un inverse dans $\widehat{G}$. Soit $\chi\in\widehat{G}$. Notons que $\overline{\chi} : G\to\mathbb{C}^*$ est aussi un caractère de G (il suffit de conjuguer la relation $\chi(g_1g_2) = \chi(g_1)\chi(g_2)$ valable pour tout $(g_1,g_2)\in G^2$), et par la question 1 on sait que χ est à valeurs dans l'ensemble des nombres complexes de module 1 (et même un peu mieux), donc :

$$\forall g\in G,\quad \overline{\chi}(g)\chi(g) = \chi(g)\overline{\chi}(g) = |\chi(g)|^2 = 1 = \chi_0(g),$$

donc χ est inversible dans $\widehat{G}$, d'inverse : $\chi^{-1} = \overline{\chi}$. Ceci achève de démontrer que $\widehat{G}$ est un groupe pour la loi $\times$.

Remarque. L'inverse de χ est aussi, plus sobrement : $\frac{1}{\chi}$.

Questions à se poser, réflexes à acquérir.

— Plus généralement, est-ce que l'ensemble des morphismes d'un groupe dans un autre a toujours une structure de groupe ? (Avec la multiplication définie comme dans ce sujet.)

— Est-il toujours vrai que si f est un morphisme de groupes, alors $\frac{1}{f}$ aussi ? Qu'est-ce qui rend cela possible ?

Première partie

4. Soit $f : G \to H$ un isomorphisme. Il en existe un par hypothèse sur G et H. Pour tout $\chi \in \widehat{G}$, l'application $\chi \circ f^{-1} : H \to \mathbb{C}^*$ est un caractère de H : c'est en effet un morphisme en tant que composition de morphismes. Par conséquent l'application :

$$\varphi : \begin{cases} \widehat{G} & \to & \widehat{H} \\ \chi & \mapsto & \chi \circ f^{-1} \end{cases}$$

est bien définie, et est bijective puisqu'elle admet pour réciproque l'application $\chi \mapsto \chi \circ f$. Montrons que c'est un morphisme. Pour tout $(\chi, \chi') \in \widehat{G}^2$ et tout $g \in G$, on a :

$$\varphi(\chi \times \chi')(g) = (\chi \times \chi')\left(f^{-1}(g)\right) = \chi(f^{-1}(g))\chi'(f^{-1}(g')) = \varphi(\chi)(g)\varphi(\chi')(g) = \left(\varphi(\chi) \times \varphi(\chi')\right)(g),$$

donc : $\forall (\chi, \chi') \in \widehat{G}^2$, $\varphi(\chi \times \chi') = \varphi(\chi) \times \varphi(\chi')$. Ainsi φ est un morphisme bijectif, donc c'est un isomorphisme de groupes entre $\widehat{G}$ et $\widehat{H}$: d'où le résultat.

Questions à se poser, réflexes à acquérir. Reconnaître là une n^{e} illustration du fait que les isomorphismes préservent tout ce qui est relatif à la structure.

5. Si χ est un caractère de $G \times H$, alors on a par propriété de morphisme (et définition de la loi sur un produit cartésien de groupes) :

$$\forall (g,h) \in G \times H, \quad \chi(g,h) = \chi\left((g,1_H)(1_G,h)\right) = \chi(g,1_H)\chi(1_G,h),$$

et on vérifie facilement que les applications $\chi_G : g \mapsto \chi(g,1_H)$ et $\chi_H : h \mapsto \chi(1_G,h)$ sont des caractères de G et H respectivement. Montrons-le uniquement pour la première application. C'est bien défini de G dans $\mathbb{C}^*$, et :

$$\forall (g,g') \in G^2, \quad \chi_G(gg') = \chi(gg',1_H) = \chi\left((g,1_H)(g',1_H)\right) = \chi(g,1_H)\chi(g',1_H) = \chi_G(g)\chi_G(g').$$

Cela permet de définir les applications :

$$\psi : \begin{cases} \widehat{G \times H} & \to & \widehat{G} \times \widehat{H} \\ \chi & \mapsto & (\chi_G, \chi_H) \end{cases}, \quad \text{et} : \quad \psi' : \begin{cases} \widehat{G} \times \widehat{H} & \to & \widehat{G \times H} \\ (\chi_1, \chi_2) & \mapsto & ((g,h) \mapsto \chi_1(g)\chi_2(h)) \end{cases},$$

dont on vérifie qu'elles sont réciproques l'une de l'autre (cela revient essentiellement à reproduire le calcul du début de résolution). On en déduit que ψ est bijective, et c'est un morphisme parce que pour tous χ et χ' dans $\widehat{G \times H}$, on a :

$$\psi(\chi \times \chi') = \left((\chi \times \chi')_G, (\chi \times \chi')_H\right) \overset{(*)}{=} (\chi_G \times \chi'_G, \chi_H \times \chi'_H) = (\chi_G, \chi_H) \times (\chi'_G, \chi'_H) = \psi(\chi) \times \psi(\chi'),$$

l'égalité $(*)$ étant vraie parce que :

$$\forall g \in G, \quad (\chi \times \chi')_G(g) = (\chi \times \chi')(g,1_H) = \chi(g,1_H)\chi'(g,1_H) = \chi_G(g)\chi'_G(g) = (\chi_G \times \chi'_G)(g),$$

et de même avec la composante selon $\widehat{H}$. Ainsi ψ est un morphisme bijectif, donc un isomorphisme entre $\widehat{G \times H}$ et $\widehat{G} \times \widehat{H}$: d'où le résultat.

Questions à se poser, réflexes à acquérir. Vérifier ce que j'ai omis (le fait que χ_G et χ_H soient effectivement des morphismes). Est-ce que $g \mapsto \chi(g,h)$, à h fixé, serait aussi un morphisme ?

6. *Caractères de* $\mathbb{Z}$. Le groupe $\mathbb{Z}$ n'est pas fini. Petite incorrection de ma part... Tant pis, je traite la question comme si les caractères de $\mathbb{Z}$ étaient définis comme pour les groupes finis (ce qui n'est pas le cas : un morphisme de $\mathbb{Z}$ dans $\mathbb{C}^*$ est un *quasi-caractère* de $\mathbb{Z}$).
Soit $\chi \in \widehat{\mathbb{Z}}$. Comme $\mathbb{Z}$ est monogène, engendré par 1, il suffit de déterminer $\chi(1)$ pour caractériser χ. Plus précisément, si l'on pose : $a = \chi(1) \in \mathbb{C}^*$, alors : $\forall k \in \mathbb{Z}$, $\chi(k) = a^k$. Réciproquement, pour tout $a \in \mathbb{C}^*$, l'application $k \mapsto a^k$ est un morphisme de $\mathbb{Z}$ dans $\mathbb{C}^*$ comme on le vérifie sans difficulté. On a donc :
$$\widehat{\mathbb{Z}} = \left\{ \chi_a : \begin{cases} \mathbb{Z} & \to & \mathbb{C}^* \\ k & \mapsto & a^k \end{cases} \mid a \in \mathbb{C}^* \right\}.$$
Le groupe $\widehat{\mathbb{Z}}$ est isomorphe à $\mathbb{C}^*$, un isomorphisme étant simplement l'application de $\mathbb{C}^*$ dans $\widehat{\mathbb{Z}}$ définie par $a \mapsto \chi_a$, qui admet pour bijection réciproque $\chi \mapsto \chi(1)$.
Caractères de $\mathbb{Z}/n\mathbb{Z}$. Soit $\chi \in \widehat{\mathbb{Z}/n\mathbb{Z}}$. Comme $\mathbb{Z}/n\mathbb{Z}$ est cyclique, engendré par $\bar{1}$, il suffit de déterminer $\chi(\bar{1})$ pour caractériser χ. Or $\bar{1}$ est d'ordre n dans $\mathbb{Z}/n\mathbb{Z}$ (c'est un générateur), donc $\chi(\bar{1})$ est d'ordre divisant n dans $\mathbb{C}^*$, c'est-à-dire : $\chi(\bar{1}) \in \mathbb{U}_n$ (on pouvait aussi utiliser la question 1 pour le justifier). Il existe donc $k \in \mathbb{Z}$ tel que : $\chi(\bar{1}) = e^{\frac{2i\pi k}{n}}$, et on a ensuite : $\forall x \in \mathbb{Z}$, $\chi(\bar{x}) = \chi(\bar{1})^x = e^{\frac{2i\pi kx}{n}}$.
Réciproquement, vérifions que pour tout $k \in \mathbb{Z}$, l'application $\chi_k : \bar{x} \mapsto e^{\frac{2i\pi kx}{n}}$ est correctement définie et est un caractère de $\mathbb{Z}/n\mathbb{Z}$. Elle est bien définie par application du théorème de factorisation des morphismes au morphisme de $\mathbb{Z}$ dans $\mathbb{C}^*$ défini par $x \mapsto e^{\frac{2i\pi kx}{n}}$: en effet $n\mathbb{Z}$ est inclus dans son noyau, du fait que l'exponentielle soit égale à 1 sur $2i\pi\mathbb{Z}$. De plus χ_k est un morphisme parce que l'exponentielle en est un. On a donc :
$$\widehat{\mathbb{Z}/n\mathbb{Z}} = \left\{ \chi_k : \begin{cases} \mathbb{Z}/n\mathbb{Z} & \to & \mathbb{C}^* \\ \bar{x} & \mapsto & e^{\frac{2i\pi kx}{n}} \end{cases} \mid k \in \mathbb{Z} \right\}.$$
On nous demande d'en déduire un isomorphisme entre $\widehat{\mathbb{Z}/n\mathbb{Z}}$ et un groupe usuel. Tout d'abord, cette description explicite permet aisément d'en déduire un morphisme surjectif $f : k \mapsto \chi_k$ de $\mathbb{Z}$ dans $\widehat{\mathbb{Z}/n\mathbb{Z}}$. Par le théorème d'isomorphisme, les groupes $\mathbb{Z}/\ker(f)$ et $\widehat{\mathbb{Z}/n\mathbb{Z}}$ sont isomorphes. Déterminons donc $\ker(f)$. Soit $k \in \mathbb{Z}$. On a :
$$k \in \ker(f) \iff \chi_k = \chi_0 \iff \forall \bar{x} \in \mathbb{Z}/n\mathbb{Z},\ e^{\frac{2i\pi kx}{n}} = 1 \iff \forall \bar{x} \in \mathbb{Z}/n\mathbb{Z},\ kx \in n\mathbb{Z},$$
ceci doit en particulier être vrai pour $\bar{x} = \bar{1}$, donc : $k \in n\mathbb{Z}$, la réciproque étant vraie également comme on le vérifie immédiatement (si $k \in n\mathbb{Z}$, alors $kx \in n\mathbb{Z}$ pour tout $\bar{x} \in \mathbb{Z}/n\mathbb{Z}$). On en déduit que l'on a : $\ker(f) = n\mathbb{Z}$, et donc $\mathbb{Z}/n\mathbb{Z}$ et $\widehat{\mathbb{Z}/n\mathbb{Z}}$ sont isomorphes d'après ce qui précède.
Caractères de $\mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$. La bijection construite dans la question précédente permet d'obtenir les caractères de ce produit cartésien à l'aide de ceux de $\mathbb{Z}/m\mathbb{Z}$ et $\mathbb{Z}/n\mathbb{Z}$, qu'on vient de déterminer. L'ensemble des caractères est alors :
$$\widehat{\mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}} = \left\{ \chi : \begin{cases} \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z} & \to & \mathbb{C}^* \\ (\bar{x}, \bar{y}) & \mapsto & e^{\frac{2i\pi kx}{m} + \frac{2i\pi \ell y}{n}} \end{cases} \mid (\bar{k}, \bar{\ell}) \in \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z} \right\},$$
et par les deux questions précédentes on a les isomorphismes suivants (le symbole « $\simeq$ » signifie : « est isomorphe à ») :
$$\widehat{\mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}} \simeq \widehat{\mathbb{Z}/m\mathbb{Z}} \times \widehat{\mathbb{Z}/n\mathbb{Z}} \simeq \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}.$$
Il y a bien transitivité de la relation « $\simeq$ » : il suffit de composer les isomorphismes.

Caractères de S_3. Soit $\chi \in \widehat{S_3}$. Comme S_3 est engendré par les transpositions (1 2), (1 3) et (2 3), il suffit de déterminer l'image par χ de ces trois transpositions pour déterminer χ complètement. Mieux : si on détermine $\chi((1\ 2))$, alors cela suffit en vertu du principe de conjugaison :

$$(1\ 3) = (2\ 3)(1\ 2)(2\ 3)^{-1}, \quad (2\ 3) = (1\ 3)(1\ 2)(1\ 3)^{-1}.$$

Comme χ est à valeurs dans $\mathbb{C}^*$ qui est commutatif, ces deux relations impliquent en effet :

$$\chi((1\ 3)) = \chi((1\ 2))\chi((2\ 3))\chi((2\ 3))^{-1} = \chi((1\ 2)), \quad \chi((2\ 3)) = \chi((1\ 2)).$$

Déterminons donc $\chi((1\ 2))$. On procède par distinction de cas.
Premier cas : $\chi((1\ 2)) = 1$. Dans ce cas, par ce qui vient d'être dit, χ et le morphisme trivial χ_0 coïncident sur les transpositions, qui engendrent S_3, donc : $\chi = \chi_0$.
Deuxième cas : $\chi((1\ 2)) = -1$. Dans ce cas, χ vaut -1 sur toutes les transpositions de S_3, comme le morphisme de signature ε. Comme les transpositions engendrent S_3, cela implique : $\chi = \varepsilon$.
Réciproquement, χ_0 et ε sont bien des caractères de S_3. On a donc montré : $\widehat{S_3} = \{\chi_0, \varepsilon\}$. Ce groupe est isomorphe à $\mathbb{Z}/2\mathbb{Z}$, en envoyant $\bar{0}$ sur χ_0 et $\bar{1}$ sur ε.

Questions à se poser, réflexes à acquérir.

- S'assurer que, dans chaque cas, on comprend comment passer de $\chi(g)$, explicité pour tout g appartenant à un système de générateurs, à $\chi(g)$ explicité pour tout $g \in G$.
- Lorsque j'écris : $\chi(\bar{x}) = \chi(\bar{1})^x$, dans la détermination des caractères de $\mathbb{Z}/n\mathbb{Z}$: pourquoi $\chi(\bar{1})^x$ ne dépend pas du représentant de $\bar{x}$? Et pourquoi j'estime superflu de le justifier ?
- Se convaincre que, comme on l'a fait dans le cas de $\mathbb{Z}/n\mathbb{Z}$: il est exactement équivalent de déterminer les morphismes $f : G/H \to K$ et de déterminer les morphismes $f : G \to K$ dont le noyau contient H.
- Se demander dans quels cas résoudre un problème sur S_n se ramène non seulement à résoudre le problème pour toute transposition, mais mieux que cela : à résoudre le problème avec au moins une transposition (comme on l'a ci-dessus : il suffit de déterminer $\chi((1\ 2))$ pour expliciter χ).

7. Soit $\chi \in \widehat{S_n}$. Comme $\mathbb{C}^*$ est commutatif, on a pour tout $(\sigma, \tau) \in S_n^2$:

$$\chi(\sigma\tau\sigma^{-1}\tau^{-1}) = \chi(\sigma)\chi(\tau)\chi(\sigma)^{-1}\chi(\tau)^{-1} = \chi(\sigma)\chi(\sigma)^{-1}\chi(\tau)\chi(\tau)^{-1} = 1.$$

Or, conformément à l'indication de l'énoncé, tous les 3-cycles de S_n peuvent s'écrire sous la forme : $(a\ b\ c) = \sigma\tau\sigma^{-1}\tau^{-1}$, avec $(\sigma, \tau) \in (S_n)^2$. En effet, $(a\ b\ c)^2$ et $(a\ b\ c)$ sont conjugués (comme tous les 3-cycles), puisqu'on peut écrire :

$$(a\ b\ c)^2 = (a\ c\ b) = (b\ c)(a\ b\ c)(b\ c)^{-1},$$

et en multipliant à droite de chaque membre de l'égalité par $(a\ b\ c)^{-1}$, on a donc :

$$(a\ b\ c) = (b\ c)(a\ b\ c)(b\ c)^{-1}(a\ b\ c)^{-1}.$$

D'après le calcul ci-dessus, avec $\sigma = (b\ c)$ et $\tau = (a\ b\ c)$, on a donc : $\chi((a\ b\ c)) = 1$. Ceci vaut pour tout 3-cycle $(a\ b\ c)$, et comme les 3-cycles engendrent A_n on en déduit : $\forall \sigma \in A_n$, $\chi(\sigma) = 1$. Autrement dit : $A_n \subseteq \ker(\chi)$, donc par le théorème de factorisation des morphismes il existe un (unique) morphisme $\overline{\chi} : S_n/A_n \to \mathbb{C}^*$ tel que : $\forall \sigma \in S_n$, $\chi(\sigma) = \overline{\chi}(\overline{\sigma})$. Déterminer χ revient donc à déterminer $\overline{\chi}$, qui est un caractère de S_n/A_n.
Or : $\mathrm{card}(S_n/A_n) = 2$, puisque A_n est le noyau du morphisme de signature $\varepsilon : S_n \to \{-1,1\}$, et un groupe de cardinal 2 est nécessairement isomorphe à $\mathbb{Z}/2\mathbb{Z}$, dont nous avons déjà déterminé les caractères ci-dessus (et même si nous ne l'avions pas fait, il est très rapide de les expliciter, puisque seule l'image de l'unique élément non trivial est à déterminer). Les deux caractères de $\mathbb{Z}/2\mathbb{Z}$ étant le morphisme trivial χ_0 et $\bar{k} \mapsto (-1)^k$, on en déduit que les deux seuls caractères de S_n/A_n sont le morphisme trivial d'une part, et d'autre part celui qui envoie $\overline{\mathrm{id}} = A_n$ sur 1, et l'autre classe (nécessairement $S_n \setminus A_n$, qui contient notamment toutes les transpositions) sur -1. Concluons :

— si $\overline{\chi}$ est le caractère trivial de S_n/A_n, alors χ est le caractère trivial de S_n (... trivialement) ;
— si $\overline{\chi}$ envoie la classe A_n sur 1 et la classe $S_n \setminus A_n$ sur -1, alors pour toute transposition τ de S_n, on a : $\chi(\tau) = \overline{\chi}(\overline{\tau}) = -1$ (en effet $\tau \in S_n \setminus A_n$), donc χ coïncide avec le morphisme de signature ε sur une partie génératrice de S_n, et on conclut : $\chi = \varepsilon$.

En résumé : $\widehat{S_n} = \{\chi_0, \varepsilon\}$, qui est isomorphe à $\mathbb{Z}/2\mathbb{Z}$ (comme tout groupe de cardinal 2).

Remarque. On pouvait aussi remarquer que l'image de χ doit être de cardinal 1 ou 2. Dans le premier cas, c'est bien sûr le caractère trivial, et dans le second cas son image est un sous-groupe de cardinal 2 de $\mathbb{C}^*$: c'est $\{-1,1\}$. Or il existe un unique morphisme de S_n dans $\{-1,1\}$, qui est le morphisme de signature : d'où le résultat.

Remarque (hors programme). En imitant le raisonnement de cette question, on peut montrer que $\widehat{G}$ est toujours isomorphe à $\widehat{G/D(G)}$, où $D(G)$ est le sous-groupe de G engendré par les éléments de la forme $ghg^{-1}h^{-1}$ avec $(g,h) \in G^2$ (on peut montrer que $D(G)$ est toujours distingué). On a montré implicitement, dans cette question, que : $D(S_n) = A_n$, où A_n est le sous-groupe de S_n engendré par les 3-cycles (et par ailleurs le noyau du morphisme de signature).

L'avantage de raisonner avec $G/D(G)$ est que c'est un groupe plus petit que G, et il est *toujours* commutatif. En effet, modulo $D(G)$ on a : $\overline{ghg^{-1}h^{-1}} = \overline{1_G}$, et donc : $\overline{gh} = \overline{hg}$, pour tout $(g,h) \in G^2$.

Questions à se poser, réflexes à acquérir.
— Généraliser la stratégie : si l'on veut déterminer tous les morphismes d'un groupe G non commutatif dans un groupe H, quel sous-groupe de G peut-on chercher à expliciter, sur lequel tout morphisme $f : G \to H$ serait trivial ?
— On a montré que $(a\ b\ c)$ et $(a\ b\ c)^2$ sont conjugués. Est-ce vrai en remplaçant $(a\ b\ c)$ par un cycle de longueur quelconque ? Avec n'importe quel exposant ?

8. Si G est isomorphe à $\prod_{i=1}^{r} \mathbb{Z}/n_i\mathbb{Z}$ alors, en compilant les résultats des questions 4, 5 et 6, on a :

$$\widehat{G} \simeq \widehat{\prod_{i=1}^{r} \mathbb{Z}/n_i\mathbb{Z}} \simeq \prod_{i=1}^{r} \widehat{\mathbb{Z}/n_i\mathbb{Z}} \simeq \prod_{i=1}^{r} \mathbb{Z}/n_i\mathbb{Z} \simeq G,$$

d'où le résultat (le symbole « $\simeq$ » signifie « est isomorphe à »). Il y a bien transitivité de la relation « $\simeq$ » : il suffit de composer les isomorphismes.

Deuxième partie

9. On a : $\frac{\text{card}(G)}{\text{card}(H)} = \text{card}(G/H) = r > 1$, donc : $\text{card}(G) \neq \text{card}(H)$, et : $G \neq H$. Pour la seconde assertion à démontrer, il suffit d'utiliser le théorème de Lagrange, puisque : $\forall g \in G$, $g^{\text{card}(G)} = 1_G \in H$. Ainsi $k = \text{card}(G) \in \mathbb{N} \setminus \{0\}$ convient.

Remarque. Un entier plus petit à convenir est $k = \text{card}(G/H) = r$. En effet, appliquer le théorème de Lagrange dans G/H donne : $\bar{g}^r = \overline{1_G}$, c'est-à-dire : $g^r \in H$.

10. L'élément g existe bien, puisque par la question précédente H est strictement inclus dans G. Remarquons que l'entier k de l'énoncé est l'ordre de $\bar{g}$ dans G/H (faire le lien si besoin grâce à la remarque de la question précédente). On peut alors utiliser la caractérisation de l'ordre comme plus petite puissance, au sens de la relation de divisibilité, à donner l'élément neutre :

$$\forall \ell \in \mathbb{Z}, \quad \left(g^\ell \in H \iff \bar{g}^\ell = \overline{1_G} \iff k \mid \ell\right).$$

Ceci étant dit, la première subtilité de la question (qui est en fait la plus grande) est que la définition de χ' semble dépendre de la façon d'écrire un élément de K sous la forme hg^ℓ. Montrons qu'il n'en est rien. Soit $x \in K$. Par définition de K, il existe $(h,\ell) \in H \times \mathbb{Z}$ tel que : $x = hg^\ell$. Considérons un autre couple $(h',\ell') \in H \times \mathbb{Z}$ tel que : $x = h'g^{\ell'}$. On veut montrer :

$$\chi(h)\omega^\ell = \chi(h')\omega^{\ell'},$$

de sorte que $\chi'(x)$ soit correctement défini. Les égalités $x = hg^\ell = h'g^{\ell'}$ impliquent : $g^{\ell'-\ell} = h'^{-1}h \in H$, donc par l'équivalence rappelée ci-dessus k divise $\ell' - \ell$, autrement dit : $\ell' \equiv \ell \bmod k$. Soit $m \in \mathbb{Z}$ tel que : $\ell' = \ell + mk$. On a :

$$\chi(h'^{-1}h) = \chi\left(g^{\ell'-\ell}\right) = \chi\left(g^{mk}\right) = \chi\left(\left(g^k\right)^m\right) = \left(\chi\left(g^k\right)\right)^m,$$

or par définition de ω on a : $\omega^k = \chi\left(g^k\right)$, donc :

$$\chi(h'^{-1}h) = \left(\omega^k\right)^m = \omega^{km} = \omega^{\ell'-\ell},$$

et de cette égalité il découle : $\chi(h)\omega^\ell = \chi(h')\omega^{\ell'}$, ce qu'on voulait démontrer. Ainsi $\chi' : K \to \mathbb{C}^*$ est correctement définie. Il reste à vérifier que c'est un morphisme. Soit $(x, y) \in K^2$, qu'on écrit sous la forme : $x = h_1 g^{\ell_1}$, et : $y = h_2 g^{\ell_2}$, avec : $((h_1, h_2), (\ell_1, \ell_2)) \in H^2 \times \mathbb{Z}^2$. Comme G est commutatif, on a : $xy = h_1 h_2 g^{\ell_1+\ell_2}$, avec $h_1 h_2 \in H$, et donc :

$$\chi'(xy) = \chi(h_1h_2)\omega^{\ell_1+\ell_2} = \chi(h_1)\chi(h_2)\omega^{\ell_1}\omega^{\ell_2} = \chi(h_1)\omega^{\ell_1}\chi(h_2)\omega^{\ell_2} = \chi'(x)\chi'(y),$$

d'où le résultat : χ' est un caractère de K.

Questions à se poser, réflexes à acquérir.

— Vérifier que χ' ne serait pas correctement défini si k était un entier non nul *quelconque* tel que $g^k \in H$.

— Comprendre la construction de χ' : pour étendre χ de H à K, pourquoi était-il naturel d'introduire une racine k^{e} de $\chi(g^k)$?

11. Rappelons que nous raisonnons par récurrence, en ayant supposé que pour tout sous-groupe de H vérifiant : $\text{card}(G/H) < r$, tout caractère de H se prolonge en un caractère de G, et nous avons fixé un sous-groupe H de G tel que : $\text{card}(G/H) = r$, ainsi qu'un caractère χ de H qu'on veut prolonger en un caractère de G. Pour ce faire : on a prolongé χ en un caractère χ' de K dans la question précédente, où K est un sous-groupe de G qui contient strictement H (en effet, si l'on a : $H = K$, alors $g \in K = \langle H \cup \{g\}\rangle$ appartient aussi à H, ce qui est contraire aux hypothèses). C'est-à-dire : $\text{card}(H) < \text{card}(K)$, donc :

$$\text{card}(G/K) = \frac{\text{card}(G)}{\text{card}(K)} < \frac{\text{card}(G)}{\text{card}(H)} = \text{card}(G/H) = r,$$

donc : $\text{card}(G/K) < r$, et par hypothèse de récurrence χ' se prolonge en un caractère χ'' de G. On a évidemment : $\chi''_{|H} = \chi$, donc on a bien prolongé χ en un caractère de G. Ceci vaut pour tout caractère de H, ce qui clôt la démonstration de l'hérédité. Par principe de récurrence : tout caractère d'un sous-groupe de G se prolonge en un caractère de G, ce qu'on voulait démontrer.

Remarque. Ce résultat de prolongement des caractères permet de montrer la seconde formule d'orthogonalité : $\forall g \in G$, $\dfrac{1}{\text{card}(G)} \displaystyle\sum_{\chi \in \widehat{G}} \chi(g) = \delta_{g,1_G}$. En effet : soit g un élément non trivial de G. Comme $\langle g\rangle$ est isomorphe à $\mathbb{Z}/n\mathbb{Z}$ avec $n \geqslant 2$ l'ordre de g, la question 6 assure l'existence d'un caractère χ_g de $\langle g\rangle$ tel que : $\chi_g(g) \neq 1_G$. On le prolonge en un caractère de G, toujours noté χ_g par commodité. Comme $\chi \mapsto \chi_g\chi$ est une permutation de $\widehat{G}$ (sa bijection réciproque est : $\chi \mapsto \chi_g^{-1}\chi$), on a : $\displaystyle\sum_{\chi \in \widehat{G}} \chi(g) = \sum_{\chi \in \widehat{G}} \chi_g^{-1}(g)\chi(g) = \chi_g^{-1}(g) \sum_{\chi \in \widehat{G}} \chi(g)$. Comme : $\chi_g^{-1}(g) \neq 1_G$, on conclut : $\displaystyle\sum_{\chi \in \widehat{G}} \chi(g) = 0$. Le calcul pour $g = 1_G$ est trivial.

Questions à se poser, réflexes à acquérir.

— Pour comprendre la philosophie de ce raisonnement par récurrence, et y reconnaître encore une fois l'idée qu'un morphisme est entièrement caractérisé par l'image d'une partie génératrice : se demander comment, « à la main », étant donné un groupe $G = \langle g_1, \dots, g_s\rangle$, on aurait construit un prolongement d'un caractère $\chi : \langle g_1\rangle \to \mathbb{C}^*$ petit à petit. Réfléchir aux subtilités que ce raisonnement aurait posées, et comment les questions précédentes en tiennent compte.

— Observer que la méthode utilisée pour calculer la somme de la remarque fut déjà utilisée en d'autres circonstances (feuilles d'exercices).

— Pourquoi la formule d'orthogonalité des caractères, telle que je l'ai formulée, est bien équivalente à celle donnée en commentaire introductif de ce corrigé ?

— Comment démontre-t-on la première formule d'orthogonalité ?

12. Si l'on espère montrer l'égalité de l'énoncé par récurrence, encore faut-il avoir une relation entre le cardinal de $\widehat{G}$ et le cardinal de sous-groupes stricts (pour l'hérédité). C'est l'objectif de ce qui suit. Soit H un sous-groupe de G. L'application de restriction $f : \chi \mapsto \chi_{|H}$ est un morphisme, surjectif de $\widehat{G}$ dans $\widehat{H}$ d'après ce qu'on vient de démontrer, donc par le théorème d'isomorphisme les groupes $\widehat{G}/\ker(f)$ et $\widehat{H}$ sont isomorphes. On en déduit :

$$\mathrm{card}(\widehat{G}) = \mathrm{card}(\ker(f))\mathrm{card}(\widehat{H}).$$

Déterminons le cardinal de : $\ker(f) = \left\{\chi \in \widehat{G} \mid \forall h \in H,\ \chi(h) = 1\right\}$. Pour cela, il suffit de remarquer que, par le théorème de factorisation des morphismes, tout $\chi \in \ker(f)$ induit un caractère $\overline{\chi}$ de G/H. L'application $\chi \mapsto \overline{\chi}$ est une bijection de $\ker(f)$ dans $\widehat{G/H}$, donc : $\mathrm{card}(\ker(f)) = \mathrm{card}\left(\widehat{G/H}\right)$. La formule ci-dessus devient donc :

$$\mathrm{card}(\widehat{G}) = \mathrm{card}\left(\widehat{G/H}\right)\mathrm{card}(\widehat{H}). \qquad (*)$$

On peut à présent montrer : $\mathrm{card}(G) = \mathrm{card}(\widehat{G})$, par récurrence forte sur le cardinal de G. Le cas où $\mathrm{card}(G) = 1$ est trivial, puisque le seul caractère de $\{1_G\}$ est évidemment $\chi_0 : 1_G \mapsto 1$, de sorte que : $\mathrm{card}(\widehat{\{1_G\}}) = \mathrm{card}(\{1_G\}) = 1$. Considérons donc un groupe fini commutatif G de cardinal $n \geqslant 2$, et supposons que pour tout groupe fini commutatif H de cardinal strictement inférieur à n, on a : $\mathrm{card}(\widehat{H}) = \mathrm{card}(H)$. Montrons : $\mathrm{card}(G) = \mathrm{card}(\widehat{G})$. Soit H un sous-groupe *cyclique* non trivial de G (il suffit de prendre le groupe engendré par n'importe quel élément non trivial de G, et il en existe puisque $n \geqslant 2$). Comme H est cyclique, $\widehat{H}$ est isomorphe à H d'après la question 6 (on a montré que $\mathbb{Z}/n\mathbb{Z}$ est isomorphe à $\widehat{\mathbb{Z}/n\mathbb{Z}}$ pour tout $n \in \mathbb{N}\backslash\{0\}$, et un groupe cyclique est isomorphe à $\mathbb{Z}/n\mathbb{Z}$ pour un entier n adéquat), donc : $\mathrm{card}(\widehat{H}) = \mathrm{card}(H)$. De plus : $\mathrm{card}(G/H) = \frac{\mathrm{card}(G)}{\mathrm{card}(H)} < \mathrm{card}(G)$, puisque H est de cardinal supérieur ou égal à 2, donc par hypothèse de récurrence appliquée à G/H on a : $\mathrm{card}(\widehat{G/H}) = \mathrm{card}(G/H)$. L'identité $(*)$ permet alors de conclure : $\mathrm{card}(\widehat{G}) = \mathrm{card}(G/H)\mathrm{card}(H) = \mathrm{card}(G)$ (la dernière égalité est le théorème de Lagrange), d'où l'hérédité.
Par récurrence, on a montré que pour tout groupe fini commutatif G, on a : $\mathrm{card}(G) = \mathrm{card}(\widehat{G})$.
Remarque. Comme toutes les fibres ont le même cardinal pour un morphisme, notre calcul de $\mathrm{card}(\ker(f))$ démontre en passant que tout caractère de H se prolonge en *exactement* $\mathrm{card}\left(\widehat{G/H}\right) = \mathrm{card}(G/H) = \frac{\mathrm{card}(G)}{\mathrm{card}(H)}$ caractères de G.

Questions à se poser, réflexes à acquérir.

— Reconnaître ici une utilité des groupes quotients, non encore illustrée jusqu'à présent : les raisonnements par récurrence sur le cardinal.

— Pourquoi $\chi \mapsto \overline{\chi}$ est-elle bien une bijection de $\ker(f)$ dans $\widehat{G/H}$?

— Dans cette question et les précédentes : pourquoi tout cela marche avec les morphismes de G dans $\mathbb{C}^*$ spécifiquement ? Si l'on change le groupe d'arrivée, qu'est-ce qui coince ? Quelles propriétés essentielles de $\mathbb{C}$ sont utilisées ?

Troisième partie

13. Soient H un sous-groupe de G et $r : G \to H$ est un morphisme tel que : $r_{|H} = \mathrm{Id}_H$. L'application $g \mapsto (\bar{g}, r(g))$ est un morphisme de groupes de G dans $G/H \times H$ parce que c'est le cas composante par composante. Montrons que c'est un isomorphisme, en montrant d'abord que c'est un morphisme injectif. Soit g un élément de son noyau. On a : $(\bar{g}, r(g)) = (\overline{1_G}, 1_G)$, donc : $\bar{g} = \overline{1_G}$, et : $r(g) = 1_G$. La première égalité équivaut à : $g \in H$, et comme la restriction de r à H est l'identité, la seconde égalité devient : $g = 1_G$. Ainsi le noyau de $g \mapsto (\bar{g}, r(g))$ ne contient que 1_G, donc c'est un morphisme injectif entre deux groupes de même cardinal (en effet, par le théorème de Lagrange : $\mathrm{card}(G/H)\mathrm{card}(H) = \mathrm{card}(G)$) : c'est donc un morphisme bijectif, c'est-à-dire un isomorphisme de G dans $G/H \times H$. D'où le résultat.

> **Questions à se poser, réflexes à acquérir.**
> — Vérifier, avec des groupes *simples*, qu'en général il est faux que G est isomorphe à $G/H \times H$ (en général, l'ordre des éléments de $G/H \times H$ est plus petit que l'ordre des éléments de G : utiliser cette observation pour trouver un contre-exemple).
> — Avec des groupes explicites et de taille raisonnable, trouver des morphismes r vérifiant la condition de l'énoncé. Constater que c'est en général difficile (voire impossible ?) d'en trouver. Cela vous convaincra que l'isomorphisme de cette question est en général exceptionnel.

14. Comme $\langle x \rangle$ est cyclique d'ordre d, il est isomorphe à $\mathbb{Z}/d\mathbb{Z}$. Un isomorphisme entre $\mathbb{Z}/d\mathbb{Z}$ et $\langle x \rangle$ est donné par $f : \bar{k} \mapsto x^k$. Or $\mathbb{Z}/d\mathbb{Z}$ est isomorphe à $\mathbb{U}_d$ puisque ce dernier groupe est aussi cyclique, engendré par $e^{\frac{2i\pi}{d}}$. Un isomorphisme est donné par $g : \bar{k} \mapsto e^{\frac{2i\pi k}{d}}$. Par transitivité, $\langle x \rangle$ et $\mathbb{U}_d$ sont isomorphes, d'où l'existence d'un isomorphisme η de $\mathbb{U}_d$ dans $\langle x \rangle$. Il suffit en effet de poser : $\eta = f \circ g^{-1}$. On a en outre :

$$\eta\left(e^{\frac{2i\pi}{d}}\right) = f\left(g^{-1}\left(e^{\frac{2i\pi}{d}}\right)\right) = f\left(\bar{1}\right) = x,$$

ce qu'il fallait démontrer.

15. On a déterminé les caractères de $\mathbb{Z}/d\mathbb{Z}$ dans la question 6, et en particulier l'application $\bar{k} \mapsto e^{\frac{2i\pi k}{d}}$ en est un. Or $\langle x \rangle$ est isomorphe à $\mathbb{Z}/d\mathbb{Z}$, un isomorphisme étant donné par $x^k \mapsto \bar{k}$. En prenant l'image du caractère $\bar{k} \mapsto e^{\frac{2i\pi k}{d}}$ de $\mathbb{Z}/d\mathbb{Z}$ par l'isomorphisme de la question 4, on en déduit l'existence d'un caractère de $\langle x \rangle$ défini par $x^k \mapsto e^{\frac{2i\pi k}{d}}$. Or il fut démontré dans la deuxième partie du problème que tout caractère d'un sous-groupe (d'un groupe fini commutatif) se prolonge en un caractère de G : on en déduit l'existence d'un caractère χ de G dont la restriction à $\langle x \rangle$ est le morphisme décrit ci-avant, c'est-à-dire tel que : $\forall k \in \mathbb{Z}$, $\chi\left(x^k\right) = e^{\frac{2i\pi k}{d}}$. D'où le résultat.

16. Posons : $r = \eta \circ \chi : G \to \langle x \rangle$. La composition est correctement définie, puisque χ est à valeurs dans $\mathbb{U}_d$ par la question 2 (en effet d est l'exposant de G par définition). On a par ailleurs :

$$\forall k \in \mathbb{Z}, \quad \eta \circ \chi(x^k) = \eta\left(e^{\frac{2i\pi k}{d}}\right) = \left(\eta\left(e^{\frac{2i\pi}{d}}\right)\right)^k = x^k,$$

donc : $\eta \circ \chi_{|\langle x \rangle} = \mathrm{Id}_{\langle x \rangle}$. Par la question 13, les groupes G et $G/\langle x \rangle \times \langle x \rangle$ sont isomorphes, d'où le résultat.

> **Questions à se poser, réflexes à acquérir.** Après avoir constaté les difficultés à définir un morphisme $r : G \to H$ en général, comprendre pourquoi le prolongement des caractères permet au contraire d'en construire facilement ici.

17. Nous allons démontrer le résultat par récurrence sur le cardinal de G. Si G est un groupe commutatif de cardinal 2, alors G est isomorphe à $\mathbb{Z}/2\mathbb{Z}$ et le résultat voulu est démontré. À présent, soit $r \in \mathbb{N} \setminus \{0,1,2\}$, et supposons que tout groupe commutatif de cardinal strictement inférieur à r vérifie le résultat de l'énoncé.

Soit G un groupe commutatif de cardinal r, et considérons un élément x d'ordre maximal d. Comme G n'est pas le groupe trivial, x n'est pas d'ordre 1. Si $G = \langle x\rangle$, alors G est isomorphe à $\mathbb{Z}/d\mathbb{Z}$ et on a le résultat voulu. Supposons donc : $G \neq \langle x\rangle$. Par la question précédente, G est isomorphe à $G/\langle x\rangle \times \langle x\rangle$, et comme $G/\langle x\rangle$ est un groupe fini commutatif de cardinal au moins 2 (puisque $\langle x\rangle \neq G$), tel que : $\mathrm{card}(G/\langle x\rangle) = \frac{\mathrm{card}(G)}{\mathrm{card}(\langle x\rangle)} < r$, appliquer l'hypothèse de récurrence à $G/\langle x\rangle$ assure l'existence de $s \in \mathbb{N}\setminus\{0\}$ et $(d_1,\dots,d_s) \in (\mathbb{N}\setminus\{0,1\})^r$ tels que : $\forall i \in [\![1, s-1]\!]$, $d_i \mid d_{i+1}$, et tels que $G/\langle x\rangle$ soit isomorphe à $\prod_{i=1}^{s} \mathbb{Z}/d_i\mathbb{Z}$. De plus $\langle x\rangle$ est isomorphe à $\mathbb{Z}/d\mathbb{Z}$ puisque c'est un groupe cyclique de cardinal d. On en déduit que G est isomorphe à $\prod_{i=1}^{s} \mathbb{Z}/d_i\mathbb{Z} \times \mathbb{Z}/d\mathbb{Z}$. Posons alors : $r = s+1$, et : $d_r = d$. Ce qui précède montre que G est isomorphe à $\prod_{i=1}^{r} \mathbb{Z}/d_i\mathbb{Z}$, et il reste à vérifier la condition de divisibilité : $\forall i \in [\![1, r-1]\!]$, $d_i \mid d_{i+1}$. Elle est déjà vérifiée pour tout $i \in [\![1, r-2]\!]$, et il reste à vérifier le cas $i = r-1$, c'est-à-dire : $d_{r-1} | d$.

Pour cela, on rappelle que d est l'exposant de G ; comme un isomorphisme préserve tout ce qui est relatif à la structure de groupe, et en particulier les ordres des éléments, d est aussi l'exposant de $\prod_{i=1}^{r} \mathbb{Z}/d_i\mathbb{Z}$. Or nous avons démontré dans la question 2 que l'ordre de tout élément d'un groupe divise son exposant ; par conséquent, pour montrer que d_{r-1} divise d, il suffit de trouver un élément d'ordre d_{r-1} dans d. Un tel élément est fourni par $(\delta_{i,r-1} \bmod d_i)_{1\leqslant i\leqslant r} \in \prod_{i=1}^{r} \mathbb{Z}/d_i\mathbb{Z}$, comme on le vérifie aisément en utilisant le fait que 1 mod d_{r-1} engendre $\mathbb{Z}/d_{r-1}\mathbb{Z}$. Par conséquent l'ordre de cet élément, c'est-à-dire d_{r-1}, divise l'exposant d de $\prod_{i=1}^{r} \mathbb{Z}/d_i\mathbb{Z}$, ce qu'il restait à démontrer et achève la récurrence.

Par principe de récurrence, pour tout groupe fini commutatif G de cardinal supérieur ou égal à 2, il existe $r \in \mathbb{N}\setminus\{0\}$ et $(d_1,\dots,d_r) \in (\mathbb{N}\setminus\{0,1\})^r$ tels que : $\forall i \in [\![1, r-1]\!]$, $d_i \mid d_{i+1}$, et tels que G soit isomorphe au groupe $\prod_{i=1}^{r} \mathbb{Z}/d_i\mathbb{Z}$.

Questions à se poser, réflexes à acquérir.

- Pourquoi ai-je besoin de distinguer le cas, selon que G soit égal ou non à $\langle x\rangle$?
- Vérifier ce que j'ai omis : pourquoi $(\delta_{i,r-1} \bmod d_i)$ est bien d'ordre d_{r-1} ?
- Dans cette question et les précédentes : pourquoi a-t-on pris x d'ordre maximal ? Est-ce que la stratégie échoue avec x quelconque ?
- Pour récapituler ce devoir, pourquoi avoir eu recours aux morphismes de G dans $\mathbb{C}^*$? Qu'ont-ils apporté que, par exemple, des morphismes de G dans $\mathbb{Q}$ ou $\mathbb{Z}/n\mathbb{Z}$ n'auraient pas permis ?

18. C'est, à mon avis, la question la plus fine du devoir.

Supposons qu'il existe $(r,s) \in (\mathbb{N}\setminus\{0\})^2$ et $(d_1,\dots,d_r,e_1,\dots,e_s) \in (\mathbb{N}\setminus\{0,1\})^{r+s}$ tels que : $\forall i \in [\![1, r-1]\!]$, $d_i \mid d_{i+1}$, $\forall i \in [\![1, s-1]\!]$, $e_i \mid e_{i+1}$, et tels que G soit isomorphe à $\prod_{i=1}^{r} \mathbb{Z}/d_i\mathbb{Z}$ et $\prod_{i=1}^{s} \mathbb{Z}/e_i\mathbb{Z}$. On veut montrer : $r = s$, et : $\forall i \in [\![1, r]\!]$, $d_i = e_i$. Il ne coûte rien de supposer $r \geqslant s$, quitte à échanger les rôles des deux produits cartésiens.

Par transitivité, les groupes $\prod_{i=1}^{r} \mathbb{Z}/d_i\mathbb{Z}$ et $\prod_{i=1}^{s} \mathbb{Z}/e_i\mathbb{Z}$ sont isomorphes. En prenant l'image de ces deux groupes par l'endomorphisme de multiplication par d_1, on en déduit que les groupes $\prod_{i=1}^{r} d_1\mathbb{Z}/d_i\mathbb{Z}$ et $\prod_{i=1}^{s} d_1\mathbb{Z}/e_i\mathbb{Z}$ sont isomorphes. Or on sait décrire le sous-groupe de $\mathbb{Z}/d_i\mathbb{Z}$ (ou $\mathbb{Z}/e_i\mathbb{Z}$) engendré par d_1 : comme on l'a vu en travaux dirigés, il est égal au sous-groupe engendré par $\mathrm{pgcd}(d_1, d_i)$ (ou

$\operatorname{pgcd}(d_1, e_i)$), lequel est l'unique sous-groupe de cardinal $\dfrac{d_i}{\operatorname{pgcd}(d_1, d_i)}$ (ou $\dfrac{e_i}{\operatorname{pgcd}(d_1, e_i)}$). Donc, en comparant les cardinaux de ces deux groupes isomorphes :

$$\prod_{i=1}^{r} \frac{d_i}{\operatorname{pgcd}(d_1, d_i)} = \prod_{i=1}^{s} \frac{e_i}{\operatorname{pgcd}(d_1, e_i)},$$

or : $\prod_{i=1}^{r} d_i = \prod_{i=1}^{s} e_i = \operatorname{card}(G)$ (car les isomorphismes préservent les cardinaux), et d_1 divise d_i pour tout $i \in [\![1, r]\!]$ par transitivité de la relation de divisibilité, donc : $\forall i \in [\![1, r]\!]$, $\operatorname{pgcd}(d_1, d_i) = d_1$. L'égalité ci-dessus équivaut donc à :

$$\frac{\operatorname{card}(G)}{d_1^r} = \frac{\operatorname{card}(G)}{\prod_{i=1}^{s} \operatorname{pgcd}(d_1, e_i)} \iff d_1^r = \prod_{i=1}^{s} \operatorname{pgcd}(d_1, e_i).$$

Or : $\prod_{i=1}^{s} \operatorname{pgcd}(d_1, e_i) \leqslant d_1^s$, donc l'égalité ci-dessus implique : $d_1^r \leqslant d_1^s$. Comme $d_1 \geqslant 2$, ce n'est possible que si : $r \leqslant s$. Ayant supposé le contraire ci-dessus, on en déduit par antisymétrie : $r = s$. Cette égalité permet d'affiner l'inégalité ci-dessus. En effet, s'il existe $i \in [\![1, r]\!]$ tel que : $\operatorname{pgcd}(d_1, e_i) < d_1$, alors :

$$d_1^r = \prod_{i=1}^{r} \operatorname{pgcd}(d_1, e_i) < d_1^r,$$

ce qui est absurde. Donc : $\forall i \in [\![1, r]\!]$, $\operatorname{pgcd}(d_1, e_i) = d_1$, ce qui signifie que d_1 divise e_i pour tout $i \in [\![1, r]\!]$. En particulier, d_1 divise e_1. Comme les d_i et e_i jouent des rôles symétriques, on montre de même que e_1 divise d_1, donc ils sont associés et positifs. On en déduit : $d_1 = e_1$.

En réitérant le procédé, où l'on multiplie par d_2, d_3, etc. (au lieu de multiplier par d_1), on obtient : $\forall i \in [\![1, r]\!]$, $d_i = e_i$, d'où le résultat.

Remarque : pourquoi cette question est difficile, et pourquoi passer par l'endomorphisme de multiplication. On aurait pu être tenté de faire le raisonnement suivant : si G est isomorphe à $\prod_{i=1}^{r} \mathbb{Z}/d_i\mathbb{Z}$, avec : $\forall i \in [\![1, r-1]\!]$, $d_i \mid d_{i+1}$, on montre aisément que d_r est l'exposant de G, et que $x = (\delta_{i,r} \bmod d_i)_{1 \leqslant i \leqslant r}$ est un élément d'ordre d_r dans $\prod_{i=1}^{r} \mathbb{Z}/d_i\mathbb{Z}$. Comme un isomorphisme $\varphi : \prod_{i=1}^{r} \mathbb{Z}/d_i\mathbb{Z} \to \prod_{i=1}^{s} \mathbb{Z}/e_i\mathbb{Z}$ préserve tout ce qui est relatif à la structure, on en déduirait d'abord que $\varphi(x)$ est un élément d'ordre maximal, c'est-à-dire e_s, d'où : $d_r = e_s$ (puisque $\varphi(x)$ est aussi de même ordre que x, c'est-à-dire d_r). À ce stade, on aimerait conclure par récurrence, en quotientant par $\langle x \rangle$: comme $\left(\prod_{i=1}^{r} \mathbb{Z}/d_i\mathbb{Z}\right)/\langle x \rangle$ est isomorphe à $\prod_{i=1}^{r-1} \mathbb{Z}/d_i\mathbb{Z}$ (conséquence facile du théorème d'isomorphisme), et $\left(\prod_{i=1}^{r} \mathbb{Z}/d_i\mathbb{Z}\right)/\langle x \rangle$ isomorphe à $\left(\prod_{i=1}^{s} \mathbb{Z}/e_i\mathbb{Z}\right)/\langle \varphi(x) \rangle$ (idem), on aimerait en déduire que $\prod_{i=1}^{r-1} \mathbb{Z}/d_i\mathbb{Z}$ et $\prod_{i=1}^{s-1} \mathbb{Z}/e_i\mathbb{Z}$ sont isomorphes (en « simplifiant » $\mathbb{Z}/d_r\mathbb{Z}$ et $\mathbb{Z}/e_s\mathbb{Z} = \mathbb{Z}/d_r\mathbb{Z}$, en quelque sorte). Le problème de ce raisonnement est qu'il n'est pas clair, *a priori*, que $\left(\prod_{i=1}^{s} \mathbb{Z}/e_i\mathbb{Z}\right)/\langle \varphi(x) \rangle$ est isomorphe à $\prod_{i=1}^{s-1} \mathbb{Z}/e_i\mathbb{Z}$. Pour affirmer cela facilement, il faudrait que $\varphi(x)$ soit égal à $(\delta_{i,r} \bmod e_i)_{1 \leqslant i \leqslant s}$ ou, du moins, de la forme $(k\delta_{i,r} \bmod e_i)_{1 \leqslant i \leqslant s}$ avec k premier avec e_s, de sorte qu'il engendre $\{0\}^{s-1} \times \mathbb{Z}/e_s\mathbb{Z}$ et que le quotient par $\langle \varphi(x) \rangle$ « fasse disparaître » $\mathbb{Z}/e_s\mathbb{Z}$. Mais là est où tout le problème : il y a beaucoup d'éléments d'ordre maximal, et ils ne sont pas tous de la forme susdite. Par exemple, dans $\mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/8\mathbb{Z}$, tous ces éléments sont d'ordre maximal :

$$(\pm 1 \bmod 4, \pm 1 \bmod 8), \quad (\pm 1 \bmod 4, \pm 3 \bmod 8), \quad (2 \bmod 4, \pm 1 \bmod 8), \quad (2 \bmod 4, \pm 3 \bmod 8)$$

donc, même si $x = (0 \bmod 4, 1 \bmod 8)$, *a priori* $\varphi(x)$ pourrait être n'importe lequel de ces huit éléments. Il n'est alors plus vrai que : $\langle\varphi(x)\rangle = \{0\}^{s-1} \times \mathbb{Z}/e_s\mathbb{Z}$, et il n'est plus si clair que $\left(\prod_{i=1}^{s} \mathbb{Z}/e_i\mathbb{Z}\right)/\langle\varphi(x)\rangle$ soit isomorphe à $\prod_{i=1}^{s-1} \mathbb{Z}/e_i\mathbb{Z}$. C'est ce qui fait toute la difficulté de cette question, et ce qui justifie notre moyen détourné pour y remédier : on ne regarde pas la structure de groupe de l'ensemble quotient, puisque celle-ci nous échappe, mais on fait un raisonnement sur les cardinaux. L'idée de passer par l'endomorphisme de multiplication est que, justement, il « élimine » des groupes du produit cartésien, du fait que $d_i \equiv 0 \bmod d_k$ pour tout $k \leqslant i$ (de sorte que, par exemple, multiplier par d_1 « élimine » $\mathbb{Z}/d_1\mathbb{Z}$ et nous ramène à $\prod_{i=2}^{r} d_1\mathbb{Z}/d_i\mathbb{Z}$: une récurrence semble désormais envisageable) : on réussit donc là où la stratégie esquissée ci-dessus échoue.

Questions à se poser, réflexes à acquérir. Vérifier les détails omis, en faisant le lien avec le cours ou des exercices classiques traités :

- Pourquoi l'endomorphisme de multiplication par d_1 préserve-t-il les isomorphismes ? Est-ce le cas de tout endomorphisme de groupe ? (Déjà, est-ce que cela a bien un sens pour tout endomorphisme ?)
- Pourquoi choisit-on de multiplier par d_1 plutôt que par d_r, par exemple ? Au vu de la démonstration de l'existence de l'isomorphisme, il semblerait pourtant plus naturel de considérer l'entier le plus grand.
- Pourquoi $\langle d_1 \bmod d_i\rangle = \langle \mathrm{pgcd}(d_1, d_i) \bmod d_i\rangle$?
- Pourquoi $\langle \mathrm{pgcd}(d_1, d_i) \bmod d_i\rangle$ est-il de cardinal $\frac{d_i}{\mathrm{pgcd}(d_1,d_i)}$?

19. On pourrait imiter le raisonnement des questions précédents, en trouvant b grâce à un élément d'ordre maximal dans $\mathbb{Z}/a\mathbb{Z} \times \mathbb{Z}/b\mathbb{Z}$ (on vérifie que l'ordre maximal d'un élément de ce groupe est $\mathrm{ppcm}(a, b)$). Mais on va plutôt utiliser le lemme chinois, en se ramenant préalablement à des entiers premiers entre eux. Soient $a = \prod_p p^{v_p(a)}$ et $b = \prod_p p^{v_p(b)}$ les décompositions en facteurs premiers de a et b (les produits sont à support fini). Par le théorème chinois, on a l'isomorphisme suivant :

$$\mathbb{Z}/a\mathbb{Z} \times \mathbb{Z}/b\mathbb{Z} \simeq \prod_p \mathbb{Z}/p^{v_p(a)}\mathbb{Z} \times \prod_p \mathbb{Z}/p^{v_p(b)}\mathbb{Z}.$$

Il va de soi que permuter l'ordre des groupes dans un produit cartésien donne des produits cartésiens isomorphes : si $G_1, \dots, G_r$ sont r groupes et σ une permutation de S_r, alors $\prod_{i=1}^{r} G_i$ et $\prod_{i=1}^{r} G_{\sigma(i)}$ sont isomorphes *via* le morphisme bijectif $(g_i)_{1\leqslant i\leqslant r} \mapsto (g_{\sigma(i)})_{1\leqslant i\leqslant r}$. Nous allons donc permuter l'ordre des groupes ci-dessus, selon que $v_p(a) = \min(v_p(a), v_p(b))$ (et dans ce cas $v_p(b)$ est le maximum des deux valuations) ou $v_p(a) = \max(v_p(a), v_p(b))$ (de même), pour obtenir :

$$\mathbb{Z}/a\mathbb{Z} \times \mathbb{Z}/b\mathbb{Z} \simeq \prod_p \mathbb{Z}/p^{\min(v_p(a),v_p(b))}\mathbb{Z} \times \prod_p \mathbb{Z}/p^{\max(v_p(a),v_p(b))}\mathbb{Z} \simeq \mathbb{Z}/\mathrm{pgcd}(a,b)\mathbb{Z} \times \mathbb{Z}/\mathrm{ppcm}(a,b)\mathbb{Z}.$$

On a répondu à la question posée, avec $r = 2$, $d_1 = \mathrm{pgcd}(a, b)$ et $d_2 = \mathrm{ppcm}(a, b)$ (notons que d_1 divise a et b, donc il divise aussi $\mathrm{ppcm}(a, b) = d_2$ par transitivité de la relation de divisibilité).

Questions à se poser, réflexes à acquérir.

- Pourquoi cette idée de passer par le théorème chinois était-elle pertinente et naturelle ?
- Peut-on généraliser ainsi le raisonnement à $\mathbb{Z}/a\mathbb{Z} \times \mathbb{Z}/b\mathbb{Z} \times \mathbb{Z}/c\mathbb{Z}$?
- Essayer d'obtenir le résultat sans le théorème chinois, mais en imitant le raisonnement des questions précédentes : commencer par prendre un élément d'ordre maximal, etc. Constater les difficultés rencontrées, qui ont justifié que je raisonne autrement.

20. Le résultat demandé est immédiat en combinant les résultats des questions 8 et 17. Pour la réciproque : on note que $\widehat{G}$ est toujours commutatif (c'est une conséquence de la commutativité de $\mathbb{C}^*$), donc : si G et $\widehat{G}$ sont isomorphes, alors G est également commutatif. Il y a donc une équivalence entre être un groupe (fini) commutatif et être isomorphe au groupe de ses caractères. C'est en cela que les caractères *caractérisent* les groupes finis commutatifs.