Feuille 2-bis : Solution

1. On raisonne par récurrence sur $[G:H]$.

- Si $[G:H]=1$, alors $H=G$ et donc il n'y a rien à démontrer.
- Soit $n \geq 1$. Supposons le résultat vrai pour tout sous-groupe de G d'indice $\leq n$ (c'est-à-dire : tout caractère d'un sous-groupe d'indice $\leq n$ se prolonge en un caractère de G).

Soit H un sous-groupe d'indice $n+1$, et $\chi \in \widehat{H}$.

Comme $[G:H] = n+1 > 1$, il existe $g \in G \setminus H$.

Soit $K := \langle H, g \rangle$. Alors comme $H \subsetneq K$ (car $g \notin H$) on a $[G:K] < [G:H]$, de sorte que l'hypothèse de récurrence s'applique aux caractères de K : ils peuvent être prolongés en des caractères de G.

Ainsi, il suffit de montrer que χ se prolonge à K pour conclure.

Or comme G/H est un groupe fini, l'élément gH est d'ordre fini dans G/H. On note $k \geq 1$ l'ordre de gH dans G/H.

Alors $g^k \in H$, donc $\chi(g^k)$ a un sens (alors que $\chi(g)$ n'a pas de sens car $g \notin H$ et χ n'est, pour l'instant, défini que sur H).

Maintenant, soit $\omega \in \mathbb{C}$ tq $\omega^k = \chi(g^k)$. On définit $\widetilde{\chi} : K \longrightarrow \mathbb{C}^\times$ par $\widetilde{\chi}(g^l h) = \omega^l \chi(h)$ pour tout $l \in \mathbb{Z}$ et $h \in H$.

Les éléments de $K = \langle H, g \rangle$ sont tous de la forme $g^l h$ ci-dessus, mais par contre il faut vérifier que la définition de $\widetilde{\chi}$

ne dépend pas de l'écriture (qui n'a pas de raison d'être unique).

Soit $x = g^l h = g^m t$, avec $m, l \in \mathbb{Z}$ et $h, t \in H$.

Montrons que $\omega^l \chi(h) = \omega^m \chi(t)$.

Comme $g^l h = g^m t$, on a $g^{l-m} = th^{-1} \in H$, donc $o(gH) = k \mid l-m$

donc $\omega^l \chi(h) = \omega^{l-m} \omega^m \chi(h) = (\omega^k)^{\frac{l-m}{k}} \chi(h) \omega^m$

$= \chi(g^k)^{\frac{l-m}{k}} \chi(h) \omega^m = \chi(\underbrace{g^{l-m} h}_{=t}) \omega^m = \chi(t) \omega^m$

Ainsi, $\widetilde{\chi}$ est bien défini.

Montrons que $\widetilde{\chi} : K \to \mathbb{C}^\times$ est un caractère :

Soit $x = g^l h$ et $y = g^m t \in \langle g, H \rangle$.

Alors $\widetilde{\chi}(xy) = \widetilde{\chi}(g^{l+m} ht) = \omega^{l+m} \chi(ht) = \omega^{l+m} \chi(h)\chi(t)$

$= \widetilde{\chi}(x)\widetilde{\chi}(y)$, ce qui conclut la preuve.

2. $\{ o(x), x \in G \}$ est une partie finie de $\mathbb{N}^*$; elle admet donc un maximum d. Soit $x \in G$ un élément d'ordre maximal, c'est-à-dire $o(x) = d$.

Soit $y \in G$, dont on note n l'ordre. On veut montrer que $y^d = e$ c'est-à-dire $n \mid d$.

Si, par l'absurde, n ne divisait pas d, alors il existerait un nombre premier p tel que $v_p(n) > v_p(d)$.

alors $\begin{cases} x^{p^{v_p(d)}} \text{ est d'ordre } \dfrac{d}{p^{v_p(d)}} \\ y^{\frac{n}{p^{v_p(n)}}} \text{ est d'ordre } p^{v_p(n)} \end{cases}$ premiers entre eux

donc leur produit est d'ordre $d\,p^{v_p(n)-v_p(d)} > d$: contredit la maximalité de d.

Rem: On a utilisé le fait suivant : si x, y sont deux éléments d'un groupe tq $\begin{cases} xy = yx \\ \text{pgcd}(o(x), o(y)) = 1 \end{cases}$ alors $o(xy) = o(x)\,o(y)$

3. Soit $x \in G$ un élément d'ordre maximal d.
Soit $H := \langle x \rangle$. C'est un groupe cyclique d'ordre d.

Soit $\eta : H \longrightarrow U_d$ un isomorphisme (obtenu par exemple en envoyant le générateur x de H sur le générateur $\zeta_d = e^{\frac{2i\pi}{d}}$ de U_d, mais ce n'est pas le seul !)

Alors $\chi : H \longrightarrow \mathbb{C}^\times$, $y \longmapsto \eta(y)$ est un caractère de H, donc d'après la q° 1, il se prolonge en un caractère $\tilde{\chi} : G \longrightarrow \mathbb{C}^\times$

G d'après la q° 2, pour tout $y \in G$, $y^d = e$, donc

$$\tilde{\chi}(y^d) = \tilde{\chi}(y)^d = 1,$$ donc $\tilde{\chi}$ est à valeurs dans U_d. Ainsi on peut bien définir

$$\Psi : G \longrightarrow H \times G/H \qquad \text{c'est un morphisme}$$
$$y \longmapsto \left((\eta^{-1} \circ \tilde{\chi})(y),\ yH\right)$$

de groupes, entre deux groupes de même cardinal, donc il suffit de montrer que Ψ est injectif pour conclure que c'est un isomorphisme

Or si $y \in G$ est tq $\psi(y) = (e_H, e_{G/H})$ alors

$yH = H$ donc $y \in H$ et $\eta^{-1}(\tilde{\chi}(y)) \underset{\uparrow}{=} \eta^{-1}(\eta(y)) = y = e_H$
$y \in H$

donc $y = e_G$, ce qui donne la conclusion.

4. On procède, comme indiqué, par récurrence sur $|G|$.

- Si $|G| \in \{1, 2, 3\}$ on a $G \simeq \{e\}$
$G \simeq \mathbb{Z}/2\mathbb{Z}$
$G \simeq \mathbb{Z}/3\mathbb{Z}$

donc le résultat est vrai dans ces petits cas.

- Soit $n \geq 1$. On suppose le résultat vrai pour tout groupe abélien fini de cardinal $\leq n$. Soit G un groupe abélien fini de cardinal $n+1$. Soit $x \in G$ un élément d'ordre maximal d.

D'après la question précédente, il existe un isomorphisme

$$\psi : G \xrightarrow{\sim} \langle x \rangle \times G/\langle x \rangle$$

Or comme $|G| = n+1 \geq 2$, on a aussi $d \geq 2$, donc $|G/\langle x \rangle| \leq \frac{|G|}{2} \leq n$: l'hypothèse de récurrence s'applique donc à $G/\langle x \rangle$, qui est isomorphe à

$$\mathbb{Z}/d_1\mathbb{Z} \times \cdots \times \mathbb{Z}/d_m\mathbb{Z} \quad \text{où } d_1 | \cdots | d_m.$$

Comme $\langle x \rangle \simeq \mathbb{Z}/d\mathbb{Z}$ on en déduit que G est isomorphe à

$$\mathbb{Z}/d_1\mathbb{Z} \times \cdots \times \mathbb{Z}/d_m\mathbb{Z} \times \mathbb{Z}/d\mathbb{Z}.$$

Comme dans ce groupe il y a des éléments d'ordre d_i pour tout $i \in [\![1, m]\!]$, et que l'on a vu que ces ordres doivent diviser l'ordre maximal d, on en déduit que $d_m \mid d$ et on a bien obtenu $G \simeq \mathbb{Z}/d_1\mathbb{Z} \times \cdots \times \mathbb{Z}/d_k\mathbb{Z}$ avec $d_1 \mid \cdots \mid d_k$.

5. La preuve repose sur le lemme suivant :

> Si $q \in \mathbb{N}$, l'équation $qx = 0$ a $(q \wedge n_1) \cdots (q \wedge n_r)$ solutions dans $\mathbb{Z}/n_1\mathbb{Z} \times \cdots \times \mathbb{Z}/n_r\mathbb{Z}$

Preuve : Pour tout $x = (x_1, \dots, x_r) \in \mathbb{Z}/n_1\mathbb{Z} \times \cdots \times \mathbb{Z}/n_r\mathbb{Z}$, on a

$$\begin{aligned} qx = 0 &\iff (qx_1, \dots, qx_r) = (0, \dots, 0) \\ &\iff \forall i \in [\![1, r]\!], \quad n_i \mid qx_i \\ &\iff \forall i \in [\![1, r]\!], \quad \frac{n_i}{n_i \wedge q} \mid \frac{q}{n_i \wedge q} x_i \end{aligned}$$

($\frac{n_i}{n_i \wedge q}$ et $\frac{q}{n_i \wedge q}$ premiers entre eux)

$$\iff \forall i \in [\![1, r]\!], \quad \frac{n_i}{n_i \wedge q} \mid x_i$$

La question se ramène donc à compter le nombre de multiples de $\frac{n_i}{n_i \wedge q}$ dans $\{1, \dots, n_i\}$: il y en a $n_i \wedge q$. □

Une fois que l'on a ce résultat, on peut revenir à l'exercice :

Supposons que $\mathbb{Z}/d_1\mathbb{Z} \times \cdots \times \mathbb{Z}/d_r\mathbb{Z} \simeq G \simeq \mathbb{Z}/e_1\mathbb{Z} \times \cdots \times \mathbb{Z}/e_s\mathbb{Z}$

$(d_1 | \cdots | d_r)$ $\qquad$ $(e_1 | \cdots | e_s)$

Notons H le groupe tout à gauche, et H' le groupe tout à droite.

Comme H et H' sont isomorphes, l'équation $q \cdot x = 0$ a autant de solutions dans l'un que dans l'autre.

En particulier, pour $q = d_1$, le nombre de $x \in H$ tq $d_1 x = 0$ est égal à $(d_1 \wedge d_1) \cdots (d_1 \wedge d_r) = d_1^r$ puisque $d_1 | d_i$

tandis que le nombre de $x \in H'$ tq $d_1 x = 0$ est égal à

$$\underbrace{(d_1 \wedge e_1)}_{\leq d_1} \cdots \underbrace{(d_1 \wedge e_s)}_{\leq d_1} \leq d_1^s$$

Ainsi, $d_1^r \leq d_1^s$ et donc $\boxed{r \leq s}$ En renversant les rôles de H et H', on montre que $\boxed{s \leq r}$ et donc $\boxed{r = s}$.

Maintenant, supposons (par l'absurde) qu'il existe $k \in \{1, \dots, r\}$ tel que $d_k \neq e_k$. Notons $j := \min \{k \in \{1, \dots, r\} \text{ tq } e_k \neq d_k\}$.

On peut supposer que $d_j < e_j$

Alors l'équation $e_j x = 0$ a

- $(e_j \wedge d_1) \cdots (e_j \wedge d_{j-1})(e_j \wedge d_j) \cdots (e_j \wedge d_r)$ solutions dans H
- $(e_j \wedge e_1) \cdots (e_j \wedge e_{j-1})(e_j \wedge e_j) \cdots (e_j \wedge e_r)$ solutions dans H'.

Or par minimalité de j, on a $e_1 = d_1, \dots, e_{j-1} = d_{j-1}$, donc on peut simplifier les $j-1$ premiers termes, d'où

$\underbrace{(e_j \wedge d_j)}_{\leq d_j < e_j}\underbrace{(e_j \wedge d_{j+1})}_{\leq e_j} \cdots (e_j \wedge d_r) = \underbrace{(e_j \wedge e_j) \cdots (e_j \wedge e_r)}_{= e_j^{r-j+1} \text{ car } e_j \mid e_k \text{ pour } k \geq j}$

donc $e_j^{r-j+1} < e_j^{r-j+1}$: contradiction.

6. Soit $G < K^\times$ un sous-groupe fini. Alors G est un groupe abélien fini, donc d'après le thm de structure, il existe une (unique) suite $d_1 | \cdots | d_r$ t.q. $G \simeq \underbrace{\mathbb{Z}/d_1\mathbb{Z} \times \cdots \times \mathbb{Z}/d_r\mathbb{Z}}_{\text{notat additive}}$

($\uparrow$ notat multiplicative ($< K^\times$))

Si, par l'absurde, on avait $r \geq 2$.

Alors l'équat° $x^{d_1} = 1$ dans G (qui correspond à l'équat° $d_1 y = 0$ dans $\mathbb{Z}/d_1\mathbb{Z} \times \cdots \times \mathbb{Z}/d_r\mathbb{Z}$)

aurait d_1^r solutions, ce qui ferait trop de racines dans K pour un polynôme à coefficients dans K.

Donc $r = 1$ et G est cyclique.