Groupes abéliens finis

Réf: Berhuy, Algèbre le grand combat, p358 p.347.

Définition: Soit G un groupe abélien. On appelle caractère linéaire de G tout morphisme de groupes :

$$\chi : G \longrightarrow \mathbb{C}^\times$$

L'ensemble des caractères est un groupe abélien pour la multiplication, on le note $\widehat{G}$.

On commence par un théorème sur le prolongement des caractères.

Théorème: Soit G un groupe abélien et soit H un sous-groupe de G. Alors l'application de restriction

$$\begin{aligned} \rho_H : \widehat{G} &\longrightarrow \widehat{H} \\ \chi &\longmapsto \chi|_H \end{aligned}$$

est un morphisme de groupes, de noyau canoniquement isomorphe à $\widehat{G/H}$. Si de plus $[G:H]$ est fini, ρ_H est surjectif.

En particulier, si G est un groupe abélien fini, tout caractère linéaire de H se prolonge en un caractère linéaire de G.

Preuve:

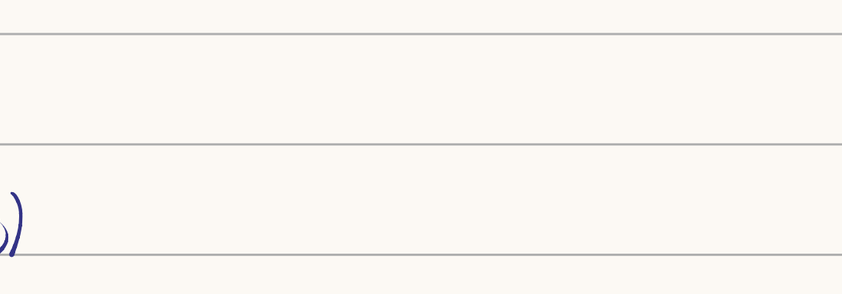
Etape 1: Noyau (pas dans le dvpt)

Le fait que ρ_H est un morphisme de groupe est clair.

Par définition, son noyau est l'ensemble des caractères linéaires de G dont le noyau contient H. Or G étant abélien H est donc distinguée donc par le théorème d'iso le noyau est isomorphe au morphisme

$$G/H \longrightarrow \mathbb{C}^\times \text{ i.e } \widehat{G/H}$$

Car on a pour tout $\rho \in \ker(\rho_H)$:



De plus $\bar{\rho}$ est unique.

Surjectivité: On suppose $[G:H]$ fini.

On va faire une récurrence sur $r=[G:H]$. Plus précisément on note (H_r) la propriété suivante:

(H_r): "Pour tout sous-groupe H de G tel que $[G:H]\leq r$, tout caractère linéaire de H se prolonge en un caractère linéaire de G."

Si $r=1$: Alors $G=H$, le résultat est immédiat.

Soit $r\geq 1$: On suppose H_r vraie et montrons H_{r+1}.

Soit H un sous-groupe de G tel que $[G:H]\leq r+1$. Si $[G:H]\leq r$ alors on applique l'hypothèse. On suppose donc que $[G:H]=r+1$.

En particulier $[G:H]\geq 2$ et $H\neq G$. On peut donc fixer $g\in G\setminus H$.

On note donc $H'=\langle H,g\rangle$ et comme G est abélien tout $h'\in H'$ s'écrit:

$$h'=hg^m \quad \text{avec } h\in H \text{ et } m\in\mathbb{Z}.$$

Soit χ un caractère de H i.e un morphisme de groupe:

$$\chi : H \longrightarrow \mathbb{C}^\times.$$

Comme $[G:H]$ est finie, G/H est un groupe fini, on note donc d l'ordre de $\bar{g}$ dans G/H. En particulier $\bar{1}=\bar{g}^{-d}=\bar{g}^d$ donc $g^d\in H$.

On fixe $z\in\mathbb{C}^\times$ une racine d-ième de $\chi(g^d)$. Et pour $h'\in H'$ qui s'écrit $h'=hg^m$, on pose:

$$\chi'(h')=\chi(h)z^m.$$

Montrons que cette quantité ne dépend pas de la décomposition.

Si $h'=h_1g^{m_1}=h_2g^{m_2}$ alors on a:

$$g^{m_2-m_1}=h_2^{-1}h_1\in H$$

donc $\bar{g}^{m_2-m_1}=\bar{1}\in G/H$ ainsi $d\mid m_2-m_1$. Donc il existe $k\in\mathbb{Z}$ tel que:

$$m_2=m_1+kd.$$

et $$h_1=h_2g^{kd}.$$

Ceci nous donne:

$$\begin{aligned}\chi(h_1)z^{m_1} &= \chi(h_2)\chi(g^d)^k z^{m_1}\\ &= \chi(h_2)\,z^{dk}z^{m_1}\\ &= \chi(h_2)\,z^{m_2}\end{aligned}$$

Par conséquent, l'application $\chi' : H' \longrightarrow \mathbb{C}^\times$ est bien définie.

Il est clair que c'est un morphisme de groupe qui prolonge χ. Comme $g\in G\setminus H$ alors $H\subsetneq H'$ donc

$$[G:H'] < [G:H]$$

En appliquant H_r à H' et χ' on obtient χ'' un caractère linéaire de G qui prolonge χ' donc χ d'où le

Résultat.

☑

Remarque: Soit G un groupe abelien fini d'ordre n et χ un caractère linéaire sur G alors:

$$\chi(G) \subseteq \mathbb{U}_n = \{z \in \mathbb{C} \mid z^n = 1\}.$$

Théorème: Soit G un groupe abélien fini.

alors il existe des entiers $d_1, \dots, d_s \geq 2$ tels que $d_1 | d_2 | \dots | d_s$ tel que:

$$G \simeq \mathbb{Z}/d_1\mathbb{Z} \times \dots \times \mathbb{Z}/d_s\mathbb{Z}.$$

De plus, la suite d'entiers $(d_1, \dots, d_s)$ est unique, et ne dépend que de la classe d'isomorphisme de G.

Preuve: On procède par récurrence sur $n = |G|$. On note (H_n) la propriété suivante:

H_n: "la partie existence est vraie pour tout groupe abélien fini G tel que $G \leq n$".

Si $n = 1$: alors G est trivial et le résultat est vraie.

Si $n \geq 1$: On suppose (H_n) vraie et montrons (H_{n+1}) vraie.

Soit G un groupe abelien, on peut supposer $|G| = n+1$. On note e l'exposant de G et on considère $x_0 \in G$ d'ordre e.

Puisque $|G| = n+1 \geq 2$, G n'est pas trivial et l'on a $e \geq 2$. Comme $\langle x_0 \rangle$ et $\mathbb{U}_e$ sont deux groupes cycliques d'ordre e, il existe un isomorphisme:

$$\chi_0 : \langle x_0 \rangle \xrightarrow{\sim} \mathbb{U}_e.$$

Ce morphisme est un caractère linéaire de $\langle x_0 \rangle$, il se prolonge donc en un caractère linéaire $\chi : G \to \mathbb{C}^\times$.

Or on sait que $\mathbb{U}_e \subset \mathrm{Im}(\chi)$ car pour tout $x \in G$,

$$\chi(x)^e = \chi(x^e) = \chi(1) = 1.$$

Ainsi $\mathrm{Im}(\chi) = \mathbb{U}_e$, on a donc un morphisme surjectif:

$$\chi : G \longrightarrow \mathbb{U}_e.$$

En utilisant que $\chi_0^{-1} : \mathbb{U}_e \longrightarrow \langle x_0 \rangle$ est un isomorphisme on peut définir un morphisme de groupe.

$$\varphi : G \longrightarrow G/\langle x_0 \rangle \times \langle x_0 \rangle$$

$$g \longmapsto (\bar{g}, \chi_0^{-1} \circ \chi(g)).$$

Montrons que φ est un isomorphisme, par cardinalité il suffit de montrer que φ est injectif.

Or pour $g \in G$ tel que $\varphi(g) = (1,1)$ on a : $\bar{g} = 1$ donc $g \in \langle x_0 \rangle$ i.e

$$\text{or } \chi_0^{-1} \circ \chi(g) = 1.$$

mais $g \in \langle x_0 \rangle$ donc $\chi(g) = \chi_0(g)$ ainsi

$$g = 1.$$

Donc φ est bien un isomorphisme on a donc :

$$G \simeq G/\langle x_0 \rangle \times \langle x_0 \rangle.$$

Or on sait que $\langle x_0 \rangle \simeq \mathbb{Z}/e \simeq \mathbb{Z}/e\mathbb{Z}$

Et comme $e \neq 1$, $|G/\langle x_0 \rangle| < n$, on sait par hypothèse de récurrence qu'il existe $(d_1, .., d_s)$ tel que $d_1 | .. | d_s$ et

$$G/\langle x_0 \rangle \simeq \mathbb{Z}/d_1\mathbb{Z} \times \dots \times \mathbb{Z}/d_s\mathbb{Z}.$$

Ce qui donne pour G : $G \simeq \mathbb{Z}/d_1\mathbb{Z} \times \dots \times \mathbb{Z}/d_s\mathbb{Z} \times \mathbb{Z}/e\mathbb{Z}$.

Il nous à reste à montrer que $d_s | e$.

Or $(0, .., 0, 1, 0)$ est un élément d'ordre d_s dans $\mathbb{Z}/d_1\mathbb{Z} \times \dots \times \mathbb{Z}/d_s\mathbb{Z} \times \mathbb{Z}/e\mathbb{Z}$, donc G admet un élément d'ordre d_s et e étant l'exposant de G on a $d_s | e$ d'où le résultat.

Unicité :

On remarque tout d'abord que pour tout $n, m \geq 1$, le groupe $n.\mathbb{Z}/m\mathbb{Z} = \langle \bar{n} \rangle$ est d'ordre $\frac{m}{pgcd(n,m)}$.

Supposons que l'on ait :

$$G \simeq \mathbb{Z}/d_1\mathbb{Z} \times \dots \times \mathbb{Z}/d_s\mathbb{Z} \simeq \mathbb{Z}/d_1'\mathbb{Z} \times \dots \times \mathbb{Z}/d_t'\mathbb{Z}$$

avec $d_1 | .. | d_s$

$d_1' | .. | d_t'$

On peut supposer que $s \geq t$ et $s \geq 1$.

On a donc :

$$d_1 G \simeq d_1.\mathbb{Z}/d_1\mathbb{Z} \times \dots \times d_1.\mathbb{Z}/d_s\mathbb{Z}$$

Ainsi

$$|d_1 G| = \frac{d_1 \cdots d_s}{d_1^s} = \frac{|G|}{d_1^s}$$

Mais de même $|d_1 G| = \frac{|G|}{pgcd(d_1, d_1') \cdots pgcd(d_1, d_t')}$

On a donc : $d_1^s = pgcd(d_1, d_1') \dots pgcd(d_1, d_t') \leq d_1^t$

Or $s \geq 1$ donc $d_1 \geq \ell$ et $s \geq t$ donc si $s > t$ l'inégalité serait fausse on a donc $s = t$. De plus si $pgcd(d_1, d_1') < d_1$ alors on a :

$$d_1^s < d_1^s$$

Ce qui est absurde donc $pgcd(d_1, d_1') = d_1$ ainsi $d_1 | d_1'$.

Or $s = t$ on peut échanger d_i et d_i' ce qui donne $d_1' | d_1$ on a donc $d_1 = d_1'$.

Ainsi $d_1' | d_2 | \dots | d_s$ et puisque $d_1 | d_2$ donc $d_2\mathbb{Z}/d_1\mathbb{Z} = 0$

$$d_2 G \simeq d_2\mathbb{Z}/d_2\mathbb{Z} \times \dots \times d_2\mathbb{Z}/d_s\mathbb{Z}$$

Mais $d_1' | d_2$ ainsi de même

$$d_2 G \simeq d_2\mathbb{Z}/d_2'\mathbb{Z} \times \dots \times d_2\mathbb{Z}/d_s'\mathbb{Z}.$$

En appliquant le même raisonnement on obtient $d_2 = d_2'$.

Ainsi de proche en proche, on a : $s = t$ et $d_i = d_i'$ $(\forall i \in [\![1, s]\!])$.

Résultat que l'on utilise.

Lemme : Soit G un groupe abélien d'exposant fini. Alors il existe $x \in G$ d'ordre $\exp(G) = ppcm(o(x), x \in G)$.

Preuve : On écrit :

$$\exp(G) = p_1^{m_1} \dots p_r^{m_r}.$$

où les p_i sont des nombres premiers distincts et $m_i \geq 1$.

Soit $i \in [\![1, r]\!]$, alors il existe $x_i \in G$ tel que $p_i^{m_i} | o(x_i)$.

En effet dans le cas contraire, pour tout $x \in G$, la plus grande puissance de p_i divisant $o(x)$ serait au plus $p_i^{m_i - 1}$. Alors $v_{p_i}(\exp(G)) = v_{p_i}(ppcm(o(x), x \in G)) < m_i$ Absurde.

On écrit $o(x_i) = p_i^{m_i} q_i$ alors on a $o(x_i^{q_i}) = p_i^{m_i}$.

Et comme $p_i^{m_i}$ et $p_j^{m_j}$ sont premier entre eux on a :

$$o(\underbrace{x_1^{q_1} \dots x_r^{q_r}}_{\in G}) = p_1^{m_1} \dots p_r^{m_r} = \exp(G).$$