Structure des groupes abéliens finis.

Rémi Lajugie

Dans tout le document, G désigne un groupe abélien fini.

Définition 1 *On appelle exposant d'un groupe fini, le plus petit entier N tel que $\forall g \in G, g^N = 1$.*

Théorème 1 *Soit H un sous-groupe de G et ξ un caractère de H. Alors H se prolonge en un caractère de G.*

Preuve :

Elle va s'effectuer par récurrence sur l'indice k de H. Le cas $k = 1$ étant évident.

Supposons que la proposition soit vraie pour tout $i < k$. Soit H d'indice k, ξ un caractère de H. On considère $u \notin H$, K le sous groupe engendré par u et H. Notons que ce sous groupe est d'indice strictement plus petit que k.

On considère ξ un caractère de H.

Nous aurons besoin du résultat suivant.

Proposition 1 *Soit n le plus petit entier tel que $v^n \in H$. Tout élément de K s'écrit de manière unique sous la forme $u^k h$ avec $h \in H$ et $k < n$.*

Preuve de la proposition : si on a $u^k h = u^{k'} h'$ (avec $k \geq k'$ pour fixer les idées) alors $u^{k-k'} = h' h^{-1}$ donc $k = k'$ car $k - k' < n$.

Notons que $n|l$. On appelle $\omega = \xi(u^n)$. On choisit une racine $\xi(u) = \omega^{1/n}$. Retour à la preuve : on étend le caractère ξ à K en posant $\xi(u^k h) = \xi(u)^k \xi(h)$. On vérifie alors que si $a = u^k h, b = u^{k'} h'$ le caractère est multiplicatif (si $k + k' > n$, écrire $u^{k+k'} = u^n u^{k+k'-n}$ et on retrouve le résultat.

Théorème 2 *Soit G un groupe abélien fini, alors il existe une unique suite finie d'entier $N_r | \ldots | N_1$ telle que $G \simeq \mathbb{Z}/N_1\mathbb{Z} \times \ldots \times \mathbb{Z}/N_r\mathbb{Z}$.*

Preuve : On peut la faire par récurrence sur l'ordre du groupe.

Si c'est vrai au rang n.

Par les lemmes arithmétiques, il existe un élément u dont l'ordre est l'exposant du groupe. On définit alors un caractère du sous groupe cyclique engendré par u. Par le lemme de prolongement on peut étendre ce caractère à G tout entier. Remarquons que, comme u a pour ordre l'exposant n du groupe, ce caractère a valeurs dans les racines $N-$emes de l'unité. Donc G admet un sous groupe H isomorphe à $\mathbb{Z}/N\mathbb{Z}$. Le noyau du caractère est un sous groupe de G d'ordre strictement plus petit que celui de G qui est donc isomorphe à $\mathbb{Z}/N_1\mathbb{Z} \times \ldots \times \mathbb{Z}/N_r\mathbb{Z}$.

Dernière étape : il suffit de vérifier que G se décompose en produit direct $H \times Ker(\xi)$.

Soit $x \in G$, comme il existe une section $h : \mathbb{Z}/n\mathbb{Z} \to H_1$ on a $h(\xi(x)) \in H_1$. De plus, $\xi(xh(\xi(x))^{-}1) = 1$. Ainsi on a bien décomposé G en un produit direct.

Quelques compléments d'ordre arithmétique

Proposition 2 *Soit $x, y \in G$ d'ordre a et b avec $a \wedge b = 1$ alors xy a pour ordre ab.*

Preuve :

Soit c l'ordre de xy. On a $(xy)^{ab} = 1$ donc $c|ab$. $(xy)^{ca} = 1$ donc $y^{ca} = 1$ donc $b|ca$ donc $b|c$ par le lemme de Gauss. De même $a|c$.

Proposition 3 *Soit $x, y \in G$ d'ordre quelconque alors il existe u d'ordre $a \vee b$.*

Preuve :

Soit a l'ordre de x, b celui de y. on écrit les décomposition en facteurs premiers : $a = \Pi_{p \in P} p^{\nu(p)}, b = \Pi_{p \in P} p^{\mu(p)}$. On a également $a \vee b = \Pi_p p^{\max(\nu(p), \mu(p))}$.

L'idée est alors de diviser les nombres premiers en deux catégories, ceux dont la valuation la plus grande est dans a et les autres (on rappelle que a et b ne sont plus supposés premiers entre eux.

On pose $l = \Pi_{p, \nu(p) \geq \mu(p)} p^{\nu(p)}$, $m = \frac{a \vee b}{l}$. Alors $l \wedge m = 1$ et $lm = a \vee b$. Les éléments $x^{a/l}$ et $y^{b/l}$ sont donc d'ordres respectifs l et m et on conclut par la proposition précédente.

Références

- Colmez.
- Peyré.