Rappels sur les groupes cycliques

Robert Rolland

11 mars 2000

1 Le théorème de Lagrange

Théorème 1.1 *Soit G un groupe fini, H un sous groupe de G. Alors l'***ordre** *de H (c'est-à dire le nombre d'éléments $\sharp H$ de H) divise l'ordre de G.*

Preuve. Soit $\mathcal{R}$ la relation sur G définie par

$$x\mathcal{R}y \Longleftrightarrow x \in yH.$$

La relation $\mathcal{R}$ est une relation d'équivalence. Si C_x est la classe d'un élément x l'application de H dans C_x qui à tout h fait correspondre xh est bijective, ce qui prouve que toutes les classes ont le même nombre déléments $\sharp H$. Par suite $\sharp H$ divise $\sharp G$.

2 Ordre d'un élément

Soit G un groupe (noté multiplicativement, d'élément neutre e) et g un élément de G. Notons

$$H = \{g^n \mid n \in \mathbb{Z}\}.$$

Alors H est un sous groupe commutatif de G, c'est le sous groupe de G engendré par g.

Deux cas peuvent se produire.

a) Tous les g^n sont distincts et alors H est infini et isomorphe à $(\mathbb{Z}, +)$.

b) Il existe $n > n'$ tels que $g^n = g^{n'}$ c'est-à-dire $g^{n-n'} = e$. Dans ce cas il existe un plus petit entier $m > 0$ tel que $g^m = e$. Si n est un entier

quelconque, $n = mq + r$ avec $0 \leq r < m$, ce qui permet d'écrire que $g^n = g^r$. De plus si $0 \leq r_1 < r_2 < m$ alors par définition de m on voit que $g^{r_1} \neq g^{r_2}$. En conséquence H est constitué des m éléments distincts

$$e, g, \cdots, g^{m-1}.$$

Remarquons encore que $g^n = g^{n'}$ équivaut à $n \equiv n' \quad (m)$. En fait, le sous groupe H est isomorphe à $\mathbb{Z}/m\mathbb{Z}$.

Dans ces conditions on dit que g est d'ordre m.

Théorème 2.1 *Soit G un groupe fini. Alors pour tout $g \in G$ on a $g^{\sharp G} = e$.*

Preuve. Soit H le sous groupe engendré par g. Ce sous groupe est fini et a pour ordre m. Par suite $g^m = e$. Mais m divise $\sharp G$ d'après le théorème de Lagrange. Donc $g^{\sharp G} = e$.

3 Groupes cycliques

Définition 3.1 *Un* **groupe cyclique** *est un groupe fini engendré par un seul élément.*

Remarquons qu'un tel groupe est commutatif.
Soit G un groupe cyclique d'ordre r et g un générateur de G. l'application

$$\begin{array}{rccc} \phi : & \mathbb{Z}/r\mathbb{Z} & \longrightarrow & G \\ & n & \longmapsto & g^n \end{array}$$

est un isomorphisme de groupes. Ainsi tout groupe cyclique d'ordre r est isomorphe à $(\mathbb{Z}/r\mathbb{Z}, +)$ et deux groupes cycliques de même ordre sont isomorphes.

Théorème 3.1 *Soit G un groupe cyclique d'ordre r.*

a) Tout sous groupe H de G est cyclique d'ordre un diviseur m de r.

b) Pour tout diviseur m de r il existe un et un seul sous groupe H d'ordre m. Ce sous groupe est cyclique et possède $\phi(m)$ générateurs. De plus H est l'ensemble des $x \in G$ tels que $x^m = e$.

Preuve. Puisque H est un sous groupe de G l'ordre m de H divise l'ordre r de G. Soit g un générateur de G et k le plus petit entier > 0 tel que $g^k \in H$. Pour tout élément $g^{k'}$ de H on a $k' = ak + b$ avec $0 \leq b < k$. Par suite $g^{k'} = (g^k)^a g^b$. On en déduit que $g^b \in H$ et donc par définition de k que $b = 0$. Donc $g^{k'} = (g^k)^a$, ce qui prouve que H est cyclique et que g^k est un générateur de H.
Soit m un diviseur de r, si bien que $r = qm$. Choisissons un générateur g de G. Les éléments g^s (avec $0 \leq s < mq$ d'un sous groupe H repondant à la question doivent vérifier $(g^s)^m = e$. Puisque g est un générateur de G, ceci est équivalent à $ms = ar = aqm$ ou encore à $s = aq$ (avec $0 \leq s < mq$). Donc s'il existe un sous groupe H répondant à la question il est nécessairement constitué des éléments

$$e, g^q, \cdots, g^{(m-1)q}.$$

On constate que cet ensemble constitue bien un sous groupe de G d'ordre m. Ce sous groupe est évidemment cyclique d'après la partie a) du théorème (on voit d'ailleurs que g^q en est un générateur).
Soit h un générateur de H. Nous allons chercher tous les autres générateurs sous la forme h^s. Pour qu'un h^s soit générateur il faut et il suffit que les $(h^s)^t$ où t varie dans $\mathbb{Z}/m\mathbb{Z}$ parcourent toutes les valeurs h^b où b varie dans $\mathbb{Z}/m\mathbb{Z}$. Ceci est équivalent à s inversible dans $\mathbb{Z}/m\mathbb{Z}$. Il y a donc $\phi(m)$ générateurs pour un groupe cyclique d'ordre m.

Théorème 3.2 *Soit G un groupe cyclique d'ordre r. Soit $s \in \mathbb{Z}$ et $t = (r, s)$ alors $\{g^s \mid g \in G\} = \{g^t \mid g \in G\}$. Cet ensemble est le sous groupe d'ordre r/t. L'ensemble des $g \in G$ tels que $g^s = e$ est le sous groupe d'ordre t.*

4 Exposant d'un groupe

Soit G un groupe fini. On note $\omega(G)$ l'**exposant** de G, c'est-à-dire le ppcm des ordres des éléments de G. C'est le plus petit entier s vérifiant $g^s = e$ pour tout $g \in G$. L'exposant de G divise l'ordre de G.

Théorème 4.1 *Si x et y sont deux éléments d'ordre fini qui commutent dans un groupe, et dont les ordres sont premiers entre eux, alors $Ordre(xy) = Ordre(x)Ordre(y)$.*

Preuve. Posons $m = Ordre(x)$ et $n = Ordre(y)$, alors $(xy)^{mn} = e$, ce qui prouve que l'ordre de xy est un diviseur de mn. Si maintenant on a un entier

$r > 0$ tel que $(xy)^r = e$, on a aussi $(xy)^{rm} = e$ et donc $y^{rm} = e$. Ceci prouve que rm est multiple de n, et comme n et m sont premiers entre eux, r est nultiple de n. De même r est multiple de m, donc r est multiple de mn.

Théorème 4.2 *Soit x et y deux éléments d'ordre fini qui commutent dans un groupe. Alors il existe un élément d'ordre le plus petit commun multiple de $Ordre(x)$ et $Ordre(y)$. En particulier si G est un groupe fini commutatif, il existe un élément de G d'ordre $\omega(G)$.*

Preuve. Posons $m = Ordre(x)$ et $n = Ordre(y)$. Soient m' et n' tels que m' divise m, n' divise n et $m'n' = ppcm(m, n)$. Soit $x' = x^{m/m'}$ et $y' = y^{n/n'}$. On peut appliquer le théorème précédent à x' et y' et obtenir ainsi un élément $x'y'$ d'ordre $m'n' = ppcm(m, n)$.

Théorème 4.3 *Parmi les groupes commutatifs finis, l'égalité $\omega(G) = \sharp G$ caractérise les groupes cycliques.*