3.2 Structure des groupes monogènes

Théorème 1 : Tout groupe monogène est isomorphe à :

$\mathbb{Z}$ s'il est infini;

$\mathbb{Z}/n\mathbb{Z}$ s'il est fini de cardinal n.

Il n'y a donc *qu'une seule structure de groupe monogène d'ordre donné* : par exemple deux groupes cycliques de même cardinal sont isomorphes.

Démonstration : soit G un groupe monogène et notons sa loi additivement. Soit φ l'application de $\mathbb{Z}$ dans G qui à n associe nx où x est un générateur de G. C'est un morphisme de groupes surjectif

Si φ est injectif alors φ est un isomorphisme de $\mathbb{Z}$ dans G et G est infini.

Sinon son noyau N est un sous-groupe de $\mathbb{Z}$ donc de la forme $a\mathbb{Z}$ pour $a \in \mathbb{N}^*$ (exercice 7, 1°/). La décomposition canonique de φ fournit un isomorphisme $\overline{\varphi}$ de $\mathbb{Z}/a\mathbb{Z}$ dans G (défini par $\overline{\varphi}(\overline{y}) = yx$) .$G$ est alors un groupe fini de cardinal a.

Exercice 27 : Théorème chinois

Déduire du théorème précédent et de l'exercice 24 que si m et n sont deux entiers premiers entre eux le groupe $\mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$ est isomorphe à $\mathbb{Z}/mn\mathbb{Z}$ (« *théorème chinois* »). Préciser l'isomorphisme.

Plus généralement si $n_1, n_2, \ldots, n_p$ sont des entiers premiers entre eux *deux à deux* le groupe $\mathbb{Z}/n_1\mathbb{Z} \times \ldots \times \mathbb{Z}/n_p\mathbb{Z}$ est isomorphisme à $\mathbb{Z}/n_1 \ldots n_p\mathbb{Z}$.

Dans un groupe fini l'ordre d'un sous-groupe divise l'ordre du groupe (théorème de Lagrange); dans un groupe cyclique pour tout diviseur d de n il existe un sous-groupe de cardinal d; plus précisément :

Théorème 2 : Soit G un groupe cyclique d'ordre n engendré par x. Alors :

(i) Tout sous-groupe H de G est cyclique; si k est le plus petit entier > 0 tel que $x^k \in H$, alors H est engendré par x^k. De plus k divise n et H est d'ordre n/k.

(ii) Si q divise n, G possède un unique sous-groupe d'ordre q : c'est le sous-groupe engendré par $x^{n/q}$.

Démonstration :

(i) Soit H un sous-groupe de G. Supposons H distinct de $\{e\}$. Posons $A = \{p \in \mathbb{N}^* / x^p \in H\}$. On a $x^n = e$ (proposition du 3.1) donc $n \in A$ et A est non vide. Soit $k = \text{Min}\{p \in \mathbb{N}^* / x^p \in H\}$ et y un élément quelconque de H. G étant cyclique et engendré par x il existe $m \in \mathbb{N}$ tel que $y = x^m$. La division euclidienne de m par k donne l'existence de $(q, r) \in \mathbb{N}\times\mathbb{N}$ tel que $m = kq + r$ et $0 \le r < k$. On a donc $x^r = x^{m-kq} = x^m.(x^k)^{-q}$. Comme x^m et x^k appartiennent à H il en est donc de même pour x^r; par suite, par définition de k, on a $r = 0$, soit $y = (x^k)^m$ donc $H \subset \langle x^k \rangle$, sous-groupe engendré par x^k. L'inclusion inverse étant évidente il en résulte que H est cyclique et engendré par x^k.

Considérons d'autre part l'ensemble $A' = \{m \in \mathbb{Z} / x^m \in H\}$: c'est un sous-groupe de $\mathbb{Z}$. D'après l'exercice 7 il est engendré par k : $A' = k\mathbb{Z}$. Comme $x^n = e$ on a $n \in A'$ soit k divise n. Il existe donc $d \in \mathbb{N}$ tel que $n = kd$.

Si $(x^k)^p = e$ on a $x^{kp} = e$ ce qui équivaut à kp multiple de $n = kd$ ou encore p multiple de d. Par conséquent l'élément x^k est d'ordre $d = n/k$ et $\text{Card}(H) = d = n/k$.

(ii) Soit q un diviseur de n. Si H est sous-groupe d'ordre q c'est nécessairement le sous-groupe engendré par $x^{n/q}$ d'après le (i).

Inversement le sous-groupe engendré par $x^{n/q}$ est d'ordre $n/(n/q) = q$ d'après la fin de la démonstration de (i) ce qui achève la démonstration du (ii).

Par exemple les sous-groupes de $\mathbb{Z}/6\mathbb{Z}$ ont ceux engendrés par $\overline{1}$ ($\mathbb{Z}/6\mathbb{Z}$), $\overline{2}$ ($2\mathbb{Z}/6\mathbb{Z}$), $\overline{3}$ ($3\mathbb{Z}/6\mathbb{Z}$), et $\overline{6} = \overline{0}$ ($\{\overline{0}\}$).

Exercice 28

Dans les conditions du théorème, montrer que pour tout entier naturel d l'ordre de x^d est $n/\text{pgcd}(d, n)$.