1.2 Sous-groupes

Définition : soit H une partie stable d'un groupe G (i.e pour tout x et y éléments de H, xy appartient à H). On dit que H est un *sous-groupe* de G ssi H muni de la loi induite par celle de G est un groupe.

Caractérisation pratique : une partie H d'un groupe G est un sous-groupe de G ssi

(i) $H \neq \emptyset$

(ii) $\forall (x, y) \in H \times H, xy^{-1} \in H$.

On peut remplacer la deuxième condition par les deux suivantes : (ii) $\forall (x, y) \in H \times H, xy \in H$ et

(ii)' $\forall\, x \in H, x^{-1} \in H$.

Exercice 6

L'intersection d'une famille quelconque de sous-groupes de G est un sous-groupe de G.

Exercice 7

1°/ Montrer que les sous-groupes H de $\mathbb{Z}$ sont de la forme $H = n\mathbb{Z}$ ($n \in \mathbb{Z}$) (où $n = \{nx / x \in \mathbb{Z}\}$).

De plus, si $H \neq \{0\}$, on peut prendre pour n le plus petit élément de H strictement positif.

2°/ Si a et b sont deux entiers relatifs non nuls montrer que $a\mathbb{Z} + b\mathbb{Z} = \delta\mathbb{Z}$, où $\delta = \text{pgcd}(a, b)$ ($a\mathbb{Z} + b\mathbb{Z}$ désigne l'ensemble $\{ax + by / x \text{ et } y \in \mathbb{Z}\}$). Généraliser à n entiers.

En déduire le *théorème de Bezout* : a et b sont premiers entre eux ssi il existe $(u, v) \in \mathbb{Z}\times\mathbb{Z}$ tel que :

$$au + bv = 1.$$

Plus généralement n entiers $a_1, a_2, \ldots, a_n$ non nuls sont premiers entre eux dans leur ensemble ssi il existe $(u_1, u_2, \ldots, u_n) \in \mathbb{Z}^n$ tel que $a_1u_1 + a_2u_2 + \ldots + a_nu_n = 1$.

3°/ Déduire du théorème de Bezout :

si a divise bc et si est a premier avec b, alors a divise c (*théorème de Gauss*);

si a est premier avec b et avec c alors il est premier avec leur produit bc.

si a et b divisent c si a et b sont premiers entre eux alors ab divise c.

Définition : soit A une partie d'un groupe G. On appelle *sous-groupe engendré par A* l'intersection de tous les sous-groupes de G contenant A.

On le note $\text{Gr}(A)$ et si $A = \{a_1, a_2,\ldots,a_n\}$, $\text{gr}(A)$ se note $< a_1, a_2,\ldots,a_n >$. Le sous-groupe engendré par A est *le plus petit (au sens de l'inclusion) sous-groupe de G contenant A.*

Exemples : $\text{Gr}(\emptyset) = \{e\}$; $\text{Gr}(2; 3) = \mathbb{Z}$ et plus généralement $\text{Gr}(a, b) = \text{pgcd}(a,b)\mathbb{Z}$ (voir exercice 7); les demi-tours engendrent $\text{Is}^+(E)$, groupe des déplacements de l'espace; les réflexions engendrent $\text{Is}(P)$, groupe des isométries du plan; S_n (groupe symétrique) est engendré par les transpositions, les cycles; il est aussi engendré par les n–1 transpositions (1; 2), (1; 3), ... , (1, n) ou : (1,2), (2, 3), ... , (n–1, n).

Exercice 8

Montrer que si A est un ensemble non vide on a : $\text{Gr}(A) = \{a_1a_2 \ldots a_n / n \in \mathbb{N} \text{ et } a_i \in A \text{ ou } a_i^{-1} \in A\}$. En particulier $<a> = \{a^n / n \in \mathbb{Z}\}$.