

1.1 Définitions

Un ensemble G muni d'une loi de composition interne $*$ est un *groupe* ssi :

- (i) $*$ est associative
- (ii) $*$ possède un élément neutre e
- (iii) tout élément de G admet un symétrique pour la loi $*$

Si la loi $*$ est commutative on dit que le groupe G est *commutatif* ou *abélien*. On note en général la loi du groupe multiplicativement : $x * y = x.y = xy$; le symétrique d'un élément x se note alors x^{-1} et l'élément neutre e . Si le groupe est commutatif on note additivement la loi : $x * y = x + y$; le symétrique d'un élément x se note dans ce cas $-x$ et l'élément neutre 0 .

On peut définir dans un groupe x^n par récurrence en posant $x^0 = e$ et $x^{n+1} = x^n x$ si $n \in \mathbb{N}$ et $x^n = (x^{-n})^{-1}$ si $n \in \mathbb{Z}^-$. On notation additive on définirait de même nx pour $n \in \mathbb{Z}$.

Exemples : $(\mathbb{Z}, +)$, $(\mathbb{R}, +)$, $(\mathbb{R}^*, \times)$ sont des groupes commutatifs.

$(S(E), \circ)$, où $S(E)$ désigne l'ensemble des bijections de l'ensemble E dans lui-même, est un groupe, non commutatif si $\text{Card } E \geq 3$, appelé *groupe symétrique*. On note S_n pour $E = \{1, \dots, n\}$.

Exercice 1

1°/ Dans $\mathbb{Z}$ la relation R_n définie par : $x R_n y \Leftrightarrow \exists k \in \mathbb{Z} / x - y = kn$ (où n est un entier relatif donné) est une relation d'équivalence (appelée « *congruence modulo n* »); on note $x \equiv y (n)$. L'ensemble quotient se note $\mathbb{Z}/n\mathbb{Z}$ (*ensemble des entiers relatifs modulo n*) et possède $|n|$ éléments si $n \neq 0$.

2°/ Montrer que cette relation est compatible avec l'addition et la multiplication et que $(\mathbb{Z}/n\mathbb{Z}, +)$ est un groupe commutatif.

3°/ Montrer que $(\mathbb{Z}/n\mathbb{Z} - \{\bar{0}\}, \times)$ est un groupe ssi n est un nombre premier.

4°/ On note $\mathbb{Z}/n\mathbb{Z}^*$ l'ensemble des éléments *inversibles* de $\mathbb{Z}/n\mathbb{Z}$. Montrer que si n est distinct de 1, $(\mathbb{Z}/n\mathbb{Z}^*, \times)$ est un groupe commutatif.

Exercice 2

Soit $\mathcal{F}$ une figure du plan. Montrer que l'ensemble des isométries du plan laissant $\mathcal{F}$ globalement invariante est un groupe pour la composition des applications.

Exercice 3

Trouver tous les groupes à 2, 3 et 4 éléments (dresser leur table de composition).

Exercice 4

Soit $(G, .)$ un groupe et a un élément de G . Montrer que les applications δ_a et γ_a de G dans G définie par $\delta_a(x) = ax$ et $\gamma_a(x) = xa$ pour tout x de G sont bijectives (δ_a et γ_a sont appelées respectivement *translations à gauche* et *translations à droite*).

Application : si p est un nombre premier et si a est un entier naturel premier avec p alors on a :

$$a^{p-1} \equiv 1 (p) \quad (\text{Théorème de Fermat}) \text{ (raisonner dans le groupe } (\mathbb{Z}/p\mathbb{Z} - \{\bar{0}\}, \times)).$$

Exercice 5

Soit p un entier naturel ≥ 2 . Montrer que :

p premier $\Leftrightarrow (p-1)! + 1 \equiv 0 (p)$ (Théorème de Wilson) (pour la condition nécessaire rechercher dans $\mathbb{Z}/p\mathbb{Z}$ les éléments égaux à leur inverse puis considérer $\bar{1} \times \bar{2} \times \dots \times \bar{p-1}$).