Arithmétique

Groupe

Groupe symétrique

— Définition

Définition

Tribus :

Soit Ω un ensemble non vide, appelé un ensemble universel. On appelle Tribu (ou σ-algèbre sur Ω un ensemble A de parties de Ω donc un sous-ensemble $A \subset P(\Omega)$) tel que :

+ $\Omega \in A$
+ A est stable par passage au complémentaire :

Groupes Exo

Ex 5 Partiel :

a) Soit $n \geq 1$ un entier. Rappeler la définition du groupe $(\mathbb{Z}/n\mathbb{Z})^\times$.
b) Dresser la liste des éléments du groupe $(\mathbb{Z}/18\mathbb{Z})^\times$.
c) Calculer les ordres des groupes $(\mathbb{Z}/8\mathbb{Z})^\times$, $(\mathbb{Z}/27\mathbb{Z})^\times$ et $(\mathbb{Z}/216\mathbb{Z})^\times$.
d) Déterminer l'ordre de la classe de 2 et celui de la classe de 8 dans le groupe $(\mathbb{Z}/27\mathbb{Z})^\times$. Ce groupe est-il cyclique ?
e) Montrer qu'il existe un unique morphisme de groupes de $(\mathbb{Z}/12\mathbb{Z}, +)$ vers $(\mathbb{Z}/27\mathbb{Z})^\times$ qui envoie la classe de 1 sur celle de 8. Déterminer son noyau et son image.

b) $(\mathbb{Z}/18\mathbb{Z})^*$

$\bar{1}$ 2 3 4 $\bar{5}$ 6 $\bar{7}$ 8 9 10 $\bar{11}$ 12 $\bar{13}$ 14 15 16 $\bar{17}$

Liste :

$\bar{1}, \bar{5}, \bar{7}, \bar{11}, \bar{13}, \bar{17}$

Le nombre de cardinal :

$$|(\mathbb{Z}/18\mathbb{Z})^*| = \varphi(18) = \varphi(2.9)$$
$$= \varphi(2) \times \varphi(9)$$
$$= \varphi(2)\varphi(3^2)$$
$$= (2^1-2^{1-1})(3^2-3^{2-1})$$
$$= 1.6 = 6$$

3) Calculer les ordres de $(\mathbb{Z},8\mathbb{Z})^*$, $(\mathbb{Z},27\mathbb{Z})^*$ $(\mathbb{Z},216\mathbb{Z})^*$

On a $|(\mathbb{Z}/n\mathbb{Z})^*| = \varphi(n)$, $\varphi(nm) = \varphi(n)\varphi(m)$ si pgcd $(n,m) = 1$ et $\varphi(p^e) = p^e - p^{e-1}$ si p est premier et $e \geq 1$ un entier

$$|(\mathbb{Z}/8\mathbb{Z})^\times| = \varphi(2^3) = (2^3 - 2^{3-1}) = 8 - 4 = 4$$

$$|(\mathbb{Z}/27\mathbb{Z})^\times| = \varphi(3^3) = (3^3 - 3^{3-1}) = 18$$

$$|(\mathbb{Z}/216\mathbb{Z})^\times| = \varphi(2^3 \times 3^3) = \varphi(2^3)\,\varphi(3^3)$$

$$\begin{array}{r|l} 216 & 2 \\ 108 & 2 \\ 54 & 2 \\ 27 & 3 \\ 9 & 3 \\ 3 & 3 \\ 1 & \end{array}$$

$$= (2^3 - 2^{3-1})(3^3 - 3^{3-1})$$
$$= (2^3 - 2^2)(3^3 - 3^2)$$
$$= 4 \times 18 = 72$$

d_p La classe de 2 = 2 mod 27 dans le groupe $(\mathbb{Z}/27\mathbb{Z})^\times$

Calculons les puissances de $\overline{2}^{27}$ dans $(\mathbb{Z}/27)^\times$

k	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18
$\overline{2}^k$	$\overline{2}$	$\overline{4}$	$\overline{8}$	$\overline{16}$	$\overline{5}$	$\overline{10}$	$\overline{20}$	$\overline{40}$	$\overline{-1}$	$\overline{-2}$	$\overline{-4}$	$\overline{-8}$	$\overline{-16}$	$\overline{-5}$	$\overline{-10}$	$\overline{-20}$	$\overline{-40}$	$\overline{1}$

Il s'ensuit que $\overline{2}$ est d'ordre 18.

Dans ce tableau, nous voyons aussi les puissances

$$\overline{8}^m = \overline{2^{3m}} \Leftarrow (8 = 2^3)$$

k	1	2	3	4	5	6
$\overline{8}^k$	$\overline{8}$	$\overline{10}$	$\overline{-1}$	$\overline{-8}$	$\overline{-10}$	$\overline{1}$

$\Rightarrow$ $\overline{8}$ est d'ordre 6

Soit G un groupe fini d'ordre p un nombre premier. Alors G est cyclique

Comme $\overline{2}$ est d'ordre 18 et $|(\mathbb{Z}/27)^{\times}| = 18$,

$\Rightarrow$ le groupe $(\mathbb{Z}/27\mathbb{Z})^{\times}$ est formé des puissances de $\overline{2}$. Donc $\overline{2}$ est un générateur de ce groupe et $(\mathbb{Z}/27\mathbb{Z})^{\times}$ est bien un groupe cyclique

e) Nous avons vu dans d) que nous avons $\overline{8}^{6} = \overline{-1}$ dans $(\mathbb{Z}/27\mathbb{Z})^{\times}$. Donc nous avons $\overline{8}^{12} = (\overline{8}^{6})^{2} = \overline{1}$

Par le lemme 2.26 du cours, il existe un unique morphisme de groupes

$$f : (\mathbb{Z}/12\mathbb{Z}, +) \longrightarrow (\mathbb{Z}/27\mathbb{Z})^{\times}$$

tel que $f({}^{12}\overline{1}) = {}^{27}\overline{8}$ et nous avons $f(\overline{k}) = \overline{8}^{k}$ pour tout $k \in \mathbb{Z}$. Nous obtenons la table

${}^{n}\overline{k}$	0	1	2	3	4	5	6	7	8	9	10	11
$f(\overline{k})$	$\overline{1}$	$\overline{8}$	$\overline{10}$	$\overline{-1}$	$\overline{-8}$	$\overline{-10}$	$\overline{1}$	$\overline{8}$	$\overline{10}$	$\overline{-1}$	$\overline{-8}$	$\overline{-10}$

$\operatorname{Im} f = \{\overline{1}, \overline{8}, \overline{10}, \overline{-1}, \overline{-8}, \overline{-10}\}$

$\ker f = \{\overline{0}, \overline{6}\}$

$\Rightarrow |\operatorname{Im} f| \cdot |\ker f| = |\mathbb{Z}/12\mathbb{Z}|$