Définition

Soient H, K sous-groupes de G avec $H \triangleleft G$. G est produit semi-direct (interne) de H par K si une des conditions équivalentes est vérifiée

$H \cap K = \{e\}$ et $G = HK$

- Tout élément de $g \in G$ s'écrit de manière unique $g = hk$ avec $h \in H$ et $k \in K$
- $K \simeq G/H$ via la surjection canonique $k \mapsto kH$

On note $G = H \rtimes K$.

Résultat. On a aussi $G = KH$ et donc $G = K \ltimes H$.

Si on a aussi $K \triangleleft G$, on dit que c'est un produit direct.

Dans ce cas, pour tout $k \in K$ et $h \in H$, on a $kh = hk$ et l'application $H \times K \to G$ définit par

$$(h, k) \mapsto hk$$

est un isomorphisme.

3. Quelques groupes particuliers

Lemme

Soit G un groupe monogène. Si G est infini alors $G \simeq \mathbb{Z}$, sinon G est cyclique et $G \simeq \mathbb{Z}/n\mathbb{Z}$ avec n l'ordre de G.

Proposition

Soit $\bar{m} \in \mathbb{Z}/n\mathbb{Z}$. L'ordre de $\bar{m}$ est $n/\mathrm{PGCD}(m,n)$ donc $\bar{m}$ est générateur ssi n et m sont premiers entre eux ssi m est inversible modulo n

Définition

L'ensemble des inversibles modulo n forme un groupe multiplicatif

$$(\mathbb{Z}/n\mathbb{Z})^* = \{\bar{m} \text{ tel que } \mathrm{PGCD}(m,n) = 1\}$$

d'ordre $\varphi(n)$ (fonction indicatrice d'Euler).

Théorème (Théorème des restes chinois)

Soient n et m deux entiers ≥ 1 et premiers entre eux, on a les isomorphismes naturels

$$\mathbb{Z}/nm\mathbb{Z} \simeq \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z} \quad \text{et} \quad (\mathbb{Z}/nm\mathbb{Z})^* \simeq (\mathbb{Z}/n\mathbb{Z})^* \times (\mathbb{Z}/m\mathbb{Z})^*$$

Problème : $b \in \mathbb{Z}/n\mathbb{Z}$, $c \in \mathbb{Z}/m\mathbb{Z}$, trouver $a \in \mathbb{Z}/nm\mathbb{Z}$ avec $\begin{cases} a \equiv b \ [n] \\ a \equiv c \ [m] \end{cases}$

Nombres d'éléments d'ordre donné dans un groupe cyclique

Soit G un groupe cyclique d'ordre n.

1. Soit $d \geq 1$ un entier. Déterminer le nombre d'éléments d'ordre d dans G.
2. En déduire la formule $\sum_{d|n} \varphi(d) = n$.

Le but de cet exercice est de déterminer la structure du groupe $\mathrm{Aut}((\mathbb{Z}/22\mathbb{Z})^*)$ des automorphismes de $(\mathbb{Z}/22\mathbb{Z})^*$.

1. Déterminer l'ordre de $(\mathbb{Z}/22\mathbb{Z})^*$.
2. Montrer que $\bar{7}$ est un générateur de $(\mathbb{Z}/22\mathbb{Z})^*$. En déduire que $(\mathbb{Z}/22\mathbb{Z})^*$ est cyclique.
3. En déduire tous les sous-groupes de $(\mathbb{Z}/22\mathbb{Z})^*$.
4. Déterminer tous les générateurs de $(\mathbb{Z}/22\mathbb{Z})^*$.
5. Déterminer tous les automorphismes de $(\mathbb{Z}/22\mathbb{Z})^*$.
6. Écrire la table de multiplication de $\mathrm{Aut}((\mathbb{Z}/22\mathbb{Z})^*)$ et en déduire que $\mathrm{Aut}((\mathbb{Z}/22\mathbb{Z})^*)$ est isomorphe à $\mathbb{Z}/4\mathbb{Z}$.

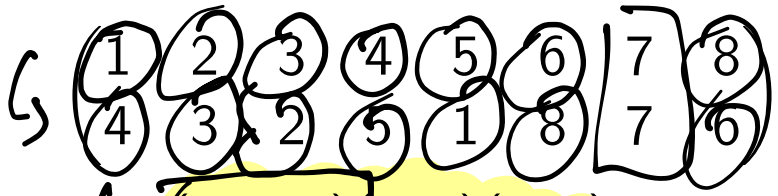
Définition

Soit $n \geq 1$, on appelle groupe symétrique sur n lettres, l'ensemble $S_n = \mathrm{Bij}(\{1, \cdots n\})$. C'est un groupe pour la composition et son ordre est $n! = 1 \times 2 \times \cdots \times n$.

éléments : permutations

Exemple

Les permutations peuvent s'écrire de deux manières essentiellement



(écriture sur deux lignes)

$(1,4,5)(2,3)(6,8) = -1$

(produit de cycles disjoints)

Remarques

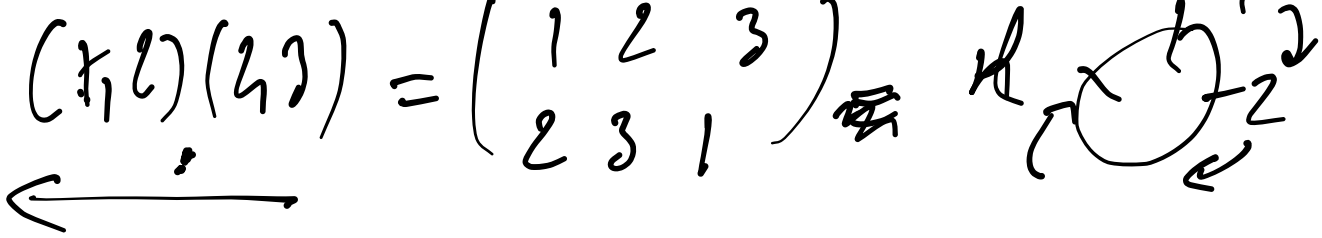
- *La multiplication se fait de droite à gauche* $(1,2)(2,3) = (1,2,3)$
- *On a* $(a_1, a_2, \ldots, a_s) = (a_2, a_3, \ldots, a_s, a_1) = \cdots = (a_s, a_1, \ldots, a_{s-1})$

Un cycle de longueur ℓ est un ℓ-cycle et on appelle un 2-cycle une transposition.

Résultat.

Les transpositions engendrent S_n.

$n=3$ $(1\,2)(2\,3) = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$



Lemme

L'ordre d'un ℓ-cycle est ℓ. L'ordre d'une permutation écrit comme produit de cycles disjoints est le PPCM des longueurs des cycles.

$\mathrm{sign}(\sigma\pi) = \mathrm{sign}(\sigma)\,\mathrm{sign}(\pi)$

Proposition

Il existe un unique morphisme $\mathrm{sign} : S_n \to \{\pm 1\}$ *non trivial. On l'appelle la signature. Soit c un ℓ-cycle, on a* $\mathrm{sign}(c) = (-1)^{\ell+1}$.
Une permutation π est paire si $\mathrm{sign}(\pi) = 1$ *et impaire si* $\mathrm{sign}(\pi) = -1$.
Le groupe des permutations paires ($=$ noyau de sign*) est le groupe alterné, noté A_n. Son ordre est $n!/2$.*
C'est le seul sous-groupe d'ordre $n!/2$ dans S_n.

G groupe fini abélien plus G est simple si $G \simeq \mathbb{Z}/p\mathbb{Z}$ p premier

Remarque

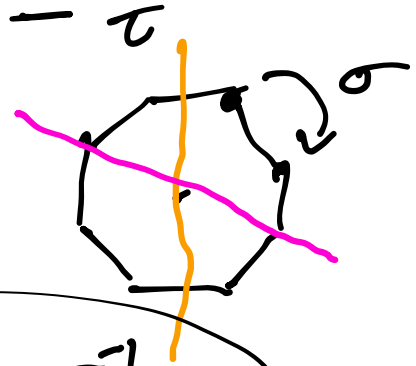
Un groupe G dont les seuls sous-groupes distingués sont $\{e\}$ et lui-même est un groupe simple. Le plus petit groupe simple non abélien est A_5 d'ordre 60 et pour tout $n \geq 5$, le groupe A_n est simple.

Soit $n \geq 3$. Le groupe diédral D_{2n} est le groupe des isométries du plan qui fixe un polygone régulier à n côtés.

C'est un groupe d'ordre $2n$ engendré par la rotation qui envoie un sommet sur le sommet suivant et une des symétries axiales ~~passant par un des sommets~~.

De manière abstraite, D_{2n} est le groupe engendré par σ et τ avec les relations

$$\sigma^n = e, \quad \tau^2 = e, \quad \tau\sigma\tau = \sigma^{-1}.$$



On a alors

- Pour tout entier i, $\tau\sigma^i\tau = \sigma^{-i}$.
- Pour tout entier i, l'élément $\tau\sigma^i$ est d'ordre 2.
- Les éléments de D_{2n} sont exactement les éléments

$$e, \sigma, \ldots, \sigma^{n-1}, \tau, \tau\sigma, \ldots, \tau\sigma^{n-1}.$$

$$D_{2n} \simeq \langle \tau \rangle \rtimes \langle \sigma \rangle \simeq \mathbb{Z}/2\mathbb{Z} \rtimes \mathbb{Z}/n\mathbb{Z}$$

4. Actions de groupe

Définition

Une action du groupe G sur un ensemble X est la donnée d'un morphisme $\Phi : G \to \mathrm{Bij}(X)$ (= groupe pour la composition).

En général, on écrit $g \cdot x$ plutôt que $\Phi(g)(x)$ pour $g \in G$ et $x \in X$, d'où

$$\forall x \in X,\ e \cdot x = x \quad \text{et} \quad \forall g, g' \in G, x \in X,\ (gg') \cdot x = g \cdot (g' \cdot x).$$

Définition

Pour $x \in X$, on pose

- $O(x) = \Omega_x = \{g \cdot x : g \in G\}$ est l'orbite de x.
- $S(x) = G_x = \{g \in G \text{ tel que } g \cdot x = x\}$ est le stabilisateur de x (sous-groupe de G)

Le noyau de l'action est l'intersection des stabilisateurs.

On note X/G l'ensemble des orbites de X.

L'action est transitive s'il existe une seule orbite.

L'action est fidèle si le noyau est trivial.

Lemme

Soit K le noyau de l'action alors K est distingué et G/K hérite d'une action fidèle sur X

Théorème (Cayley)

Soit G un groupe d'ordre n. Alors G est isomorphe à un sous-groupe de S_n.

Théorème (Formules des classes)

Deux orbites sont ou bien égales, ou bien disjointes, et donc

$$\mathrm{card}(X) = \sum_{\Omega \in X/G} \mathrm{card}(\Omega)$$

Soit $x \in X$, on a

$$\mathrm{card}(\Omega_x) = \frac{|G|}{|G_x|}$$

Soit R un système de représentants des orbites de X, on a

$$\mathrm{card}(X) = \sum_{x \in R} \frac{|G|}{|G_x|}$$

Quelques résultats sur les p-groupes

Un p-groupe, avec p premier, est un groupe fini dont l'ordre est une puissance (non triviale) de p.

1. Soit G un p-groupe. On montre que $Z(G)$ n'est pas réduit à $\{e\}$.

   1.1 Soit X un ensemble fini sur lequel G agit. On note X^G l'ensemble des points fixes de X sous cette action. Montrer que

   $$\mathrm{card}(X) \equiv \mathrm{card}(X^G) \pmod{p}.$$

   1.2 Déterminer une action de G pour laquelle l'ensemble des points fixes est $Z(G)$, puis conclure.

2. Soit G un groupe fini. On suppose que $G/Z(G)$ est un groupe cyclique. Montrer que G est abélien.

   En déduire la structure des groupes d'ordre p^2 avec p premier.

Sous-groupes d'indice p avec p plus petit facteur premier de $|G|$

1. Soit H un sous-groupe d'indice 2 dans G. Montrer que $H \triangleleft G$.
2. Soit G un groupe fini. Soit p le plus petit premier divisant $|G|$.
   Soit H sous-groupe d'indice p, on montre que $H \triangleleft G$.
   On considère l'action de G sur G/H par multiplication à gauche.
   - 2.1 Montrer que cette action est transitive.
   - 2.2 Soit K le noyau de l'action. Montrer que $K \subseteq H$.
   - 2.3 Montrer que G/K est isomorphe à un sous-groupe de S_p.
   - 2.4 En déduire que $H = K$ et le résultat.