1 Généralités

[Groupe] Un groupe $(G, *)$ est un ensemble G muni d'une loi de composition interne $*$ vérifiant :

1. Associativité : $\forall a, b, c \in G, (a * b) * c = a * (b * c)$
2. Élément neutre : $\exists e \in G, \forall a \in G, a * e = e * a = a$
3. Symétrique : $\forall a \in G, \exists b \in G, a * b = b * a = e$

— $(, +)$ est un groupe

— $(^*, \times)$ est un groupe

— $(\mathcal{S}_n, \circ)$ le groupe symétrique

2 Théorèmes fondamentaux

[Lagrange] Soit G un groupe fini et H un sous-groupe de G. Alors $|H|$ divise $|G|$.

[Cauchy] Si G est fini d'ordre divisible par un premier p, alors G contient un élément d'ordre p.

[Sylow] Soit $|G| = p^a m$ avec $p \nmid m$. Alors :

1. Il existe des sous-groupes d'ordre p^a (p-Sylow)
2. Tous les p-Sylow sont conjugués
3. Leur nombre n_p vérifie $n_p \equiv 1 \pmod{p}$ et $n_p \mid m$

3 Exercices

Montrer qu'un groupe d'ordre p^2 (p premier) est abélien.
Par analyse des classes de conjugaison et utilisation du théorème de Sylow.
Anneaux et corps

4 Définitions

[Anneau] $(A, +, \times)$ est un anneau si :

1. $(A, +)$ est un groupe abélien
2. $\times$ est associative, distributive sur $+$, et possède un neutre 1_A

[Morphisme d'anneaux] Une application $f : A \to B$ est un morphisme si :

1. $f(a + b) = f(a) + f(b)$
2. $f(a \times b) = f(a) \times f(b)$
3. $f(1_A) = 1_B$

5 Exercices

Montrer que $[i] = \{a + ib \mid a, b \in\}$ est un sous-anneau de .
Vérification directe des propriétés des sous-anneaux.
Arithmétique

6 Théorèmes fondamentaux

[Bézout] $\forall a, b \in^*, \exists u, v \in$ tels que $au + bv = a \wedge b$
[Gauss] Si $a \mid bc$ et $a \wedge b = 1$, alors $a \mid c$
[Euler-Fermat] Pour $a \wedge n = 1$:

$$a^{\varphi(n)} \equiv 1 \pmod{n}$$

En particulier pour p premier :

$$a^{p-1} \equiv 1 \pmod{p}$$

7 Exercices

Résoudre $x^2 \equiv -1 \pmod{5^k}$ pour $k \geq 1$.
Par récurrence et lemme de Hensel.
Applications avancées

8 Théorème chinois

[Restes chinois] Si $m \wedge n = 1$ alors :

$$/mn \simeq /m \times /n$$

Résoudre :

$$\begin{cases} x \equiv 2 \pmod{3} \\ x \equiv 3 \pmod{5} \\ x \equiv 2 \pmod{7} \end{cases}$$

Par substitutions successives : solution $x \equiv 23 \pmod{105}$.

9 Groupes abéliens finis

[Classification] Tout groupe abélien fini est isomorphe à :

$$\prod_{i=1}^{k} /d_i \text{ avec } d_1 \mid \cdots \mid d_k$$

Les groupes d'ordre 8 : $/8$, $/4 \times /2$, $(/2)^3$

10 Exercices finals

[Wilson] Montrer que pour p premier : $(p-1)! \equiv -1 \pmod{p}$
En associant chaque élément avec son inverse dans $/p$.
Montrer qu'un groupe d'ordre 15 est cyclique.
Analyse des p-Sylow et produit direct.