Séance 1 : Rappel sur les structures algébriques fondamentales

Hervé Talé Kalachi

1 Théorie des groupes

1.1 Définitions de groupe et de sous-groupe

Définition 1.1 (Groupe)**.** Un **groupe** $(G, *)$ est un ensemble muni d'une opération binaire $*$ telle que :

— **Associativité** : $\forall a, b, c \in G,\ (a * b) * c = a * (b * c)$.

— **Élément neutre** : $\exists e \in G,\ \forall a \in G,\ a * e = e * a = a$.

— **Inverse** : $\forall a \in G,\ \exists b \in G,\ a * b = b * a = e$.

Définition 1.2 (Sous-groupe)**.** Soit $(G, *)$ un groupe. Une partie H de G est dite **sous-groupe** de $(G, *)$ si la structure de G induit sur H une structure de groupe, On note alors $H \leq G$.

Théorème 1.1 (Critère de sous-groupe)**.** Une partie $H \subseteq G$ est un sous-groupe de G si et seulement si :

1. $H \neq \varnothing$,
2. $\forall a, b \in H,\ a * b^{-1} \in H$.

Démonstration. Exercice □

1.2 Groupes cycliques et générateurs

Définition 1.3 (Groupe cyclique)**.** Un groupe $(G, *)$ est dit **cyclique** s'il existe un élément $g \in G$ tel que

$$G = \{g^n : n \in \mathbb{Z}\}.$$

L'élément g est appelé **générateur** de G.

Exemple 1.1. Le groupe $(\mathbb{Z}/7\mathbb{Z}, +)$ est cyclique car tout élément peut s'écrire comme une somme répétée de 1. Ici, 1 est un générateur.

Remarque 1.1. Dans un groupe cyclique fini d'ordre n, tout générateur g vérifie $g^n = e$, et l'ordre de tout élément divise n (résultat découlant du théorème de Lagrange).

1.3 Théorème de Lagrange et preuve (esquisse)

Théorème 1.2 (Lagrange)**.** Soit G un groupe fini et H un sous-groupe de G. Alors, l'ordre (le nombre d'éléments) de H divise l'ordre de G.

Esquisse de preuve. Considérons l'ensemble des classes à gauche de H dans G :

$$\{gH : g \in G\}.$$

Ces classes forment une partition de G. De plus, pour tout $g \in G$, la classe gH a exactement le même nombre d'éléments que H. Ainsi, si k est le nombre de classes, on a :

$$|G| = k \cdot |H|.$$

Par conséquent, $|H|$ divise $|G|$. □

2 Anneaux et corps

2.1 Définitions et propriétés

Définition 2.1 (Anneau)**.** Un **anneau** $(A, +, \times)$ est un ensemble muni de deux opérations telles que :

- $(A, +)$ est un groupe abélien.
- La multiplication est associative et distributive par rapport à l'addition.
- Un élément neutre multiplicatif 1 peut exister (ceci n'est pas exigé pour tous les anneaux).

Définition 2.2 (Corps)**.** Un **corps** est un anneau commutatif muni d'un neutre multiplicatif dans lequel tout élément non nul possède un inverse pour la multiplication.

2.2 Exemples dans le cas fini

Théorème 2.1. $\mathbb{Z}/p\mathbb{Z}$ est un corps si et seulement si p est un nombre premier.

Preuve. **(Si)** Supposons p premier. Soit $\overline{a}$ un élément non nul dans $\mathbb{Z}/p\mathbb{Z}$. Comme p est premier, les entiers a et p sont premiers entre eux, ce qui garantit l'existence d'entiers x et y tels que :

$$ax + py = 1.$$

En passant au modulo p, on obtient :

$$ax \equiv 1 \mod p,$$

donc $\overline{x}$ est l'inverse de $\overline{a}$ dans $\mathbb{Z}/p\mathbb{Z}$.

(Seulement si) Supposons que $\mathbb{Z}/n\mathbb{Z}$ soit un corps. Si n n'était pas premier, il existerait des entiers a et b, avec $1 < a, b < n$, tels que n divise ab. Dans $\mathbb{Z}/n\mathbb{Z}$, cela signifierait que $\overline{a} \neq \overline{0}$ et $\overline{b} \neq \overline{0}$, mais $\overline{a} \times \overline{b} = \overline{0}$, ce qui contredit le fait que tout élément non nul doit être inversible dans un corps. □

Corollaire 2.1 (Petit théorème de Fermat)**.** Soit p un nombre premier et $a \in \mathbb{Z}$ tel que $p \nmid a$. Alors :

$$a^{p-1} \equiv 1 \mod p.$$

2.3 Exemples sur les corps finis

Exemple 2.1. La construction de $\mathbb{F}_2$ (corps à deux éléments) est donnée par les tables :

$+$	0	1
0	0	1
1	1	0

$\times$	0	1
0	0	0
1	0	1

3 Applications calculatoires

3.1 Inversion modulaire

Algorithme d'Euclide étendu :

Input: $a, n \in \mathbb{N}$
Output: $a^{-1} \mod n$ si existe
$old\_r, r \leftarrow a, n$;
$old\_s, s \leftarrow 1, 0$;
while $r \neq 0$ **do**
    quotient $\leftarrow \lfloor old\_r / r \rfloor$;
    $(old\_r, r) \leftarrow (r, old\_r - quotient \times r)$;
    $(old\_s, s) \leftarrow (s, old\_s - quotient \times s)$;
end
if $old\_r > 1$ **then**
    return "Pas inversible";
end
return $old\_s \mod n$;

Algorithm 1: Algorithme d'inversion modulaire

3.2 Implémentation en Python

```python
def inverse_mod(a, n):
    old_r, r = a, n
    old_s, s = 1, 0
    while r != 0:
        quotient = old_r // r
        old_r, r = r, old_r - quotient * r
        old_s, s = s, old_s - quotient * s
    if old_r > 1:
        return None  # a n'est pas inversible modulo n
    return old_s % n

# Test : dans Z/13Z, 4*10 = 40 = 1 mod 13
print(inverse_mod(4, 13))
```

4 Exercices

4.1 Exercices sur les groupes

Exercice 4.1 (Groupe multiplicatif)**.** Montrer que $(\mathbb{Z}/9\mathbb{Z})^{\times} = \{1, 2, 4, 5, 7, 8\}$ forme un groupe pour la multiplication modulo 9.

Exercice 4.2 (Groupe cyclique)**.** Montrer que $((\mathbb{Z}/p\mathbb{Z})^*, \times)$ est cyclique pour tout nombre premier p. Identifier un générateur.

4.2 Exercices sur les anneaux et corps

Exercice 4.3 (Inverse modulaire et petit théorème de Fermat)**.** Soit p un nombre premier et $a \in \{1, 2, \dots, p-1\}$. Vérifiez numériquement que l'inverse de a dans $\mathbb{Z}/p\mathbb{Z}$ est donné par a^{p-2}, c'est-à-dire que :

$$a \times a^{p-2} \equiv 1 \mod p.$$

Exercice 4.4 (Équations de congruence)**.** Résoudre l'équation suivante dans $\mathbb{Z}/11\mathbb{Z}$:

$$3x + 4 \equiv 2 \mod 11.$$

Indice : Calculez d'abord l'inverse modulaire de 3 modulo 11.

4.3 Exercices complémentaires

Exercice 4.5 (Table d'opérations)**.** Construisez la table de multiplication du groupe $(\mathbb{Z}/7\mathbb{Z})^\times$. Vérifiez que chaque ligne et chaque colonne contient exactement une fois chacun des éléments du groupe.

Exercice 4.6 (Implémentation et test)**.** Écrire une fonction Python qui, pour un entier n, construit la table d'addition de $\mathbb{Z}/n\mathbb{Z}$. Testez-la pour $n = 5$.