Anneaux $\mathbb{Z}/n\mathbb{Z}$. Applications.

Extrait du rapport de jury

Dans cette leçon, l'entier n n'est pas forcément un nombre premier. Il serait bon de connaître les idéaux de $\mathbb{Z}/n\mathbb{Z}$ et, plus généralement, les morphismes de groupes de $\mathbb{Z}/n\mathbb{Z}$ dans $\mathbb{Z}/m\mathbb{Z}$.

Il est nécessaire de bien maîtriser le théorème chinois et sa réciproque. S'ils le désirent, les candidats peuvent poursuivre en donnant une généralisation du théorème chinois lorsque deux éléments ne sont pas premiers entre eux, ceci en faisant apparaître le PGCD et le PPCM de ces éléments.

Il faut bien sûr savoir appliquer le théorème chinois à l'étude du groupe des inversibles et, ainsi, retrouver la multiplicativité de l'indicatrice d'Euler. Toujours dans le cadre du théorème chinois, il est bon de distinguer clairement les propriétés de groupes additifs et d'anneaux, de connaître les automorphismes, les nilpotents et les idempotents.

Enfin, il est indispensable de présenter quelques applications arithmétiques des propriétés des anneaux $\mathbb{Z}/n\mathbb{Z}$, telles que l'étude de quelques équations diophantiennes bien choisies. De même, les applications cryptographiques telles que l'algorithme RSA sont naturelles dans cette leçon.

S'ils le désirent, les candidats peuvent aller plus loin en s'intéressant au calcul effectif des racines carrées dans $\mathbb{Z}/n\mathbb{Z}$.

Plan

I. L'anneau $(\mathbb{Z}/n\mathbb{Z}, +, \times)$

I.1. Construction et premières propriétés

- Les idéaux de $\mathbb{Z}$ sont les $n\mathbb{Z}$ pour $n \in \mathbb{N}$.
- L'anneau $\mathbb{Z}/n\mathbb{Z}$ est le quotient de l'anneau $\mathbb{Z}$ par l'idéal $n\mathbb{Z}$.
- Les idéaux de $\mathbb{Z}/n\mathbb{Z}$ sont les $d\mathbb{Z}/n\mathbb{Z}$ avec $d \mid n$.
- Morphisme d'anneaux de $\mathbb{Z}/m\mathbb{Z}$ dans $\mathbb{Z}/n\mathbb{Z}$.
- Exemple : Si $n = p_1^{\alpha_1} \cdots p_r^{\alpha_r}$ est la décomposition en facteurs premiers de n , alors l'idéal des nilpotents de $\mathbb{Z}/n\mathbb{Z}$ est engendré par $p_1 \cdots p_r$.
- Définition de la relation de congruence sur $\mathbb{Z}$ modulo n . Propriétés.

I.2. Le théorème Chinois

- Théorème Chinois.
- Généralisation : Si $(m, n) \in (\mathbb{N}^*)^2$, l'application $\alpha : \mathbb{Z} \rightarrow \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$ définie par $x \mapsto (\bar{x}, \bar{x})$ est un morphisme d'anneaux de noyau $(m \vee n)\mathbb{Z}$ et on a $\text{Im}(\alpha) = \{(\bar{x}, \bar{y}) \in \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z} \mid x \equiv y [m \wedge n]\}$.
- Application : Résolution d'un système de congruences.

I.3. Le groupe $(\mathbb{Z}/n\mathbb{Z})^\times$

- Un élément $\bar{k} \in \mathbb{Z}/n\mathbb{Z}$ est inversible si et seulement si $k \wedge n = 1$.
- L'anneau $\mathbb{Z}/n\mathbb{Z}$ est un corps si et seulement si n est premier.
- Théorème de Wilson.
- Le groupe $(\mathbb{Z}/n\mathbb{Z})^\times$ est d'ordre $\varphi(n)$.
- Théorème d'Euler et petit théorème de Fermat.
- Exemple : Calcul du reste d'une puissance.
- Application : Test de primalité de Fermat.
- Multiplicativité de l'indicatrice d'Euler.
- Structure du groupe $(\mathbb{Z}/n\mathbb{Z})^\times$.

II. Le groupe $(\mathbb{Z}/n\mathbb{Z}, +)$

II.1. Généralités

- Un groupe G est cyclique si et seulement si $G \simeq \mathbb{Z}/n\mathbb{Z}$ avec $n \in \mathbb{N}^*$.
- Les sous-groupes de $\mathbb{Z}/n\mathbb{Z}$ sont les $d\mathbb{Z}/n\mathbb{Z}$ avec $d \mid n$.
- Morphisme de groupes de $\mathbb{Z}/m\mathbb{Z}$ dans $\mathbb{Z}/n\mathbb{Z}$.
- Les générateurs du groupe $\mathbb{Z}/n\mathbb{Z}$ sont les éléments de $(\mathbb{Z}/n\mathbb{Z})^\times$.
- On a $\text{Aut}(\mathbb{Z}/n\mathbb{Z}) \simeq (\mathbb{Z}/n\mathbb{Z})^\times$.

II.2. Structure des groupes abéliens finis

- Théorème de structure sur les groupes abéliens finis.
- Application : Il y a 3 groupes abéliens d'ordre 120 à isomorphisme près.
- Application : Le groupe $(\mathbb{Z}/n\mathbb{Z})^\times$ est cyclique si et seulement si $n \mid 4$ ou $n = p^k$ ou $n = 2p^k$ avec $k \in \mathbb{N}^*$ et p est un nombre premier impair.

III. Applications

III.1. Le cryptage RSA

- Explication du cryptage RSA.

III.2. La loi de réciprocité quadratique

- Définition du symbole de Legendre d'un élément de $\mathbb{Z}/p\mathbb{Z}$.
- Propriétés élémentaires du symbole de Legendre.
- Symbole de Legendre de -1 et de 2 .
- Loi de réciprocité quadratique.
- Exemples.

III.3. Le théorème de Dirichlet faible

- Théorème de Dirichlet faible.
- Remarque : Théorème de la progression arithmétique de Dirichlet.

III.4. Le théorème des deux carrés

- Anneau des entiers de Gauss.
- L'anneau des entiers de Gauss est euclidien.
- Caractérisation des nombres premiers qui sont la somme de deux carrés.
- Théorème des deux carrés.
- Exemple de décomposition en somme de deux carrés.

Remarques sur le plan

Préciser durant la présentation du plan que le théorème de la progression arithmétique est mentionné pour compléter la version faible, mais que sa démonstration dépasse largement le cadre du programme.

On peut aussi choisir de consacrer une partie à la résolution d'équations diophantiennes explicites.

Développements

Voici une liste non exhaustive de développements possibles pour cette leçon.

- **La loi de réciprocité quadratique.**
- **Le théorème de Dirichlet faible.**
- **Le théorème des deux carrés.**

Bibliographie

- [Com98] F. COMBES – *Algèbre et géométrie*, Bréal, 1998.
- [Gou09] X. GOURDON – *Algèbre, 2^e édition*, Ellipses, 2009.
- [Per96] D. PERRIN – *Cours d'algèbre*, Ellipses, 1996.