Leçon 120 : Anneaux $\mathbb{Z}/n\mathbb{Z}$. Applications.

Développements :

Dirichlet faible, $\mathrm{GL}_2(\mathbb{Z}/n\mathbb{Z})$.

Bibliographie :

Calais (Ca), Combes (Co), Risler Boyer (RB), Perrin (P), Gourdon Alg (Gou), Gozard ou Duverney

Notes

Merci à Matthieu Romagny pour ses corrections.

Plan

Définition 1 (C p.74)**.** Congruence modulo n, c'est une relation d'équivalence

Proposition 2. *Les idéaux/sous-groupes de* $\mathbb{Z}$

1 Structures de $\mathbb{Z}/n\mathbb{Z}$

1.1 Structure de groupe

Définition 3 (RB p.10 ou Ca p. 74)**.** $\mathbb{Z}/n\mathbb{Z}$ par groupe quotient, groupe cyclique de cardinal n, abélien.

Proposition 4 (RB p.11 ou Ca p. 90)**.** *Isomorphisme monogène et cyclique avec* $\mathbb{Z}/n\mathbb{Z}$*.*

Exemple 5 (Ca p.90)**.** Racines de l'unité

1.1.1 Sous-groupes de $\mathbb{Z}/n\mathbb{Z}$

Proposition 6 (RB p.11 ou Ca p.95)**.** *Les sous-groupes de* $\mathbb{Z}/n\mathbb{Z}$

Corollaire 7 (Ca p.95)**.** *Le nb de sg de* $\mathbb{Z}/n\mathbb{Z}$

Exemple 8 (Ca p.95)**.** Les sous-groupes de $\mathbb{Z}/6\mathbb{Z}$

1.1.2 Générateurs de $\mathbb{Z}/n\mathbb{Z}$ et indicatrice d'Euler

Définition 9 (Co p. 59 ou Ca p.99)**.** Indicatrice d'Euler comme nb d'éléments premiers avec n.

Exemple 10.

Proposition 11 (Co p.59 ou Ca p.99)**.** *Si* k *est premier avec* n *alors* k *est d'ordre* n*.*

Corollaire 12 (Co p.59 ou Ca p.99)**.** $\phi(n)$ *est le cardinal des générateurs de* $\mathbb{Z}/n\mathbb{Z}$*.*

Proposition 13 (Ca p.100)**.** *Les générateurs de* $\mathbb{Z}/n\mathbb{Z}$

Exemple 14 (Co p.60)**.**

Corollaire 15 (Co p.61)**.** *Automorphismes de* $\mathbb{Z}/n\mathbb{Z}$*, avec* p *premiers avec* n

Proposition 16. *Morphismes de groupes de* $\mathbb{Z}/n\mathbb{Z}$ *dans* $\mathbb{Z}/m\mathbb{Z}$

Proposition 17 (Co p.63 ou RB p.14)**.** *Pour tout diviseur* d *de* n*,* $\mathbb{Z}/n\mathbb{Z}$ *possède* $\phi(d)$ *éléments d'ordre* d*.*

Exemple 18 (Co p.62)**.** Elements d'ordre 6 dans le groupe $\mathbb{U}_6$.

Proposition 19 (Co p.63 ou RB p.14)**.** $n = \sum_{d|n} \phi(d)$.

1.1.3 Théorème de structure

Théorème 20 (Co p.66)**.** *Thm de structure des groupes abéliens finis*

Exemple 21 (Co .68)**.**

1.2 Structure d'anneau

Proposition 22 (RB p.13)**.** *Idéaux de* $\mathbb{Z}/n\mathbb{Z}$

Proposition 23 (RB p.13)**.** $\mathbb{Z}/n\mathbb{Z}$ *est un anneau commutatif*

Proposition 24 (??????)**.** *Structure de* $\mathbb{Z}/p^\alpha\mathbb{Z}$ *: nilpotent, inversible etc*

Proposition 25 (????)**.** *Nilpotents et idempotents de* $\mathbb{Z}/n\mathbb{Z}$ *: Les nilpotents de* $\mathbb{Z}/n\mathbb{Z}$ *sont les* $p_1 \cdots p_r\mathbb{Z}/n\mathbb{Z}$ *où* $n = p_1^{\alpha_1} \cdots p_r^{\alpha_r}$*. Il y a* 2^r *idempotents.*

1.2.1 Les inversibles de $(\mathbb{Z}/n\mathbb{Z}, \times)$

Proposition 26 (Ca p.100 ou RB p.13)**.** *Les éléments inversibles +groupe multiplicatif*

Remarque 27. Réécriture de la propriété sur les automorphismes

Théorème 28 (RB p.13)**.** *p premier ssi corps ssi intègre. On le note* $\mathbb{F}_p$*.*

Proposition 29 (RB p.15)**.** $(\mathbb{Z}/p\mathbb{Z})^*$ *est cyclique etc*

Proposition 30 (P p.25)**.** $(\mathbb{Z}/p^\alpha\mathbb{Z})^*$

Théorème 31 (RB p.15)**.** *Thm d'Euler*

Remarque 32. Test de primalité

Corollaire 33 (RB p.15)**.** *Petit thm de Fermat*

Exemple 34 (RB p.21)**.**

Théorème 35 (RB p.15)**.** *Wilson*

1.2.2 Théorème chinois

Théorème 36 (RB p.16)**.** *Thm chinois*

Exemple 37.

Application 38 (Ca p.104)**.** Calcul de $\phi(n)$

Corollaire 39 (RB p.18)**.** *Isomorphismes de groupes entre les inversibles*

Application 40 (G p.34)**.** Cryptographie RSA

(Regarder le logarithme discrêt : Elgamal)

Application 41. Cardinal de $\mathrm{GL}_2(\mathbb{Z}/n\mathbb{Z})$

2 Le cas p premier

2.1 Etude des carrés de $\mathbb{F}_p$

blabla habituel [Goz ou Duverney]

2.2 Polynômes sur $\mathbb{F}_p$

[Goz] à voir ce qu'on met dedans.. +critère de réduction mod p + Dirichlet faible

2.3 Application à la résolution d'équations diophantiennes

[Co cf 126]