NOM : MEYER Prénom : Nicolas Jury :

Algèbre ← Entourez l'épreuve → Analyse

Sujet choisi : Anneau $\mathbb{Z}/n\mathbb{Z}$. Applications. ↙ exples ↙ base

Autre sujet : Ref : Perrin, Combes (Alg & géom), Debeaumarché

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

1. Groupe cyclique

Prop 1 : Les sous-groupes de $(\mathbb{Z},+)$ sont les $n\mathbb{Z}$, avec $n \in \mathbb{N}$.

Déf 2 : On définit le groupe $(\mathbb{Z}/n\mathbb{Z},+)$ comme le groupe quotient de $(\mathbb{Z},+)$ par $n\mathbb{Z}$.

Ex 3 : Cas triviaux : • $n=0$, $n\mathbb{Z}=\{0\}$, $\mathbb{Z}/n\mathbb{Z}=\mathbb{Z}$

• $n=1$, $n\mathbb{Z}=\mathbb{Z}$, $\mathbb{Z}/n\mathbb{Z}=\{0\}$

→ Désormais, $n \geq 2$.

Prop 4 : Soit $(G,\cdot)$ un groupe monogène, $a \in G$ un générateur et $\varphi : \mathbb{Z} \to G$, $k \mapsto a^k$.
Alors φ est un morphisme de groupes surjectif et
• si G est cyclique d'ordre n, alors $G \simeq \mathbb{Z}/n\mathbb{Z}$
• sinon, $G \simeq \mathbb{Z}$.

Ex 5 : $\mathbb{U}_n := \{z \in \mathbb{C} \,/\, |z|^n = 1\} \simeq \mathbb{Z}/n\mathbb{Z}$

Déf 6 : On définit l'indicatrice d'Euler par $\varphi(n) = \mathrm{Card}\{k \in [\![1,n]\!],\ k \wedge n = 1\}$

Ex 7 : Si p est premier, $\varphi(p^k) = (p-1)p^{k-1}$

Prop 8 : Soit a un générateur de $\mathbb{Z}/n\mathbb{Z}$; $k \in \mathbb{N}$, alors l'ordre de ka est $\frac{n}{n \wedge k}$.

Corollaire 9 : • k est générateur ssi $k \wedge n = 1$
• Il y a $\varphi(n)$ générateurs dans $\mathbb{Z}/n\mathbb{Z}$

Application 10 : Il y a un seul élément d'ordre 2 dans $\mathbb{Z}/n\mathbb{Z}$ pour n pair, à savoir $n/2$.

2. Sous-groupes

Prop 11 : Tout sous-groupe de $\mathbb{Z}/n\mathbb{Z}$ est cyclique et si d divise n, il existe un unique sous-groupe H_d de $\mathbb{Z}/n\mathbb{Z}$ d'ordre d.
De plus $H_d = \{a \in \mathbb{Z}/n\mathbb{Z} \,/\, da = 0\} \simeq \mathbb{Z}/d\mathbb{Z}$

Exemple 12 : $\mathbb{Z}/20\mathbb{Z}$ admet 4 sous-groupes stricts : $\mathbb{Z}/2\mathbb{Z}$, $\mathbb{Z}/4\mathbb{Z}$, $\mathbb{Z}/5\mathbb{Z}$ et $\mathbb{Z}/10\mathbb{Z}$

Application 13 : $n = \sum_{d|n} \varphi(d)$ (Gauss)

Application 14 : Si K est un corps, alors tout sous-groupe fini de K^* est cyclique.

3. Produit de $\mathbb{Z}/n\mathbb{Z}$

Théorème 15 (chinois)
$\mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z} \simeq \mathbb{Z}/nm\mathbb{Z} \iff n \wedge m = 1$

Applications 16 • $n \wedge m = 1 \Rightarrow \varphi(nm) = \varphi(n)\varphi(m)$
• si $n = p_1^{\alpha_1} \dots p_k^{\alpha_k}$ (décomposition en facteurs premiers), alors $\varphi(n) = n\left(1-\frac{1}{p_1}\right)\cdots\left(1-\frac{1}{p_k}\right)$

Lemme 17 : Soit G un groupe abélien fini et H un sous-groupe de G ; pour tout caractère χ de H, il existe $\tilde{\chi}$ caractère de G tel que $\tilde{\chi}|_H = \chi$

Lemme 18 : Si G est un groupe abélien fini d'exposant n, alors il existe $x \in G$ d'ordre n.

Théorème 19 : Soit G un groupe abélien fini non trivial, il existe $r \geq 1$ et $n_1 | \dots | n_r$ tels que
$G \simeq \mathbb{Z}/n_1\mathbb{Z} \times \dots \times \mathbb{Z}/n_r\mathbb{Z}$.

Développement 1

[Peyré]

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

1. Anneau et corps $\mathbb{Z}/n\mathbb{Z}$

Prop 20 : - Les idéaux de $\mathbb{Z}$ sont les $n\mathbb{Z}$, avec $n \in \mathbb{N}$.
- Les idéaux premiers de $\mathbb{Z}$ sont les $p\mathbb{Z}$, avec p premier / $\{0\}$
- Les idéaux maximaux de $\mathbb{Z}$ sont les $p\mathbb{Z}$, avec p premier.

Déf 21 : On définit l'anneau $\mathbb{Z}/n\mathbb{Z}$ comme l'anneau quotient de $\mathbb{Z}$ par $n\mathbb{Z}$.

Prop 22 : Soit $s \in \mathbb{Z}$;
$s \wedge n = 1 \iff \bar{s}$ est générateur de $(\mathbb{Z}/n\mathbb{Z}, +) \iff \bar{s} \in (\mathbb{Z}/n\mathbb{Z})^\times$

Csq 23 : • $|(\mathbb{Z}/n\mathbb{Z})^\times| = \varphi(n)$
• p premier $\iff \mathbb{Z}/p\mathbb{Z}$ est un corps

Applications 24 : (1) Si k est premier avec n, alors $k^{\varphi(n)} \equiv 1\ [n]$ (Fermat-Euler)
(2) Pour tout $x \in \mathbb{Z}$, $x^p \equiv x\ [p]$ (p premier) (Fermat)
(3) $p \geq 2$ est un nombre premier ssi $(p-1)! \equiv -1\ [p]$ (Wilson)

Exemple 25 : Le chiffre des unités de 27^{1995} est 3.

2. Caractéristique d'un anneau

A anneau commutatif

Déf 26 : On considère le morphisme d'anneaux $\phi : \mathbb{Z} \to A$, $k \mapsto k \cdot 1_A$. Alors $\operatorname{Ker}\phi = c\mathbb{Z}$ et c est appelée la caractéristique de l'anneau A, notée $\operatorname{car}(A)$.

Exemple 27 : $\operatorname{Car}(\mathbb{Z}/n\mathbb{Z}) = n$

Prop 28 : Si A est intègre, alors $\operatorname{car}(A) = 0$ ou un nombre premier p.

Cor 29 : Si K est un corps fini, alors $\operatorname{car} K = p > 0$, p premier.

Déf - Prop 30 : Soit K un corps de caractéristique c. On appelle sous-corps premier de K le sous-corps P de K engendré par 1. Deux cas sont alors possibles :
1. $c = 0$ et alors $P \simeq \mathbb{Q}$
2. $c = p$ premier et alors $P \simeq \mathbb{Z}/p\mathbb{Z}$

Csq 31 : Tout corps fini de cardinal p premier est isomorphe à $\mathbb{Z}/p\mathbb{Z}$.

3. Théorème chinois (version anneaux) et automorphismes de $\mathbb{Z}/n\mathbb{Z}$

Théorème 32 : $\mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z} \underset{\text{anneau}}{\simeq} \mathbb{Z}/nm\mathbb{Z} \iff n \wedge m = 1$

Prop 33 : $\operatorname{Aut}(\mathbb{Z}/n\mathbb{Z}) \simeq (\mathbb{Z}/n\mathbb{Z})^\times \simeq \prod_{i=1}^{k} (\mathbb{Z}/p_i^{\alpha_i}\mathbb{Z})^\times$
avec $n = \prod_{i=1}^{k} p_i^{\alpha_i}$ (décomposition en facteurs premiers) structure des automorphismes de $\mathbb{Z}/n\mathbb{Z}$

Théorème 34 : 1. Cas $p = 2$: • $(\mathbb{Z}/2\mathbb{Z})^\times \simeq \{1\}$
• $(\mathbb{Z}/4\mathbb{Z})^\times \simeq \mathbb{Z}/2\mathbb{Z}$ • $(\mathbb{Z}/2^\alpha\mathbb{Z})^\times \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2^{\alpha-2}\mathbb{Z}$ $(\alpha \geq 3)$
2. Cas $p \geq 3$: $(\mathbb{Z}/p^\alpha\mathbb{Z})^\times \simeq \mathbb{Z}/\varphi(p^\alpha)\mathbb{Z} \simeq \mathbb{Z}/p^{\alpha-1}(p-1)\mathbb{Z}$

Dev pt 2 [Perrin]

Rque 35 : On a une suite exacte, pour $\alpha \geq 3$: $(p = 2)$

$$1 \to \mathbb{Z}/2^{\alpha-2}\mathbb{Z} \to (\mathbb{Z}/2^\alpha\mathbb{Z})^\times \to \mathbb{Z}/2\mathbb{Z} \to 1$$

On peut aussi mettre la suite exacte pour p impair

automorphismes de gp?

120

III. Applications

1. Arithmétique dans $\mathbb{Z}$ [Combes]

Prop 36: Soit $n = a_k \dots a_0$ un entier écrit sous forme décimale ; alors :

1. $n \equiv a_0 \; [2]$
2. $n \equiv a_0 + \dots + a_k \; [3]$
3. $n \equiv a_0 \; [5]$
4. $n \equiv a_0 + 3a_1 + 2a_2 - a_3 - 3a_4 - 2a_5 + a_6 \dots \; [7]$
5. $n \equiv a_0 - a_1 + a_2 - a_3 \dots \; [11]$

Exemples d'application de Fermat (37):

1. Pour tout $n \in \mathbb{N}^*$, $10^{(10^n)} \equiv 4 \; [7]$
2. Il existe un multiple de 1996 dont l'écriture décimale ne comporte que des 4.

2. Equations sur $\mathbb{Z}/n\mathbb{Z}$ [Perrin]

Prop 38: Soit à résoudre le système (E) : $\begin{cases} x \equiv a \; [n] \\ x \equiv b \; [m] \end{cases}$ avec $n \wedge m = 1$. Si x_0 est une solution de (E), alors les solutions de (E) sont les $x_0 + nmk$, $k \in \mathbb{Z}$.

Rq 39: Le lemme chinois assure l'existence de x_0.

Ex 40: $\begin{cases} x \equiv 10 \; [47] \\ x \equiv 5 \; [111] \end{cases} \Rightarrow x = 4334 + 5217k, \; k \in \mathbb{Z}$

Théorème 41: Soit p un nombre premier impair ; Alors p est somme de deux carrés d'entiers ssi $p \equiv 1 \; [4]$

du lemme chinois

Application 42: L'équation $6n^2 + 5n + 1 = 0$ admet une solution dans $\mathbb{Z}/p\mathbb{Z}$ pour tout p premier.

Corollaire 43: Un entier $n = \prod_{i=1}^{k} p_i^{\alpha_i}$, p_i premier est somme de deux carrés ssi α_i est pair pour $p_i \equiv 3 \; [4]$

3. Arithmétique et polynômes [Perrin]

Théorème 44 (Critère d'Eisenstein) Soit $P = \sum_{k=0}^{n} a_k X^k \in \mathbb{Z}[X]$, p un entier premier ; on suppose que :

1. p ne divise pas a_n
2. p divise a_k pour $k \in [\![0, n-1]\!]$
3. p^2 ne divise pas a_0

Alors P est irréductible dans $\mathbb{Q}[X]$ (et $\mathbb{Z}[X]$ si $\mathrm{pgcd}(a_i) = 1$)

Exemple 45: $X^{p-1} + X^{p-2} + \dots + X + 1$ est irréductible sur $\mathbb{Z}$ pour p premier.

Théorème 45: Soit p un entier premier, $P = \sum_{k=0}^{n} a_k X^k \in \mathbb{Z}[X]$ et $\overline{P}$ sa réduction modulo p : $\overline{P} \in \mathbb{Z}/p\mathbb{Z}[X]$. On suppose $\overline{a_n} \neq 0$. Alors, si $\overline{P}$ est irréductible sur $\mathbb{Z}/p\mathbb{Z}$, alors P est irréductible sur $\mathbb{Q}$.

Exemple 46: $X^3 + 462X^2 + 2433X - 67691$ est irréductible sur $\mathbb{Z}$.

I) Défense de plan

1. $(\mathbb{Z},+) \to$ sg $n\mathbb{Z} \Rightarrow (\mathbb{Z}/n\mathbb{Z},+)$

   ↳ G gpe cyclique $G \simeq \mathbb{Z}/n\mathbb{Z}$

   ↳ G gpe abélien fini $G \simeq \mathbb{Z}/d_1\mathbb{Z} \times \dots \times \mathbb{Z}/d_r\mathbb{Z}$

2. $(\mathbb{Z},+,\cdot) \to$ idéaux $n\mathbb{Z} \Rightarrow (\mathbb{Z}/n\mathbb{Z},+,\cdot)$

   ↳ caractéristique

Commentaires : - plus défendre les dvts.
- dvt 1 : pas vraiment magique ni audacieux
- motivations de $\mathbb{Z}/n\mathbb{Z}$:
  * s'injecte ds tt anneau
  * se ramener à un ?? fini = des infos supplémentaires (Lagrange, ppe des tiroirs, ...)

II) Plan

Commentaires : - bien, assez exhaustif

II.2. → caractéristique + aspect sous corps premier → corps finis de card p^k bien à mettre ici

A rajouter : - on peut utiliser $\mathbb{Z}/n\mathbb{Z}$ pour RSA
- primalité
- ds le sillage : nombres de Carmichael

III) Exercices / Questions

1. Ordre max d'un élt de $\mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}$ pour la loi + ?

   ↳ ppcm(n,m)

2. Expliciter les flèches du thm chinois

3. Caractéristique de $\mathbb{Z}/a\mathbb{Z} \times \mathbb{Z}/b\mathbb{Z}$, $a,b \in \mathbb{N}^*$ ↳ ppcm(a,b)

4. Même question pour $\prod_{k \in \mathbb{N}^*} \mathbb{Z}/k\mathbb{Z}$ ↳ 0 pcq $k(1,1,\dots) = (k,\dots,k) = 0$
   $\Leftrightarrow n \mid k \ \forall n \geq 1$
   $\Leftrightarrow k = 0$

c'est rigolo, c'est de car 0 ms ça contient ts les $\mathbb{Z}/n\mathbb{Z}$
(et $\mathbb{Z}$ car $k \mapsto k \cdot (1,\dots,1) = (k,\dots,k)$)

5. Montrer l'appli 12

↳ $6n^2+5n+1 = 6\left(n+\frac{5}{12}\right)^2 - \frac{1}{24}$

On travaille ds $\mathbb{Q}$ et une fois qu'on a une sol° on vérifie que ça marche

$6n^2+5n+1=0 \Leftrightarrow \underbrace{24\times 6}_{=12^2}\left(n+\frac{5}{12}\right)^2 = 1$

$\Leftrightarrow (12n+5)^2 = 1$

Dans $\mathbb{Z}/p\mathbb{Z}$: $(12n+5)-1 \equiv 0\ [p]$.

6. Résoudre $\begin{cases} x \equiv 1\ [3] \\ x \equiv 4\ [5] \\ x \equiv 0\ [7] \end{cases}$

↳ 2 sol° : . trouver une rela° de Bezout $3+5-7=1$

. résoudre 2 à 2, 3 et 5 puis 5 et 7 puis . = multiple de $\prod p_i$

7. Nilpotents de $\mathbb{Z}/n\mathbb{Z}$?

↳ si $n = \prod p_i^{\alpha_i}$ p_i 2 à 2 distincts, les $m = \prod p_i^{\beta_i} \times r$, $r \in \mathbb{Z}$

pour k assez gd ($\max \alpha_i$ convient), on a $n \mid m^k$

réciproquement il faut que tous les p_i divisent m.

⚠ Nilpotent $\neq$ non inversible. On peut retomber sur soi-m au lieu de tomber sur 0.

ex : 2 ds $\mathbb{Z}/6\mathbb{Z}$: $2 - 4 - 8 = 2 \ldots$

8. $n \geq 2$. e premier avec $\varphi(n)$. Mq $\begin{cases} (\mathbb{Z}/n\mathbb{Z})^\times \to (\mathbb{Z}/n\mathbb{Z})^\times \\ x \mapsto x^e \end{cases}$ bijection.

Exhiber la bijection réciproque.

↳ = RSA

9. $p \neq q$ premiers impairs $\varphi : \begin{cases} (\mathbb{Z}/pq\mathbb{Z})^\times \to (\mathbb{Z}/p\mathbb{Z})^\times \times (\mathbb{Z}/q\mathbb{Z})^\times \\ x \mapsto (x, x) \end{cases}$

$E = \{x \in (\mathbb{Z}/pq\mathbb{Z})^\times,\ 1 \leq x < \frac{pq}{2}\}$

$\mathrm{Im}_\varphi(E)$?

10. Condi° nécessaire pour que $P \in \mathbb{Z}/n\mathbb{Z}[X]$ inversible ?

Dvt 2

inv. de l'anneau

Soit φ automorph $\mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$. Comme φ morph, $\varphi(k) = k\varphi(1)$ donc φ entièrement déterminé par $\varphi(1)$ et $\varphi(1) \in (\mathbb{Z}/n\mathbb{Z})^\times$ car il doit engendrer $(\mathbb{Z}/n\mathbb{Z}, +)$.

= gén de $(\mathbb{Z}/n\mathbb{Z}, +)$

On a donc $\begin{cases} \mathrm{Aut}(\mathbb{Z}/n\mathbb{Z}) \simeq (\mathbb{Z}/n\mathbb{Z})^\times \\ \varphi \mapsto \varphi(1) \end{cases}$ Il faut donc étudier $(\mathbb{Z}/n\mathbb{Z})^\times$

Lemme chinois $\to$ $\mathbb{Z}/n\mathbb{Z} \simeq \prod \mathbb{Z}/p_i^{\alpha_i}\mathbb{Z}$. $(\mathbb{Z}/n\mathbb{Z})^\times \simeq \prod (\mathbb{Z}/p_i^{\alpha_i}\mathbb{Z})^\times$

- si $\alpha = 1$: $\mathbb{Z}/p\mathbb{Z} = \mathbb{F}_p$, $(\mathbb{Z}/p\mathbb{Z})^\times \simeq \mathbb{Z}/(p-1)\mathbb{Z}$
- si $\alpha \geq 2$: * cas $p = 2$
  - $(\mathbb{Z}/4\mathbb{Z})^\times \simeq \mathbb{Z}/2\mathbb{Z}$
  - si $\alpha \geq 3$, on passe par la suite exacte

$$1 \to \mathbb{Z}/2^{\alpha-2}\mathbb{Z} \to (\mathbb{Z}/2^\alpha\mathbb{Z})^\times \to \mathbb{Z}/2\mathbb{Z} \to 1$$

$$\mathbb{Z}/2^\alpha\mathbb{Z} \to \mathbb{Z}/4\mathbb{Z} \Rightarrow (\mathbb{Z}/2^\alpha\mathbb{Z})^\times \xrightarrow{\psi} \mathbb{Z}/2\mathbb{Z}$$

$$|\mathrm{Ker}\,\psi| = \dots = 2^{\alpha-2}$$

  * cas $p \geq 3$ ...

⚠ On parle ici du gpe $(\mathbb{Z}/n\mathbb{Z}, +)$ en utilisant des outils liés à l'anneau $(\mathbb{Z}/n\mathbb{Z}, +, \cdot)$ (lemme chinois + générateurs de $(\mathbb{Z}/n\mathbb{Z}, +)$)