Groupes cycliques et théorème des restes

1 Rappels

Anneau $\mathbb{Z}/n\mathbb{Z}$ et indicatrice d'Euler

Le groupe $\mathbb{Z}/n\mathbb{Z}$ est l'unique (à isomorphisme près) groupe cyclique de cardinal n. Il bénéficie d'une structure d'anneau. Le cardinal de ses inversibles est

$$\#(\mathbb{Z}/n\mathbb{Z})^\times = \varphi(n) = \#\{d \in \mathbb{N}/1 \leq d \leq n \text{ et } \operatorname{pgcd}(d,n) = 1\}.$$

La fonction φ est appelée l'*indicatrice d'Euler* et c'est une fonction multiplicative, i.e., pour n, m **premiers entre eux** $\varphi(nm) = \varphi(n)\varphi(m)$.

Théorème des restes et inverse

Soit $n = p_1^{\alpha_1} \dots p_r^{\alpha_r}$, on considère le morphisme de réduction sur modulo $p_i^{\alpha_i}$ sur chaque composante

$$\begin{aligned} \pi\colon \quad \mathbb{Z}/n\mathbb{Z} &\longrightarrow \mathbb{Z}/p_1^{\alpha_1}\mathbb{Z} \times \dots \times \mathbb{Z}/p_r^{\alpha_r}\mathbb{Z} \\ x &\longmapsto (x \mod p_1^{\alpha_1}, \dots, x \mod p_r^{\alpha_r}). \end{aligned}$$

Théorème (Théorème des restes)**.** *L'application π est un isomorphisme d'**anneaux**.*

Bien que l'isomorphisme π soit explicite, son inverse l'est moins. Considérons une relation de Bézout

$$u_1 p_2^{\alpha_2} \dots p_r^{\alpha_r} + \dots + u_r p_1^{\alpha_1} \dots p_{r-1}^{\alpha_{r-1}} = 1, u_i \in \mathbb{Z}$$

alors $\pi^{-1}(\mathbf{a_1}, \dots, \mathbf{a_r}) = u_1 p_2^{\alpha_2} \dots p_r^{\alpha_r} \mathbf{a_1} + \dots + u_r p_1^{\alpha_1} \dots p_{r-1}^{\alpha_{r-1}} \mathbf{a_r}$.

Morphisme caractéristique

Pour tout anneau unitaire A, il existe un **unique** morphisme d'anneau $\operatorname{char}\colon \mathbb{Z} \to A$ défini par $\operatorname{char}(n) = n\operatorname{char}(1) = 1_A + \dots + 1_A$. Son noyau est de la forme $\ker \operatorname{char} = n\mathbb{Z}$ pour un unique n positif. Cet entier n est appelé *caractéristique* de A.

2 Exercices

Exercice 1 - Anneaux, groupes, morphismes ($\star$)

On pose $q = p^\alpha$ avec p un nombre premier et $\alpha \geq 2$.

1. Les groupes suivants sont-ils isomorphes ? Si oui, sont-ils isomorphes en tant qu'anneaux ?
   (a) $\mathbb{Z}/q\mathbb{Z}$ et $(\mathbb{Z}/p\mathbb{Z})^\alpha$.
   (b) $\mathbb{F}_q$ et $(\mathbb{Z}/p\mathbb{Z})^\alpha$.
2. À quelle condition existe-t-il un morphisme d'anneaux de $\mathbb{Z}/n\mathbb{Z}$ vers $\mathbb{Z}/m\mathbb{Z}$? Existe-t-il un morphisme d'anneaux de $\mathbb{Z}/p\mathbb{Z}$ vers $\mathbb{Z}/q\mathbb{Z}$? L'application suivante est-elle bien définie ? Est-ce un morphisme de groupes ?

$$\begin{aligned} \pi\colon \quad (\mathbb{Z}/q\mathbb{Z})^\times &\longrightarrow (\mathbb{Z}/p\mathbb{Z})^\times \\ a &\longmapsto a \mod p. \end{aligned}$$

3. Montrer que $\operatorname{Aut}_{\mathbb{Z}}(\mathbb{Z}/n\mathbb{Z}) \simeq (\mathbb{Z}/n\mathbb{Z})^\times$.

Exercice 2 - Théorème d'Euler et petit théorème de Fermat ($\star$)

Montrer que pour tout a premier avec n on a

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

En déduire le petit théorème de Fermat.

Exercice 3 - Exemples d'utilisation du théorème des restes ($\star$)

1. Résoudre $x^2 + x + 1 = 0$ dans $\mathbb{Z}/91\mathbb{Z}$ ($91 = 7 \times 13$).
2. L'entier 56 est-il un carré modulo 60 ?

Exercice 4 - Générateurs de groupes multiplicatifs ($\star$)

On rappelle que pour a d'ordre n dans un groupe G on a $\operatorname{ord}(a^d) = \frac{n}{\operatorname{pgcd}(n,d)}$.

1. Montrer que pour tout $a, b \in G$ qui commutent d'ordre n et m premiers entre eux alors ab est d'ordre nm. Sans l'hypothèse n et m premiers entre eux, a-t-on $\operatorname{ord}(ab) = \operatorname{ppcm}(n,m)$?
2. Donner un générateur du groupe $(\mathbb{Z}/13\mathbb{Z})^\times$. Donner tous les générateurs de ce groupe.

Exercice 5 - Carrés modulo p ($\star\star$)

Soit p un nombre premier **impair**.

1. Rappeler la valeur de $\#(\mathbb{Z}/p\mathbb{Z})^\times$. Pour $x \in (\mathbb{Z}/p\mathbb{Z})^\times$, que vaut x^{p-1} ?
2. Combien y a-t-il de carrés non nuls dans $\mathbb{Z}/p\mathbb{Z}$? (on pourra étudier un morphisme).
3. Quelles sont les valeurs possible de $x^{\frac{p-1}{2}}$ pour $x \in (\mathbb{Z}/p\mathbb{Z})^\times$? Montrer que $x^{\frac{p-1}{2}} = 1$ si, et seulement si, x est un carré dans $(\mathbb{Z}/p\mathbb{Z})^\times$.

(tous les résultats ci-dessus sont vrais plus généralement dans un corps fini $\mathbb{F}_q$ en remplaçant $\mathbb{Z}/p\mathbb{Z}$ par $\mathbb{F}_q$ et p par q).

Exercice 6 - Critère de Wilson ($\star\star$)

Montrer que n est un nombre premier si, et seulement si, $(n-1)! \equiv -1 \mod n$.

Exercice 7 - Le groupe $(\mathbb{Z}/p^\alpha\mathbb{Z})^\times$ est cyclique pour p premier impair ($\star\star\star$)

1. Quel est le cardinal de $(\mathbb{Z}/p^\alpha\mathbb{Z})^\times$?
2. Soit U le sous-groupe des éléments de $(\mathbb{Z}/p^\alpha\mathbb{Z})^\times$ congrus à $1 \mod p$. Quel est son cardinal ?
3. Montrer par récurrence que pour $n \geq 1$, $(1+pa)^{p^n} = 1 + p^{n+1}a \pmod{p^{n+2}}$.
4. Montrer que si $x \in \mathbb{Z}$ vérifie $x = 1 \pmod p$ et $x \neq 1 \pmod{p^2}$, alors x est d'ordre $p^{\alpha-1}$ dans $(\mathbb{Z}/p^\alpha\mathbb{Z})^\times$. En déduire que U est cyclique.
5. En utilisant que $(\mathbb{Z}/p\mathbb{Z})^\times$ est cyclique, montrer que $(\mathbb{Z}/p^\alpha\mathbb{Z})^\times$ possède un élément y dont l'ordre est un multiple de $p-1$.
6. Conclure que $(\mathbb{Z}/p^\alpha\mathbb{Z})^\times$ est cyclique.
7. Où utilise-t-on que $p \neq 2$?

Exercice 8 - $(\mathbb{Z}/2^\alpha\mathbb{Z})^\times$ n'est pas cyclique, mais presque ($\star\star\star$)

1. Décrire les groupes $(\mathbb{Z}/2\mathbb{Z})^\times$, $(\mathbb{Z}/4\mathbb{Z})^\times$ et $(\mathbb{Z}/8\mathbb{Z})^\times$. Sont-ils cycliques ?
2. Montrer par récurrence que $(1+4a)^{2^n} = 1 + 2^{n+2}a \mod 2^{n+3}$.

Soit $\alpha \geq 3$.

3. Montrer que 5 est d'ordre $2^{\alpha-2}$ dans $(\mathbb{Z}/2^\alpha\mathbb{Z})^\times$. Donner au groupe cyclique $U' = \langle 5 \rangle$ une description analogue a celle de U dans l'exercice précédent.
4. Conclure que $(\mathbb{Z}/2^\alpha\mathbb{Z})^\times$ est le produit direct $\{\pm 1\} \times U'$.

Applications des exercices 7 et 8

Exercice 9 - Pour quelles valeurs de n le groupe $(\mathbb{Z}/n\mathbb{Z})^\times$ est-il cyclique ? ($\star\star$)

1. Soient G, H deux groupes cycliques d'ordres n, m. Montrer que $G \times H$ est cyclique si et seulement si n et m sont premiers entre eux.
2. Pour quelles valeurs de n le groupe $(\mathbb{Z}/n\mathbb{Z})^\times$ est-il cyclique ?

Exercice 10 - Nombre de carrés dans $\mathbb{Z}/n\mathbb{Z}$ ($\star\star$)

On s'intéresse au nombre de solution de l'équation $x^2 = 1$ dans $\mathbb{Z}/n\mathbb{Z}$.

1. Combien y a-t-il de solutions dans $\mathbb{Z}/p^\alpha\mathbb{Z}$ pour p premier impair ?
2. Combien y a-t-il de solutions dans $\mathbb{Z}/2^\alpha\mathbb{Z}$? (on distinguera les cas $\alpha = 1, 2$ et $\alpha \geq 3$).
3. Combien y a-t-il de carrés inversibles dans $\mathbb{Z}/n\mathbb{Z}$ avec $n = 2^\alpha p_1^{\alpha_1} \dots p_r^{\alpha_r}$.

Exercice 11 - Carrés dans $\mathbb{Z}/p^\alpha\mathbb{Z}$ ($\star\star$)

Soit p un nombre premier impair.

1. Montrer que $a \in \mathbb{Z}$ premier à p est un carré modulo p^α si, et seulement si, c'est un carré modulo p.
2. Les entiers 52 et 20 sont-ils des carrés modulo 81 ?

Étant donnée la longueur de la feuille nous n'auront pas le temps de tout corriger pendant sur le créneau de 2h du TD. Si vous souhaitez des indications ou que vous avez des remarques ou corrections à apporter vous pouvez me contacter à fabien.narbonne@posteo.net ou venir me voir au bureau 634 du bâtiment 23.

Bonne préparation :) !