Plaquette 3 – Anneaux, idéaux, Z/nZ et théorème chinois

Structures algébriques — Prépa MP / MPI (2e année)

Exercices

Méthode

Dans un anneau commutatif, les **idéaux** jouent pour la divisibilité le rôle que jouent les sous-groupes pour les groupes : $a \mid b \Leftrightarrow bA \subset aA$. Dans $\mathbb{Z}$ et $\mathrm{K}[X]$, tout idéal est **principal**, d'où le pgcd et Bézout. L'anneau $\mathbb{Z}/n\mathbb{Z}$ s'étudie par ses inversibles (classes premières avec n), ses diviseurs de zéro et ses nilpotents ; le **théorème chinois** le découpe en morceaux $\mathbb{Z}/p^{\alpha}\mathbb{Z}$ et ramène les équations modulo n à des équations modulo chaque p^{α}. On calcule les inverses par l'algorithme d'Euclide étendu, et les grandes puissances par le théorème d'Euler.

Exercice 1 – Les idéaux de Z/nZ

Soit $n \geq 2$ et $\pi : \mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$ la projection.

a) Montrer que l'image réciproque d'un idéal J de $\mathbb{Z}/n\mathbb{Z}$ est un idéal de $\mathbb{Z}$ contenant $n\mathbb{Z}$.

b) En déduire que les idéaux de $\mathbb{Z}/n\mathbb{Z}$ sont les $\overline{d}\,\mathbb{Z}/n\mathbb{Z}$ pour $d \mid n$, et qu'il y en a autant que de diviseurs de n.

c) Lister les idéaux de $\mathbb{Z}/12\mathbb{Z}$ et indiquer lesquels sont **maximaux** (non contenus strictement dans un idéal propre).

Exercice 2 – Diviseurs de zéro et nilpotents de Z/nZ

a) Montrer que tout élément non nul de $\mathbb{Z}/n\mathbb{Z}$ est soit inversible, soit diviseur de zéro.

b) Montrer que $\overline{k}$ est **nilpotent** si et seulement si tout facteur premier de n divise k.

c) Lister les nilpotents de $\mathbb{Z}/12\mathbb{Z}$ et de $\mathbb{Z}/72\mathbb{Z}$ (combien ?).

d) Montrer que $\mathbb{Z}/n\mathbb{Z}$ n'a pas de nilpotent non nul si et seulement si n est sans facteur carré.

Exercice 3 – Calculer un inverse modulaire

a) Par l'algorithme d'Euclide étendu, déterminer l'inverse de $\overline{7}$ dans $\mathbb{Z}/26\mathbb{Z}$.

b) Résoudre $7x + 3 \equiv 11 \pmod{26}$.

c) L'équation $6x \equiv 4 \pmod{26}$ a-t-elle des solutions ? Les déterminer.

d) Énoncer une condition nécessaire et suffisante pour que $ax \equiv b \pmod{n}$ ait des solutions, et leur nombre.

Exercice 4 – Résoudre un système de congruences

On cherche les entiers x tels que $x \equiv 2 \pmod{3}$, $x \equiv 3 \pmod{5}$, $x \equiv 2 \pmod{7}$ (problème de Sunzi).

a) Justifier l'existence et l'unicité d'une solution modulo 105.

b) Trouver e_3, e_5, e_7 tels que $e_3 \equiv 1 \pmod{3}$, $e_3 \equiv 0 \pmod{35}$, etc.

c) En déduire la solution.

mathlvl.fr — Tous droits réservés. Toute reproduction, diffusion, revente ou exploitation commerciale, même partielle, est strictement interdite.
Tout contrevenant s'expose à des poursuites en vertu du Code de la propriété intellectuelle (art. L.335-2 et suivants).

d) Un système $x \equiv 1 \pmod 4$, $x \equiv 3 \pmod 6$ a-t-il des solutions ?

Exercice 5 – Indicatrice d'Euler multiplicative

a) Déduire du théorème chinois que, si $m \wedge n = 1$, $(\mathbb{Z}/mn\mathbb{Z})^\times \simeq (\mathbb{Z}/m\mathbb{Z})^\times \times (\mathbb{Z}/n\mathbb{Z})^\times$, puis $\varphi(mn) = \varphi(m)\varphi(n)$.

b) Calculer $\varphi(p^\alpha)$ pour p premier.

c) En déduire $\varphi(n) = n\prod_{p \mid n}\left(1 - \frac{1}{p}\right)$ et calculer $\varphi(360)$.

d) La fonction φ est-elle multiplicative sans hypothèse ($\varphi(4)$ et $\varphi(2)^2$) ?

Exercice 6 – Grandes puissances modulo n

a) Calculer les deux derniers chiffres de 7^{2026} (utiliser 7^4 modulo 100).

b) Calculer 3^{100} mod 13 par le petit théorème de Fermat.

c) Calculer 2^{2026} mod 15 par le théorème chinois (calculer modulo 3 et modulo 5).

d) Montrer que $n^{13} - n$ est divisible par $2730 = 2 \times 3 \times 5 \times 7 \times 13$ pour tout entier n.

Exercice 7 – Idempotents de Z/nZ

Un élément e d'un anneau est **idempotent** si $e^2 = e$.

a) Déterminer les idempotents de $\mathbb{Z}/p^\alpha\mathbb{Z}$ (p premier) : montrer que ce sont $\overline{0}$ et $\overline{1}$.

b) En utilisant le théorème chinois, montrer que $\mathbb{Z}/n\mathbb{Z}$ possède 2^r idempotents si n a r facteurs premiers distincts.

c) Les déterminer pour $n = 12$ et vérifier.

Exercice 8 – Racines carrées de l'unité modulo n

a) Résoudre $x^2 \equiv 1 \pmod p$ pour p premier impair, puis modulo p^α (montrer que p^α divise $x - 1$ ou $x + 1$).

b) En déduire, par le théorème chinois, le nombre de solutions de $x^2 \equiv 1 \pmod{15}$, et les lister.

c) Montrer que si l'on connaît une solution $x \neq \pm 1$ de $x^2 \equiv 1 \pmod n$, alors $\mathrm{pgcd}(x - 1, n)$ est un diviseur non trivial de n. Vérifier sur $n = 15$.

Exercice 9 – Idéaux de polynômes et pgcd

Dans $\mathbb{Q}[X]$, soient $P = X^3 - 1$ et $Q = X^2 - 3X + 2$.

a) Factoriser P et Q, et déterminer le générateur unitaire de l'idéal $(P) + (Q)$.

b) Trouver U, V tels que $UP + VQ = X - 1$.

c) Déterminer l'idéal $(P) \cap (Q)$.

d) $X^2 + 1$ appartient-il à $(P) + (Q)$?

Exercice 10 – Un idéal non principal

Dans $\mathbb{Z}[X]$, soit $I = (2, X) = \{2A + XB \mid A, B \in \mathbb{Z}[X]\}$.

a) Montrer que I est l'ensemble des polynômes à coefficient constant pair.

mathlvl.fr — Tous droits réservés. Toute reproduction, diffusion, revente ou exploitation commerciale, même partielle, est strictement interdite.
Tout contrevenant s'expose à des poursuites en vertu du Code de la propriété intellectuelle (art. L.335-2 et suivants).

b) Supposons $I = (D)$. Montrer que D divise 2, donc $D = \pm 1$ ou ± 2, et conclure à une contradiction.

c) Que montre cet exemple sur l'anneau $\mathbb{Z}[X]$? Pourquoi l'argument échoue-t-il dans $\mathbb{Q}[X]$?

Exercice 11 – Un anneau intègre fini est un corps

Soit A un anneau commutatif intègre et fini, et $a \neq 0$.

a) Montrer que $x \mapsto ax$ est injective, puis bijective.

b) En déduire que a est inversible : A est un corps.

c) Application : $\mathbb{Z}/p\mathbb{Z}$ (p premier) et $\mathrm{F}_2[X]/(X^2 + X + 1)$ (on admet qu'il est intègre) sont des corps.

d) L'hypothèse « fini » est-elle nécessaire ?

Exercice 12 – Morphismes d'anneaux entre Z/nZ

Les morphismes d'anneaux envoient 1 sur 1.

a) Montrer qu'il existe un morphisme d'anneaux $\mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}/m\mathbb{Z}$ si et seulement si $m \mid n$, et qu'il est alors unique.

b) Combien y a-t-il de morphismes de **groupes** de $\mathbb{Z}/12\mathbb{Z}$ dans $\mathbb{Z}/4\mathbb{Z}$? de morphismes d'anneaux ?

c) Existe-t-il un morphisme d'anneaux de $\mathbb{Z}/4\mathbb{Z}$ dans $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$? Un isomorphisme ?

Exercice 13 – Caractéristique d'un anneau intègre

Soit A un anneau. L'application $\chi : \mathbb{Z} \to A$, $k \mapsto k \cdot 1_A$ est un morphisme d'anneaux ; son noyau est $c\mathbb{Z}$ ($c \geq 0$ est la **caractéristique**).

a) Montrer que si A est intègre, $c = 0$ ou c est premier.

b) Montrer que si A est un corps fini, c est un premier p et A contient un sous-corps isomorphe à $\mathbb{Z}/p\mathbb{Z}$.

c) En déduire que $\mathrm{card} A$ est une puissance de p (voir A comme espace vectoriel sur ce sous-corps).

Exercice 14 – Le morphisme de Frobenius

Soit A un anneau commutatif de caractéristique p premier, et $F : x \mapsto x^p$.

a) Montrer que F est un morphisme d'anneaux (utiliser $p \mid \binom{p}{k}$ pour $0 < k < p$).

b) Montrer que F est injectif si A est intègre, et bijectif si de plus A est fini.

c) Dans F_p, montrer que $F = \mathrm{id}$. Dans $\mathrm{F}_p[X]$, calculer $F(1 + X)$ et en déduire $(1 + X)^p = 1 + X^p$.

d) Application : dans $\mathrm{F}_3[X]$, développer $(1 + X)^9$.

mathlvl.fr — Tous droits réservés. Toute reproduction, diffusion, revente ou exploitation commerciale, même partielle, est strictement interdite.
Tout contrevenant s'expose à des poursuites en vertu du Code de la propriété intellectuelle (art. L.335-2 et suivants).

Exercice 15 – Synthèse : RSA avec le théorème chinois

On prend $p = 5$, $q = 11$, $n = 55$, et l'exposant public $e = 3$.

a) Calculer $\varphi(n)$ et l'exposant privé d, inverse de e modulo $\varphi(n)$.

b) Chiffrer le message $m = 2$: $c = m^e \bmod n$.

c) Montrer que $c^d \equiv m \pmod{n}$ pour tout m premier avec n (Euler), et vérifier sur l'exemple en calculant c^d modulo 5 et modulo 11 séparément.

d) Montrer que le déchiffrement marche aussi pour m multiple de 5 (raisonner modulo 5 et modulo 11).

mathlvl.fr — Tous droits réservés. Toute reproduction, diffusion, revente ou exploitation commerciale, même partielle, est strictement interdite.
Tout contrevenant s'expose à des poursuites en vertu du Code de la propriété intellectuelle (art. L.335-2 et suivants).