TD1 : Généralités sur les anneaux

Diego Izquierdo

La question 1 de l'exercice 5 a été corrigée. *Tous les anneaux considérés sont commutatifs. L'exercice 1 est à préparer avant la séance de TD. Pendant la séance, nous traiterons les exercices dans l'ordre suivant : 1, 2, 3, 7, 10, 15.*

Exercice 1 (à préparer) : Groupe des unités de $\mathbb{Z}/n\mathbb{Z}$

Dans cet exercice, nous voulons étudier la structure du groupe des unités d'un groupe cyclique. On rappelle que tout sous-groupe fini du groupe des unités d'un corps est cyclique. Cela entraîne en particulier que $(\mathbb{Z}/p\mathbb{Z})^\times \cong \mathbb{Z}/(p-1)\mathbb{Z}$ pour tout nombre premier p.

1. Rappeler quel est l'ordre de $(\mathbb{Z}/n\mathbb{Z})^\times$.

2. Soient p un nombre premier impair et $m > 1$ un entier.

(a) Montrer que $(1+p)^{p^{m-2}} \equiv 1 + p^{m-1} \mod p^m$, puis que $1+p$ est d'ordre p^{m-1} dans $(\mathbb{Z}/p^m\mathbb{Z})^\times$.

(b) En déduire que le noyau de la projection naturelle $(\mathbb{Z}/p^m\mathbb{Z})^\times \to (\mathbb{Z}/p\mathbb{Z})^\times$ est isomorphe à $\mathbb{Z}/p^{m-1}\mathbb{Z}$.

(c) Montrer qu'il existe $x_0 \in (\mathbb{Z}/p^m\mathbb{Z})^\times$ d'ordre $p-1$.

(d) Montrer que $\mathbb{Z}/(p-1)\mathbb{Z} \times \mathbb{Z}/p^{m-1}\mathbb{Z} \to (\mathbb{Z}/p^m\mathbb{Z})^\times, (a,b) \mapsto x_0^a(1+p)^b$ est un isomorphisme. En déduire que $(\mathbb{Z}/p^m\mathbb{Z})^\times \cong \mathbb{Z}/(p-1)p^{m-1}\mathbb{Z}$.

3. Soit $m > 2$ un entier.

(a) Montrer que $5^{2^{m-3}} \equiv 1 + 2^{m-1} \mod 2^m$, puis que 5 est d'ordre 2^{m-2} dans $(\mathbb{Z}/2^m\mathbb{Z})^\times$.

(b) En déduire que le noyau de la projection naturelle $(\mathbb{Z}/2^m\mathbb{Z})^\times \to (\mathbb{Z}/4\mathbb{Z})^\times$ est isomorphe à $\mathbb{Z}/2^{m-2}\mathbb{Z}$.

(c) En s'inspirant de la question 2.(d), montrer que $(\mathbb{Z}/2^m\mathbb{Z})^\times \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2^{m-2}\mathbb{Z}$.

4. Quelle est la structure de $(\mathbb{Z}/n\mathbb{Z})^\times$? Quand ce groupe est-il cyclique ?

5. *Exemples :* Donner un générateur du groupe $(\mathbb{Z}/162\mathbb{Z})^\times$. Donner un élément d'ordre maximal dans $(\mathbb{Z}/2592\mathbb{Z})^\times$.

Exercice 2 : Autour de $\mathbb{Z}/n\mathbb{Z}$

Soit $n > 0$ un entier.

1. (a) Quels sont les diviseurs de 0 de $\mathbb{Z}/n\mathbb{Z}$? Quels sont les éléments réguliers de $\mathbb{Z}/n\mathbb{Z}$?

(b) À quelle condition sur n l'anneau $\mathbb{Z}/n\mathbb{Z}$ est-il intègre ?

2. (a) Quel est le nilradical de $\mathbb{Z}/n\mathbb{Z}$?

(b) À quelle condition sur n l'anneau $\mathbb{Z}/n\mathbb{Z}$ est-il réduit ?

3. (a) Combien d'idempotents possède l'anneau $\mathbb{Z}/n\mathbb{Z}$?

(b) À quelle condition sur n existe-t'il des anneaux non nuls A et B tels que $\mathbb{Z}/n\mathbb{Z} = A \times B$?

3. Quels sont les idéaux de $\mathbb{Z}/n\mathbb{Z}$? Sont-ils principaux ?

4. Quels sont les idéaux premiers de $\mathbb{Z}/n\mathbb{Z}$?

5. Soit $m > 0$ un entier. Quels sont les morphismes d'anneaux :

(a) de $\mathbb{Z}$ dans $\mathbb{Z}/n\mathbb{Z}$?

(b) de $\mathbb{Z}/n\mathbb{Z}$ dans $\mathbb{Z}$?

(c) de $\mathbb{Z}/n\mathbb{Z}$ dans $\mathbb{Z}/m\mathbb{Z}$?

(d) de $\mathbb{Q}$ dans $\mathbb{Z}/n\mathbb{Z}$?

Exercice 3 : Entiers algébriques rationnels

Quels éléments de $\mathbb{Q}$ sont des entiers algébriques ?

Exercice 4 : Anneau des entiers algébriques

1. En exhibant un polynôme annulateur, montrer que le nombre $\sqrt{2}+\sqrt[3]{11}$ est un entier algébrique.

2. Soient $a = \sqrt[3]{2} + \sqrt[3]{3}$ et $A = \mathbb{Z}[a]$. Montrer qu'en tant que groupe, A est libre de type fini. En déduire que a est un entier algébrique.

3. Généraliser le raisonnement précédent pour montrer que l'ensemble des éléments de $\mathbb{C}$ qui sont des entiers algébriques est un anneau.

Exercice 5 : Anneau des entiers algébriques, le retour

1. Soient P et Q deux polynômes à coefficients dans $\mathbb{Q}$ de degrés respectifs d et e. On considère l'application $\mathbb{Q}$-linéaire :

$$f : \mathbb{Q}[X]_{<e} \times \mathbb{Q}[X]_{<d} \mapsto \mathbb{Q}[X]_{<d+e}, (U, V) \mapsto PU + QV,$$

On appelle résultant de P et Q le déterminant de f (dans les bases $((1,0),(X,0),...,(X^{e-1},0),(0,1),(0,X),...,(0,X^{d-1}))$ de $\mathbb{Q}[X]_{<e}\times\mathbb{Q}[X]_{<d}$ et $(1, X, ..., X^{d+e-1})$ de $\mathbb{Q}[X]_{<d+e}$). On le note $\mathrm{Res}(P, Q)$. Montrer que $\mathrm{Res}(P, Q)$ est non nul si, et seulement si, P et Q n'ont pas de racines communes dans $\mathbb{C}$. Remarquer que le résultat subsiste si l'on remplace $\mathbb{Q}$ par un autre corps contenu dans $\mathbb{C}$.

2. En déduire que l'ensemble des entiers algébriques est un anneau.

3. Exhiber un polynôme annulateur unitaire à coefficients dans $\mathbb{Z}$ de l'entier algébrique $\sqrt[3]{2} + \sqrt[3]{3}$.

Exercice 6 : Un entier algébrique

Montrer que $a = \frac{1+\sqrt[3]{10}+\sqrt[3]{100}}{3}$ est un entier algébrique. On pourra étudier le morphisme de groupes :

$$\phi : \mathbb{Z}[\sqrt[3]{10}] \to \mathbb{Z}[\sqrt[3]{10}], x \mapsto ax.$$

Exercice 7 : L'anneau $\mathbb{Z}[i\sqrt{5}]$

Soit $A = \mathbb{Z}[i\sqrt{5}]$.

1. (a) Quels sont les éléments inversibles de A ?

(b) Montrer que 3, 7, $4 - i\sqrt{5}$ et $4 + i\sqrt{5}$ sont irréductibles dans A.

(c) Montrer qu'il n'y a pas d'unicité de la décomposition de 21 en facteurs irréductibles dans A.

(d) Considérons les idéaux :

$$\mathfrak{p}_1 = (3, i\sqrt{5} - 1), \quad \mathfrak{p}_2 = (3, i\sqrt{5} + 1),$$

$$\mathfrak{q}_1 = (7, i\sqrt{5} + 3), \quad \mathfrak{q}_2 = (7, i\sqrt{5} - 3).$$

Vérifier que :

$$(3) = \mathfrak{p}_1\mathfrak{p}_2, \quad (7) = \mathfrak{q}_1\mathfrak{q}_2, \quad (4 + i\sqrt{5}) = \mathfrak{p}_2\mathfrak{q}_2, \quad (4 - i\sqrt{5}) = \mathfrak{p}_1\mathfrak{q}_1.$$

On peut vérifier que les idéaux $\mathfrak{p}_1$, $\mathfrak{p}_2$, $\mathfrak{q}_1$ et $\mathfrak{q}_2$ sont premiers.

2. (a) Justifier que tous les éléments de A sont des entiers algébriques. Considérons $K = \mathbb{Q}[i\sqrt{5}]$ le corps des fractions de A. Soit $x = a + bi\sqrt{5} \in K$ avec $a, b \in \mathbb{Q}$. Supposons que x est un entier algébrique.

(b) Quels sont les morphismes d'anneaux de K dans K ? Montrer que si ϕ est un tel morphisme, alors $\phi(x)$ est un entier algébrique. En déduire que $2a \in \mathbb{Z}$ et que $a^2 + 5b^2 \in \mathbb{Z}$.

(c) Montrer que $x \in A$.

L'anneau A est intégralement clos.

Exercice 8 : L'anneau $\mathbb{Z}[\sqrt{5}]$

Soit $A = \mathbb{Z}[\sqrt{5}]$.

1. (a) Montrer que A possède une infinité d'éléments inversibles.

(b) Montrer que 2, $3 + \sqrt{5}$ et $3 - \sqrt{5}$ sont irréductibles dans A.

(c) Montrer qu'il n'y a pas d'unicité de la décomposition de 4 en facteurs irréductibles dans A.

2. (a) Justifier que tous les éléments de A sont des entiers algébriques. Considérons $K = \mathbb{Q}[\sqrt{5}]$ le corps des fractions de A.

(b) Exhiber un entier algébrique dans $K \setminus A$.

Soit $x = a + b\sqrt{5} \in K$ avec $a, b \in \mathbb{Q}$. Supposons que x est un entier algébrique.

(c) Montrer que $2a \in \mathbb{Z}$ et que $a^2 - 5b^2 \in \mathbb{Z}$.

(d) Montrer que $x \in \mathbb{Z}\left[\frac{1+\sqrt{5}}{2}\right]$.

L'anneau A n'est pas intégralement clos, mais il est contenu dans $\mathbb{Z}\left[\frac{1+\sqrt{5}}{2}\right]$ qui est intégralement clos.

(e) Vérifier que 2 et $3+\sqrt{5}$ sont associés dans $\mathbb{Z}\left[\frac{1+\sqrt{5}}{2}\right]$. De même, vérifier que 2 et $3-\sqrt{5}$ sont associés dans $\mathbb{Z}\left[\frac{1+\sqrt{5}}{2}\right]$.

On peut montrer que l'anneau $\mathbb{Z}\left[\frac{1+\sqrt{5}}{2}\right]$ est principal (donc factoriel).

Exercice 9 : Une équation diophantienne
Trouver tous les couples $(x,y) \in \mathbb{Z}^2$ tels que $y^2 = x^3 + 16$.

Exercice 10 : Une équation dans $\mathbb{C}[T]$
Trouver tous les couples $(x,y) \in \mathbb{C}[T]^2$ tels que $y^2 + T = x^3$.

Exercice 11 : Finitude et intégrité
Soit k un corps. Soit A une k-algèbre de dimension finie intègre. Montrer que A est un corps. En déduire qu'un anneau fini intègre est un corps.

Exercice 12 : Produits d'anneaux
Soient A un anneau.

1. Supposons que A s'écrit sous la forme $A_1 \times .... \times A_n$ où $A_1, ..., A_n$ sont des anneaux non nuls. Montrer que A possède des idempotents non nuls $e_1, ..., e_n$ tels que $e_i e_j = 0$ pour $i \neq j$ et $e_1 + ... + e_n = 1$.

2. Réciproquement, montrer que si A possède des idempotents non nuls $e_1, ..., e_n$ tels que $e_i e_j = 0$ pour $i \neq j$ et $e_1 + ... + e_n = 1$, alors A s'écrit sous la forme $A_1 \times .... \times A_n$ où $A_1, ..., A_n$ sont des anneaux non nuls. Décrire alors les idéaux de A.

3. Soit $m > 0$ un entier. Quel est le plus grand entier n tel qu'il existe des anneaux non nuls A_1, ..., A_n vérifiant $\mathbb{Z}/m\mathbb{Z} = A_1 \times ... \times A_n$?

Exercice 13 : Anneau de polynômes
Soit A un anneau.

1. Supposons A intègre.
   (a) Montrer que $A[X]$ est intègre.
   (b) Quels sont les éléments inversibles de $A[X]$?

2. On ne suppose plus A intègre.
   (a) Quel est le nilradical de $A[X]$?
   (b) Quels sont éléments inversibles de $A[X]$?
   (c) À quelle condition sur A peut-on écrire $A[X] = B_1 \times B_2$ pour certains anneaux non nuls B_1 et B_2 ?

Exercice 14 : Opérations sur les idéaux de $\mathbb{Z}$
Soient $a, b \in \mathbb{Z}$. Donner des générateurs de $(a)+(b)$, de $(a)(b)$ et de $(a) \cap (b)$.

Exercice 15 : Radical d'un idéal

Soient A un anneau et I un idéal de A. On appelle radical de I l'ensemble $\sqrt{I} = \{a \in A | \exists n \in \mathbb{N}^*, a^n \in I\}$.

1. Montrer que $\sqrt{I}$ est un idéal.

2. Reconnaître $\sqrt{A}$ et $\sqrt{(0)}$.

3. Soit J un idéal de A. Déterminer si les assertions suivantes sont vraies ou fausses. Corriger celles qui sont fausses.

(a) $\sqrt{\sqrt{I}} = \sqrt{I}$.

(b) $\sqrt{I \cap J} = \sqrt{I} \cap \sqrt{J}$.

(c) $\sqrt{IJ} = \sqrt{I} \cdot \sqrt{J}$.

(d) $\sqrt{I + J} = \sqrt{I} + \sqrt{J}$.

4. Montrer que $\sqrt{I}$ est l'intersection des idéaux premiers contenant I. On pourra utiliser le lemme de Zorn.

5. Prenons $A = \mathbb{Z}$ et $I = N\mathbb{Z}$. Calculer $\sqrt{I}$.