Rectorat de Grenoble / Université Grenoble Alpes

Préparation à l'agrégation interne 2023-2024

Arithmétique

Tous les anneaux de cette feuille sont commutatifs.

Un anneau A est muni de lois notées par défaut $+$ et $\times$, les neutres sont notés 0 et 1, le groupe multiplicatif des éléments inversibles de A est noté $A^\times$. On note $\mathrm{Div}\,(a)$ l'ensemble des diviseurs d'un élément a de A et aA l'ensemble de ses multiples, qui est l'idéal de A engendré par a (noté aussi (a)).

Pour p un nombre premier, on note $\mathbb{F}_p$ le corps $\mathbb{Z}/p\mathbb{Z}$.

I. Arithmétique dans les anneaux. Des principes fondamentaux.

Exercice 1 : Le cas des anneaux finis

Soit A un anneau commutatif. On rappelle qu'un *diviseur de zéro* de A est un élément a non nul de A tel qu'il existe un élément b non nul de A vérifiant $ab = 0$. Un anneau est intègre s'il n'a pas de diviseur de zéro.

1. Montrer que l'ensemble des diviseurs de zéro de A et l'ensemble $A^\times$ des inversibles de A sont des parties disjointes de A.
2. Montrer que dans un anneau commutatif fini, tout élément non nul est soit un diviseur de zéro, soit un inversible (indication : pour tout élément a de l'anneau A, construire un morphisme du *groupe additif* de A dans lui-même, et discuter s'il est injectif ou non en utilisant l'argument de cardinal). En déduire qu'un anneau commutatif fini est un corps si et seulement si il est intègre.

L'arithmétique (étude des propriétés de divisibilité) se fait sur des anneaux commutatifs intègres qui ne sont pas des corps. La notion de diviseurs ou multiples dans un anneau fini, comme $\mathbb{Z}/n\mathbb{Z}$, n'est donc presque jamais considérée. Cela n'empêche pas d'introduire des anneaux finis pour faire de l'arithmétique : la propriété de divisibilité par n dans $\mathbb{Z}$ se voit dans $\mathbb{Z}/n\mathbb{Z}$.

Exercice 2 : Éléments associés

Soit A un anneau commutatif intègre. On dit que deux éléments a, a' de A sont *associés* s'il existe un inversible e de A tel que $a' = ea$ (par exemple dans $\mathbb{Z}$ les entiers 7 et -7 sont associés). Cela définit une relation d'équivalence sur A, on la notera $\sim$.

1. Montrer l'équivalence entre les propriétés suivantes :

a. $a|a'$ et $a'|a$,

b. $aA = a'A$ (a et a' ont même multiples),

c. $\mathrm{Div}\,(a) = \mathrm{Div}\,(a')$ (a et a' ont mêmes diviseurs),

d. a et a' sont associés.

2. On note $A/\sim$ l'ensemble des classes d'équivalence de A pour la relation $\sim$.

a. Montrer que la relation $|$ sur A induit naturellement une relation $|$ sur $A/\sim$ qui est une relation d'ordre.

b. Déterminer $\mathbb{Z}/\sim$ et sa relation d'ordre $|$.

Dans l'anneau des polynômes $\mathbb{K}[X]$ sur un corps $\mathbb{K}$, on a l'habitude de prendre le polynôme unitaire comme représentant d'une classe de polynôme pour $\sim$ (il est unique dans chaque classe d'équivalence).

Exercice 3 : Identité de Bezout dans un anneau principal

Soit A un anneau principal. Soient $a, b, c \in A$.

1. Montrer l'équivalence suivante :

$$\mathrm{Div}\,(a) \cap \mathrm{Div}\,(b) = \mathrm{Div}\,(c) \;\Leftrightarrow\; aA + bA = cA.$$

(relation de "dualité" entre les diviseurs et les multiples.)

2. En déduire que tout ensemble fini d'éléments d'un anneau principal possède un p.g.c.d. Que peut-on dire de l'unicité du p.g.c.d. ?

On dit que a et b sont premiers entre eux si $\mathrm{Div}\,(a) \cap \mathrm{Div}\,(b) = \{1\}$. D'après la première question, dans un anneau principal, c'est équivalent à $aA + bA = A$, donc à $1 \in aA + bA$, c'est-à-dire à l'identité de Bezout.

Exercice 4 : Des anneaux non principaux

1. Soit A un anneau commutatif. Montrer que $A[X]$ est principal si et seulement si A est un corps.

2. Donner des idéaux non principaux dans $\mathbb{R}[X, Y]$ et dans $\mathbb{Z}[X]$.

Les trois exercices suivants portent sur l'étude d'extensions de l'anneau des entiers $\mathbb{Z}$. Ils introduisent les outils et résultats de l'étude de l'anneau $\mathbb{Z}[i]$ des entiers de Gauss (exercice 10).

Exercice 5 : Les anneaux $\mathbb{Z}[\frac{1}{2}]$ et $\mathbb{Z}[\frac{1}{10}]$

On note $\mathbb{Z}[\frac{1}{2}] = \{P(\frac{1}{2}),\ P \in \mathbb{Z}[X]\}$.

1. Montrer que $\mathbb{Z}[\frac{1}{2}]$ est l'image d'un morphisme d'anneau défini sur $\mathbb{Z}[X]$ et que c'est un anneau commutatif intègre.

2. Montrer que tout polynôme à coefficients entiers ayant $\frac{1}{2}$ comme racine est divisible dans $\mathbb{Z}[X]$ par le polynôme $2X - 1$. En déduire que $\mathbb{Z}[\frac{1}{2}] \simeq \mathbb{Z}[X]/(2X - 1)$.

3. a. Caractériser les éléments de $\mathbb{Q}$ appartenant à $\mathbb{Z}[\frac{1}{2}]$.

b. Déterminer les éléments inversibles et les éléments irréductibles de $\mathbb{Z}[\frac{1}{2}]$.

c. Montrer que $\mathbb{Z}[\frac{1}{2}]$ est un anneau principal. Est-il euclidien ?

d. Décrire la décomposition des éléments de $\mathbb{Z}[\frac{1}{2}]$ en produit d'irréductibles.

4. Reprendre les questions précédentes pour l'anneau $\mathbb{Z}[\frac{1}{10}]$.

Exercice 6 : Les anneaux $\mathbb{Z}[\sqrt{2}]$ et $\mathbb{Z}[i\sqrt{2}]$

On considère $\mathbb{Z}[\sqrt{2}] = \{P(\sqrt{2}),\ P \in \mathbb{Z}[X]\}$.

1. Montrer que $\mathbb{Z}[\sqrt{2}]$ est le sous-anneau de $\mathbb{C}$ engendré par $\sqrt{2}$ et que ses éléments sont de la forme $a + b\sqrt{2}$, $a, b \in \mathbb{Z}$.

2. Montrer que $\mathbb{Z}[\sqrt{2}]$ est un anneau commutatif intègre.

Pour tout $a + b\sqrt{2} \in \mathbb{Z}[\sqrt{2}]$, on note $\overline{a + b\sqrt{2}} = a - b\sqrt{2}$ et $N(a + b\sqrt{2}) = a^2 - 2b^2$.

3. Montrer que $x \mapsto \overline{x}$ et $x \mapsto N(x)$ sont des applications multiplicatives, de $\mathbb{Z}[\sqrt{2}]$ dans $\mathbb{Z}[\sqrt{2}]$ et de $\mathbb{Z}[\sqrt{2}]$ dans $\mathbb{Z}$ respectivement.

4. Montrer que $x \in \mathbb{Z}[\sqrt{2}]$ est inversible si et seulement si $N(x) = \pm 1$.

5. Montrer qu'il y a une infinité d'éléments inversibles dans $\mathbb{Z}[\sqrt{2}]$.

6. Reprendre les questions précédentes en remplaçant $\sqrt{2}$ par $i\sqrt{2}$.

Exercice 7 : $\mathbb{Z}[i\sqrt{5}]$ n'est pas factoriel

On considère l'anneau $\mathbb{Z}[i\sqrt{5}] = \{P(i\sqrt{5}),\ P \in \mathbb{Z}[X]\}$.

En s'inspirant de l'exercice précédent, définir une norme sur cet anneau et montrer que l'élément 9 possède deux écritures non équivalentes comme produit d'éléments irréductibles. En déduire que cet anneau n'est pas factoriel.

II. Arithmétique des entiers : équations diophantiennes.

Exercice 8 : Équations diophantiennes de degré 1.

Résoudre les équations diophantiennes suivantes (c'est-à-dire trouver toutes leurs solutions $(x, y) \in \mathbb{Z}^2$) :

a. $7x - 9y = 0$ **b.** $7x - 9y = 1$ **c.** $7x - 9y = 5$

a. $21x - 49y = 12$ **b.** $21x - 49y = 14$.

Les deux exercices suivants s'intéressent à des équations diophantiennes de degré 2.

Exercice 9 : L'équation diophantienne $x^2 - y^2 = n$.

1. Résoudre l'équation diophantienne $x^2 - y^2 = p$ en $x, y \in \mathbb{Z}$, avec p premier.

2. Résoudre l'équation diophantienne $x^2 - y^2 = 15$ en $x, y \in \mathbb{Z}$.

Exercice 10 : L'équation diophantienne $x^2 + y^2 = p$. Entiers de Gauss.

Le problème est de déterminer les entiers qui s'écrivent comme somme de deux carrés. Dans cet exercice on résoudra le cas des entiers premiers, le cas général s'en déduisant (voir [Perrin] p.56).

Soit $\Sigma = \{n \in \mathbb{N} \mid n = x^2 + y^2,\ x, y \in \mathbb{N}\}$.

1. Déterminer les carrés de $\mathbb{Z}/4\mathbb{Z}$ et en déduire que si $n \in \Sigma$, alors $n \not\equiv 3$ [4].

2. Montrer que $2 \in \Sigma$ et que 2 n'est pas irréductible dans $\mathbb{Z}[i]$.

Pour mimer la méthode de l'exercice précédent dans $\mathbb{Z}$, on est naturellement conduit à étudier les éléments irréductibles de $\mathbb{Z}[i]$.

A. *La norme et les inversibles de $\mathbb{Z}[i]$.*

On considère l'application $N : \mathbb{Z}[i] \to \mathbb{N}$, appelée "norme", définie par $N(a+ib) = a^2+b^2$.

3. Montrer que N est multiplicative : pour tout $z, z' \in \mathbb{Z}[i]$, on a $N(z\,z') = N(z)\,N(z')$.

4. Déterminer $U(\mathbb{Z}[i])$.

5. En déduire qu'un nombre premier p appartient à Σ si et seulement si il n'est pas irréductible dans $\mathbb{Z}[i]$.

B. *L'anneau $\mathbb{Z}[i]$ est euclidien (donc principal, donc factoriel).*

6. Montrer que tout nombre complexe z est à distance euclidienne inférieure ou égale à $\frac{\sqrt{2}}{2}$ d'un élément de $\mathbb{Z}[i]$.

7. En déduire qu'il existe une division euclidienne dans $\mathbb{Z}[i]$ relativement à la norme N :

$$\forall a, b \in \mathbb{Z}[i],\ b \neq 0,\ \exists c, r \in \mathbb{Z}[i] \ \text{ tels que } a = bc + r \text{ et } N(r) < N(b)$$

(sans nécessairement unicité).

8. Faire la divisition euclidienne de $3 + 2i$ par $1 - 3i$ dans $\mathbb{Z}[i]$.

C. *Quotient par l'idéal engendré par un élément non irréductible.*

Soit p un nombre premier.

9. Montrer que p est irréductible dans $\mathbb{Z}[i]$ si et seulement si $\mathbb{Z}[i]/(p)$ est intègre (indication : utiliser le fait que l'anneau $\mathbb{Z}[i]$ est euclidien, donc factoriel).

10. En utilisant l'isomorphisme $\mathbb{Z}[i]/(p) \simeq \mathbb{F}_p[X]/(X^2+1)$ (voir exercice 18), en déduire que p est irréductible dans $\mathbb{Z}[i]$ si et seulement si le polynôme X^2+1 n'a pas de racine dans $\mathbb{F}_p$.

11. En déduire pour tout nombre premier p impair l'équivalence des propriétés suivantes :

a. p appartient à Σ

b. -1 est un carré dans $\mathbb{F}_p$

c. $(-1)^{\frac{p-1}{2}} = 1$

d. $p \equiv 1$ [4].

Les nombres premiers qui appartiennent à Σ sont donc 2 et les nombres premiers p tels que $p \equiv 1$ [4].

III. Arithmétique des polynômes.

Exercice 11 : Factorisation dans les anneaux de polynômes

Dans cet exercice on note 1 le neutre multiplicatif des corps ou anneaux. Donc pour les corps finis, en notation habituelle, on note 1 l'élément $\overline{1}$.

1. Factoriser le polynôme $X^4 - X^2 - 2$ en produit d'irréductibles dans les anneaux $\mathbb{C}[X]$, $\mathbb{R}[X]$ et $\mathbb{Q}[X]$.

2. Factoriser les polynômes $X^4 + X^2 + 1$ et $X^4 + 1$ en produit d'irréductibles dans les anneaux $\mathbb{C}[X]$, $\mathbb{R}[X]$, $\mathbb{Q}[X]$ et $\mathbb{F}_2[X]$ (indication : on peut utiliser une différence de deux carrés).

3. Montrer que le polynôme $X^4 + 1$ de l'anneau $\mathbb{F}_3[X]$ n'a pas de racine et le factoriser en produit d'irréductibles (indication : on peut à nouveau utiliser une différence de deux carrés).

4. Déterminer tous les diviseurs du polynôme $X^6 + 1$ dans les anneaux $\mathbb{F}_3[X]$, $\mathbb{F}_2[X]$, $\mathbb{Q}[X]$, $\mathbb{Z}[X]$.

Exercice 12 : Racines rationnelles d'un polynôme de $\mathbb{Z}[X]$ ou $\mathbb{Q}[X]$

Soit $P(X) = a_n X^n + \cdots + a_0$ un polynôme de $\mathbb{Q}[X]$ dont les coefficients $a_0, \ldots, a_n$ sont entiers.

1. Montrer que si un rationnel $x = \frac{p}{q}$ est racine de P, où p et q sont des entiers premiers entre eux, alors p divise a_0 et q divise a_n.

2. Les polynômes suivants de $\mathbb{Q}[X]$ ont-ils des racines dans $\mathbb{Q}$?

a. $5X^3 + X^2 - 1$ **b.** $X^4 + 3X^3 - 3X^2 - 12X - 4$ **c.** $X^3 + \frac{3}{2}X^2 - \frac{4}{3}X + \frac{1}{6}$.

Exercice 13 : Irréductibilité par réduction modulo 2 et 3

Soit P un polynôme unitaire de $\mathbb{Z}[X]$. Pour tout entier $n > 1$, on note $\overline{P}$ la réduction de P modulo n dans l'anneau de polynômes $\mathbb{Z}/n\mathbb{Z}[X]$ (le contexte donnant le n).

1. Montrer que si $\overline{P}$ est irréductible dans $\mathbb{Z}/n\mathbb{Z}[X]$ pour un certain entier $n > 1$, alors P est irréductible dans $\mathbb{Z}[X]$. La réciproque est-elle vraie ?
2. On considère le polynôme $P(X) = X^5 - 6X^3 + 2X^2 - 4X + 5$ de $\mathbb{Z}[X]$.
   (a) Calculer la réduction de P modulo 2 et la factoriser en produits d'irréductibles dans $\mathbb{F}_2[X]$ (indication : on pourra montrer et utiliser que $X^2 + X + 1$ est le seul polynôme irréductible de degré 2 de $\mathbb{F}_2[X]$).
   (b) En déduire que si P n'est pas irréductible dans $\mathbb{Z}[X]$, alors P possède un facteur unitaire de degré 1 (donc une racine dans $\mathbb{Z}$).
   (c) En utilisant la réduction de P modulo 3, montrer que P est irréductible dans $\mathbb{Z}[X]$.

Exercice 14 : Un polynôme sur le corps fini $\mathbb{F}_p$

Soit p un nombre premier.

1. Factoriser le polynôme $X^p - X$ dans l'anneau $\mathbb{F}_p[X]$ (indication : chercher ses racines).

2. En déduire que $(p-1)! \equiv -1\ [p]$ (théorème de Wilson).

3. En déduire également que $(X + \overline{1})^p = X^p + \overline{1}$ (indication : comparer les polynômes $(X + \overline{1})^p - (X + \overline{1})$ et $X^p - X$).

Exercice 15 : Un algorithme de factorisation dans $\mathbb{Z}[X]$

On considère le polynôme $P(X) = X^5 + X^4 + 2X^2 - 1$.

1. Montrer que si P n'est pas irréductible dans $\mathbb{Z}[X]$, alors il existe un polynôme de degré au plus deux qui divise P dans $\mathbb{Z}[X]$.

2. Soit $Q \in \mathbb{Z}[X]$ un polynôme de degré au plus 2 et qui divise P. À l'aide de $P(0)$, $P(1)$ et $P(-1)$, déterminer toutes les valeurs possibles pour $Q(0)$, $Q(1)$ et $Q(-1)$, puis toutes les valeurs possibles de Q.

3. Factoriser P dans $\mathbb{Z}[X]$.

Exercice 16 : Construction de corps finis [Skandalis, exercice 4.16]

1. Montrer que tout corps fini est de cardinal p^α pour un nombre premier p et un entier $\alpha \geq 1$.

2. Soit $\mathbb{K}$ un corps fini à q éléments. Combien y a-t-il de polynômes irréductibles unitaires de degré 2 dans $\mathbb{K}[X]$? de degré 3 ?

3. Déterminer les polynômes irréductibles unitaires de degré 2 et 3 dans $\mathbb{F}_2[X]$ et $\mathbb{F}_3[X]$.

4. **a.** Construire des corps à 4, 8, 9, 27 éléments.

b. Construire des corps à 25, 49, 121 éléments.

Exercice 17 : Anneau des polynômes sur un anneau non intègre et lemme chinois.

1. Déterminer les racines du polynôme $X^2 - \overline{1}$ de $\mathbb{Z}/15\mathbb{Z}[X]$, en remarquant qu'une racine est un élément de $(\mathbb{Z}/15\mathbb{Z})^\times$.

2. Soit n un entier impair, $n \geq 3$. Montrer que le nombre de racines du polynôme $X^2 - \overline{1}$ de $\mathbb{Z}/n\mathbb{Z}[X]$ est 2^k où k est le nombre de facteurs premiers de la décomposition de n (indication : réduire l'équation $x^2 - 1 \equiv 0\ [n]$ aux diviseurs de n).

Exercice 18 : Isomorphismes et quotients.

Pour tout $\omega \in \mathbb{C}$, on note $\mathbb{Z}[\omega] = \{P(\omega),\ P \in \mathbb{Z}[X]\}$.

1. Décrire les éléments de $\mathbb{Z}[\sqrt{2}]$, $\mathbb{Z}[i]$, $\mathbb{Z}[j]$, $\mathbb{Z}[i\sqrt[3]{5}]$, $\mathbb{Z}[\pi]$.

2. Montrer que les anneaux suivants sont isomorphes :

a. $\mathbb{Z}[\sqrt{2}]$ et $\mathbb{Z}[X]/(X^2 - 2)$. **b.** $\mathbb{Z}[i]$ et $\mathbb{Z}[X]/(X^2 + 1)$.

3. Décrire $\mathbb{Z}[j]$, $\mathbb{Z}[\frac{1+i}{2}]$ comme des quotients de l'anneau $\mathbb{Z}[X]$.

4. Montrer les isomorphismes suivants pour p premier et d entier, $d \geq 1$:

$$\mathbb{Z}[i\sqrt{d}]/(p) \simeq \mathbb{Z}[X]/(X^2 + d, p) \simeq \mathbb{F}_p[X]/(X^2 + d).$$