UNIVERSITÉ DE RENNES 1

Théorie des nombres

Feuille n°4 : Anneaux d'entiers

1 Rappels sur les anneaux

Exercice 1

1. Soit A un anneau (commutatif unitaire) et J un idéal de A. Montrer que les idéaux de A/J sont en bijection avec les idéaux de A contenant J.
2. Quels sont les idéaux de l'anneau $\mathbb{Z}/3^3 7^2\mathbb{Z}$? Quelles sont les relations d'inclusions entre eux ? Lesquels sont premiers ?

Exercice 2

Soit A un anneau commutatif intègre. Soit I l'idéal de $A[X,Y]$ engendré par $X+Y$.

1. Montrer que $A[X,Y]/I$ est isomorphe à l'anneau $A[X]$.
2. L'idéal I est-il premier ? Est-il maximal ?

Exercice 3

Soit A un anneau commutatif. On dit que $x \in A$ est nilpotent si il existe $n > 0$ tel que $x^n = 0$

1. Montrer que l'ensemble N des éléments nilpotents de A est un idéal de A.
2. Montrer que le quotient A/N n'a pas d'élément nilpotent.
3. Trouver un exemple d'anneau A avec deux éléments x et y nilpotents tels que $x+y$ n'est pas nilpotent.
4. Montrer que A n'a pas d'élément nilpotent si et seulement si tout élément inversible de $A[X]$ est constant.

2 Entiers algébriques

Exercice 4

Le nombre réel $\sqrt{5}$ est-il dans le corps $\mathbb{Q}(\sqrt[3]{5})$? et dans $\mathbb{Q}(\sqrt[6]{5})$? Existe-t-il un morphisme de corps de $\mathbb{Q}(\sqrt[3]{5})$ dans $\mathbb{C}$ qui envoie $\sqrt[3]{5}$ sur 5 ?

Exercice 5

1. Montrer que le polynôme $2X^3 - 2X + 5$ n'a pas de racine rationnelle.
2. Soit ζ une solution complexe de l'équation $2X^3 - 2X + 5$. Est-ce un entier algébrique ? Déterminer un entier naturel c tel que $c\zeta$ soit un entier algébrique.
3. Les solutions complexes de l'équation
$$X^2 + \left(\frac{1+\sqrt{5}}{2}\right) X - 1$$
sont-elles des nombres algébriques ? sont-elles des entiers algébriques ? Déterminer pour elles, un polynôme annulateur sur $\mathbb{Z}$.
4. Déterminer un polynôme annulateur sur $\mathbb{Z}$ de $\sqrt{2} + \sqrt[3]{5}$.

Exercice 6

1. Déterminer le degré sur $\mathbb{Q}$ de l'extension $\mathbb{Q}(\sqrt[3]{5})$.
2. Le nombre réel $\sqrt{5}$ est-il dans $\mathbb{Q}(\sqrt[6]{5})$? et dans $\mathbb{Q}(\sqrt[3]{5})$?
3. Le nombre complexe $\theta = j\sqrt[3]{5}$ est-il dans l'image de tous les plongements complexes de $\mathbb{Q}(\theta)$?
4. Existe-t-il un plongement de $\mathbb{Q}(\sqrt[3]{5})$ dans $\mathbb{C}$ qui envoie $\sqrt[3]{5}$ sur 5 ?

Exercice 7

1. Soit K un corps de nombres. Soit a un élément primitif de K. Rappeler le lien entre le polynôme minimal de a sur $\mathbb{Q}$ et la trace ou la norme de a.
2. Calculer la norme de $a + 1$ et celle de $a^2 + a$ dans $\mathbb{Q}[X]/(X^3 - X - 2)$ où a est la classe de X.

Exercice 8

1. Montrer qu'après un changement de variable affine tout polynôme P unitaire de $\mathbb{Q}[X]$ de degré 3 s'écrit sous la forme $X^3 + pX + q$. Montrer que P est alors irréductible si et seulement si $X^3 + pX + q$ l'est.

2. Soit X^3+pX+q un polynôme irréductible de $\mathbb{Q}[X]$. Soit $K=\mathbb{Q}[X]/(X^3+pX+q)$ et a un élément de $\sigma(K)$ où σ est un plongement complexe de K. Montrer que a est un entier algébrique si et seulement si $\mathrm{Tr}(a)$, $\mathrm{Tr}(a^2)$ et $\mathrm{Tr}(a^3)$ sont des entiers relatifs.
3. Montrer que si a et b sont deux entiers algébriques $\mathrm{Tr}(ab)$ est un entier.

Exercice 9

Soient p un nombre premier et $P \in \mathbb{Z}[X]$. On note $\bar{P}$ la réduction modulo p de P, c'est à dire l'élément de $\mathbb{Z}/p\mathbb{Z}[X]$ dont les coefficients sont les coefficients de P réduits modulo p.

1. Soit $P \in \mathbb{Z}[X]$ un polynôme unitaire. Montrer que si $\bar{P}$ est irréductible dans $\mathbb{Z}/p\mathbb{Z}[X]$, alors P est irréductible dans $\mathbb{Z}[X]$.
2. Le polynôme X^3-X-1 est-il irréductible dans $\mathbb{Q}[X]$?
3. Montrer que X^2+4 est irréductible dans $\mathbb{Z}[X]$ mais réductible dans $\mathbb{Z}/2\mathbb{Z}[X]$.

Exercice 10

1. Enoncer le critère d'Eisenstein.
2. L'équation X^5+6X^4-12 a-t-elle des solutions dans $\mathbb{Z}$, dans $\mathbb{Q}$?

3 Anneaux d'entiers

Exercice 11

On considère l'anneau $A=\mathbb{Z}[i]$. Montrer que $(1-i)$ est irréductible dans A. Vérifier que l'on a dans A

$$5=(2+i)(2-i)=(1+2i)(1-2i),$$

et que ceci ne contredit pas la factorialité de A.

Exercice 12

1. Montrer que l'anneau $\mathbb{Z}[(1+\sqrt{N})/2]$ est le $\mathbb{Z}$-module libre de base $(1,(1+\sqrt{N})/2)$
2. Montrer que si a et b sont deux entiers de même parité $\frac{a+b\sqrt{N}}{2}$ est dans $\mathbb{Z}[(1+\sqrt{N})/2]$.

Exercice 13

1. Montrer que les unités de l'anneau des entiers d'un corps de nombres sont les entiers de norme 1 ou -1.

2. Soit ζ un entier algébrique, unité de l'anneau des entiers d'un corps de nombres, de polynôme minimal sur $\mathbb{Z}$: $P(X) = a_d X^d + a_{d-1} X^{d-1} + \cdots + a_1 X + a_0$. Que peut-on dire de a_d et de a_0 ? Déterminer en fonction de ζ et des a_i l'inverse de ζ.

Exercice 14

Considérons l'anneau $\mathbb{Z}[\sqrt{13}]$. À tout élément $x = a + b\sqrt{13}$ de $\mathbf{Z}[\sqrt{13}]$ on associe son conjugué $\overline{x} = a - b\sqrt{13}$.

1. Montrer que pour tous $x, y \in \mathbb{Z}[\sqrt{13}]$ on a

$$\overline{x+y} = \overline{x} + \overline{y} \quad \text{et} \quad \overline{xy} = \overline{x}\,\overline{y}.$$

2. En considérant l'application $N\colon \mathbb{Z}[\sqrt{13}] \to \mathbb{Z}, x \mapsto x\overline{x}$, caractériser le groupe U des éléments inversibles de $\mathbb{Z}[\sqrt{13}]$. Vérifier que ± 1, $\pm 18 \pm 5\sqrt{13}$ sont dans U.
3. Montrer que les éléments 2, $3 + \sqrt{13}$, $-3 + \sqrt{13}$ sont irréductibles dans $\mathbb{Z}[\sqrt{13}]$.
4. Montrer que l'anneau $\mathbb{Z}[\sqrt{13}]$ n'est pas factoriel.