Feuille d'exercices n° 4

ANNEAUX ET CORPS

1 Généralités

1.1

Soit A un anneau. Il contient un neutre pour l'addition, 0, et un neutre pour le produit, 1. Montrer que si $0 = 1$, alors $A = \{0\}$.

1.2 Éléments non nuls, diviseurs de zéro, etc.

Dans un anneau A commutatif unitaire, on considère les parties suivantes :

1. les éléments qui ne sont pas diviseurs de zéro ;
2. les éléments non nuls ;
3. les éléments inversibles.

Quelle relation y a-t-il entre ces différentes parties ? Donner un exemple où elles sont toutes distinctes. Comment appelle-t-on un anneau où elles sont toutes égales ?

1.3

Pour quels entiers n est-ce que $\mathbb{Z}/n\mathbb{Z}$ est un corps ?

1.4

Lesquels de ces sous-ensembles donnés de $\mathbb{C}$ sont des anneaux ? Lesquels sont des corps ?

1. $\bigcup_{n\in\mathbb{N}} 10^{-n}\mathbb{Z}$;
2. $\{\frac{m}{n} \mid m \in \mathbb{Z}, n \in \mathbb{N}^*, (m,n) = 1, p \nmid n\}$ (p est un nombre premier fixé) ;
3. $\mathbb{Z}[\sqrt{-1}] = \mathbb{Z} + \mathbb{Z}\sqrt{-1}$;
4. $\mathbb{Q}[\sqrt{-1}] = \mathbb{Q} + \mathbb{Q}\sqrt{-1}$.

2 Vols de canards

2.1 Étude algébrique

Soit $A = \mathbb{Z}[\sqrt{2}] = \{x + y\sqrt{2},\ (x,y) \in \mathbb{Z}^2\}$. Pour $(x,y) \in \mathbb{Z}^2$, on note $N(x + y\sqrt{2}) = x^2 - 2y^2$.

1. Vérifier que $N(zz') = N(z)N(z')$ pour tout $(z,z') \in A^2$.
2. Soit $z \in A$. Montrer que z est inversible si et seulement si $N(z) = \pm 1$.
3. Montrer que les éléments inversibles de A sont, au signe près, les puissances de $1 + \sqrt{2}$.

2.2

Les canards volent en groupes triangulaires constitués d'un chef suivi de deux sous-chefs, trois sous-sous-chefs, etc. Un vol de canards subit un violent coup de vent et se divise en deux groupes de même taille. Par chance, ces deux groupes peuvent à nouveau former deux vols de canards. Combien peut-il y avoir de canards ? [*Multiplier par* 4 *après avoir chassé les dénominateurs.*]

2.3

Quels sont les nombres qui sont à la fois triangulaires et carrés ? *Résoudre* $n(n+1)/2 = m^2$.

3 Idéaux

3.1

Soit I un idéal d'un anneau commutatif A. On note par $(a) = a \cdot A$ l'idéal principal engendré par a. Montrer que :

1. $I = A$ si et seulement si I contient une unité ;
2. $(a) = A$ ssi a est inversible ;
3. Supposons A intègre. Montrer que les conditions suivantes sont équivalentes :
   (a) On a $(a) = (b)$;
   (b) Il existe un élément inversible $u \in A$ tel que $a = ub$.
4. Un anneau A est un corps ssi (0) est le seul idéal propre de A.

3.2

1. Rappeler quels sont les idéaux de $\mathbb{Z}$.
2. Déterminer les idéaux de $\mathbb{Z}/12\mathbb{Z}$ et de $\mathbb{Z}/48\mathbb{Z}$.

3.3 Idempotents et nilpotents

1. Résoudre dans $\mathbb{Z}/35\mathbb{Z}$, puis dans $\mathbb{Z}/48\mathbb{Z}$, l'équation $x^2 = x$. Établir un lien avec le théorème chinois.
2. Déterminer les éléments nilpotents (ceux dont une puissance est nulle) de $\mathbb{Z}/48\mathbb{Z}$.

3.4 Sommes, intersection et produits d'idéaux

1. Soient I, J deux idéaux d'un anneau A. Montrer que
$$I \cap J, \qquad I + J = \{x + y \,|\, x \in I, y \in J\}$$
sont des idéaux de A.
2. Montrer que $I + J$ est le plus petit idéal de A contenant I et J.
3. Soit $n, m \in \mathbb{Z}$, $I = (n) = n\mathbb{Z}$, $J = (m) = m\mathbb{Z}$. Trouver $I \cap J$ et $I + J$.
4. Montrer que
$$I \cdot J = \{x_1y_1 + x_2y_2 + \ldots x_ny_n \,|\, n \in \mathbb{N},\ x_k \in I,\ y_k \in J \text{ pour } 1 \leqslant k \leqslant n\}$$
est un idéal. Il s'appelle *produit des idéaux* I et J.

3.5

Dans un anneau A, on appelle *radical* d'un idéal I et on note $\sqrt{I}$ l'ensemble des éléments $a \in A$ tels qu'il existe $n \in \mathbb{N}^*$ tel que $a^n \in I$.

1. Montrer que $\sqrt{I}$ est un idéal de A.
2. Vérifier que $I \subset \sqrt{I}$ et que $\sqrt{\sqrt{I}} = \sqrt{I}$.
3. Soient I et J des idéaux de A. Montrer que l'on a $\sqrt{I \cap J} = \sqrt{I} \cap \sqrt{J} = \sqrt{I \cdot J}$.
4. Dans $\mathbb{Z}$, déterminer $\sqrt{48\mathbb{Z}}$.

4 Corps

4.1

Donner quatre exemples de corps autres que $\mathbb{Q}$, $\mathbb{R}$ et $\mathbb{C}$.

4.2 Morphisme

Montrer que tout morphisme de corps est injectif.

4.3

Soit $\mathbb{K}$ un corps, on note $\varphi : \mathbb{Z} \to \mathbb{K}$ l'application définie par : $\varphi(0) = 0$ et, pour $n \in \mathbb{N}$, $\varphi(n+1) = \varphi(n)+1$ et $\varphi(-n) = -\varphi(n)$. Vérifier que φ est un morphisme et que son noyau est de la forme $p\mathbb{Z}$, où p est un nombre premier ou zéro. En déduire qu'un corps fini contient $\mathbb{Z}/p\mathbb{Z}$ pour p premier convenable.

4.4

Construire un corps de cardinal 4 (resp. 9) : donner ses tables d'addition et de multiplication.

4.5

Soit p un nombre premier, soit $n = p - 1$ et soit $G = (\mathbb{Z}/p\mathbb{Z})^*$. On veut montrer que G est cyclique.

1. Quels sont les ordres possibles des éléments de G ?
2. Soit d un diviseur de n. Montrer qu'il y a au plus $\varphi(d)$ éléments d'ordre d dans G.
3. En déduire que G contient des éléments d'ordre n : combien y en a-t-il ?

5 Polynômes

5.1

Rappeler le théorème de division euclidienne dans $\mathbb{K}[X]$ (où $\mathbb{K}$ est un corps).

5.2

1. Soit A un anneau quelconque. Alors l'anneau de polynômes $A[X]$ n'est pas un corps.
2. Montrer que pour un anneau intègre A, les polynômes unitaires linéaires de $A[X]$ sont irréductibles.
3. Décrire tous les polynômes irréductibles de $\mathbb{C}[X]$ et de $\mathbb{R}[X]$.
4. Démontrer que pour tout corps $\mathbb{K}$, l'anneau de polynômes $\mathbb{K}[X]$ a une infinité de polynomes unitaires irréductibles.

5.3 Anneau principal

1. Montrer que l'idéal (X, n) où $n \in \mathbb{Z}$, $n > 1$ de l'anneau $\mathbb{Z}[X]$ n'est pas principal.
2. Soit A un anneau intègre. Montrer que $A[X]$ est principal ssi A est un corps.

5.4

Soient m et n deux entiers supérieurs ou égaux à 2. Calculer le reste de la division euclidienne de $(X-2)^m + (X-1)^n - 1$ par $(X-1)(X-2)$ dans $\mathbb{Z}[X]$.

5.5

Soient a et b deux entiers naturels non nuls.

1. Soient q et r le quotient et le reste de la division de a par b. Effectuer la division de $X^a - 1$ par $X^b - 1$. En déduire que le reste est $X^r - 1$.
2. En déduire que le PGCD de $X^a - 1$ et $X^b - 1$ est $X^d - 1$, où d est le PGCD de a et b.

5.6

Vrai ou faux ?

1. Tout polynôme de degré 3 sur $\mathbb{R}$ est réductible.
2. Tout polynôme de degré 3 sur $\mathbb{Q}$ est réductible.

5.7

Écrire sous forme de produits de polynômes irréductibles les polynômes suivants :

1. $X^2 + bX + c \in \mathbb{C}[X]$, où $b, c \in \mathbb{C}$;
2. $X^2 + bX + c \in \mathbb{R}[X]$, où $b, c \in \mathbb{R}$;
3. $X^4 + 1 \in \mathbb{C}[X]$ puis dans $\mathbb{R}[X]$ et dans $\mathbb{Q}[X]$;
4. $X^3 - X - 30$ et $X^3 + X + 30$ dans $\mathbb{Q}[X]$ et dans $\mathbb{Z}[X]$;
5. $X^{2017} + 21X^{49} + 49X^{21} + 70$ dans $\mathbb{Q}[X]$;
6. $X^4 - X$ dans $\mathbb{Z}[X]$.

5.8

Montrer que f est irréductible dans $\mathbb{Q}[x]$:

1. $f = X^4 - 8X^3 + 12X^2 - 6X + 2$;
2. $f = X^5 - 12X^3 + 36X - 12$;
3. $f = X^4 - X^3 + 2X + 1$;
4. $f = X^{p-1} + \cdots + X + 1$, où p est premier.

5.9 Polynômes positifs

Un polynôme réel $P \in \mathbb{R}[X]$ est dit positif si $P(a) \geqslant 0$ pour tout a réel. On veut montrer que tout polynôme positif est la somme de deux carrés.

1. Rappeler quels sont les polynômes irréductibles de $\mathbb{R}[X]$. En déduire qu'un polynôme positif est le produit de puissances paires de polynômes de degré 1 et de polynômes de degré 2 sans racine réelle.
2. Démontrer que la propriété est vraie pour les polynômes de degré 2 sans racine réelle.
3. En s'inspirant du fait que le produit des modules est le module du produit, montrer que le produit de la somme de deux carrés est une somme de deux carrés.
4. Prouver la propriété.

5.10 Polynômes sur un corps fini

1. Si $\mathbb{K}$ est un corps, montrer qu'un polynôme P de degré 2 ou 3 dans $\mathbb{K}[X]$ est irréductible si et seulement si il n'a pas de zéro dans $\mathbb{K}$.
2. Trouver tous les polynômes irréductibles de degré 2, 3 à coefficients dans $\mathbb{Z}/2\mathbb{Z}$.
3. En utilisant la partie précédente, montrer que les polynômes
$$5X^3 + 8X^2 + 3X + 15 \qquad \text{et} \qquad X^5 + 2X^3 + 3X^2 - 6X - 5$$
sont irréductibles dans $\mathbb{Z}[X]$.
4. Décrire tous les polynômes irréductibles de degré 4 et 5 sur $\mathbb{Z}/2\mathbb{Z}$.

6 Polynômes cyclotomiques

Pour $n \in \mathbb{N}^*$, on considère le polynôme
$$\Phi_n(X) = \prod_{0 \leqslant k < n,\ k \wedge n = 1} (X - exp^{2i\pi/n}).$$

6.1 Définition et propriétés standards

Soit $n \in \mathbb{N}^*$. On note μ_n est l'ensemble des racines primitives n-ièmes de l'unité dans $\mathbb{C}$. Le n-ième polynôme cyclotomique est le polynôme
$$\Phi_n(X) = \prod_{\zeta \in \mathcal{P}_n} (X - \zeta).$$

1. Calculer Φ_n pour $1 \leqslant n \leqslant 8$.
2. Rappeler pourquoi $\deg \Phi_n = |\mu_n| = \varphi(n)$, l'indicatrice d'Euler.
3. Démontrer que l'on a :
$$X^n - 1 = \prod_{d|n} \Phi_d(X).$$
Quelle relation retrouve-t-on en comparant les degrés de ces polynômes ?
4. A priori, on a : $\Phi_n \in \mathbb{C}[X]$. Montrer par récurrence que l'on a en fait : $\Phi_n \in \mathbb{Z}[X]$.
5. Montrer que pour $n = p$ premier, Φ_p est irréductible. [*Considérer* $P = X^p - 1$ *et poser* $X = Y + 1$ *; appliquer le critère d'Eisenstein.*]
REMARQUE : On peut montrer que Φ_n est irréductible pour tout $n \geqslant 1$.