Feuille de TD n° 1
Révisions sur les anneaux, corps, algèbres sur un corps

Exercice 1

Soient k un corps, A un anneau et $\varphi : k \to A$ un morphisme d'anneaux. Montrer que φ est injectif.

Exercice 2

Soient A et B des anneaux commutatifs unitaires. Une structure de A-*algèbre* sur B est la donnée d'une application

$$\begin{aligned} A \times B &\to B \\ (a,b) &\mapsto a \cdot b \end{aligned}$$

(permettant de multiplier un élément de B par un élément de A), vérifiant les conditions suivantes :
- pour tout $b \in B$, $\quad 0 \cdot b = 0$ et $1 \cdot b = b$,
- pour tous $a \in A$, $b, b' \in B$, $\quad a \cdot (b + b') = a \cdot b + a \cdot b'$,
- pour tous pour tous $a, a' \in A$, $b \in B$, $\quad (a + a') \cdot b = a \cdot b + a' \cdot b$,
- pour tous $a \in A$, $b, b' \in B$, $\quad (a \cdot b)b' = a \cdot (bb')$.
- pout tous $a, a' \in A$, $b \in B$, $\quad (aa') \cdot b = a \cdot (a' \cdot b)$.

(1) Montrer que tout anneau commutatif B a une structure naturelle de $\mathbb{Z}$-algèbre.

(2) Soit k un corps, et B une k-algèbre. Vérifier que B a une structure de k-espace vectoriel.

(3) Soit k un corps, et B une k-algèbre. Montrer que tout idéal I de B a une structure de k-espace vectoriel.

(4) Soit k un corps.

  (a) Vérifier que l'anneau de polynômes $k[X]$ est une k-algèbre.

  (b) Soit $f \in k[X]$ un polynôme non constant. Vérifier que $B = k[X]/(f)$ est une k-algèbre. Trouver les idéaux de B.

  (c) Les anneaux $\mathbb{R}[X]/(X^2+1)$ et $\mathbb{C}[X]/(X^2+1)$ sont-ils des corps ? Sinon, exhiber un élément non nul non inversible.

(5) Soient A et B des anneaux commutatifs unitaires. Une autre définition de A-algèbre est la suivante. Une structure de A-algèbre sur B est la donnée d'un morphisme d'anneaux ϕ de A dans B (appelé *morphisme structurel*).

Montrer l'équivalence de ces deux définitions.

Exercice 3

Soit X un espace topologique. Soit $\mathscr{C}(X,\mathbb{R})$ l'ensemble des fonctions continues de X dans $\mathbb{R}$.

(1) Montrer que $\mathscr{C}(X,\mathbb{R})$ est une $\mathbb{R}$-algèbre.

(2) Soit $x \in X$, notons φ_x l'application d'évaluation en x :

$$\begin{aligned} \varphi_x : \mathscr{C}(X,\mathbb{R}) &\longrightarrow \mathbb{R} \\ f &\mapsto f(x). \end{aligned}$$

  (a) Soit $x \in X$. Montrer que φ_x est surjective.

  (b) Déterminer le noyau M_x de φ_x.

(c) Montrer que M_x est un idéal maximal de $\mathscr{C}(X, \mathbb{R})$.

Exercice 4

Soit A un anneau intègre (en particulier, commutatif). On dit que A est un anneau euclidien s'il existe une fonction $f : A \setminus \{0\} \to \mathbb{N}$ (appelée *stathme* ou *jauge euclidienne*) satisfaisant la condition suivante (i.e. on peut faire une division euclidienne)

– pour tout $a \in A$ et tout $b \in A \setminus \{0\}$, il existe $q, r \in A$ tels que $a = bq + r$ et et ($r = 0$ ou $f(r) < f(b)$).

(1) L'anneau $\mathbb{Z}$ est euclidien, rappeler pour quel stathme.

(2) Soit k un corps. On rappelle que l'anneau $k[X]$ est euclidien. Pour quel stathme ?

(3) Montrer que tout anneau euclidien est principal. Conclure que $\mathbb{Z}$ et $k[X]$ sont principaux, et donc factoriels.

(4) Soit A un anneau intègre qui n'est pas un corps.

(a) Soit $a \in A$ un élément non nul non inversible. Montrer que l'idéal $I = (a, X) \subset A[X]$ engendré par a et X est contenu *strictement* dans $A[X]$.

(b) Montrer par l'absurde que I n'est pas un idéal principal. Conclure que $A[X]$ n'est pas principal.

(c) Conclure que, pour tout anneau commutatif unitaire A, on a les équivalences suivantes :

$$A[X] \text{ est euclidien } \Leftrightarrow A[X] \text{ est principal } \Leftrightarrow A \text{ est un corps.}$$

(d) Donner un exemple d'anneau A tel que $A[X]$ est factoriel mais pas principal.

(e) Soit k un corps. L'anneau $k[X, Y]$ est-il principal ?

Exercice 5

On note $\mathbb{Z}[i]$ le sous-anneau de $\mathbb{C}$ engendré par i. C'est l'anneau des entiers de Gauß.

1. Montrer que $\mathbb{Z}[i]$ est un anneau intègre.
2. Montrer que $\mathbb{Z}[i] = \{a + bi \mid a, b \in \mathbb{Z}\}$.
3. Construire un isomorphisme de $\mathbb{Z}[X]/(X^2 + 1)$ dans $\mathbb{Z}[i]$.
4. Montrer que l'application $N : \mathbb{Z}[i] \to \mathbb{N}$ définie par $N(a + ib) = a^2 + b^2 = |a + ib|^2$ est multiplicative, c'est-à-dire vérifie $N(zz') = N(z)N(z')$ pour tous $z, z' \in \mathbb{Z}[i]$.
5. Quel est le groupe des éléments inversibles de l'anneau $\mathbb{Z}[i]$? (On l'appelle aussi groupe des unités de $\mathbb{Z}[i]$).
6. Montrer que $\mathbb{Z}[i]$ est euclidien (et donc principal).
7. Déterminer un générateur de l'idéal de $\mathbb{Z}[i]$ engendré par $3 + 4i$ et $1 + 3i$.
8. Soit p un nombre premier impair, considérons les conditions suivantes :

   (a) -1 est un carré modulo p ;

   (b) le polynôme $X^2 + 1 \in \mathbb{Z}/p\mathbb{Z}[X]$ n'est pas irréductible ;

   (c) l'idéal (p) de $\mathbb{Z}[i]$ n'est pas premier ;

   (d) l'entier p est une somme de carrés dans $\mathbb{Z}$;

   Montrer que ces conditions sont équivalentes.

Exercice 6

Soit k un corps et soit A l'ensemble des polynômes de $k[X]$ sans terme en X, c'est-à-dire $A = \mathrm{Vect}_k(X^i, i \in \mathbb{N} \setminus \{1\})$.

(1) Montrer que A est un sous-anneau de $k[X]$. Quels sont les éléments inversibles de A ?

(2) Soit m un nombre entier, $m \geqslant 2$.

(a) Donner les diviseurs de X^m dans A.

(b) Pour quelles valeurs de m le polynôme X^m est-il un élément irréductible de A ?

(c) Pour quelles valeurs de m le polynôme X^m est-il un élément premier de A ?

(d) L'anneau A est-il factoriel ?

(3) Soit I l'idéal de A engendré par X^2 et X^3. Est-il principal ?

(4) Donner deux factorisations non équivalentes de X^6 en produit d'irréductibles dans A.

Exercice 7

(1) Soit k un corps fini. Calculer $\prod_{x \in k^*} x$.

(2) En déduire le théorème de Wilson : pour tout nombre premier p,

$$(p-1)! \equiv -1 \ [p].$$

Exercice 8

Soit f un endomorphisme du groupe $\mathbb{R}$.

(1) Montrer que f est $\mathbb{Q}$-linéaire.

(2) On suppose que f vérifie au moins une des propriétés suivantes :

(i) f est continue

(ii) f est continue en 0.

(iii) Il existe $a, b \in \mathbb{R}$ avec $a < b$ tels que f est bornée sur l'intervalle $]a, b[$.

(iv) f est monotone.

Montrer que f est $\mathbb{R}$-linéaire. En déduire que f est une homothétie.

(3) Quels sont les automorphismes de corps de $\mathbb{R}$?