CP GE RÉSEAU IBNGHAZI

Classe MP*1
Groupe 2

My Ismail Mamouni

http ://myismail.net

Feuille d'exercices N° 4

Structures : Anneaux & Corps

Exercice 1 : Anneau quotient

Soit A un anneau, I un idéal de A. On définit la relation d'équivalence sur I $\mathscr{R}_I$ par

$$x\mathscr{R}_I y \iff x - y \in I\,.$$

L'ensemble quotient se note A/I (c'est bien entendu cohérent avec la notation usuelle puisque I est un sous-groupe du groupe additif A et $\mathscr{R}_I$ la relation habituelle).

1) Soit $\mathscr{R}$ une relation d'équivalence sur un anneau A. Montrer qu'il existe sur $A/\mathscr{R}$ une structure de groupe telle que la surjection canonique π soit un morphisme d'anneaux (cette structure étant alors unique) si et seulement si $\mathscr{R}$ est compatible avec les deux lois de A. De plus, montrer que si ces conditions sont vérifiées, il existe un idéal I de A tel que $\mathscr{R} = \mathscr{R}_I$ (remarquer que I est nécessairement la class de 0).

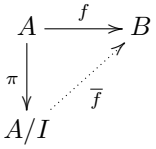
2) Décrire la classe de x pour $\mathscr{R}_I$.

3) Montrer que la relation $\mathscr{R}_I$ est compatible avec les lois de A. En déduire qu'il existe une unique structure d'anneau sur A telle que la surjection canonique soit un morphisme d'anneaux.

4) Montrer que tout idéal de A est le noyau d'un morphisme (qu'on peut supposer surjectif) d'anneaux.

5) **Propriété universelle du quotient.** Soient A un anneau, I un idéal de A et $\pi : A \to A/I$ la surjection canonique. On considère un anneau B et $f : A \to B$ un morphisme d'anneaux. Montrer l'équivalence des trois propriétés suivantes

(i) Il existe une application $\overline{f} : A/I \to B$ telle que $f = \overline{f} \circ \pi$ i.e. telle que le diagramme suivant soit commutatif



(ii) $I \subset \ker f$

(iii) $f(I) = \{0_A\}$.

Montrer que lorsque ces conditions sont vérifiées, l'application $\overline{f}$ est uniquement définie et que c'est un morphisme de d'anneaux. Vérifier que $\operatorname{Im}\overline{f} = \operatorname{Im} f$ et $\ker\overline{f} = \ker f/H$ et que $\overline{f}$ est donnée par $\overline{f}(\overline{x}) = f(x)$ pour tout $x \in A$ (où $\overline{x} = \pi(x)$ désigne la classe de x dans A/I).

Morale (à retenir) : *se donner un morphisme d'anneaux issu d'un quotient, c'est la même chose que de se donner un morphisme trivial sur l'idéal par lequel on veut quotienter. C'est donc très facile de construire des morphismes issus de quotients.*

6) Montrer que l'application

$$\begin{aligned} \operatorname{Hom}_{\text{ann.}} A/IB &\longrightarrow \operatorname{Hom}_{\text{gr.}} AB \\ \varphi &\longmapsto \varphi \circ \pi \end{aligned}$$

est une application injective dont on déterminera l'image. Pour un élément de l'image, on décrira l'unique antécédent.

Exercice 2 : Eléménts nilpotent et radical

1) Déterminer les éléments nilpotents de $\mathbb{Z}/n\mathbb{Z}$.

2) Soit k un corps et $P \in k[X]$. Déterminer les éléments nilpotents de $k[X]/(P)$.

3) On suppose que A est un anneau commutatif. Montrer que l'ensemble des éléments nilpotents de A est un idéal de A ? Le résultat s'étend-il à un anneau non commutatif ?

4) On suppose encore que A est commutatif. On considère un idéal I de A. Montrer que l'ensemble

$$\sqrt{I} = \{x \in A \mid \exists n \in \mathbb{N},\ x^n \in I\}$$

est un idéal contenant I. Que vaut $\sqrt{0}$? Calculer $\sqrt{\sqrt{I}}$?

5) Décrire l'idéal de A/I correspondant à $\sqrt{I}$.

6) Montrer que l'intersection des idéaux premiers de A contenant I est $\sqrt{I}$ (c'est une question difficile : on pourra montrer que si $x \notin \sqrt{I}$, l'ensemble des idéaux contenant I ne rencontrant pas l'ensemble $\{x^n \mid n \in \mathbb{N}\}$ est non vide et admet un élément maximal qui est un idéal premier de A).

7) Montrer que $A/\sqrt{0}$ est un anneau réduit (i.e. n'a pas d'élément nilpotent non nul).

Exercice 3 : Caractéristique

1) Propriété universelle de l'anneau $\mathbb{Z}$. Soit A un anneau unitaire. Montrer qu'il existe un unique morphisme d'anneaux unitaires $f : \mathbb{Z} \to A$. Vérifier qu'il est donné par $f(k) = k1_A$.

Le noyau de l'unique morphisme $f : \mathbb{Z} \to A$ est de la forme $n\mathbb{Z}$ pour un unique $n \in \mathbb{N}$. Cet entier n est appelé la *caractéristique de l'anneau* A. C'est le plus petit entier non nul (s'il existe) tel que $n1_A = 0$. Il vérifie aussi $na = 0$ pour tout $a \in A$ (pourquoi ?).

2) Montrer que le sous-anneau premier de A est isomorphe à $\mathbb{Z}/\mathrm{car}(A)\mathbb{Z}$.

3) Montrer que si A est un sous-anneau de B alors $\mathrm{car}(A) = \mathrm{car}(B)$.

4) Soit $g : A \to B$ un morphisme d'anneau. Comparer la caractéristique de A et celle de B. En déduire que si $\mathrm{car}(A)$ et $\mathrm{car}(B)$ sont premiers entre eux alors il n'y a pas de morphisme d'anneaux entre A et B.

5) Quelle est la caractéristique de $\mathbb{Z}/n\mathbb{Z}$, de $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{R}[X]$?

6) Quelle est la caractéristique de $\mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$? et celle de $\mathbb{Z}/8\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z}$?

7) Quelle est la caractéristique de $\prod_{n\in\mathbb{N}} \mathbb{Z}/n\mathbb{Z}$?

8) Quelle peut être la caractéristique d'un anneau intègre ? d'un corps ?

9) Montrer qu'il n'existe pas de morphisme de corps entre deux corps n'ayant pas la même caractéristique.

10) Montrer qu'un anneau de caractéristique p (premier) peut être muni d'une structure d'espace vectoriel sur le corps $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$.

11) Montrer que si A et B sont deux anneaux de caractéristique p et $f : A \to B$ un morphisme d'anneaux alors f est $\mathbb{F}_p$ linéaire pour la structure définie dans la question précédente.

12) Montrer qu'il n'existe aucun morphisme d'anneaux unitaires de $\mathbb{Q}$ (resp. $\mathbb{R}, \mathbb{C}, \mathbb{Z}/n\mathbb{Z}$ avec $n \geq 1$) dans $\mathbb{Z}$.

13) Montrer que l'unique morphisme d'anneaux unitaires $f : \mathbb{Z} \to \mathbb{Q}$ vérifie que pour tous morphismes d'anneaux unitaires $g, h : \mathbb{Q} \to A$ tel que $g \circ f = h \circ f$, on a $h = g$.

Exercice 4 : Morphisme de IR

Soit $f : \mathbb{R} \to \mathbb{R}$ un endomorphisme d'anneau.

1) Calculer $f(n)$ pour $n \in \mathbb{Z}$ puis pour $f \in \mathbb{Q}$.

2) Montrer que $f(x) \geq 0$ si $x \geq 0$ (on caractérisera la positivité d'un réel en terme algébrique).

3) En déduire que f est croissante.

4) En déduire que $f = \mathrm{Id}_{\mathbb{R}}$.

5) Soit $f : \mathbb{C} \to \mathbb{C}$ un endomorphisme d'anneau. Montrer l'équivalence

(i) f est l'identité ou la conjugaison ;

(ii) f est continu ;

(iii) $f(\mathbb{R}) \subset \mathbb{R}$;

(iv) $f(x) = x$ pour tout $x \in \mathbb{R}$.

Definition 1 (Idéal premier)**.** Soit I un idéal de A un anneau commutatif. On dit que I est un idéal premier si les propriétés équivalentes suivantes sont vérifiées

(i) A/I est intègre ;

(ii) $I \neq A$ et $xy \in I \Longleftrightarrow x \in I$ ou $y \in I$.

(iii) $A \setminus I$ est une partie multiplicative de A.

Definition 2 (Idéal maximal)**.** Soit I un idéal de A un anneau commutatif. On dit que I est un idéal maximal si les propriétés équivalentes suivantes sont vérifiées

(i) A/I est un corps ;

(ii) $I \neq A$ et si J est un idéal tel que $I \subset J$ alors $J = A$ ou $J = I$;

(iii) I est un élément maximal (pour l'inclusion) parmi les idéaux distincts de A.

Exercice 5 : Idéaux premiers, maximaux

1) Soit A un anneau intègre. Montrer que si A contient un nombre fini d'idéaux alors A est un corps (on pourra considérer les idéaux de la forme (a^n)).

2) Montrer que tout idéal premier de A est maximal.

Soit A un anneau commutatif. Montrer qui si A contient un nombre fini d'idéaux alors tout idéal premier est maximal.

3) Soit A un anneau tel que tout idéal est premier. Montrer que A est un corps (on pourra considérer les idéaux de la forme (x^2)).

Exercice 6 : Lemme de Zorn

Soit A un anneau commutatif.

1) On suppose que $A \neq \{0\}$. Montrer que A admet un idéal maximal.

2) Soit $I \neq A$ un idéal de A. Montrer qu'il existe un idéal maximal de A contenant I (on pourra appliquer la question précédente à A/I).

3) Soit $f \in A$. On note $S = \{f^n \mid n \in \mathbb{N}\}$. à quelle condition l'ensemble des idéaux ne rencontrant pas S admet un élément maximal. Montrer qu'un tel idéal maximal est premier. En déduire que l'intersection des idéaux premiers de A est formée des éléments nilpotents de A.

Exercice 7 : Les carrés dans un corps fini

1) On suppose dans cette question que k est un corps fini de caractéristique 2. Montrer que tout élément de k est un carré.

On suppose pour le reste de l'exercice que k est un corps fini de caractéristique $p \neq 2$. On note $q = p^d = |k|$. Pour les questions c et e, proposer deux méthodes : l'une élémentaire (avec le théorème de Lagrange et le fait que dans un corps, un polynôme de degré d a au plus d racines), l'autre reposant sur la cyclicité de $k^\times$.

2) Déterminer les solutions de l'équation $x^2 = 1$ dans k.

3) Montrer que, dans k, il y a exactement $(q+1)/2$ carrés (indication pour la méthode élémentaire : étudier le morphisme de groupes $x \in k^\times \mapsto x^2 \in k^\times$).

4) Montrer que $x^{(q-1)/2} \in \{\pm 1\}$ pour tout $x \in k^\times$.

5) Montrer que $x \in k^\times$ est un carré dans k si et seulement si $x^{(q-1)/2} = 1$.

6) Montrer que -1 est un carré dans k si et seulement si $q = 1[4]$. En déduire que -1 est un carré modulo p si et seulement si $p = 1[4]$.

Exercice 8 : Elements premiers, irréductibles

Soit A un anneau commutatif.

1) Soit $p \in A$. Montrer l'équivalence des deux propriétés suivantes

(i) p est non nul non inversible et si $p \mid ab$ alors $p \mid a$ ou $p \mid b$;

(ii) (p) est un idéal premier non nul.

Un élément vérifiant ces propriétés est appelé *élément premier de A*.

2) Soit $p \in A$. On suppose que A est **intègre**. Montrer l'équivalence des deux propriétés suivantes

(i) p est non inversible et si $p = ab$ alors a est inversible ou b est inversible ;

(ii) (p) est non nul et maximal parmi les idéaux de A qui sont principaux et distincts de A.

Un élément vérifiant ces propriétés est appelé *élément irréductible de A*.

3) Déterminer les éléments premiers (resp. irréductible) d'un corps, de $\mathbb{Z}$, $k[T]$.

4) Montrer que T est un élément premier de $A[T]$ si et seulement si A est intègre.

5) Montrer qu'un élément premier est toujours irréductible (si A est intègre).

6) Montrer que dans un anneau principal, un élément irréductible est premier.

Exercice 9 : Les anneaux de Gauss

Soit $n \in \mathbb{Z}$ un entier qui n'est pas un carré. On note $x \in \mathbb{C}$ une racine du polynôme $X^2 - n$.

1) Montrer que $\mathbb{Q}[x] := \{a + bx \mid a, b \in \mathbb{Q}\}$ est un sous-corps de $\mathbb{C}$ de dimension 2 sur $\mathbb{Q}$ et isomorphe à $\mathbb{Q}[X]/X^2 - n$ via le morphisme d'évaluation en x. En déduire que l'écrire sous la forme $a + bx$ détermine a et b.

2) On définit l'application

$$\begin{aligned} \sigma : \quad \mathbb{Q}[x] &\longrightarrow \mathbb{Q}[x] \\ a + bx &\longmapsto a - bx. \end{aligned}$$

Montrer que l'application σ est un automorphisme de $\mathbb{Q}$-algèbre. Calculer son inverse.

3) On désigne par $\mathbb{Z}[x] := \{a + bx, a, b \in \mathbb{Z}\}$. Montrer que $\mathbb{Z}[x]$ est un sous-anneau de $\mathbb{Q}[x]$ et que σ induit par restriction un isomorphisme de $\mathbb{Z}[x]$.

4) Pour $z = a + bx \in \mathbb{Q}[x]$, on pose $N(z) = z\sigma(z) = a^2 - b^2 n$. Montrer que $N(zz') = N(z)N(z')$ pour tous $z, z' \in \mathbb{Q}[x]$.

5) Montrer que $N(z) = 0$ si et seulement si $z = 0$.

6) Montrer que si $z \in \mathbb{Z}[x]$ alors $N(z) \in \mathbb{Z}$.

7) Montrer que si $z \in \mathbb{Z}[x]$ alors z est inversible dans $\mathbb{Z}[x]$ si et seulement si $N(z) \in \{-1, 1\}$.

8) Montrer qu'il existe une décomposition en irréductible dans $\mathbb{Z}[x]$.

9) Dans le cas où $n = -5$, montrer que $\mathbb{Z}[x]$ n'est pas factoriel : on pourra considérer $6 = 2 \cdot 3 = (1-x)(1+x)$. Déterminer les inversibles de $\mathbb{Z}[x]$. Trouver un idéal non principal de $\mathbb{Z}[x]$.

10) Dans le cas où $n = -1$, montrer que l'anneau $\mathbb{Z}[i]$ des entiers de Gauss est euclidien pour la fonction N (pour effectuer la division euclidienne de a par b dans $\mathbb{Z}[i]$, on pourra considérer le quotient ab^{-1} dans $\mathbb{Q}[i]$ et choisir l'élément de $\mathbb{Z}[i]$ le plus proche : on fera un dessin). Déterminer les inversibles de $\mathbb{Z}[i]$.

11) Montrer que le résultat de la question précédente s'étend au cas où $n = -2$, $n = 2$ et $n = 3$.

Exercice 10 : Les anneaux euclidiens

Soit A un anneau euclidien est un *intègre* tel qu'il existe une fonction appelée stathme $\varphi : A \setminus \{0\} \to \mathbb{N}$ telle que pour tout $a, b \in A \times A \setminus \{0\}$, il existe $q, r \in A$ tel que $a = bq + r$ avec $r = 0$ ou $\varphi(r) < \varphi(b)$

1) Dans un anneau euclidien, écrire un algorithme d'Euclide étendu permettant le calcul d'une relation de Bézout.

2) Montrer qu'un anneau euclidien est principal.

3) Montrer que $k[X]$ et $\mathbb{Z}$ sont euclidiens.

Exercice 11 : le théorème des deux carrés

$$\mathbb{Z}[i] = \{a + ib, \quad a, b \in \mathbb{Z}\} \subset \mathbb{C}.$$

1) Montrer que c'est un sous-anneau de $\mathbb{C}$ appelé l'*anneau des entiers de Gauss*.

2) On définit l'application norme

$$N : \mathbb{Z}[i] \longrightarrow \mathbb{N}$$
$$z \longmapsto z\overline{z}\,.$$

Montrer que N est une fonction multiplicative puis déterminer les inversibles de l'anneau $\mathbb{Z}[i]$.

3) Montrer que $\mathbb{Z}[i]$ est euclidien.

4) Montrer si m et n sont tous deux sommes de deux carrés d'entiers, alors mn est somme de deux carrés également.

5) Soit p un entier premier. Montrer que p est une somme de deux carrés si et seulement si p n'est pas irréductible dans $\mathbb{Z}[i]$.

6) **à SAVOIR FAIRE ABSOLUMENT.** Soit p un entier premier. Montrer que les anneaux $\mathbb{Z}[i]/(p)$ et $\mathbb{F}_p[X]/(X^2+1)$ sont isomorphes. En déduire que p est irréductible dans dans $\mathbb{Z}[i]$ si et seulement si -1 n'est pas un carré dans $\mathbb{Z}/p\mathbb{Z}$.

7) Soit p un entier premier. Déduire de ce qui précède que p est une somme de deux carrés si et seulement si $p = 1$ ou 2 [4].

8) Démontrer le théorème des deux carrés : soit n un entier naturel et

$$n = \prod_p p^{v_p(n)}$$

sa décomposition en facteurs premiers. Alors n est somme de deux carrés d'entiers si et seulement si $v_p(n)$ est pair pour tout entier premier p tel que $p = 3$ [4].

Exercice 11 : Exemple d'anneau principal non euclidien

$A = \mathbb{Z}[\alpha] = \{P(\alpha), \quad P \in \mathbb{Z}[X]\}$. A de $\mathbb{C}$ engendré par $\alpha := (1 + i\sqrt{19})/2$:

Le but de cet exercice est de démontrer que A n'est pas euclidien, puis de démontrer que A est principal en utilisant une "division euclidienne affaiblie".

1) Vérifier que $\alpha^2 - \alpha + 5 = 0$. Montrer que $A = \{a + b\alpha \mid a, b \in \mathbb{Z}\}$.

2) Montrer que A est stable par conjugaison. On définit $N(z) = z\overline{z}$ pour $z \in A$. à l'aide de N, décrire $A^\times$.

3) Montrer que A n'est pas euclidien (utiliser le critère de l'exercice 45).

4) Soient $z, z' \in A$ non nuls. Montrer qu'il existe $q, r \in A$ vérifiant les deux conditions suivantes :

(i) $N(r) < N(z')$,

(ii) $z = z'q + r$ ou $2z = z'q + r$.

(on pourra écrire $z/z' = u + v\alpha$ avec $u, v \in \mathbb{Q}$, soit $n = E(v)$ et discuter selon que $v \in \left]n + \frac{1}{3}, n + \frac{2}{3}\right[$ ou pas).

5) Montrer que (2) est un idéal maximal de A (on pourra vérifier que $A \cong_{ann.} \mathbb{Z}[X]/(X^2 - X + 5)$).

6) Montrer que A est principal.