MAT4111
Premier semestre — 2021–2022

Fiche 0: Révisions sur les anneaux

1. Soit k un sous-anneau de $\mathbb{R}$. Soit $\mathsf{ev}_{\sqrt{2}} : k[X] \to \mathbb{R}$ le morphisme d'anneaux qui au polynôme $P \in k[X]$ associe $P(\sqrt{2})$.

(*a*) Calculer le noyau $\mathsf{Ker}(\mathsf{ev}_{\sqrt{2}})$ de $\mathsf{ev}_{\sqrt{2}}$ pour $k = \mathbb{R}$, $k = \mathbb{Q}$ et $k = \mathbb{Z}$. Le noyau est-il un idéal premier de $k[X]$? Et maximal ?

(*b*) On fixe désormais $k = \mathbb{Z}$.

(i) Donner un idéal maximal de $\mathbb{Z}[X]$ qui contient $\mathsf{Ker}(\mathsf{ev}_{\sqrt{2}})$.

(ii) Existe-t-il un idéal maximal de $\mathbb{Z}[X]$ qui contient $X + 1$ et $\mathsf{Ker}(\mathsf{ev}_{\sqrt{2}})$?

(iii) Existe-t-il un idéal maximal de $\mathbb{Z}[X]$ qui contient $X + 4$ et $\mathsf{Ker}(\mathsf{ev}_{\sqrt{2}})$?

2. *Anneau des décimaux.*

(*a*) Montrer que $10X - 1$ est irréductible dans $\mathbb{Z}[X]$.

(*b*) On note $\mathbb{D}$ *l'anneau des décimaux*, *i.e.* l'ensemble des réels ayant un développement décimal fini. Montrer que $\mathbb{D}$ est un anneau. Est-ce un corps ?

(*c*) Montrer que $\mathbb{D} = \mathbb{Z}[1/10]$, *i.e.* est égal au plus petit sous-anneau de $\mathbb{Q}$ contenant $\mathbb{Z}$ et $1/10$.

(*d*) Montrer que $\mathbb{D} \simeq \mathbb{Z}[X]/(10X - 1)$.

(*e*) L'idéal $(10X - 1)$ de $\mathbb{Z}[X]$ est-il premier ? maximal ? Le cas échéant, trouver un idéal propre de $\mathbb{Z}[X]$ contenant $(10X - 1)$. *Indication :* on pourra montrer que si un tel idéal existe, il ne peut être principal.

(*f*) Montrer que $\mathbb{D}$ est principal.

3. *Morphismes d'anneaux et idéaux.* Soit $f : A \to B$ un morphisme d'anneaux.

(*a*) Montrer que si K est un idéal de B, alors $f^{-1}(K)$ est un idéal de A.

(*b*) Montrer que si J est un idéal de A et f est surjective, alors $f(J)$ est un idéal de B.

4. *Idéaux d'un anneau quotient.* Soit I un idéal d'un anneau A et soit $\pi : A \to A/I$ le morphisme quotient.

(*a*) Montrer que l'application image réciproque $\pi^{-1} : \mathscr{P}(A/I) \to \mathscr{P}(A)$, où $\mathscr{P}(E)$ désigne l'ensemble des parties de l'ensemble E, réalise une bijection entre l'ensemble des idéaux de A/I et l'ensemble des idéaux de A contenant I. Par abus de notation, on notera par la suite J/I l'idéal $\pi(J)$.

(*b*) Montrer que si J est un idéal de A contenant I, alors $(A/I)/(J/I)$ est isomorphe à A/J.

(*c*) Montrer que A/I est un corps si et seulement si I est maximal.

(*d*) Si A est principal, montrer que tout idéal de A/I est principal.

(*e*) Donner la liste des idéaux de $\mathbb{Z}/n.\mathbb{Z}$, où n est un entier strictement positif.

5. On considère les six anneaux suivants :

$$\mathbb{R}[X]/(X^2-1),\ \mathbb{R}[X]/(X^2+X+1),\ \mathbb{R}[X]/(X^3-1),$$
$$\mathbb{R}[X]/(X^2+1),\ \mathbb{R}[X]/(X^2-5X+6)\ \text{ et }\ \mathbb{R}[X]/(X^2+2X+1).$$

Lesquels sont isomorphes entre eux ?

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

⋆ **7.** *Anneau local.* On appelle *anneau local* un anneau ayant un unique idéal à gauche maximal. On suppose désormais que l'anneau est commutatif et l'on appelle *corps résiduel* d'un anneau local son quotient par l'unique idéal maximal.

(*a*) Soit A un anneau local d'idéal maximal $\mathfrak{m}$. Montrer que $\mathfrak{m}$ est égal à $A\backslash A^\times$, l'ensemble des éléments non inversibles de A. *Indication :* utiliser le théorème de Krull (*i.e.* tout idéal propre d'un anneau est contenu dans un idéal maximal).

(*b*) Montrer qu'un anneau non nul A est local si et seulement si l'ensemble de ses éléments non inversibles est un idéal, et si et seulement si la somme de deux éléments non inversibles n'est jamais inversible.

(*c*) On va construire un exemple d'anneau local. Soit $K[X]$ l'anneau des polynômes à une indéterminée sur un corps K et $R \in K[X]$ un polynôme irréductible. On considère

$$A = \left\{ \frac{P}{Q} : R \nmid Q \right\}.$$

Montrer que A est un sous-anneau du corps des fractions rationnelles à une indéterminée $K(X)$ et qu'il est local d'idéal maximal RA.

(*d*) Montrer que son corps résiduel est isomorphe à $K[X]/(R)$.

⋆ **8.** *Divisibilité et éléments associés.*

(*a*) Soient A un anneau commutatif intègre et $a, b \in A$ non nuls tels que $a|b$ et $b|a$. Montrer que a et b sont fortement associés, *i.e.* qu'il existe un élément u inversible de A tel que $a = ub$.

(*b*) Ceci n'est pas forcément vrai dans un anneau non intègre. Soit K un corps, on pose $A = K[X,Y,Z]/(X - XYZ)$. On note x, y, z les classes de X, Y, Z dans A.

(i) Montrer que A n'est pas intègre.

(ii) Montrer que $x|xy$ et $xy|x$, *i.e.* x et xy sont associés.

(iii) Soit $u \in A$ tel que $xy = xu$. On cherche à montrer par l'absurde que u n'est pas inversible. On suppose que v est un inverse de u et on note respectivement U et V les représentants de u et v dans $K[X,Y,Z]$. En particulier, il existe $P, Q \in K[X,Y,Z]$ tels que $UV = 1 + X(1-YZ)P$ et $Y = U + (1-YZ)Q$. Montrer que $YV(0,Y,Z) - 1 = (1-YZ)Q(0,Y,Z)V(0,Y,Z)$ et en déduire une contradiction en raisonnant sur le degré de $V(0,Y,Z)$ par rapport à Z.

9. *Diviseurs de zéro et éléments non inversibles.* Soit A un anneau commutatif et $x \in A$ un élément non nul. On considère l'application $f : A \to A$ donnée par $a \mapsto xa$.

(*a*) Montrer que f est injective si et seulement si x n'est pas un diviseur de 0.

(*b*) Montrer que f est surjective si et seulement si x est inversible.

(*c*) Montrer que si A est de cardinalité finie, alors tout élément non nul de A est soit inversible soit un diviseur de 0.

(*d*) Même question lorsque A est une K-algèbre de dimension finie.

(*e*) Donner un exemple d'anneau admettant des éléments non inversibles et non diviseurs de zéro.

10. *Anneaux* $\mathbb{Z}[\sqrt{d}]$. Soit d un entier non carré.

(*a*) Montrer que $\mathbb{Z}[\sqrt{d}] = \{a + b\sqrt{d} : a, b \in \mathbb{Z}\}$ est un anneau (où par convention $\sqrt{d} = i\sqrt{|d|}$, quand d est négatif) et qu'il est isomorphe à $\mathbb{Z}[X]/(X^2 - d)$.

(*b*) Si $w = a + b\sqrt{d}$, on note $\bar{w} = a - b\sqrt{d}$. Montrer que $w \mapsto \bar{w}$ est un automorphisme de $\mathbb{Z}[\sqrt{d}]$.

(*c*) On pose $N : \mathbb{Z}[\sqrt{d}] \to \mathbb{Z}$, $w = a + b\sqrt{d} \mapsto w\bar{w} = a^2 - db^2$.

(i) Montrer que N est *multiplicative*, *i.e.* $N(xy) = N(x)N(y)$.

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

(iii) Montrer que si $N(x)$ est un nombre premier, alors x est irréductible. En considérant par exemple $3 \in \mathbb{Z}[i]$, montrer que la réciproque est fausse en général.

(*d*) Déterminer $\mathbb{Z}[\sqrt{d}]^\times$ pour $d < 0$.

11. *PGCD et PPCM.* Soient a et b deux éléments d'un anneau commutatif intègre A. On rappelle que $d \in A$ est un *PGCD* de a et b si $d|a$ et $d|b$ et si pour tout élément $c \in A$ tel que $c|a$ et $c|b$ on a $c|d$. Similairement, on dit que $m \in A$ est un *PPCM* de a et b si $a|m$ et $b|m$ et si pour tout élément $c \in A$ tel que $a|c$ et $b|c$ on a $m|c$.

(*a*) On suppose que a et b admettent un PGCD d. Montrer que l'ensemble des PGCD de a et b est exactement l'ensemble des associés de d. Même question pour le PPCM.

(*b*) On suppose que A est principal.

(i) En considérant les ensembles $(a)+(b)$ et $(a)\cap(b)$, montrer que tout couple d'éléments de A possède un PGCD et un PPCM.

(ii) Soient $a, b \in A$. Déterminer l'ensemble des éléments $c \in A$ tels que l'équation $au + bv = c$ admette des solutions (u, v).

(*c*) On prend $A = \mathbb{R}[X, Y]$. Déterminer un PGCD de X et Y . L'équation $uX + vY = 1$ admet-elle des solutions ?

12. *Sur l'anneau* $\mathbb{Z}[i\sqrt{3}]$. On prend $A = \mathbb{Z}[i\sqrt{3}] = \{a + ib\sqrt{3} : a, b \in \mathbb{Z}\}$.

(*a*) Vérifier que A est un sous-anneau de $\mathbb{C}$ (donc intègre).

(*b*) Montrer que le carré du module de tout élément de A est un entier non négatif. En déduire que 2 et $1 \pm i\sqrt{3}$ sont irréductibles dans A.

(*c*) Montrer que 4 possède deux factorisations non équivalentes comme produits des irréductibles.

(*d*) Est-ce que l'idéal $(2) \subseteq \mathbb{Z}[i\sqrt{3}]$ est premier ?

(*e*) Montrer que 4 et $2 + 2i\sqrt{3}$ n'admettent pas de PGCD.

(*f*) Montrer qu'ils n'ont pas de PPCM non plus.

13. *Quelques racines de l'unité.* On considère le sous-groupe $\boldsymbol{\mu}_8$ de $\mathbb{C}$ constitué des racines huitièmes de l'unité dans $\mathbb{C}$, *i.e.* $\boldsymbol{\mu}_8 = \{z \in \mathbb{C} : z^8 = 1\}$.

(*a*) Montrer qu'un élément z de $\boldsymbol{\mu}_8$ est d'ordre 8 si et seulement si $z^4 = -1$.

(*b*) En déduire que $\boldsymbol{\mu}_8$ possède exactement 4 éléments d'ordre 8.

(*c*) Établir la liste des éléments d'ordre 8 de $\boldsymbol{\mu}_8$.

(*d*) Quelle est la décomposition du polynôme $X^4 + 1$ en produit de facteurs irréductibles de $\mathbb{C}[X]$?

(*e*) Quelle est la décomposition du polynôme $X^4 + 1$ en produit de facteurs irréductibles de $\mathbb{R}[X]$?

(*f*) Le polynôme X^4+1 est-il irréductible dans $\mathbb{Q}[X]$?

(*g*) On considère $\zeta_8 = e^{i\pi/4}$ et le morphisme d'évaluation $\mathrm{ev}_{\zeta_8} : \mathbb{Q}[X] \to \mathbb{C}$ qui à un polynôme $P \in \mathbb{Q}[X]$ associe $P(\zeta_8)$.

(i) L'image $\mathsf{Img}(\mathrm{ev}_{\zeta_1})$ de ev_{ζ_8} est-elle un sous-anneau de $\mathbb{C}$?

(ii) Déterminer le noyau de ev_{ζ_8}.

(iii) Existe-t-il un morphisme d'anneaux $f : \mathbb{Q}[X]/(X^8-1) \to \mathbb{C}$ tel que ev_{ζ_8} soit égal à $f \circ \pi$, où $\pi : \mathbb{Q}[X] \to \mathbb{Q}[X]/(X^8-1)$ est le morphisme de passage au quotient ?

(iv) Existe-t-il un morphisme d'anneaux $g : \mathbb{Q}[X]/(X^4+1) \to \mathbb{C}$ tel que ev_{ζ_8} soit égal à $g \circ \pi$, où $\pi : \mathbb{Q}[X] \to \mathbb{Q}[X]/(X^4+1)$ est le morphisme de passage au quotient ?

(v) L'image $\mathsf{Img}(\mathrm{ev}_{\zeta_1})$ de ev_{ζ_1} est-elle un sous-corps de $\mathbb{C}$?

(*h*) On note $\zeta_8^3 = e^{i3\pi/4}$ et on considère le morphisme d'anneaux $\mathrm{ev}_{\zeta_8^3} : \mathbb{Q}[X] \to \mathbb{C}$ qui à un polynôme $P \in \mathbb{Q}[X]$ associe $P(\zeta_8^3)$.

(i) Quel est le noyau de $\mathrm{ev}_{\zeta_8^3}$?

(ii) Montrer que ζ_8^3 est dans l'image $\mathsf{Img}(\mathrm{ev}_{\zeta_8})$ de ev_{ζ_8} et ζ_8 est dans l'image $\mathsf{Img}(\mathrm{ev}_{\zeta_8^3})$ de $\mathrm{ev}_{\zeta_8^3}$. En déduire que $\mathsf{Img}(\mathrm{ev}_{\zeta_8}) = \mathsf{Img}(\mathrm{ev}_{\zeta_8^3})$, que l'on notera A.

(iii) Montrer qu'il existe un isomorphisme d'anneaux $\phi : A \to A$ qui satisfait que $\phi(\zeta_8) = \zeta_8^3$.

14. *Les entiers de Gauss. Application au théorème des deux carrés.*
Soit $\mathbb{Z}[i] = \{a+ib : a, b \in \mathbb{Z}\} \subseteq \mathbb{C}$.

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

(*b*) On définit l'application norme $N : \mathbb{Z}[i] \to \mathbb{N}$, $z \mapsto z\bar{z}$. Montrer que N est une fonction multiplicative, puis déterminer les inversibles de l'anneau $\mathbb{Z}[i]$.

(*c*) Montrer que pour tout $z \in \mathbb{C}$, il existe $w \in \mathbb{Z}[i]$ tel que $|z-w| < 1$.

(*d*) Montrer que $\mathbb{Z}[i]$ est euclidien, *i.e.* qu'il existe une division euclidienne pour la norme N. Plus précisément, montrer que pour tout couple $a, b \in \mathbb{Z}[i]$, $b \neq 0$, il existe $q, r \in \mathbb{Z}[i]$ tels que $a = bq + r$ et $N(r) < N(b)$.

(*e*) En déduire que $\mathbb{Z}[i]$ est un anneau principal.

(*f*) Soit p un entier premier. Montrer que les anneaux $(\mathbb{Z}/p\mathbb{Z})[X]/(X^2+1)$ et $\mathbb{Z}[i]/(p)$ sont isomorphes. En déduire que p est irréductible dans $\mathbb{Z}[i]$ si et seulement si -1 n'est pas un carré dans $\mathbb{Z}/p\mathbb{Z}$, et donc si et seulement si $p = 3 \pmod 4$.

(*g*) Soit p un entier premier non congru à $3 \pmod 4$. En considérant la norme, montrer qu'il existe un élément irréductible π tel que $p = \pi\bar{\pi}$.

(*h*) Soit π un élément irréductible de $\mathbb{Z}[i]$. Montrer que $(\pi) \cap \mathbb{Z}$ est un idéal premier de $\mathbb{Z}$. En déduire que les irréductibles de $\mathbb{Z}[i]$ sont :

(i) les nombres entiers premiers congrus à $3 \pmod 4$ et leurs associés,

(ii) les éléments dont la norme est un entier premier, non congru à $3 \pmod 4$.

(*i*) 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 $2 \pmod 4$.

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

(*k*) Démontrer finalement le théorème des deux carrés : soit n un entier naturel et soit $n = \prod_p p^{v_p(n)}$ sa décomposition en facteurs premiers. Alors n est une somme de deux carrés d'entiers si et seulement si $v_p(n)$ est pair pour tout entier premier p tel que $p = 3 \pmod 4$.

⋆ **15.** *Fibonacci et* $\mathbb{Z}[\varphi]$.
On considère le sous-anneau A de $\mathbb{C}$ engendré par $\varphi = (1+\sqrt{5})/2$, *i.e.*

$$A = \mathbb{Z}[\varphi] = \{P(\varphi) : P \in \mathbb{Z}[X]\}.$$

(*a*) Vérifier que $\varphi^2 - \varphi - 1 = 0$. En déduire que $A = \{a + b\varphi : a, b \in \mathbb{Z}\}$.

(*b*) On note $\bar{\varphi} = (1-\sqrt{5})/2 = 1 - \varphi$ et si $w = a + b\varphi \in A$, on note $\bar{w} = a + b\bar{\varphi}$. Montrer que $w \mapsto \bar{w}$ est un automorphisme de A.

(*c*) On pose $N : A \to \mathbb{Z}$, $w = a + b\varphi \mapsto w\bar{w} = (a + b\varphi)(a + b\bar{\varphi})$.

(i) Montrer que $x \in A$ est inversible si et seulement si $N(x) = \pm 1$.

(ii) Montrer que φ est inversible dans A d'inverse $-\bar{\varphi} = \varphi - 1$.

(*d*) Soit $(F_n)_{n\in\mathbb{N}}$ la suite de Fibonacci. On rappelle que cette suite est définie par $F_0 = 0$, $F_1 = 1$ et $F_{n+2} = F_{n+1} + F_n$.

(i) Montrer que pour tout $n \in \mathbb{N}^*$, $\varphi^n = F_{n-1} + F_n\varphi$.

(ii) En déduire que l'ensemble des inversibles de A est de cardinalité infinie.

(iii) En déduire que $\mathbb{Z}[\sqrt{5}]^\times$ est infini.