Vincent Beck

Arithmétique

Exercice 1

a) Montrer que 2 et X sont premiers entre eux dans $\mathbb{Z}[X]$ mais que 1 n'est pas dans l'idéal $(2, X)$.

b) Montrer que $(2, X)$ n'est pas un idéal principal de $\mathbb{Z}[X]$.

c) Montrer que (X, Y) n'est pas un idéal principal de $A[X, Y]$ (où A est un anneau commutatif unitaire).

d) Montrer que (X) est un idéal premier de $K[X, Y]$. Quel est le quotient ?

e) Parmi les idéaux $(2X)$, (X, Y) et $(2, X, Y)$ de $\mathbb{Z}[X, Y]$, lesquels sont premiers ? maximaux ?

f) Soit $a \in A$. Montrer que $A[X]/(X - a)$ est isomorphe à A.

Exercice 2 Soit A un anneau commutatif unitaire. Montrer l'équivalence des trois propriétés suivantes

(i) A est un corps ;
(ii) A[X] est un anneau euclidien ;
(iii) A[X] est un anneau intègre.

Exercice 3 Soit k un corps et $P \in k[X]$. Montrer que $k[X]/(P)$ est un corps si et seulement si P est irréductible.

Exercice 4 soit K un corps. Montrer que $K[[X]]$ est un anneau euclidien.

Exercice 5 – Théorème chinois. Résoudre dans $\mathbb{Z}$ le système d'équation

a) $\begin{cases} x = 1\,[3] \\ x = 4\,[5] \\ x = 0\,[7] \end{cases}$

b) $\begin{cases} x = 4\,[15] \\ x = 8\,[21] \end{cases}$

c) $\begin{cases} x = 11\,[15] \\ x = 8\,[21] \end{cases}$

d) Trouver dans $\mathbb{Z}/7\mathbb{Z}[X]$ les polynômes tel que $f(0) = 3$, $f(1) = 0$ et $f(2) = 6$.

Exercice 6 Soit $n \in \mathbb{Z}$ un entier qui n'est pas un carré. On note $x \in \mathbb{C}$ une racine du polynôme $X^2 - n$.

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

b) On définit l'application

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

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

c) 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 $\mathbb{Z}[x]$.

d) 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 tout $z, z' \in \mathbb{Q}[x]$.

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

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

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

h) Il existe une décomposition en irréductible dans $\mathbb{Z}[x]$.

i) 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 $\mathbb{Z}[x]$.

j) 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 $\mathbb{Z}[i]$.

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

Exercice 7 — Questions en vrac.

a) Soit A un anneau euclidien de stathme ν. Montrer que si $\nu(x) = 0$ alors x est inversible.

b) Montrer que $\text{pgcd}\,(a_1, \ldots, a_m) = \text{pgcd}\,(\text{pgcd}\,(a_1, \ldots, a_k), \text{pgcd}\,(a_{k+1}, \ldots, a_n))$. Même question pour le ppcm.

Exercice 8

a) Calculer le pgcd de $\mathrm{P} = 2\mathrm{X}^4 - 3\mathrm{X}^2 + 1$ et $\mathrm{Q} = \mathrm{X}^3 + \mathrm{X}^2 - \mathrm{X} - 1$ dans $\mathbb{Q}[\mathrm{X}]$ et $\mathrm{U}, \mathrm{V} \in \mathbb{Q}[\mathrm{X}]$ tel que $\text{pgcd}\,(\mathrm{P}, \mathrm{Q}) = \mathrm{UP} + \mathrm{VQ}$. Même question dans $\mathbb{R}[\mathrm{X}]$.

b) Calculer l'inverse de $\mathrm{X}^3 - \mathrm{X} + 1$ dans $\mathbb{Q}[\mathrm{X}]/(\mathrm{X}^2 + \mathrm{X} + 1)$.

c) Calculer $\text{pgcd}\,(\mathrm{X}^n - 1, \mathrm{X}^m - 1)$.

d) Montrer que $\text{pgcd}\,(m, n) = 1$ si et seulement si m est inversible dans $\mathbb{Z}/n\mathbb{Z}$.

Exercice 9

a) Donner la liste des polynômes irréductibles de degré inférieure où égal à 4 dans $\mathbb{F}_2[\mathrm{X}]$.

b) Calculer s'il existe l'inverse de $\mathrm{X}^2 + 1$ dans $\mathbb{F}_2[\mathrm{X}]/(\mathrm{X}^5 + \mathrm{X}^2 + 1)$.

c) L'anneau $\mathbb{F}_2[\mathrm{X}]/(\mathrm{X}^5 + \mathrm{X}^2 + 1)$ est-il un corps ?

d) Montrer que $\mathbb{F}_5[\mathrm{X}]/(\mathrm{X}^2 + \mathrm{X} + 2)$ et $\mathbb{F}_5[\mathrm{X}]/(\mathrm{X}^2 + 2)$ sont des corps. Quel est leur cardinal ? On note α (resp. β) la classe de X dans $\mathbb{F}_5[\mathrm{X}]/(\mathrm{X}^2 + \mathrm{X} + 2)$ (resp. dans $\mathbb{F}_5[\mathrm{X}]/(\mathrm{X}^2 + 2)$) Définit-on un morphisme de $\mathbb{F}_5$-algèbres en posant $\varphi(\alpha) = \beta^6$ (resp. $\varphi(\alpha) = 2\beta + 2$) ? Si oui, est-ce un isomorphisme ?

Exercice 10 — Critère d'Eisenstein. Soit A un anneau factoriel, $\mathrm{P} \in \mathrm{A}[\mathrm{X}]$ avec $\mathrm{P} = a_n\mathrm{X}^n + \cdots + a_0$ ($a_n \neq 0$) et $p \in \mathrm{A}$ un irréductible. On suppose que $p \nmid a_n$, $p \mid a_i$ pour tout $i \in [\![\, 0\,,\, n-1 \,]\!]$ et $p^2 \nmid a_0$. L'objectif est de montrer que P est irréductible sur $\text{Frac}(\mathrm{A})[\mathrm{X}]$.

a) On suppose que P n'est pas irréductible sur $\text{Frac}(\mathrm{A})[\mathrm{X}]$. Montrer qu'on peut écrire $\mathrm{P} = \mathrm{QR}$ avec $\deg \mathrm{Q} < \deg \mathrm{P}$ et $\deg \mathrm{R} < \deg \mathrm{P}$ et $\mathrm{QR} \in \mathrm{A}[\mathrm{X}]$.

b) Montrer que Q et R ont tous leurs coefficients sauf le coefficient dominant qui sont divisibles par p (on pourra réduire modulo p l'égalité $\mathrm{P} = \mathrm{QR}$).

c) Obtenir une contraction en considérant le coefficient de plus bas degré de P.

d) En déduire que si P est primitif alors P est irréductible sur $\mathrm{A}[\mathrm{X}]$.

e) Donner un exemple où P n'est pas primitif. En déduire que le critère d'Eisenstein ne donne pas l'irréductibilité dans $\mathrm{A}[\mathrm{X}]$.

Exercice 11 — Application du critère d'Eisenstein.

a) Soit P un nombre premier. Montrer que $\mathrm{P}(\mathrm{X}) = \mathrm{X}^{p-1} + \mathrm{X}^{p-2} + \cdots + \mathrm{X} + 1$ est irréductible sur $\mathbb{Q}$ (considérer $\mathrm{P}(\mathrm{X} + 1)$)

b) Montrer que $\mathrm{X}^n - 2$ est irréductible sur $\mathbb{Q}$ et sur $\mathbb{Z}$.

c) Soit A un anneau factoriel de caractéristique différentes de 2, $n \in \mathbb{N}$ et $n \geqslant 2$. Montrer que ${\mathrm{X}_1}^2 + \cdots + {\mathrm{X}_n}^2 - 1$ est irréductible dans $\mathrm{A}[\mathrm{X}_1, \ldots, \mathrm{X}_n]$. Que se passe-t-il en caractéristique 2 ?

Exercice 12

a) Montrer que tout idéal de $\mathbb{Z}/n\mathbb{Z}$ est principal et que si n n'est pas premier alors $\mathbb{Z}/n\mathbb{Z}$ n'est pas principal.

b) Généraliser au cas d'un quotient d'un anneau principal quelconque.

c) Montrer que tout idéal de $\mathbb{Z}^2$ est principal et mais $\mathbb{Z}^2$ n'est pas principal.

d) Généraliser à un produit d'anneaux principaux.

Exercice 13 — PPCM et PGCD. Soit A un anneau commutatif intègre.

a) Soit $a \neq 0$. Montrer que la famille $(a_1, \ldots, a_n)$ admet un ppcm si et seulement si la famille $(aa_1, \ldots, aa_n)$ en admet un. Donner le lien entre les deux ppcm.

b) Montrer que le résultat précédent n'est pas vrai pour les pgcd. Cependant, montrer qu'on a le résultat suivant : si le pgcd de la famille $(aa_1, \ldots, aa_n)$ existe, montrer que celui de la famille $(a_1, \ldots, a_n)$ existe et qu'on a la relation $\text{pgcd}\,(aa_1, \ldots, aa_n) = a\text{pgcd}\,(a_1, \ldots, a_n)$.

c) On suppose que x et y ont un ppcm. Montrer que $m \mid xy$. On écrit alors $xy = md$. Montrer que d est un pgcd pour x et y et que, pour tout $a \in \mathrm{A} \setminus \{0\}$, $\mathrm{pgcd}\,(ax, ay)$ existe et vaut ad (avoir un ppcm implique avoir un pgcd).

d) Montrer que si x, y et d sont tel que ad soit un pgcd de ax et ay pour tout $a \in \mathrm{A} \setminus \{0\}$ alors on peut définir m tel que $md = xy$ et m est un ppcm de x et y. En déduire que (avoir un pgcd n'implique pas avoir un ppcm).

e) Montrer que l'idéal (x, y) est principal alors $(x) \cap (y)$ l'est.

f) On dit que x et y sont *fortement premiers entre eux* si x et y ont un ppcm qui est xy. Montrer que des éléments qui sont fortement premiers entre eux sont premiers entre eux mais que la réciproque n'est pas vraie.

g) Montrer que si x et y sont fortement premiers entre eux et si $x \mid yz$ alors $x \mid z$ (le lemme d'Euclide ou de Gauss est vrai dans un anneau intègre sous l'hypothèse fortement premier entre eux).

h) Montrer que dans un anneau factoriel, des éléments sont fortement premiers entre eux si et seulement si ils sont premiers entre eux. En déduire que des éléments fortement premier entre eux ne sont pas forcément étrangers.

i) Soit A un anneau intègre. Montrer l'équivalence des propriétés suivantes

(i) L'intersection de deux idéaux principaux de A est un idéal principal.
(ii) Tout couple d'éléments de A admet un ppcm.
(iii) Tout couple d'éléments de A admet un pgcd.

Si les conditions précédentes sont vérifiées alors les produits xy et $\mathrm{pgcd}\,(x, y)\mathrm{ppcm}\,(x, y)$ sont associés ; deux éléments sont premiers entre eux si et seulement si ils sont fortement premiers entre eux. Tout élément irréductible est premier.

j) Montrer qu'un anneau intègre est factoriel si et seulement si tout élément irréductible est premier et il n'existe pas de suite infinie $(x_i)_{i\in\mathbb{N}}$ telle que pour tout $i > 0$ on a $x_i \mid x_{i-1}$ et x_i n'est pas associé à x_{i-1}.

k) Montrer qu'un anneau intègre est factoriel si et seulement si toute suite croissante d'idéaux principaux est stationnaire et l'intersection de deux idéaux principaux est principal.

l) Montrer qu'un élément p est irréductible si et seulement si $\mathrm{pgcd}\,(a, p)$ existe et vaut 1 ou p pour tout $a \in \mathrm{A}$.

m) Montrer qu'un élément irréductible p est premier si et seulement si $\mathrm{ppcm}\,(a, p)$ existe, pour tout $a \in \mathrm{A}$.

Exercice 14 On considère l'anneau $\mathrm{A} = \mathbb{Z}[\mathrm{X}, \mathrm{Y}, \mathrm{Z}, \mathrm{T}]/(\mathrm{X} - \mathrm{ZY}, \mathrm{Y} - \mathrm{XT})$. On note x, y les classes de X et Y dans A. Montrer que x et y sont associés mais qu'il n'existe pas d'élément inversible u tel que $xu = y$ (voir un autre exemple dans [Perrin]).

Exercice 15 Soit A un anneau factoriel tel que tout idéal de la forme (a, b) est principal. Montrer que A est principal.

Exercice 16 Soit A un anneau intègre

a) Montrer que a et b n'ont pas de diviseur commun alors $a\mathrm{X} + b$ est irréductible dans $\mathrm{A}[\mathrm{X}]$.

b) Montrer que si les éléments a, b, c n'ont pas de diviseur commun et si $b^2 - 4ac$ n'est pas un carré dans R alors le polynôme $a\mathrm{X}^2 + b\mathrm{X} + c$ est irréductible dans $\mathrm{A}[\mathrm{X}]$.

c) Montrer que la réciproque à la question précédente est vrai si A est factoriel et 2 est inversible dans R.

d) Soit K un corps. On note $\mathrm{M} = (\mathrm{X}_{ij}) \in \mathrm{M}_n(\mathrm{K}[\mathrm{X}_{ij}, i, j])$ la matrice de taille $n \times n$ dont les coefficients sont des indéterminées. Montrer que $\det \mathrm{M}$ est un élément irréductible de $\mathrm{K}[\mathrm{X}_{ij}, i, j]$.

e) Montrer que χ_{M} est un élément irréductible de $\mathbb{Z}[\mathrm{X}, \mathrm{X}_{ij}, i, j]$.

f) On écrit $\mathrm{P} = \mathrm{P}_0 + \cdots + \mathrm{P}_d \in \mathrm{A}[\mathrm{X}_1, \ldots, \mathrm{X}_n]$ où les P_i sont les composantes homogènes de P (où A est factoriel). Monter que si P_d est irréductible alors P l'est. Montrer que si $\mathrm{P} = \mathrm{P}_{d-1} + \mathrm{P}_d$ avec P_d et P_{d-1} sont non nuls et sans facteurs communs alors P est irréductible. On suppose que $\mathrm{P} = \mathrm{P}_{d-2} + \mathrm{P}_d$ avec P_d et P_{d-2} sont non nuls et sans facteurs communs et d est impair alors P est irréductible. Trouver un contre-exemple si d est pair.