

Université de Lille
Master Mathématiques, 2020-21
Feuille d'exercices 1

§1. Notions fondamentales

1. Problème

Soient A et B des anneaux. On munit $A \times B$ de la structure d'anneau telle que $(a_1, b_1) + (a_2, b_2) = (a_1 + a_2, b_1 + b_2)$, $(a_1, b_1) \cdot (a_2, b_2) = (a_1 a_2, b_1 b_2)$, avec $1_{A \times B} = (1_A, 1_B)$ comme unité.

Partie 1 (caractérisation catégorique du produit cartésien).

1.1) Montrer que les applications $p : A \times B \rightarrow A$ et $q : A \times B \rightarrow B$ définies par $p(a, b) = a$ et $q(a, b) = b$ sont des morphismes d'anneaux et montrer que $T = A \times B$ satisfait la propriété universelle suivante :

(*) Pour tout anneau R avec des morphismes d'anneaux $f : R \rightarrow A$ et $g : R \rightarrow B$, il existe un unique morphisme d'anneaux $\phi : R \rightarrow T$ tel que $p\phi = f$ et $q\phi = g$.

1.2) Montrer que la propriété (*) du paragraphe précédent caractérise T à isomorphisme près : si on a un second anneau T' avec des morphismes $p' : T' \rightarrow A$ et $q' : T' \rightarrow B$ vérifiant (*), alors on peut construire des morphismes $\phi : T \rightarrow T'$ et $\phi' : T' \rightarrow T$ tels que $\phi\phi' = id$ et $\phi'\phi = id$, de sorte que ϕ et ϕ' définissent des isomorphismes inverses l'un de l'autre entre T et T' .

Partie 2 (produit cartésien et idempotents orthogonaux).

1.3) Montrer que les éléments $e = (1_A, 0)$ et $f = (0, 1_B)$ dans $A \times B$ vérifient les relations $e^2 = e$, $f^2 = f$, $ef = 0$ et $e + f = 1_{A \times B}$. (On dit que e et f définissent une décomposition de l'unité en idempotents orthogonaux.)

1.4) Inversement, on se donne un anneau R avec des éléments $e, f \in R$ tels que $e^2 = e$, $f^2 = f$, $ef = 0$ et $e + f = 1_R$. Prouver que l'on a alors une décomposition $R \simeq A \times B$ pour des anneaux A et B que l'on définira explicitement à partir de R . (*Indication*: on considérera les ensembles $A = eR = \{ex \mid x \in R\}$ et $B = fR = \{fx \mid x \in R\}$.)

1.5) Soient (m, n) des entiers tels que $\text{pgcd}(m, n) = 1$. Utiliser l'existence d'une relation de Bezout $um + vn = 1$ pour construire des idempotents orthogonaux $e, f \in \mathbb{Z}/mn\mathbb{Z}$ tels que $e\mathbb{Z}/mn\mathbb{Z} \simeq \mathbb{Z}/m\mathbb{Z}$, $f\mathbb{Z}/mn\mathbb{Z} \simeq \mathbb{Z}/n\mathbb{Z}$ et retrouver le résultat du théorème des restes chinois $\mathbb{Z}/mn\mathbb{Z} \simeq \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$.

§2. Division, anneaux euclidiens, principaux, factoriels

1. Problème

Un anneau A est *euclidien* lorsque l'on a une application $d : A \setminus \{0\} \rightarrow \mathbb{N}$ telle que :

(*) pour tout couple $(a, b) \in A \times A$ avec $b \neq 0$, on a un couple $(q, r) \in A \times A$ tel que $a = bq + r$, avec $r = 0$ ou $d(r) < d(b)$ sinon.

Il est parfois commode d'étendre d à A tout entier en posant $d(0) = -\infty$ et en prenant avec la convention $-\infty < n, \forall n \in \mathbb{N}$.

Partie 1.

1.1) Rappeler la définition de la structure d'anneau euclidien sur l'anneau des entiers $A = \mathbb{Z}$ et sur l'anneau des polynômes $A = \mathbb{K}[X]$ (où K est un corps).

BF, Courriel: Benoit.Fresse@univ-lille.fr

1.2) L'ensemble des entiers de Gauss $\mathbb{Z}[i]$ est constitué des nombres complexes $z = a + bi$ tels que $(a, b) \in \mathbb{Z} \times \mathbb{Z}$. Les entiers de Gauss forment un sous-anneau de \mathbb{C} (vérifier cette assertion). On veut prouver que $\mathbb{Z}[i]$ est euclidien pour l'application $d : \mathbb{Z}[i] \setminus \{0\} \rightarrow \mathbb{N}$ telle que $d(a + bi) = a^2 + b^2$.

Soit $z = (a + bi)/(c + di) = u + vi$. Prouver que l'on a au moins un nombre $\zeta = p + qi \in \mathbb{Z}[i]$ parmi les sommets du carré $Q = \{s + it, E(u) \leq s \leq E(u) + 1, E(v) \leq t \leq E(v) + 1\}$ tel que $|z - \zeta| < 1$. (On pourra s'aider d'une figure.) Puis montrer que $r + si = (a + bi) - (c + di)(p + qi)$ est un entier de Gauss vérifiant $r^2 + s^2 < c^2 + d^2$. Conclure.

Partie 2.

1.3) Soit I un idéal dans un anneau euclidien. On choisit un élément $\alpha \in I \setminus \{0\}$ tel que $d(\alpha)$ soit minimal. Prouver que tout élément $a \in I$ est multiple de α . Conclure que tout anneau euclidien est principal.

Remarque : Tous les anneaux principaux ne sont pas euclidiens. Par exemple, on peut montrer que l'anneau $\mathbb{Z}[\alpha]$ constitué des complexes de la forme $m + \alpha n$, $(m, n) \in \mathbb{Z}$, est principal sans être euclidien lorsque $\alpha = 1/2(1 + i\sqrt{19})$.

1.4) Rappel : Le pgcd d'une famille $a_i \in A$, $i \in I$, est défini dans un anneau principal quelconque comme l'élément $\text{pgcd}(a_i, i \in I) \in A$, unique à un facteur inversible près, tel que $A \text{pgcd}(a_i, i \in I) = \sum_{i \in I} Aa_i$.

Donner une version de l'algorithme d'Euclide étendu, valable dans un anneau euclidien quelconque A , permettant de calculer le pgcd $\text{pgcd}(a, b)$ de deux éléments $(a, b) \in A \times A$ et des éléments $(u_0, v_0) \in A \times A$ tels que $\text{pgcd}(a, b) = au_0 + bv_0$.

Donner des exemples dans l'anneau des entiers $A = \mathbb{Z}$, dans un anneau de polynômes $A = \mathbb{K}[x]$, pour illustrer l'algorithme. Calculer $\text{pgcd}(3 + i, -2 + 4i)$ pour illustrer l'algorithme dans le cas $A = \mathbb{Z}[i]$.

Partie 3.

1.5) Dans un anneau principal A , quel est la condition nécessaire et suffisante sur un triplet (a, b, c) pour que l'équation $c = ax + by$ possède au moins une solution?

Comment se déduit l'ensemble des solutions de cette équation d'une solution particulière?
Indication : on considérera les quotients $a_0 = a/\text{pgcd}(a, b)$ et $b_0 = b/\text{pgcd}(a, b)$ pour se ramener au cas de deux nombres (a_0, b_0) premiers entre eux.

Donner des exemples dans l'anneau des entiers $A = \mathbb{Z}$, dans un anneau des polynômes $A = \mathbb{K}[x]$, pour illustrer le résultat.

2. Exercice

On note $\mathbb{Z}[i\sqrt{5}]$ le sous-anneau de \mathbb{C} constitué des nombres complexes $z = a + bi\sqrt{5}$ tels que $(a, b) \in \mathbb{Z} \times \mathbb{Z}$. Montrer que $9 = 3 \times 3 = (2 + i\sqrt{5})(2 - i\sqrt{5})$ fournit deux décompositions de 9 en produit d'éléments irréductibles dans $\mathbb{Z}[i\sqrt{5}]$. Conclure que l'anneau $\mathbb{Z}[i\sqrt{5}]$ n'est pas factoriel.
Indication : on s'intéressa aux propriétés de $N(z) = z\bar{z}$ pour $z = 3, 2 + i\sqrt{5}, 2 - i\sqrt{5}$, en observant que $N(\alpha\beta) = N(\alpha)N(\beta)$ et que $z \in \mathbb{Z}[i\sqrt{5}] \Rightarrow N(z) \in \mathbb{N}$.

§3. Division et factorialité dans les anneaux de polynômes

1. Problème

Soit R un anneau factoriel. On s'intéresse à l'anneau des polynômes $R[X]$. On veut montrer que $R[X]$ est également factoriel.

On utilisera le corps des fractions $K = \text{Fr}(R)$, formellement défini comme l'ensemble des classes de fractions $x = a/b$, $a \in R$, $b \in R \setminus \{0\}$, muni de la relation d'équivalence classique

$$\frac{a}{b} \equiv \frac{c}{d} \Leftrightarrow ad = bc.$$

On utilise l'abus habituel de noter $=$ plutôt que \equiv l'identité déduit de cette relation dans le corps des fractions. On définit la somme et le produit des fractions par les formules habituelles

$$\frac{a}{b} + \frac{c}{d} = \frac{ad + bc}{bd} \quad \text{et} \quad \frac{a}{b} \cdot \frac{c}{d} = \frac{ac}{bd}.$$

On a un morphisme d'anneaux naturel $\eta : R \rightarrow Fr(R)$ qui identifie $a \in R$ à la fraction $a/1 \in Fr(R)$ de sorte que l'on écrit aussi $a = a/1$ par abus de notation.

Partie 1 (contenu et lemme de Gauss).

Soit $F(X) = c_0X^n + c_1X^{n-1} + \dots + c_{n-1}X + c_n \in R[X]$. On pose $c(F) = \text{pgcd}(c_0, c_1, \dots, c_n)$ et on appelle ce nombre le contenu de F . On dit que F est primitif lorsque $c(F) = 1$.

1.1) Soit $F(X) = c_0X^n + c_1X^{n-1} + \dots + c_{n-1}X + c_n \in R[X]$. On fixe $c \in R$. Prouver que l'on a la relation $c|F(X)$ dans $R[X]$ si et seulement si on a la relation $c|c_i$ pour tout i dans R , et donc si et seulement si on a $c|c(F)$.

1.2) Montrer que l'on a $F(X) = c(F) \cdot F_0(X)$, avec $F_0(X)$ primitif, pour tout polynôme $F(X) \in R[X]$. Montrer également qu'en général, pour un polynôme de la forme $F(X) = cF_0(X)$, on a la formule $c(F) = c \cdot c(F_0)$.

1.3) (lemme de Gauss). Soient $F(X) = a_0X^k + a_1X^{k-1} + \dots + a_{k-1}X + a_k \in R[X]$ et $G(X) = b_0X^l + b_1X^{l-1} + \dots + b_{l-1}X + b_l \in R[X]$. Soit p un élément irréductible de R . Montrer que l'on a l'implication :

$$p \nmid F(X) \quad \text{et} \quad p \nmid G(X) \Rightarrow p \nmid F(X)G(X).$$

Indication : Fixer i_0 minimal tel que $p \nmid a_{i_0}$ en utilisant que p ne divise pas tous les coefficients de $F(X)$ d'après la question précédente (donc $p|a_i$ pour $i = 0, \dots, i_0 - 1$, mais $p \nmid a_{i_0}$). Fixer de même j_0 minimal tel que $p \nmid b_{j_0}$ (donc $p|a_j$ pour $j = 0, \dots, j_0 - 1$, mais $p \nmid a_{j_0}$). Puis montrer que p ne divise pas le coefficient $c_{i_0+j_0}$ du polynôme produit $F(X)G(X) = c_0X^{k+l} + c_1X^{k+l-1} + \dots + c_{k+l-1}X + c_{k+l}$.

1.4) Montrer que l'on a $c(F) = c(G) = 1 \Rightarrow c(FG) = 1$ en utilisant les résultats de la question précédente.

1.5) Montrer que l'on a en général $c(FG) = c(F)c(G)$ en utilisant les résultats des deux questions précédentes.

Partie 2 (caractérisation des polynômes irréductibles dans $R[X]$).

1.6) Soit $F(X)$ un polynôme irréductible dans $R[X]$ tel que $\deg(F) > 0$. Prouver que l'on a nécessairement $c(F) = 1$ puis montrer que $F(X)$ est également irréductible dans $K[X]$. *Indication :* On se donne une décomposition $F(X) = U(X)V(X)$ dans $K[X]$. On observera que l'on peut écrire $U(X) = U_1(X)/a$, avec $U_1(X) \in R[X]$, $a \in R$, ainsi que $V(X) = V_1(X)/b$, avec $V_1(X) \in R[X]$, $b \in R$. On montrera alors que l'on a $ab = c(U_1)c(V_1)$ en utilisant les résultats de la partie précédente. On déduira de ce résultat que l'on a soit $U_1(X)/c(U_1) = 1$, soit $V_1(X)/c(V_1) = 1$, ce qui permettra d'aboutir à la conclusion voulue.

1.7) Prouver la réciproque du résultat de la question précédente : si $F(X) \in R[X]$ vérifie $c(F) = 1$ et est irréductible dans $K[X]$, alors $F(X)$ est irréductible dans $R[X]$.

1.8) Conclure de l'analyse de cette partie que les éléments irréductibles de $R[X]$ sont les éléments $p \in R$ irréductibles dans R et les polynômes primitifs $F(X)$ de degré $\deg(F) > 0$ qui sont irréductibles dans $K[X]$.

Partie 3 (lemme d'Euclide dans $R[X]$).

1.9) Soit $P(X) \in R[X]$ un polynôme tel que $c(P) = 1$. Soit $F(X) \in R[X]$. On suppose que l'on a la relation $P(X)|F(X)$ dans l'anneau $K[X]$, soit $F(X) = P(X)Q(X)$, avec $Q(X) \in K[X]$.

Montrer que l'on a alors $Q[X] \in R[X]$, et donc $F(X)|G(X)$ dans $R[X]$. *Indications* : On écrira $Q(X) = Q_0(X)/c$, avec $Q_0(X) \in R[X]$, $c \in R$, et on utilisera les résultats de la partie 1 pour prouver que l'on a $c|c(Q_0)$ et pour conclure.

1.10) Soit $P(X)$ un polynôme irréductible dans $R[X]$ tel que $\deg(P) > 0$. Montrer que si on a $P(X)|F(X)G(X)$ dans $R[X]$, alors on a nécessairement $P(X)|F(X)$ ou $P(X)|G(X)$ dans $R[X]$.

Indications : On passera par $K[X]$ et on utilisera le résultat de la question précédente.

1.11) Soit p un élément irréductible de R . Montrer que si on a $p|F(X)G(X)$ dans $R[X]$, alors on a nécessairement $p|F(X)$ ou $p|G(X)$ dans $R[X]$. *Indication* : Reprendre le résultat du lemme de Gauss établi dans la partie 1.

1.12) Conclure que le lemme d'Euclide est satisfait dans $R[X]$: si $P(X)$ est un élément irréductible quelconque de $R[X]$, alors $P(X)|F(X)G(X)$ implique $P(X)|F(X)$ ou $P(X)|G(X)$.

Partie 4 (factorialité de $R[X]$).

1.13) Soit $F(X) \in R[X]$ un polynôme tel que $c(F) = 1$. Si on a $F(X) = U(X)V(X)$ dans $R[X]$, alors montrer que l'on a nécessairement $c(U) = c(V) = 1$, puis montrer que le processus de décomposition de $F(X)$ se termine nécessairement dans $R[X]$, de sorte que l'on a $F(X) = P_1(X) \cdots P_r(X)$, avec $P_1(X), \dots, P_r(X) \in R[X]$ des polynômes irréductibles tels que $\deg(P_1), \dots, \deg(P_r) > 0$ et $c(P_1) = \cdots = c(P_r) = 1$.

1.14) Construire la décomposition en produit de facteurs irréductibles d'un polynôme arbitraire $F(X) \in R[X]$. *Indication* : On utilisera la décomposition $F(X) = c(F)F_0(X)$ avec $F_0(X) \in R[X]$ tel que $c(F_0) = 1$.

1.15) Dédire des résultats précédemment obtenus que cette décomposition est unique et conclure que $R[X]$ est factoriel, comme annoncé au début de ce problème.

2. Exercice (critère d'Eisenstein)

Soit $F(X) = c_0X^n + c_1X^{n-1} + \cdots + c_n$ un polynôme de $\mathbb{Z}[X]$. Soit p un nombre premier. On suppose que les coefficients de $F(X)$ satisfont les propriétés suivantes :

- (i) $p \nmid c_0$
- (ii) $p|c_1, \dots, c_n$
- (iii) $p^2 \nmid c_n$ On veut montrer que $F(X)$ est alors irréductible dans $\mathbb{Q}[X]$.

2.1) On suppose par l'absurde que $F(X)$ possède une décomposition $F(X) = U(X)V(X)$ dans $\mathbb{Q}[X]$, avec $\deg(U), \deg(V) > 0$. Prouver par une variante des arguments utilisés dans la question 1.6) du problème précédent que l'on peut supposer $U(X), V(X) \in \mathbb{Z}[X]$ dans une telle décomposition. On écrit $U(X) = a_0X^k + a_1X^{k-1} + \cdots + a_k$ et $V(X) = b_0X^l + b_1X^{l-1} + \cdots + b_l$.

2.2) On passe à $\mathbb{F}_p[X]$, où $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$. Si $P(X) \in \mathbb{Z}[X]$, alors on note $\bar{P}(X) \in \mathbb{F}_p[X]$ le polynôme obtenu en réduisant les coefficients de $P(X)$ modulo p . Que peut-on dire de $\bar{F}(X) = \bar{c}_0X^n + \bar{c}_1X^{n-1} + \cdots + \bar{c}_n$ sous les hypothèses (i-iii) du critère? Que peut-on en déduire quant aux polynômes $\bar{U}(X) = \bar{a}_0X^k + \bar{a}_1X^{k-1} + \cdots + \bar{a}_k$ et $\bar{V}(X) = \bar{b}_0X^l + \bar{b}_1X^{l-1} + \cdots + \bar{b}_l$ résultant de la décomposition $F(X) = U(X)V(X)$ de la question précédente?

2.3) Dédire de la question précédente que l'on a $p|a_k, p|b_l$ et montrer que ceci aboutit à une contradiction avec l'hypothèse (iii) du critère. Conclure.

2.4) Prouver que le polynôme

$$F(X) = \frac{X^p - 1}{X - 1} = X^{p-1} + X^{p-2} + \cdots + X + 1,$$

pour p un nombre premier, est irréductible dans $\mathbb{Z}[X]$. *Indication* : On appliquera le critère d'Eisenstein au polynôme $G(Y) = F(Y+1)$ obtenu en faisant le changement de variable $Y = X - 1$.