Université de Lille

Master Mathématiques, 2019-20

Feuille d'exercices 1

§1. Division euclidienne et algorithme d'Euclide

1. Problème

Un anneau A est *euclidien* lorsque l'on a une application $d : A \setminus \{0\} \to \mathbb{N}$ 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) Observer que l'anneau des entiers $A = \mathbb{Z}$, l'anneau des polynômes sur un corps $A = \mathbb{K}[X]$, sont des exemples d'anneaux euclidiens.

1.2) L'ensemble des entiers de Gauss $\mathbb{Z}[i]$ 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 $d : \mathbb{Z}[i] \setminus \{0\} \to \mathbb{N}$ 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 : Tout les anneaux principaux ne sont pas euclidien. 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 $pgcd(a_i, i \in I) \in A$, unique à un facteur inversible près, tel que $A\, pgcd(a_i, i \in I) = \sum_{i \in I} A a_i$.

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

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 $pgcd(3 + i, -2 + 4i)$ 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 $a_0 = a/\, pgcd(a, b)$ et $b_0 = b/\, pgcd(a, b)$ pour se ramener au cas de deux nombres (a_0, b_0) premiers entre eux.

BF, Courriel: `Benoit.Fresse@math.univ-lille1.fr`

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. Quiz

On fixe un entier $q > 1$.

2.1) Donner un algorithme pour calculer le développement d'un entier x en base q. *Indication :* Si le développement de x en base q s'écrit $x = x_0 + x_1 q + \cdots + x_i q^i + \cdots + x_r q^r$ pour des chiffres $0 \leq x_i \leq q-1$, $i = 0, \ldots, r$, alors comment s'identifient le reste et le quotient de la division euclidienne de x par q?

2.2) Comment s'écrit le développement de $x = q^n - 1$ en base q?

3. Exercice

Soit $E_n = 2^{2^n} + 1$, $n \in \mathbb{N}$. Expliciter une relation de récurrence entre $E_{n+1} - 1 = 2^{2^{n+1}}$ et $E_n - 1 = 2^{2^n}$. En déduire une relation de récurrence entre E_{n+1} et E_n. Quel est le reste de la division euclidienne de E_{n+1} par E_n? Quel est le plus grand diviseur commun de E_{n+1} et E_n?

4. Exercice

4.1) On considère la suite des nombres de Fibonacci $F_0 = 0$, $F_1 = 1$, $F_n = F_{n-1} + F_{n-2}$. Comment s'écrit la division euclidienne de F_n par F_{n-1}? Quel est le reste de cette division? Quel est le pgcd de F_n et F_{n-1}?

4.2) ! Soit $c(a,b)$ le nombre de divisions que fait intervenir l'algorithme d'Euclide pour calculer $pgcd(a,b)$. Que vaut $c(a,b)$ dans le cas $a = F_{n-1}$ et $b = F_n$? Prouver que l'on a en général

$$c(a,b) \leq \frac{\log(\max(|a|,|b|)}{\log(\theta)}$$

où $\theta = (1+\sqrt{5})/2$. Conclusion?

§2. 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 $K = Fr(R)$, 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 est 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 $\eta : R \to Fr(R)$ 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 $F(X) = c_0 X^n + c_1 X^{n-1} + \cdots + c_{n-1} X + c_n \in R[X]$. On pose $c(F) = pgcd(c_0, c_1, \ldots, c_n)$ et on appelle ce nombre le contenu de F. On dit que F est primitif lorsque $c(F) = 1$.

1.1) Soit $F(X) = c_0 X^n + c_1 X^{n-1} + \cdots + c_{n-1} X + c_n \in R[X]$. 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 $F(X) = a_0X^k + a_1X^{k-1} + \cdots + a_{k-1}X + a_k \in R[X]$ et $G(X) = b_0X^l + b_1X^{l-1} + \cdots + b_{l-1}X + b_l \in R[X]$. Soit p un élément irréductible de R. Montrer que l'on a l'implication :

$$p \not| F(X) \quad \text{et} \quad p \not| G(X) \Rightarrow p \not| F(X)G(X).$$

Indication : Fixer i_0 minimal tel que $p \not| a_{i_0}$ en utilisant que p ne divise pas tout les coefficients de $F(X)$ d'après la question précédente (donc $p|a_i$ pour $i = 0, \ldots, i_0 - 1$, mais $p \not| a_{i_0}$). Fixer de même j_0 minimal tel que $p \not| b_{j_0}$ (donc $p|a_j$ pour $j = 0, \ldots, j_0 - 1$, mais $p \not| a_{j_0}$). Puis montrer que p ne divise pas le coefficient $c_{i_0+j_0}$ du polynôme produit $F(X)G(X) = c_0X^{k+l} + c_1X^{k+l-1} + \cdots + c_{k+l-1}X + c_{k+l}$.
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 précédentes. 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 $P_1(X),\ldots,P_r(X) \in R[X]$ des polynômes irréductibles tels que $\deg(P_1),\ldots,\deg(P_r) > 0$ 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) Déduire des résultats précédemment obtenus que cette décomposition est unique et conclure que $R[X]$ est factoriel, comme annoncé au début de ce problème.

2. Quiz
2.1) Prouver que l'anneau $\mathbb{C}[X,Y]$ est factoriel mais pas principal. (Par exemple, on montrera que l'idéal (X,Y) n'est pas principal dans $\mathbb{C}[X,Y]$.)
2.2) Prouver que l'anneau $\mathbb{Z}[X]$ est factoriel mais pas principal. (Par exemple, on montrera que l'idéal $(2,X)$ n'est pas principal dans $\mathbb{Z}[X]$.)
2.3) Montrer plus généralement que si $R[X]$ est principal, alors R est nécessairement un corps.

3. 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) $p \not| c_0$
(ii) $p|c_1,\ldots,c_n$
(iii) $p^2 \not| c_n$ On veut montrer que $F(X)$ est alors irréductible dans $\mathbb{Q}[X]$.
3.1) On suppose par l'absurde que $F(X)$ possède une décomposition $F(X) = U(X)V(X)$ dans $K[X]$, avec $\deg(U),\deg(V) > 0$. Prouver par une variante des arguments utilisé 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 $V(X) = b_0X^l + b_1X^{l-1} + \cdots + b_l$.
3.2) 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?
3.3) Déduire 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.
3.4) Prouver que le polynôme

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

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 $Y = X-1$.