Université de Rennes 1 — Année universitaire 2017-2018
Licence de mathématiques
Module Anneaux et Arithmétique

Feuille de TD n°5

Exercice 1

Soit $\mathbf{K}$ un corps. Si $P = \sum_{n\geqslant 0} a_n T^n$ est un élément non nul de $\mathbf{K}[[T]]$, on pose

$$\mathrm{val}(P) := \mathrm{Min}\{n \in \mathbf{N}, \quad a_n \neq 0\}.$$

Montrer que val est un stathme euclidien sur $\mathbf{K}[[T]]$. Démontrer directement que $\mathbf{K}[[T]]$ est un anneau factoriel (expliciter la liste des irréductibles de $\mathbf{K}[[T]]$ à association près et la décompostion en produits d'irréductibles d'un élément non nul de $\mathbf{K}[[T]]$; on pourra comparer avec l'exercice 6 de la feuille de TD n°2).

Exercice 2

Pour chacun des couples (a, b) d'éléments de $\mathbf{Z}[i]$ donnés ci-dessous, calculer un pgcd δ de a et b et déterminer un couple (u, v) d'éléments de $\mathbf{Z}[i]$ tel que $\delta = a\,u + b\,v$:

$$(6 + 3\,i, -1 + 7\,i), (35, 9 + 6\,i), (10, 14).$$

Exercice 3

Montrer que les anneaux suivants sont euclidiens :

1. $\mathbf{Z}[i\sqrt{2}]$ (on pourra s'inspirer de la démonstration de la proposition 6.14 du cours) ;
2. $\mathbf{Z}[\sqrt{2}]$ (on pourra considérer $N\colon a + b\sqrt{2} \mapsto a^2 - 2b^2$) ;
3. $\mathbf{Z}[\sqrt{3}]$.

Exercice 4

Soit $\mathbf{K}$ un corps et $a, b \in \mathbf{K}[X]$ tels que $b \neq 0$. On applique l'algorithme d'Euclide étendu à a et b : on pose $r_{-1} := a$, $u_{-1} := 1$, $v_{-1} := 0$, $r_0 := b$, $u_0 := 0$, $v_0 := 1$. Ensuite, pour n entier positif, et tant que r_n est non nul, on écrit la division euclidienne de r_{n-1} par r_n :

$$r_{n-1} = q_n r_n + r_{n+1}$$

ce qui définit r_{n+1}. En outre on pose

$$u_{n+1} := u_{n-1} - q_n\,u_n, \quad v_{n+1} := v_{n-1} - q_n\,v_n.$$

On désigne par N le plus grand entier positif n que $r_n \neq 0$.

1. Montrer que pour tout entier n vérifiant $1 \leqslant n \leqslant N + 1$, on a
$$\deg(r_n) < \deg(r_{n-1}).$$
2. Montrer que pour tout entier n vérifiant $1 \leqslant n \leqslant N$, on a
$$\deg(r_{n-1}) = \deg(q_n) + \deg(r_n).$$

3. On suppose en outre que $\deg(a) \geqslant \deg(b)$; montrer que pour tout entier n vérifiant $1 \leqslant n \leqslant N$, on a
$$\deg(v_n) = \deg(r_{-1}) - \deg(r_{n-1}).$$

Exercice 5

Soit r un entier strictement positif, $p_1, \dots, p_r$ des nombres premiers et d un entier supérieur à 2.

1. Montrer qu'il existe une infinité de polynômes unitaires irréductibles de degré d de $\mathbf{Z}[X]$ qui sont réductibles modulo tous les p_i (*indication :* lemme chinois).
2. Montrer qu'il existe une infinité de polynômes unitaires irréductibles de degré d de $\mathbf{Z}[X]$ qui sont réductibles modulo tous les p_i et tels que le critère d'Eisenstein ne s'applique pour aucun des p_i.

Exercice 6

Soit $P \in \mathbf{Z}[X]$ et p un nombre premier. On suppose que P est irréductible modulo p. P est-il nécessairement irréductible ?

Exercice 7

Soit $P = X^4 + 1$.

1. Montrer que P est un élément irréductible de $\mathbf{Z}[X]$ (*cf.* l'exercice 3 de la feuille de TD n°3)
2. Soit p un nombre premier. En utilisant des identités remarquables, montrer que P est réductible modulo p si l'une des propriétés suivantes est vraie :
   (a) -1 est un carré modulo p ;
   (b) 2 est un carré modulo p ;
   (c) -2 est un carré modulo p.
3. Soit $\mathbf{K}$ un corps fini. Soit $\alpha, \beta \in \mathbf{K}$ des éléments qui ne sont pas des carrés dans $\mathbf{K}$. Montrer qu'alors $\alpha\beta$ est un carré dans $\mathbf{K}$.
4. En déduire que pour tout nombre premier p, $X^4 + 1$ est réductible modulo p.

Exercice 8

1. Soit A un anneau factoriel, d un entier, $P = \sum_{i=0}^{d} a_i X^i \in A[X]$ un polynôme de degré au plus d. Soit $x \in \mathrm{Frac}(A)$ une racine de P dans $\mathrm{Frac}(A)$. Montrer qu'on peut écrire $x = \frac{\alpha}{\beta}$, où $\alpha \in A$ et $\beta \in A \setminus \{0\}$ sont premiers entre eux. Montrer que α divise a_0 et que β divise a_d.
2. Le polynôme $7\,X^3 - 5\,X^2 - 9\,X + 4$ a-t-il des racines rationnelles ? et le polynôme $X^4 - 2X^2 - 3$?
3. Montrer, par au moins trois méthodes différentes, que les polynômes $X^2 + 3X - 15$ et $X^3 - 7X^2 + 14X - 7$ sont des éléments irréductibles de $\mathbf{Z}[X]$.
4. Montrer, par au moins deux méthodes différentes, que le polynôme $X^4 + 5X^3 - 15X^2 + 25X + 15$ est un élément irréductible de $\mathbf{Z}[X]$.

Exercice 9

1. Soit A un anneau intègre, $P \in A[X]$ et $a \in A$. Montrer que P est irréductible si et seulement si $P(X + a)$ est irréductible.

2. Soit p un nombre premier. Montrer que le polynôme $\frac{X^p-1}{X-1} \in \mathbf{Z}[X]$ est irréductible
3. Soit $\mathbf{K}$ un corps de caractéristique différente de 2 et $\alpha \in \mathbf{K}^\times$. Montrer que $X^2+Y^2-\alpha^2$ est un élément irréductible de $\mathbf{K}[X,Y]$. En déduire que pour tout entier $n \geqslant 2$, $\sum_{i=1}^n X_i^2 - \alpha^2$ est un élément irréductible de $\mathbf{K}[X_1,\dots,X_n]$. (on pourra considérer le morphisme de $\mathbf{K}[X_1,\dots,X_{n-1}]$-algèbres $\mathbf{K}[X_1,\dots,X_n] \to \mathbf{K}[X_1,\dots,X_{n-1}]$ qui envoie X_n sur 0).

Exercice 10

Dans le critère d'Eisenstein, pourquoi est-il important de supposer π irréductible ? (question posée à l'oral de l'agrégation externe).

Exercice 11

Soit A un anneau intègre.

1. Soit a et b des éléments de A premiers entre eux. Montrer que l'ensemble des pgcd de a et b est $A^\times$.
2. Soit a et b des éléments associés de A. Montrer que l'ensemble des pgcd de a et b est l'ensemble des éléments de A associés à a.
3. Soit $a \in A$. Montrer que l'ensemble des pgcd de a et 0 est l'ensemble des éléments de A associés à a.
4. Soit $a, b \in A$. Montrer que a et b admettent un ppcm si et seulement si l'idéal $aA \cap bA$ est principal, et qu'alors l'ensemble des ppcm de a et b est l'ensemble $\{c \in A, \quad cA = aA \cap bA\}$.
5. Soit $a, b \in A$. On suppose que a et b admettent un pgcd δ (respectivement un ppcm μ).
   (a) Soit $c \in A$. Montrer que c est un pgcd (respectivement un ppcm) de a et b si et seulement si c est associé à δ (respectivement à μ).
   (b) Soit $\alpha \in A$. Montrer que $\alpha\delta$ (respectivement $\alpha\mu$) est un pgcd (respectivement un ppcm) de $\alpha\, a$ et $\alpha\, b$.
   (c) Soit $\alpha \in A \setminus \{0\}$ un diviseur commun à a et b. Montrer que $\frac{\delta}{\alpha}$ (respectivement $\frac{\mu}{\alpha}$) est un pgcd (respectivement un ppcm) de $\frac{a}{\alpha}$ et $\frac{b}{\alpha}$.
   En déduire que $\frac{a}{\delta}$ et $\frac{b}{\delta}$ sont premiers entre eux.
6. Soit $a, b \in A$. On suppose que a et b admettent un ppcm μ. Montrer qu'alors a et b admettent un pgcd δ, et que $\delta\mu$ est associé à ab.
7. Montrer que dans l'anneau $\mathbf{Z}[i\sqrt{5}]$, les éléments 2 et $1+i\sqrt{5}$ sont premiers entre eux mais n'ont pas de ppcm, et que les éléments 9 et $2+i\sqrt{5}$ n'ont pas de pgcd (donc pas de ppcm).

Exercice 12

En utilisant par exemple l'identité $2^2 = (1+i\sqrt{3})(1-i\sqrt{3})$ dans $\mathbf{Z}[i\sqrt{3}]$ et l'exercice 5 de la feuille 3, montrer qu'en général dans un anneau intègre un produit d'éléments premiers entre eux et qui ne sont pas des carrés peut néanmoins être un carré.

Exercice 13

Soit $\mathbf{K}$ un corps. Montrer que les anneaux suivants sont intègres mais ne sont pas factoriels :

1. $\mathbf{K}[X,Y]/\langle X^2 - Y^3 \rangle$;
2. le sous-$\mathbf{K}$ espace vectoriel de la $\mathbf{K}$-algèbre $\mathbf{K}[X,Y]$ engendré par les éléments de la forme X^iY^j où $i, j \in \mathbf{N}$ et $i+j$ est pair ;

3. $\mathbf{Z}[i\sqrt{5}]$ (*cf.* exercice 11.7).

Exercice 14

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

Exercice 15

Soit A un anneau factoriel. Montrer que l'ensemble des éléments irréductibles de $A[X]$ est la réunion disjointes des deux ensembles suivants :

1. l'ensemble des polynômes constants qui sont des éléments irréductibles de A ;
2. l'ensemble des polynômes qui sont primitifs et irréductibles dans $\mathrm{Frac}(A)[X]$.

Exercice 16

Soit A un anneau intègre et S une partie multiplicative de A ne contenant pas 0_A.

1. On suppose A principal ; montrer qu'alors $S^{-1}A$ est principal.
2. On suppose A factoriel ; montrer qu'alors $S^{-1}A$ est factoriel.

Exercice 17

1. Soit A un anneau intègre vérifiant le théorème de Bézout. Montrer que tout idéal de A engendré par un nombre fini d'éléments est principal.
2. Soit A un anneau factoriel. Montrer que toute suite croissante (pour l'inclusion) d'idéaux *principaux* de A est stationnaire.
3. Soit A un anneau factoriel. On suppose que A vérifie le théorème de Bézout. Montrer qu'alors A est principal. *Indication :* soit $\mathcal{I}$ un idéal de A, $a \in \mathcal{I}$ et $\mathcal{I}_1 = aA$; si $\mathcal{I}_1 \neq \mathcal{I}$, soit $a_1 \in \mathcal{I} \setminus \mathcal{I}_1$ et $\mathcal{I}_2 := \mathcal{I}_1 + a_1 A$; si $\mathcal{I}_2 \neq \mathcal{I}$, soit $a_2 \in \mathcal{I} \setminus \mathcal{I}_2$ et $\mathcal{I}_3 := \mathcal{I}_2 + a_2 A\ldots$

Exercice 18

Soit p un nombre premier et $P \in \mathbf{F}_p[X]$ un polynôme. On souhaite déterminer de manière effective la factorisation de P en facteurs irréductibles. Il existe un agorithme naïf pour ce faire : déterminer tous les polynômes irréductibles de $\mathbf{F}_p[X]$ de degré au plus égal à celui de P (*cf.* l'exercice 11 de la feuille de TD n°3) et tester s'ils divisent P (par division euclidienne). Cette méthode s'avère fort peu efficace dans la pratique. Cet exercice présente un algorithme beaucoup plus efficace, appelé *algorithme de Berlekamp* (du nom de son inventeur), et basé notamment sur des outils d'algèbre linéaire (calcul du rang d'une matrice).

1. Soit P un polynôme de $\mathbf{F}_p[X]$ tel que $P' = 0$. Montrer qu'il existe un polynôme Q (que l'on explicitera en fonction de P) vérifiant $Q^p = P$.

   Ceci montre que pour factoriser n'importe quel polynôme de $\mathbf{F}_p[X]$, il suffit d'avoir à disposition un algorithme $\mathcal{A}$ qui factorise les polynômes sans facteur multiple ; en effet, partant d'un polynôme non constant P quelconque, on applique la procédure $\mathcal{F}$ suivante : on calcule $\mathrm{pgcd}(P, P')$; puis :

   (a) si $\mathrm{pgcd}(P, P') = 1$, P est d'après le cours sans facteur multiple et on applique $\mathcal{A}$;

   (b) si $1 \leqslant \deg \mathrm{pgcd}(P, P') \leqslant \deg(P) - 1$, $\frac{P}{\mathrm{pgcd}(P,P')}$ et $\mathrm{pgcd}(P, P')$ sont des facteurs non triviaux de P, auquel on applique récursivement la procédure $\mathcal{F}$;

(c) si $\operatorname{pgcd}(P, P') = P$*, on a nécessairement* $P' = 0$*, donc* $P = Q^p$ *et on applique récursivement la procédure* $\mathcal{F}$ *à* Q*.*

Comme toute application récursive de la procédure $\mathcal{F}$ *s'applique à des polynômes dont le degré chute strictement par rapport au polynôme initial, cette procédure garantit bien une factorisation de* P *en un nombre fini d'étapes. La suite de l'exercice est consacrée à l'algorithme de Berelekamp proprement dit, qui permet de calculer une factorisation d'un polynôme de* $\mathbf{F}_p[X]$ *sans facteur multiple.*

2. Soit $P = \prod_{i=1}^{r} P_i$ un produit de polynômes irréductibles deux à deux distincts et $d = \deg(P)$. Soit A la $\mathbf{F}_p$-algèbre $\mathbf{F}_p[X]/\langle P\rangle$. Soit $a \in A$, image dans A d'un élément $Q \in \mathbf{F}_p[X]$. Soit $\mathcal{B}(a)$ l'image dans A du reste de la division euclidienne de Q^p par P. Montrer que l'application $\mathcal{B}\colon A \to A$ est bien définie et est une application $\mathbf{F}_p$ linéaire.
3. Soit $Q \in \mathbf{F}_p[X]$. Montrer qu'on a $Q^p - Q = \prod_{\alpha\in\mathbf{F}_p} Q - \alpha$.
4. Soit $\mathcal{K} := \operatorname{Ker}(\mathcal{B} - \mathrm{Id}_A)$ et $\theta\colon A \to \prod_{i=1}^{r} \mathbf{F}_p[X]/\langle P_i\rangle$ l'isomorphisme chinois. Soit $Q \in \mathbf{F}_p[X]$ un élément dont l'image dans A est dans $\mathcal{K}$. Soit $i \in \{1, \dots, r\}$. Montrer qu'il existe $\alpha_i \in \mathbf{F}_p$ tel que P_i divise $Q - \alpha_i$. En déduire que θ induit un isomorphisme de $\mathcal{K}$ sur $\prod_{i=1}^{r} \mathbf{K}$ et que $r = d - \operatorname{rg}(\mathcal{B} - \mathrm{Id}_A)$.
5. Expliquer comment calculer dans la pratique la matrice de $\mathcal{B}$ (et donc le rang de $\mathcal{B} - \mathrm{Id}_A$) dans la $\mathbf{F}_p$-base $\bar{1}, \dots, \bar{X}^{d-1}$ de A. Faire le calcul pour $p = 2$ et $P = X^3 + X^2 + X$ et $p = 3$ et $P = X^4 - 1$ et vérifier la cohérence des résultats. Montrer en utilisant ce qui précède que le polynôme $X^4 + 2X^3 + X + 1$ est irréductible sur $\mathbf{F}_3$.
6. Soit $Q \in \mathbf{F}_p[X]$ un élément dont l'image $\bar{Q}$ dans A est dans $\mathcal{K}$. Montrer que si Q est constant modulo P si et seulement si $\theta(\bar{Q}) \in \prod_{i=1}^{r} \mathbf{K}$ a toutes ses composantes égales. En déduire que si $r \geqslant 2$ il existe $Q \in \mathbf{F}_p[X]$ non constant modulo P tel que $\bar{Q}$ est dans $\mathcal{K}$. Montrer que pour un tel Q il existe $\alpha \in \mathbf{F}_p$ tel que $\operatorname{pgcd}(P, Q - \alpha)$ est un facteur non trivial de P.

   Ainsi, une factorisation de P *s'obtient de la manière suivante. On calcule* $\operatorname{rang}(\mathcal{B} - \mathrm{Id}_A)$*, ce qui donne* r*. Si* $r = 1$*,* P *est irréductible et on a terminé. Si* $r \geqslant 2$*, on détermine une base de* $\mathcal{K}$ *(dans la pratique on identifie* A *à* $\mathbf{F}_p^d$ *via la* $\mathbf{F}_p$*-base* $\bar{1}, \dots, \bar{X}^{d-1}$*) ce qui permet d'exhiber* Q *tel que* $\bar{Q} \in \mathcal{K}$ *est non constant modulo* P *; puis on calcule* $\operatorname{pgcd}(P, Q - \alpha)$ *successivement pour tous les* α *de* $\mathbf{F}_p$ *jusqu'à ce qu'on obtienne un facteur non trivial* R *de* P *; on reprend alors la procédure pour* R *et* $\frac{P}{R}$ *(qui sont nécessairement sans facteur multiple, et de degrés respectifs strictement inférieurs à celui de* P*)*

   Appliquer l'algorithme de factorisation aux deux premiers exemples numériques de la question 5 et vérifier la cohérence des résultats.