Université Claude Bernard Lyon 1

MASTER M1G

Algèbre

Fiche TD 3

Exercice 1 *Passage au quotient dans* $\mathbb{Z}[X]$

Montrer l'isomorphisme $\mathbb{Z}[X]/\mathbb{Z}[X](X^2+1) \simeq \mathbb{Z}[i]$.

On part d'un morphisme naturel, puis, on est amené à déterminer l'idéal défini par $\mathbb{Z}[X] \cap \mathbb{Q}[X](X^2+1)$.

Exercice 2 *Factoriel implique intégralement clos*

Soit A un anneau factoriel et $P := \sum_{k=0}^{n} a_k X^k \in A[X]$. Soit $\alpha = \frac{p}{q}$ une racine de P, avec p et q premiers entre eux dans A.

1. Montrer que q divise a_n et p divise a_0.
   Utiliser le lemme de Gauss.
2. On suppose que P est unitaire, montrer que $\alpha \in A$.
3. En déduire un joli théorème qui résume la situation.

Exercice 3 *Critère d'Eisenstein*

Soit A un anneau factoriel, p premier dans A . On suppose que

$$P := X^n + a_{n-1}X^{n-1} + \cdots + a_1 X + a_0 \in A[X]$$

est tel que p divise a_i pour tout i et p^2 ne divise pas a_0.

1. On suppose que $P = QR$ avec

   $$Q := X^m + b_{m-1}X^{m-1} + \cdots + b_1 X + b_0,\ R := X^k + c_{k-1}X^{k-1} + \cdots + c_1 X + c_0 \in A[X]$$

   non constants. Montrer que p divise b_0 ou c_0. On supposera sans perte de généralité que p divise b_0.
2. A l'aide de l'égalité $a_0 = b_0 c_0$, montrer que p ne divise pas c_0. Puis, déduire par récurrence que p divise tous les b_i.
3. A l'aide de l'égalité $a_m = \sum_{j=1}^{\min\{k,m\}} b_{m-j}c_j + c_0$, montrer que p divise c_0.
4. En déduire que P est irréductible sur $A[X]$, puis, qu'il est irréductible sur $\mathbb{K}[X]$, où $\mathbb{K}$ est le corps de fraction de A.
5. En déduire le critère d'Eisenstein. Pourquoi ce critère ne sert à rien si A est un corps ?
6. Montrer que $X^3 - 5X + 10$ est irréductible dans $\mathbb{Z}[X]$, dans $\mathbb{Q}[X]$.

7. Montrer que $Y^3 - X^2Y + X$ est irréductible dans $\mathbb{K}[X, Y]$.

Exercice 4 *Irréductibilité d'un polynôme à plusieurs variables*

1. Montrer que sur un corps $\mathbb{K}$ de caractéristique 2, le polynôme $X^2 + Y^2 + Z^2$ est réductible.
2. Montrer que sur un corps $\mathbb{K}$ de caractéristique différente de 2, $X^2 + Y^2 + Z^2$ est irréductible.

   On pourra voir ce polynôme comme un polynôme de degré 2 dans $L[X]$, avec $L := \mathbb{K}(Y, Z)$. A quelle condition ce polynôme est irréductible, sachant qu'il est de degré 2 ?

Exercice 5 *L'anneau des décimaux est principal*

Soit $\mathbb{D}$ l'anneau des décimaux.

1. Soit I un idéal de $\mathbb{D}$. En considérant l'idéal $\mathbb{Z} \cap I$ de $\mathbb{Z}$, montrer que I est principal.

   Considérer le générateur z de l'idéal $\mathbb{Z} \cap I$ de $\mathbb{Z}$. Montrer que $I = \mathbb{D}z$ par double inclusion. On notera que si $a \in I$, il existe n dans $\mathbb{N}$ tel que $10^n a \in \mathbb{Z} \cap I$.
2. Quelles sont les unités de $\mathbb{D}$?
3. Quel est, dans $\mathbb{D}$, le pgcd de 0,42 et 38500 ?

   Voici une question qui décoiffe. Au fait, le pgcd est-il unique ? Modulo quoi ?
4. Généralisation : soit d un entier non nul. Montrer que $\mathbb{Z}[\frac{1}{d}]$ est principal.

   On remplace juste 10 par d.

Remarque 0.1. L'anneau $\mathbb{D}$ est également euclidien. Vous pourriez en définir un stathme ?

Exercice 6 *Agreg 2011*

Soit P et Q unitaires dans $\mathbb{Q}[X]$ tels que P est dans $\mathbb{Z}[X]$ et Q divise P dans $\mathbb{Q}[X]$. On veut montrer que Q est dans $\mathbb{Z}[X]$ et qu'il divise P dans $\mathbb{Z}[X]$.

1. Montrer que R est unitaire.
2. Soit $Q = X^m + \sum_{i=0}^{m-1} \frac{p_i}{q_i} X^i$, avec p_i premier à q_i pour tout i. Montrer que si a est le ppcm de q_i, alors aQ est de contenu 1 dans $\mathbb{Z}(X]$.

   aQ est clairement dans $\mathbb{Z}[X]$. Maintenant, soit p premier divisant tous ses coefficients, alors, il divise a, puisque Q est unitaire, et donc il divise un des q_i. On choisit i tel que la p-valuation soit maximale, alors p ne divise pas $\frac{a}{q_i}$. Donc, p divise p_i, absurde.
3. Conclure.

   De même, il existe b dans $\mathbb{Z}$ tel que bR soit de contenu 1 dans $\mathbb{Z}[X]$. On applique la formule des contenus à l'égalité $abP = Q_0 R_0$.

Exercice 7 *Borne pour la dimension d'un corps de décomposition*

Montrer que le corps de décomposition d'un polynôme P de $\mathbb{K}[X]$ de degré d est un $\mathbb{K}$-espace de degré $m \leq d!$.

Si a est une racine de P, alors $\mathbb{K}[a]$ est de degré $\leq d$ sur $\mathbb{K}$. Comme P se scinde sur $\mathbb{K}[a]$ en $P = Q(X-a)$, avec $Q \in \mathbb{K}[a][X]$, de degré $d-1$, on peut faire une récurrence.

Exercice 8 *$\mathbb{C}$-semblable vs $\mathbb{K}$-semblable*
On considère un sous-corps $\mathbb{K}$ de $\mathbb{C}$.

1. Démontrer, par récurrence sur d, qu'un polynôme à d variables, à coefficients dans $\mathbb{C}$, non nul sur $\mathbb{C}^d$ est non nul sur $\mathbb{K}^d$.

   On rappelle que sur un corps infini, on peut assimiler polynôme et fonction polynôme.

2. Soit A et A' deux matrices de $\mathcal{M}_n(\mathbb{K})$. On suppose que A et A' sont semblables sur $\mathbb{C}$. On veut montrer qu'elle sont semblables sur $\mathbb{K}$.

   (a) Soit $\mathbb{L}$ le corps de décomposition du polynôme caractéristique de A. Montrer que A et A' sont semblables sur $\mathbb{L}$.

   On utilisera le théorème de Jordan qui dit que si χ_A est scindé sur un corps, alors A est semblable à une matrice qui se décompose en blocs de Jordan, uniques à permutation près.

   (b) Conclure que A et A' sont semblables sur $\mathbb{K}$.

   On pose donc P une matrice de $\mathrm{GL}_n(\mathbb{L})$ telle que $A' = PAP^{-1}$, c'est-à-dire $A'P = PA$. On note $(e_i)_{1\leq i\leq m}$ une base de $\mathbb{L}$ sur $\mathbb{K}$. On peut alors décomposer $P = \sum_i P_i e_i$, avec $P_i \in \mathcal{M}_n(\mathbb{K})$ pour tout i.

   On a alors $A'P_i = P_i A$ pour tout i.

   La fonction $\mathbb{L}^m \to \mathbb{L}$ qui envoie $(x_i)_{1\leq i\leq m}$ envoie $\det(\sum_i P_i x_i)$ est polynomiale et non nulle car elle ne s'annule pas en $(e_i)_{1\leq i\leq m}$. Donc, elle ne s'annule pas sur $\mathbb{K}^m$. On peut donc trouver $(y_i)_{1\leq i\leq m}$ dans $\mathbb{K}$ tel que $Q = \sum_i P_i y_i$ soit inversible. On a donc $A'Q = QA$, puis $A' = QAQ^{-1}$.

Exercice 9 *Sous-anneaux quadratiques de $\mathbb{C}$*
On posera successivement $\alpha = i$, $i\sqrt{2}$, $i\sqrt{3}$, $\frac{1+i\sqrt{3}}{2}$, $\frac{1+i\sqrt{7}}{2}$, $\frac{1+i\sqrt{19}}{2}$.

1. Montrer que l'anneau $\mathbb{Z}[\alpha]$ est stable par conjugaison.
2. Trouver un polynôme de degré 2 à coefficients entiers qui annule α. Montrer que tout élément de $\mathbb{Z}[\alpha]$ s'écrit de façon unique sous la forme $x + y\alpha$, avec $x, y \in \mathbb{Z}$.

   Apprendre en s'amusant : donner une représentation matricielle de $x+y\alpha$ et utiliser Cayley-Hamilton.

3. Calculer la norme d'un élément de la forme $x + y\alpha$ avec x, y réels. En déduire que la norme définit une application multiplicative de $\mathbb{Z}[\alpha]$ dans $\mathbb{N}$.
4. Montrer que les éléments inversibles de $\mathbb{Z}[\alpha]$ sont les éléments de norme 1. Décrire le groupe multiplicatif $\mathbb{Z}[\alpha]^*$.

   SI un élément est inversible, il vérifie $\overline{z}z = 1$. Il faut tout de même utiliser que $\mathbb{Z}[\alpha]$ est stable par conjugaison !

5. Soit z dans $\mathbb{C}$, que l'on décompose en $z = x + y\alpha$, avec $x, y \in \mathbb{R}$. Pour quels α dans la liste existe-t-il toujours $z_0 = x_0 + y_0\alpha \in \mathbb{Z}[\alpha]$ tel que $N(z - z_0) < 1$. Montrer que dans ce cas, l'anneau $\mathbb{Z}[\alpha]$ est euclidien.

Exercice 10 *Anneaux non factoriels*

1. Montrer que l'anneau $\mathbb{C}[X,Y]/(X^2-Y^3)$ est non factoriel. Par exemple, en montrant qu'il est isomorphe au sous-anneau $\mathbb{C}[T^2,T^3]$ de $\mathbb{C}[T]$.
2. Montrer que l'anneau $A := \mathbb{Z}[i\sqrt{5}]$ est non factoriel. On pourra remarquer que $(1+i\sqrt{5})(1-i\sqrt{5}) = 2\times 3$.
   On pourra se référer au document sur les anneaux non factoriels distribué en TD.

Exercice 11 *Lemme préliminaire pour certaines équations diophantiennes* Soit A un anneau factoriel. On suppose que x, y sont premiers entre eux et qu'il existe z dans A tel que

$$xy = z^k$$

1. Montrer qu'il existe u et v dans A^* ainsi que x_0, y_0 dans A tels que

   $$x = ux_0^k,\ y = vy_0^k.$$

   Interpréter les hypothèses en termes de valuation.
2. On suppose que A^* est d'ordre fini premier avec k. Montrer alors que qu'il existe x_1, y_1 dans A tels que

   $$x = x_1^k,\ y = y_1^k.$$

   Pourquoi le morphisme $w \mapsto w^k$ de A^* dans lui-même est-il injectif ? Surjectif ?

Exercice 12 *Une équation de Mordell*
On veut montrer que les solutions de l'équation diophantienne

$$y^2 = x^3 - 2$$

sont $(3, \pm 5)$. On suppose dans la suite que (x, y) est un couple de solutions entières de l'équation.

1. Montrer que $y + i\sqrt{2}$ et $y - i\sqrt{2}$ sont premiers entre eux dans l'anneau factoriel $A := \mathbb{Z}[i\sqrt{2}]$.
   Prendre un diviseur commun d, qu'il ne coûte pas plus cher de choisir premier. Montrer que forcément d est associé à $i\sqrt{2}$, puis, on en déduit que 2 divise y et x. Ceci aboutit facilement à une contradiction.
2. En déduire que $y + i\sqrt{2}$ est un cube de A et conclure. *Quelles sont les unités de A ?*

Exercice 13 *Une autre équation de Mordell*
Montrer que si les entiers x, y vérifient

$$y^2 + 4 = x^3,$$

alors $(x, y) = (2, \pm 2)$ ou $(5, \pm 11)$.

Soluce

On travaille sur l'anneau euclidien (donc factoriel) $\mathbb{Z}[i]$.

$$x^3 = (y+2i)(y-2i). \ (*)$$

Nous allons montrer que ceci implique que les deux facteurs du membre de droite sont des cubes de $\mathbb{Z}[i]$. Montrons tout d'abord que ceci nous mènera avec puissance et élégance à la solution de l'énoncé. Supposons donc

$$y+2i = (m+ni)^3, m, n \in \mathbb{Z}.$$

On obtient alors $y = m(m^2-3n^2)$, $2 = n(3m^2-n^2)$. La seconde équation donne $n = \pm 1$ ou $n = \pm 2$.
On obtient cas par cas les solutions suivantes $(n,m) = (1, \pm 1)$, ou $(-2, \pm 1)$. Le premier cas donne $(x,y) = (2, \pm 2)$ et le second $(5, \pm 11)$.

Reste à montrer que $y+2i$ et $y-2i$ sont des cubes. En fait, par (*), il suffit de le montrer pour un des deux.
L'équation $y^2+4 = x^3$ quotientée dans $\mathbb{Z}/2\mathbb{Z}$ montre que x et y sont de même parité.

1er Cas. x et y sont impairs. Montrons que $y+2i$ et $y-2i$ sont premiers entre eux dans $\mathbb{Z}[i]$.
Soit d un diviseur commun à $(y+2i)$ et $(y-2i)$. Alors d divise $4i$. Donc, dans $\mathbb{Z}$, $N(d)$ divise 16 et $N(y+2i) = y^2+4$ qui est impair et ainsi $N(d) = 1$, ce qui fait de d une unité. Il vient que $y+2i$ et $y-2i$ sont bien premiers entre eux et donc l'équation montre que ce sont des cubes à unité près dans $\mathbb{Z}[i]$. Mais les unités de $\mathbb{Z}[i]$ sont elles-mêmes des cubes (ce sont les racines quatrièmes de l'unité et 3 est inversible dans $\mathbb{Z}/4\mathbb{Z}$), et donc notre assertion est vérifiée dans ce cas.

2ème cas. On suppose maintenant que x et y sont tous deux pairs. On pose $x = 2t$ et $y = 2z$, de sorte que

$$z^2+1 = 2t^3.$$

ce qui donne que z est impair et regardant cette équation modulo 2 et t est impair, en la regardant modulo 4. Donc, $z+i$ est divisible par $(1+i)$ dans $\mathbb{Z}[i]$ et de même, $z-i$ est divisible par $(1+i)$. D'où

$$-it^3 = \frac{z+i}{1+i}\frac{z-i}{1+i}.$$

Ces deux facteurs sont de plus premiers entre eux dans $\mathbb{Z}[i]$, puisque si d est un diviseur commun, alors, d divise leur différence $\frac{2i}{1+i}$. Ce qui donne $N(d)$ divise $N(\frac{2i}{1+i}) = 2$. Or, comme d divise t^3, $N(d)$ divise aussi $N(t^3) = t^6$ qui est impair. Donc d est une unité et on conclut comme dans le premier cas que $\frac{z+i}{1+i}$ est un cube, puis que $y+2i = 2(z+i) = i^3(1+i)^3\frac{z+i}{1+i}$ en est un aussi.

Exercice 14 $\mathbb{Z}[\frac{1+i\sqrt{19}}{2}]$ *non euclidien*
On se propose de montrer que $A := \mathbb{Z}[\alpha]$, avec $\alpha = \frac{1+i\sqrt{19}}{2}$, n'est pas euclidien. On suppose donc par l'absurde qu'il existe un stathme

$$A : A\backslash\{0\} \to \mathbb{N}$$

sur A.

1. Quels sont les éléments inversibles de A ?
   Toujours grâce à la norme !
2. Montrer qu'il existe x tel que x non inversible et $\phi(x)$ minimal (parmi les x non inversibles).
3. Montrer que la restriction sur $A^* \cup \{0\}$ de la projection canonique π de A sur $A/(x)$ est surjective.
4. En déduire que l'anneau $A/(x)$ est soit $\mathbb{Z}/2\mathbb{Z}$, soit $\mathbb{Z}/3\mathbb{Z}$.
   Si B est un anneau unitaire de cardinal 2 ou 3, on peut écrire à la main sa règle de multiplication.
5. En regardant l'image de α par π, conclure à une absurdité.
   Trouver un polynôme annulateur de α sur $\mathbb{Z}$ et considérer l'image de α par π.