TD n°10 : Anneaux

8-9/12/2022

Exercice 1. Factorisation dans $\mathbb{Z}[i]$

Donner une factorisation en irréductibles dans l'anneau principal $\mathbb{Z}[i]$ des éléments suivants :

1. L'élément 21.
2. L'élément 13.
3. L'élément $2+11i$.
4. L'élément $11+2i$.
5. L'élément $22-3i$

Correction de l'exercice 1 :

1. Dans $\mathbb{Z}$, l'entier 21 se factorise comme $21 = 3 \times 7$. Les deux nombres premiers 3 et 7 sont congrus à 3 modulo 4, ce qui implique qu'ils sont irréductibles dans $\mathbb{Z}[i]$. Ainsi, la décomposition suivante est une décomposition en irréductibles non associés dans $\mathbb{Z}[i]$:

$$21 = 3 \times 7.$$

2. Dans $\mathbb{Z}$, l'entier 13 est premier. Puisqu'il est congru à 1 modulo 4, il se factorise dans $\mathbb{Z}[i]$ comme $(a+ib)(a-ib)$ où $13 = a^2+b^2$. Ici, nous avons $13 = 2^2+3^2$. Les deux entiers de Gauss qui apparaissent sont non associés et irréductibles puisque de norme première. Ainsi, la décompositon suivante est une décomposition en irréductibles non associés dans $\mathbb{Z}[i]$:

$$13 = (2+3i)(2-3i).$$

3. La norme de $2+11i$ vaut $2^2+11^2 = 125 = 5^3$. L'entier 5 est congur à 1 modulo 4 donc se décompose en deux éléments irréductibles de norme 5 non associés $5 = (1+2i)(1-2i)$. Les associés de ces deux éléments sont les seuls éléments de norme 5 de $\mathbb{Z}[i]$. De plus, en considérant les coefficients de $2+11i$ dans la base $(1, i)$, nous voyons que $5 \not| 2+11i$. Il en découle que $2+11i$ est associé au cube de l'un des deux irréductibles précédemment cités. Reste à savoir lequel des deux irréductibles le divise. On calcule

$$\frac{2+11i}{1+2i} = \frac{(2+11i)(1-2i)}{5} = \frac{24+7i}{5} \text{ et } \frac{2+11i}{1-2i} = \frac{(2+11i)(1+2i)}{5} = \frac{-20+15i}{5} = -4+3i.$$

On calcule alors le cube $(1-2i)^3 = -11+2i$. Ainsi, la décomposition suivante est une décomposition en irréductibles dans $\mathbb{Z}[i]$:

$$2+11i = -i(1-2i)^3.$$

4. Il se trouve que $11+2i = i\overline{(2+11i)}$ ce qui permet en réutilisant la question précédente d'écrire la décomposition suivante en irréductibles dans $\mathbb{Z}[i]$:

$$11+2i = -(1+2i)^3.$$

5. La norme de cet élément est $493 = 17 \times 29$. Avec les techniques des questions précédentes, on trouve la décomposition en irréductibles non associés suivante dans $\mathbb{Z}[i]$:

$$22-3i = (1-4i)(2+5i).$$

Exercice 2. L'anneau $\mathbb{Z}[j]$

On appelle $j = (-1+i\sqrt{3})/2$ qui est une racine primitive 3-ième de l'unité.

1. Prouver que le sous-groupe $\mathbb{Z}[j] := \mathbb{Z} + j\mathbb{Z}$ est un sous-anneau de $\mathbb{C}$. Donner son groupe des unités.
2. Démontrer que la norme $z \mapsto |z|^2$ est un stathme restreinte à $\mathbb{Z}[j]$.

Nous nous intéressons à présent à l'écriture d'un nombre premier sous la forme $A^2 + 3B^2$ où $A, B \in \mathbb{Z}$.

3. Soit $p \geq 5$ un nombre premier qui s'écrive $a^2 + 3b^2$. Démontrer que $p \equiv 1 \mod 3$.
4. Exhiber une bijection entre les solutions (a, b) au problème et les $c + dj \in \mathbb{Z}[j]$ de norme p et tels que d est pair.
5. Nous supposons à présent que $p \equiv 1 \mod 3$. Démontrer que $X^2 + X + 1$ possède une racine modulo p, puis en déduire par un raisonnement par l'absurde que p ne peut être irréductible dans $\mathbb{Z}[j]$.

Indication : on pourra remarquer que sur $\mathbb{Z}[j]$, nous avons l'égalité $X^2 + X + 1 = (X - j)(X - j^2)$.

6. Démontrer qu'il existe $c + dj$ de norme p dans $\mathbb{Z}[j]$, et que c et d ne peuvent être tous les deux pairs. Prouver ensuite que l'on peut supposer d pair, i.e. qu'il existe une solution entière (a, b) au problème $p = A^2 + 3B^2$. Démontrer que les solutions au problème sont exactement $\{\pm a, \pm b\}$.
7. Démontrer qu'un nombre premier $p > 7$ s'écrit $A^2 + 7B^2$ si et seulement si -7 est un carré modulo p. Démontrer que dans ce cas, il existe exactement quatre solutions.

Correction de l'exercice 2 :

1. Puisque c'est un sous-groupe dont un connaît des générateurs, il suffit de prouver que les produits de ces générateurs restent dedans. Ici, il suffit de le prouver pour j^2 qui vaut $-j - 1$. Dans $\mathbb{C}$, l'inverse de z est donné par $\overline{z}/|z|^2$. Nous remarquons que la conjugaison complexe stabilise $\mathbb{Z}[j]$ puisque $\overline{j} = j^2$, puis que $z \mapsto |z|^2$ est à valeurs entières, une fois restreintes à $\mathbb{Z}[j]$: en effet,

$$\begin{aligned} |c + dj|^2 &= (c + dj)(c + dj^2) \\ &= c^2 + cd(j + j^2) + d^2 \\ &= c^2 - cd + d^2 \end{aligned}$$

Ainsi, les unités de $\mathbb{Z}[j]$ sont exactement les éléments de norme 1. Nous réécrivons

$$|c + dj|^2 = \left(c - \frac{d}{2}\right)^2 + 3\left(\frac{d}{2}\right)^2.$$

En examinant le second terme, un élément de norme 1 vérifie $|d| \leq 1$. Si $d = 0$, la condition sur c devient $c = \pm 1$. Si $d = \pm 1$, la condition devient $|c \pm 1/2|^2 = 1/4$ donc $c = 0$ ou $c = \pm 1$ avec le signe opposé à l'autre signe. Nous obtenons ainsi

$$\mathbb{Z}[j]^\times = \{1, -1, j, -1 + j = j^2, -j, -j^2\}.$$

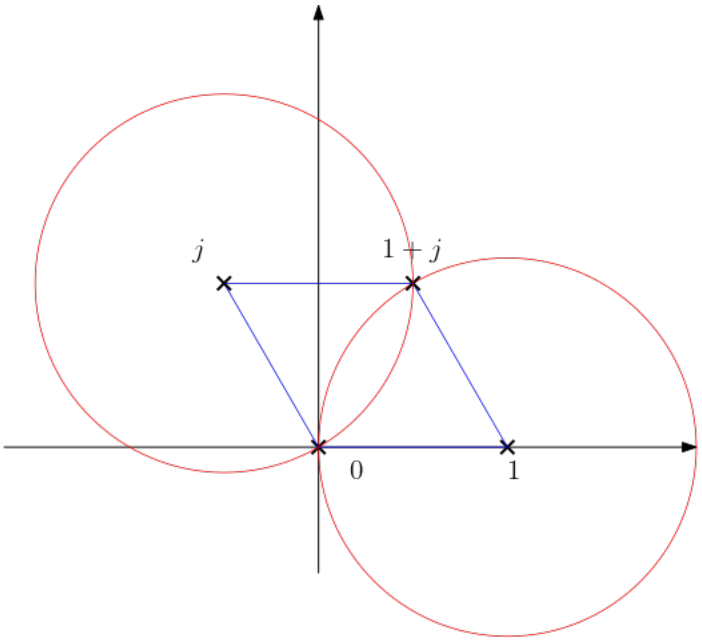
2. Comme pour $\mathbb{Z}[i]$, on commence par démontrer que pour tous $z_1, z_2 \in \mathbb{Z}[j]$, il existe $q \in \mathbb{Z}[j]$ tel que

$$|z_1/z_2 - q| < 1.$$

Nous donnons une preuve graphique en disant qu'en ôtant un élément de $\mathbb{Z}[j]$, nous pouvons supposer que le quotient appartient à la maille fondamentale du réseau $\mathbb{Z} + j\mathbb{Z}$, i.e. qu'il est dans le losange suivant :

où l'on voit que tout élément sauf 0 et $1 + j$ sont dans l'intérieur de l'un des cercles. Plus algébriquement, nous écrivons dans $\mathbb{C}$,

$$z_1/z_2 = x + jy.$$



En choisissant x_0 et y_0 les entiers les plus proches de x et y, nous avons

$$|z_1/z_2 - x_0 - jy_0|^2 = \left(x - x_0 + \frac{y-y_0}{2}\right)^2 + 3\left(\frac{y-y_0}{2}\right)^2 \leq \left(\frac{3}{4}\right)^2 + 3\left(\frac{1}{2}\right)^2 < 1.$$

Soit I un idéal non nul de $\mathbb{Z}[j]$. On considère z_2 un élément non nul de norme minimale dans I. Alors pour tout $z_1 \in I$, la propriété précédente fournit $q \in \mathbb{Z}[j]$ tel que $|z_1 - qz_2|^2 < |z_2|^2$. Puisque $z_1 - qz_2 \in I$, il est nul ce qui prouve que $I = (z_2)$.

3. Les carrés sont congrus à 0 ou 1 modulo 3. Puisque p est premier, congru à a^2 modulo 3, et différent de 3, il doit vérifier $p \equiv 1 \mod 3$.

4. Rappelons que a norme d'un élément s'écrit $|c+dj|^2 = \left(c - \frac{d}{2}\right)^2 + 3\left(\frac{d}{2}\right)^2$. Ainsi, un élément de norme p tel que d est pair fournit une solution $(c - \frac{d}{2}, d/2)$ au problème d'écriture et une solution (a, b) fournit un élément $(a+b) + 2bj$ de norme p avec $2b$ pair. On vérifie sans problème que ces applications sont inverses l'une de l'autre.

5. Puisque $p \equiv 1 \mod 3$, le polynôme $Y^{p-1} - 1$ se factorise en $(X-1)(X^2+X+1)$ où $X = Y^{\frac{p-1}{3}}$. Puisque le polynôme initial possède $p-1$ racines dans $\mathbb{Z}/p\mathbb{Z}$, le polynôme X^2+X+1 en possède également.

   Ainsi, il existe un entier n tel que $p|n^2+n+1$. Dans $\mathbb{Z}[j]$, ceci se traduit par $p|(n-j)(n-j^2)$. Si p était irréductible, par lemme de Gauss il diviserait $n-j$ ou $n-j^2 = (n+1)+j$. Les coefficients de j de ces deux complexes ne sont pas divisibles par p, ce qui implique que p ne peut les diviser. Absurde.

6. Soit $c+dj$ un diviseur irréductible de p, qui doit être de norme p. Puisque la norme s'écrit $c^2 - cd + d^2$ et que p est impair, les entiers c et d ne peuvent simultanément être pairs. L'élément $c+dj^2$ n'est pas associé à $c+dj$ (considérer le quotient) et puisque $p = (c+dj)(c+dj^2)$ nous connaissons les 12 éléments de norme p dans $\mathbb{Z}[j]$:

$$\{c+dj, \ , j(c+dj) = -d + (c-d)j, \ j^2(c+dj) = (d-c) - cj\} \text{ leurs opposés,}$$

leurs conjugués et les opposés de leurs conjugués.

Ceci fait des paquet de 4 éléments de norme p (un élément, son opposé, son conjugué et l'opposé de son conjugué) pour lesquels la condition "d est pair" ne dépend pas du représentant. Les trois premiers élément ci-dessus sont des représentants et, parmi eux, exactement un vérifie la condition

"d est pair". Supposons que l'on a choisit celui-ci pour $c+dj$, alors les éléments de norme p avec condition de parité sont exactement

$$\{c+dj,\ -c-dj,\ c+dj^2,\ -c-dj^2\}$$

ce qui fournit $\{(\pm a,\pm b)\}$ comme solutions au problème d'écriture.

7. Plus subtil, demandez-moi si vous voulez une correction avant l'année prochaine.

Exercice 3. Un anneau factoriel non principal

Pour tout polynôme $P\in\mathbb{Z}[X]$ non nul, nous définissons le *contenu* de P, noté $\mathrm{c}(P)$ comme le PGCD de ses coefficients.

1. Démontrer que le contenu est multiplicatif, i.e. que
$$\forall P,Q\in\mathbb{Z}[X]\backslash\{0\},\ \ \mathrm{c}(PQ)=\mathrm{c}(P)\mathrm{c}(Q).$$
2. Rappeler pourquoi $\mathbb{Q}[X]$ est factoriel, puis en déduire que $\mathbb{Z}[X]$ est factoriel. Donner ses irréductibles.
3. Démontrer que $\mathbb{Z}[X]$ n'est pas principal.

Correction de l'exercice 3 :

1. Quitte à diviser P et Q par leurs contenus, on peut se restreindre au cas où $\mathrm{c}(P)=\mathrm{c}(Q)=1$. Supposons par l'absurde que $\mathrm{c}(PQ)\neq 1$. Choisissons un premier ℓ. En réduisant les polynômes modulo ℓ, nous obtenons que $P,Q\not\equiv 0 \mod \ell$ puisque ℓ ne divise pas leurs contenus. Comme $\mathbb{Z}/\ell\mathbb{Z}[X]$ est intègre, il en découle que $PQ\not\equiv 0 \mod \ell$, autrement dit que ℓ ne divise pas le contenu de PQ. Ceci étant vrai pour tout nombre premier, nous obtenons que $\mathrm{c}(PQ)=1$.
2. rédiger avec le contenu dans $\mathbb{Q}$? L'anneau des polynômes sur un corps est factoriel. Commençons par donner les inversibles : si P est inversible dans $\mathbb{Z}[X]$, il est de degré nul, donc inversible dans $\mathbb{Z}$. Par conséquent $\mathbb{Z}[X]^\times=\{\pm 1\}$. Ainsi, un polynôme de contenu différent de 1 n'est pas irréductible puisqu'il se factorise par son contenu. À présent, soit P un polynôme de contenu 1. Supposons que $P=\prod Q_n$ est une décomposition en irréductibles dans $\mathbb{Q}[X]$. Posons d_n le PPCM des dénominateurs des coefficients et k_n le contenu de d_nQ_n. Alors ${}^{d_nQ_n}/_{k_n}$ est un polynôme à coefficients entiers, de contenu 1. Puisque P est de contenu 1, pour que $\widetilde{P}=(\prod {}^{d_n}/_{k_n})P$ soit à coefficients entiers, il faut que $\prod {}^{d_n}/_{k_n}$ soit entier. En utilisant ensuite la multiplicativité du contenu, nous en déduisons que $\mathrm{c}(\widetilde{P})=(\prod {}^{d_n}/_{k_n})=1$. Ainsi, $\widetilde{P}=P$ et est produit de polynômes de $\mathbb{Z}[X]$ associés dans $\mathbb{Q}[X]$ aux Q_n. Il en découle que P de contenu 1 est irréductible dans $\mathbb{Z}[X]$ si et seulement s'il l'est dans $\mathbb{Q}[X]$. Les irréductibles sont donc exactement les nombres premiers et les polynômes de contenu 1 irréductibles dans $\mathbb{Q}[X]$.

   Démontrons la factorialité. L'existence est donnée par ce qui précède, on se ramène à un polynôme de contenu 1 puis on décompose dans $\mathbb{Q}[X]$ est on raccomode les propriétés d'intégralité. Supposons à présent que l'on a deux décompositions égales
$$\pm\prod p^{n_p}\prod_I Q_i=\pm\prod p^{m_p}\prod_J R_j$$
où les Q_i et les R_j sont des polynômes de contenu 1, irréductibles sur $\mathbb{Q}$. Le contenu de chacun de ces produits est le produit de nombres premiers devant : l'unicité de la décomposition dans $\mathbb{Z}$ permet de se retreindre au cas où le contenu est 1. La factorialité de $\mathbb{Q}[X]$ affirme alors qu'il existe une bijection $f:I\xrightarrow{\sim}J$ et des rationnels q_i tels que $Q_i=r_iP_{f(i)}$. Reste donc à prouver que si $Q=rP$ où Q,P sont des polynômes irréductibles sur $\mathbb{Q}$ et de contenu 1 alors $Q=\pm P$. En écrivant sous forme réduite $r={}^a/_b$ nous obtenons dans $\mathbb{Z}[X]$ l'identité $aQ=bP$ ce qui se traduit sur les contenus par $|a|=|b|$ et conclut.

3. Considérons l'idéal $(2, X)$. Il est strict puisque l'on vérifie aisément qu'il vaut $2\mathbb{Z}+X\mathbb{Z}[X]$. De plus, s'il était principal, nous aurions un polynôme P non inversible tel que $P|2$ et $P|X$. La première condition donne que $\deg(P) = 0$, la deuxième que son contenu est 1. Absurde puisque seuls ± 1 vérifient ces deux conditions.

Exercice 6. Anneaux non principaux liés aux corps quadratiques

Le but de cet exercice est de démontrer que pour $d < -2$, l'anneau $\mathbb{Z}[\sqrt{d}] = \mathbb{Z} + \sqrt{d}\mathbb{Z}$ n'est pas principal.

1. Démontrer pour $d \in \{-3, -4\}$ que l'anneau n'est pas factoriel en exhibant deux écritures distinctes en irréductibles non associés d'un même élément.

Dans les cas restants, nous posons $\alpha = \sqrt{d}$ si d est pair et $\alpha = 1 + \sqrt{d}$ si d est impair.

2. Pour $d < -4$, lister les éléments $z \in \mathbb{Z}[\sqrt{d}]$ tels que $|z|^2$ divise 4.
3. Démontrer que l'idéal engendré par 2 et α vaut $(2, \alpha) = 2\mathbb{Z} + \alpha\mathbb{Z}$.
4. En déduire que $(2, \alpha)$ est un idéal strict et non principal de $\mathbb{Z}[\sqrt{d}]$.

Correction de l'exercice 6 :

1. Pour $d = -3$, nous examinons la norme $z \mapsto |z|^2$ qui s'écrit $|a+\sqrt{-3}b|^2 = a^2+3b^2$. Nous réalisons qu'il n'est pas d'élément de norme égale à 2. Ceci implique que tout élément de norme 4 est irréductible. Les écritures
$$4 = 2^2 = (1 + i\sqrt{3})(1 - i\sqrt{3})$$
illustrent que $\mathbb{Z}[\sqrt{-3}]$ n'est pas factoriel. Reste à voir que 2 et $1 + i\sqrt{3}$ ne sont pas associés, ce qui est limpide puisque 2 ne divise pas les coefficients de $1 + i\sqrt{3}$ dans la base $(1, i\sqrt{3})$.

   Pour $d = -4$, faire de même avec les écritures
$$4 = 2^2 = -(2i)^2.$$
2. Faire les calculs en considérant que la norme s'écrit $|a + b\sqrt{d}|^2 = a^2 + |d|b^2$.
3. Il faut simplement vérifier que $2\sqrt{d}$ et $\alpha\sqrt{d}$ appartiennent à $2\mathbb{Z} + \alpha\mathbb{Z}$. Dans le cas où $d = 2d'$ est pair
$$2\sqrt{d} = 2\alpha \text{ et } \alpha\sqrt{d} = d = 2d'.$$
   Dans le cas où $d = 2d' + 1$ est impair
$$2\sqrt{d} = 2\alpha - 2 \text{ et } \alpha\sqrt{d} = \sqrt{d} + d = \alpha + 2d'.$$
4. Puisque $(1, \alpha)$ est une famille libre et génératrice de $\mathbb{Z}[\sqrt{d}]$, l'élément 1 ne peut appartenir à $(2, \alpha)$. S'il était principal, il existerait un élément z divisant 2 et α non inversible. Comme $z|2$ une analyse des normes à la question 2 démontre que z est associé à 2. Il en découle que 2 divise α, ce qu'une analyse des coefficients dans la base $(1, \sqrt{d})$ dément. Absurde.