TD n°10 : Anneaux

8 et 12/12/2023

Nous traiterons dans l'ordre les exercices 1, 2, 3 et 6. Vous pouvez naviguer librement parmi les exercices restants ou parmi ceux de votre polycopié. Les exercices les plus délicats de la feuille sont marqués d'un ●.

Je reste disponible pour toute question concernant le TD, des maths, ou toute autre chose au bureau T13 (j'y suis à coups sûrs les mardis et vendredis juste avant le TD). Vous pouvez également m'envoyer un mail à nataniel.marquis@dma.ens.fr.

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 $22 - 3i$

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.

Remarque : grâce à la réciprocité quadratique, ceci équivaut au fait que p est un carré modulo 7, i.e. que $p \equiv 1, 2, 4 \mod 7$. On remarquera qu'il s'agissait d'une condition nécessaire, autrement dit que la question précédente démontre une implication dans la réciprocité quadratique.

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.

Exercice 4. Autour des anneaux euclidiens

Dans cet exercice, nous considérons un anneau commutatif A. On définit une suite croissante de sous-ensembles comme suit
$$A_0 = \emptyset \text{ et } A'_0 = \{0\}$$
$$\forall n \geq 0, \;\; A_{n+1} = \left\{ x \in A \,\middle|\, A = (x) + A'_n \right\} \text{ et } A'_{n+1} = A_{n+1} \cup \{0\}.$$

1. Supposons que A est euclidien de stathme v. Démontrer que
$$\forall n \geq 0, \forall a \in A \backslash \{0\}, \;\; \mathrm{v}(a) \leq n \Rightarrow a \in A_{n+1}.$$
2. Nous définissons l'application suivante :
$$\nu \,:\, \bigcup_{n \geq 0} A_n \to \mathbb{N}, \;\; a \mapsto \min\{k \geq 0 \,|\, a \in A_{k+1}\}.$$
Démontrer que A est euclidien si et seulement si $\cup A'_n = A$. Dans le cas où A est euclidien, démontrer que ν est le plus petit stathme (au sens de la comparaison évaluation par évaluation des stathmes), puis que ν vérifie que si $a|b$ alors $\nu(a) \leq \nu(b)$.
3. Que donne cette construction sur $\mathbb{Z}$? Sur $k[X]$ pour un corps k ?
4. Soit A un anneau euclidien. Exhiber un élément non inversible x tel que $A^\times \cup \{0\} \to A/xA$ est surjective.

Exercice 5. Un anneau principal non euclidien

Considérons dans cet exercice l'anneau $A = \mathbb{Z}\left[\frac{1+\sqrt{-19}}{2}\right]$. Nous commençons par démontrer que cet anneau n'est pas euclidien.

1. Démontrer que les éléments $z \in A$ vérifient $|z|^2 \in \mathbb{Z}$.
2. Lister les éléments tels que $|z|^2 \leq 9$. En déduire les inversibles de A, puis que 2 et 3 sont irréductibles.
3. En déduire grâce à l'exercice précédent que A n'est pas euclidien.

Finissons en démontrant qu'il est principal. On fixe un idéal I non nul et w un élément de plus petite norme dans I. Soit $z \in I$.

1. Démontrer qu'il existe un entier b tel que $z' = z - bw$ vérifie que z'/w est de partie imaginaire inférieure à $\sqrt{19}/4$ en valeur absolue.
2. Si cette partie imaginaire est strictement inférieure à $\sqrt{3}/2$ en valeur absolue, démontrer que z'/w est à distance strictement inférieure à 1 d'un entier, puis que $z \in wA$.
3. Sinon, en considérant que $\sqrt{3}/2 > \sqrt{19}/2 - \sqrt{3} \geq 0$, démontrer que z ou $2z$ appartient à wA. Conclure.

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 $\mathbb{Z}[\sqrt{d}]$.

Exercice 7. Anneaux de Bézout

Un anneau A sera dit de Bézout si tout idéal *de type fini* est principal.

1. Démontrer qu'un anneau est de Bézout si et seulement si toute paire d'éléments admet un PGCD et une relation de Bézout associée.
2. Démonter qu'un anneau factoriel de Bézout est principal.

Nous cherchons enfin à établir un contre-exemple à l'assertion "un anneau de Bézout est factoriel". Considérons l'anneau $A = \{P \in \mathbb{Q}[X] \mid P(0) \in \mathbb{Z}\}$.

3. Montrer que A n'est pas factoriel en considérant le polynôme X.
4. Montrer que A est de Bézout.

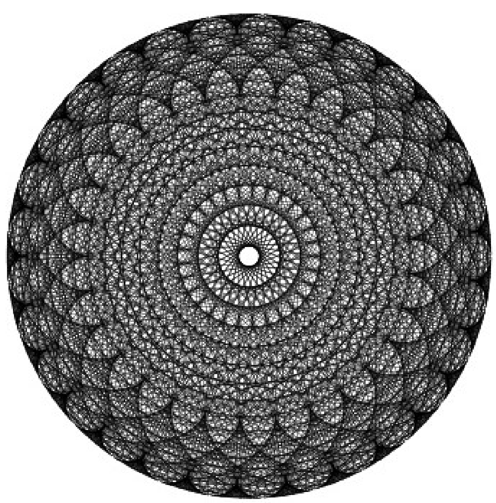

Figure 1 – Puissance 30^{e} appliquée aux racines 1073-ièmes de l'unité.