ALGÈBRE - LEÇON 122 : ANNEAUX PRINCIPAUX. APPLICATIONS

SIMON RICHE

1. Commentaires du jury (rapport 2022)

Comme l'indique son intitulé, cette leçon ne doit pas se cantonner aux aspects théoriques. L'arithmétique des anneaux principaux doit être décrite et les démonstrations doivent être maîtrisées (lemme d'Euclide, théorème de Gauss, décomposition en irréductibles, PGCD et PPCM, etc.). Les anneaux euclidiens représentent une classe importante d'anneaux principaux et l'algorithme d'Euclide a toute sa place dans cette leçon pour effectuer des calculs. Les applications en algèbre linéaire ne manquent pas et doivent être mentionnées (par exemple, le lemme des noyaux ou la notion de polynôme minimal pour un endomorphisme, pour un endomorphisme relativement à un vecteur ou pour un nombre algébrique). Si les anneaux classiques $\mathbf{Z}$ et $\mathbf{K}[X]$ doivent impérativement figurer, il est possible d'en évoquer d'autres (décimaux, entiers de Gauss $\mathbf{Z}[i]$ ou d'Eisenstein $\mathbf{Z}[e^{2i\pi/3}]$) accompagnés d'une description de leurs inversibles, de leurs irréductibles et éventuellement d'applications à des problèmes arithmétiques (équations diophantiennes).

S'ils le désirent, les candidats peuvent aller plus loin en s'intéressant à l'étude des réseaux, à des exemples d'anneaux non principaux, mais aussi à des exemples d'équations diophantiennes résolues à l'aide d'anneaux principaux. À ce sujet, il sera fondamental de savoir déterminer les unités d'un anneau, et leur rôle au moment de la décomposition en facteurs premiers. De même, le calcul effectif des facteurs invariants de matrices à coefficients dans un anneau principal peut être présenté.

2. Plan

Une référence qui couvre la plupart des choses à savoir pour ce chapitre est [Pe].

2.1. **Ce qui doit apparaître.** Définition des anneaux principaux.

Définition du PGCD et du PPCM dans les anneaux principaux (en utilisant les idéaux).

Définition des anneaux euclidiens.
Les anneaux euclidiens sont principaux.
Exemples : $\mathbb{Z}$, $\mathbb{K}[X]$.
Algorithme d'Euclide pour calculer le PGCD et une relation de Bézout.

Éléments irréductibles.
Les anneaux principaux sont factoriels.

Théorème chinois.
Application aux systèmes de congruences.

Date: Année 2022–2023.

Résolution d'équations $ax + by = c$ en utilisant Bézout.
Calcul de l'inverse dans $\mathbb{Z}/n\mathbb{Z}$ via Bézout.

Applications en algèbre linéaire :
— définition du polynôme minimal,
— lemme des noyaux,
— caractérisation de la diagonalisabilité par le polynôme minimal.

Théorème des deux carrés via les entiers de Gauss.

2.2. **Ce qui peut apparaître.** Exemples d'anneau principal non euclidien, d'anneau factoriel non principal, d'anneau non factoriel. [1]

Contenu d'un polynôme à coefficients dans un anneau factoriel. Lemme de Gauss. Application au critère d'irréductibilité d'Eisenstein. [2]

Description des irréductibles de $A[X]$ avec A factoriel. (Un polynôme non constant est irréductible si et seulement si il est de contenu inversible et irréductible dans $\mathrm{Frac}(A)[X]$.)
Exemples pour $A = \mathbb{Z}$.

Endomorphismes cycliques, [3] endomorphismes semi-simples. [4]

Polynôme minimal d'un nombre algébrique.

Classification des modules de type fini sur les anneaux principaux.
Applications : groupes abéliens finis, invariants de similitude.

3. Quelques questions bêtes auxquelles il faut absolument savoir répondre rapidement

(1) Donner un exemple d'idéal non principal dans l'anneau $\mathbb{Z}[X]$. [5]
(2) Que peut-on dire des idéaux dans un quotient d'un anneau principal ? À quelle condition un tel quotient est-il principal ?
(3) Étant donné un corps $\mathbb{K}$, quels sont les éléments de $\mathbb{K}[X]$ qui sont les polynômes minimaux d'un endomorphisme d'un $\mathbb{K}$-espace vectoriel de dimension finie ? Quels sont les éléments qui sont les polynômes minimaux d'un élément d'une extension finie de $\mathbb{K}$?

4. Exercices

4.1. Éléments premiers, éléments irréductibles.

Exercice 1. Soit A un anneau commutatif intègre. On rappelle qu'un élément $a \in A$ non nul et non inversible est dit :
— *premier* s'il vérifie la propriété suivante : si $b, c \in A$ et si a divise bc, alors a divise b ou a divise c ;
— *irréductible* s'il vérifie la propriété suivante : si $b, c \in A$ et si $a = bc$, alors b ou c est inversible.

1. Voir notamment le §5.4 pour quelques indications et références.
2. Voir par exemple [FGN, Exercice 5.16].
3. Voir Exercice 12 ci-dessous.
4. Si ce thème est abordé, il me semble indispensable de connaitre le lien avec la diagonalisabilité sur une clôture algébrique du corps de base ; voir l'Exercice 13 ci-dessous.
5. Si nécessaire, voir [FGN, Exercice 3.9].

(1) Montrer qu'un élément premier est toujours irréductible.
(2) On rappelle qu'un idéal I d'un anneau commutatif B est dit *premier* si le quotient B/I est intègre [6]. Montrer que si A est comme ci-dessus, alors un élément $a \in A$ est premier si et seulement si l'idéal $aA \subset A$ est premier.
(3) Montrer que dans l'anneau $\mathbb{Z}[i\sqrt{5}]$ l'élément 2 est irréductible mais pas premier. (*Indication* : on pourra considérer le produit $(1+i\sqrt{5})(1-i\sqrt{5})$.
(4) Montrer que si A est factoriel, un élément $a \in A$ est irréductible si et seulement si il est premier.
(5) Montrer que si A est principal les propriétés suivantes sont équivalentes :
   (a) a est premier ;
   (b) a est irréductible ;
   (c) l'idéal $aA \subset A$ est maximal.

Notons que cet exercice implique en particulier que, dans un anneau principal, tout idéal premier non nul est maximal.

4.2. **Idéaux.**

Exercice 2. (1) Soit M dans $\mathrm{M}_n(\mathbb{K})$ avec $\mathbb{K}$ un corps. À quelle condition la sous-algèbre de $\mathrm{M}_n(\mathbb{K})$ engendrée par M est-elle un anneau principal ?
(2) Décrire les idéaux bilatères de l'anneau $\mathrm{M}_n(\mathbb{K})$. Même chose pour les idéaux à gauche, resp. à droite.

Indication : Pour (1), on pourra penser au polynôme minimal. Pour les idéaux bilatères dans (2), on pourra considérer la multiplication par une matrice élémentaire $E_{i,j}$. (Voir [FGN, Exercice 6.24].) Pour le cas (plus difficile) des idéaux à gauche et à droite, voir [FGN, Exercices 6.25–26].

Exercice 3. Montrer que si A et B sont des anneaux principaux, alors tout idéal de $A \times B$ est principal. Cet anneau est-il principal ?

Exercice 4. (1) Soit A un anneau principal. Montrer que si I est un idéal non nul, l'anneau A/I n'a qu'un nombre fini d'idéaux. (*Indication* : on pourra utiliser la décomposition en produit d'irréductibles.)
(2) Si E est un espace vectoriel de dimension finie, un endomorphisme u de E est dit *cyclique* s'il existe un vecteur x tel que E est engendré par les vecteurs $(u^i(x) : i \in \mathbb{Z}_{\geq 0})$. Montrer que si u est cyclique, alors E n'admet qu'un nombre fini de sous-espace vectoriels stables par u.

Pour plus de détails sur les sous-espaces stables par un endomorphisme cyclique, voir [CG, Chap. II, Exercices B.5–7].

4.3. **Exemples d'anneaux principaux.**

Exercice 5. Montrer que l'anneau des nombres décimaux (c'est-à-dire ceux qui s'écrivent sous la forme $a \times 10^k$ avec $a, k \in \mathbb{Z}$) est principal. (*Indication* : étant donné un idéal de cet anneau, pour en trouver un générateur on pourra considérer son intersection avec $\mathbb{Z}$.) Décrire les inversibles et les irréductibles de cet anneau.

Référence : [FGN, Exercice 3.8].

6. Rappelons que, par convention, l'anneau nul n'est *pas* intègre.

Exercice 6. Montrer que les anneaux $\mathbb{C}[X,Y]/(Y-X^2)$ et $\mathbb{C}[X,Y]/(XY-1)$ sont principaux.

Indication : On pourra essayer de décrire ces anneaux plus "concrètement" comme anneaux de polynômes.

4.4. **Division euclidienne, PGCD.**

Exercice 7. Soit $\mathbb{K} \subset \mathbb{L}$ une extension de corps.

(1) Si $P, Q \in \mathbb{K}[X]$, comparer les pgcd de P et Q dans l'anneau principal $\mathbb{K}[X]$ et dans l'anneau principal $\mathbb{L}[X]$.

(2) Si M est un matrice carrée à coefficients dans $\mathbb{K}$, comparer les polynômes minimaux de M vue comme matrice à coefficients dans $\mathbb{K}$ et comme matrice à coefficients dans $\mathbb{L}$.

Indication : Pour (2), on pourra étudier le comportement du rang d'une famille de vecteurs de $\mathbb{K}^n$ par extension de corps, et en déduire une information concernant le degré du polynôme minimal.

Exercice 8. Soit A un anneau factoriel, de corps des fractions K, et soient $P, Q \in A[X]$.

(1) Montrer que si P est unitaire et divise Q dans $K[X]$, alors le quotient $\frac{Q}{P}$ appartient à $A[X]$.

(2) Montrer plus généralement que si P est primitif (c'est-à-dire de contenu 1) et divise Q dans $K[X]$, alors le quotient $\frac{Q}{P}$ appartient à $A[X]$.

Indication : Pour (1), on pourra réfléchir à la façon "concrète" utilisée pour calculer le quotient. Pour (2), on pourra utiliser le fait que l'application envoyant un polynôme sur son contenu est multiplicative (voir par exemple [Pe, Chap. II, Lemme 4.3]).

Exercice 9 (Idéaux premiers des polynômes en deux variables)**.** On fixe un corps infini k.

(1) Soit $I = (P)$ un idéal principal de $k[X,Y]$ (avec $P \in k[X,Y]$).
   (a) À quelle condition I est-il premier ?
   (b) Montrer que I n'est pas maximal. (*Indication* : on pourra considérer $x \in k$ qui n'annule pas le coefficient de plus haut de P vu comme élément de $(k[X])[Y]$, puis montrer que l'inclusion $(P) \subset (P, X-x)$ est stricte.)

(2) Montrer que si $F, P \in k[X,Y] \smallsetminus \{0\}$, il existe $Q, R \in k[X,Y]$ et $a \in k[X]$ tels que $a(X)F(X,Y) = P(X,Y)Q(X,Y) + R(X,Y)$ et $\deg_Y(R) < \deg_Y(P)$.

(3) Le but de cette question est de décrire les idéaux premiers non principaux de $k[X,Y]$. On considère donc un idéal premier non principal $I \subset k[X,Y]$.
   (a) Notons d le degré minimal en Y d'un polynôme de I. Soit $P \in I$, tel que $\deg_Y(P) = d$ et $\deg_X(P)$ est minimal parmi les polynômes $Q \in I$ tels que $\deg_Y(Q) = d$. Montrer que P est irréductible.
   (b) En considérant un élément $F \in I \smallsetminus (P)$, montrer que $P \in k[X]$, et que P est irréductible dans $k[X]$.
   (c) Montrer qu'il existe $Q \in I$, dont l'image dans $(k[X]/P)[Y]$ est irréductible, et tel que $I = (P, Q)$.

(d) Montrer que I est maximal, et que $k[X,Y]/I$ est de dimension finie sur k.

(4) Montrer que si k est algébriquement clos, les idéaux maximaux de $k[X,Y]$ sont exactement les idéaux de la forme $(X, a, Y-b)$ avec $a, b \in k$.

(5) Décrire les idéaux premiers non principaux de $\mathbb{R}[X,Y]$.

Référence : [FG, Exercice 2.22].

4.5. **Applications classiques.**

Exercice 10. Soient $P, Q \in \mathbb{C}[X,Y]$ sans diviseur commun non constant.

(1) Montrer qu'il existe $A, B \in \mathbb{C}[X,Y]$ et $D \in \mathbb{C}[X] \setminus \{0\}$ tels que

$$D = AP + BQ.$$

(*Indication* : on pourra travailler dans l'anneau euclidien $\mathbb{C}(X)[Y]$, et utiliser l'Exercice 8.)

(2) En déduire que

$$\{(x,y) \in \mathbb{C}^2 \mid P(x,y) = Q(x,y) = 0\}$$

est fini.

Référence : [FG, p. 73–74].

Exercice 11 (Version faible du théorème de Dirichlet)**.** Pour $n \geq 1$, on note

$$\Phi_n(X) = \prod_{\substack{1 \leq k \leq n \\ \text{pgcd}(k,n)=1}} (X - e^{\frac{2ik\pi}{n}})$$

le n-ième polynôme cyclotomique.

(1) Rappeler comment on démontre que

$$X^n - 1 = \prod_{d|n} \Phi_d,$$

et comment on en déduit que :

(a) chaque Φ_n est à coefficients entiers ;

(b) le terme constant de Φ_n est -1 is $n = 1$, et 1 si $n \geq 2$.

(2) Fixons $n \geq 1$ et p un nombre premier, et supposons qu'il existe $a \in \mathbb{Z}$ tel que p divise $\Phi_n(a)$ mais aucun des $\Phi_d(a)$ pour d un diviseur strict de n.

(a) Montrer que l'image de a dans $\mathbb{Z}/p\mathbb{Z}$ est inversible, et d'ordre n dans $(\mathbb{Z}/p\mathbb{Z})^\times$.

(b) En déduire que $p \equiv 1 \mod n$.

(3) Le but de cette question est de démontrer que, si $n \geq 2$, il existe une infinité de nombres premiers congrus à 1 modulo n. On raisonne par l'absurde, en supposant qu'il n'existe qu'un nombre fini de tels nombres premiers, et on les note $p_1, \cdots, p_r$. On pose alors $N = np_1 \cdots p_r$.

(a) Posons

$$B = \prod_{\substack{d|N \\ d<N}} \Phi_d.$$

Montrer qu'il existe $U, V \in \mathbb{Q}[X]$ tels que

$$1 = U\Phi_N + VB.$$

(*Indication* : on pourra utiliser l'Exercice 7.)

(b) Montrer qu'il existe $a \in \mathbb{Z}$ tel que $aU \in \mathbb{Z}[X]$, $aV \in \mathbb{Z}[X]$ et $\Phi_N(a) \notin \{1, -1\}$.

(c) On fixe a comme dans la question précédente. Montrer que si p est un nombre premier divisant $\Phi_N(a)$, alors p ne divise pas $B(a)$.

(d) Montrer que si p est comme dans la question précédente, alors p est congru à 1 modulo n et distinct des p_i.

(e) Conclure.

Référence : [FGN, Exercice 4.18].

Exercice 12 (Endomorphismes cycliques)**.** Soit E un espace vectoriel de dimension finie sur un corps $\mathbb{K}$. On rappelle qu'un endomorphisme u de E est dit *cyclique* s'il existe $x \in E$ tel que les vecteurs $\{u^n(x) : n \in \mathbb{Z}_{\geq 0}\}$ engendrent E. Le but de cet exercice est de démontrer l'équivalence entre les propriétés suivantes :

($\star$) u est cyclique ;

($\star\star$) le polynôme minimal de u coincide avec son polynôme caractéristique ;

($\star\star\star$) l'ensemble des endomorphismes de E qui commutent avec u est l'ensemble des polynômes en u.

(1) Montrer que si u est un endomorphisme de E et $x \in E$, alors

$$I_{u,x} := \{P \in \mathbb{K}[X] \mid P(u)(x) = 0\}$$

est un idéal de $\mathbb{K}[X]$.

(2) Dans le contexte de la question précédente, on note $P_{u,x}$ le générateur unitaire de $I_{u,x}$. Montrer que $P_{u,x}$ divise le polynôme minimal m_u de u, et que l'espace vectoriel engendré par les vecteurs $\{u^n(x) : n \in \mathbb{Z}_{\geq 0}\}$ est de dimension $\deg(P_{u,x})$.

(3) Le but de cette question est de montrer qu'il existe $x \in E$ tel que $P_{u,x} = m_u$. Pour cela on écrit $m_u = \prod_{i=1}^r P_i^{k_i}$ avec les P_i irréductibles deux à deux distincts, et chaque $k_i \geq 1$.

(a) Rappeler pourquoi on a

$$E = \bigoplus_{i=1}^{r} \ker((P_i^{k_i})(u)),$$

avec chaque facteur stable par u, et pourquoi pour tout i l'inclusion $\ker((P_i^{k_i-1})(u)) \subset \ker((P_i^{k_i})(u))$ est stricte.

(b) Montrer que si $x \in \ker((P_i^{k_i})(u)) \smallsetminus \ker((P_i^{k_i-1})(u))$, alors $P_{u,x} = P_i^{k_i}$.

(c) Montrer que si pour tout i on choisit un vecteur $x_i \in \ker((P_i^{k_i})(u)) \smallsetminus \ker((P_i^{k_i-1})(u))$, alors le vecteur $x := x_1 + \cdots + x_r$ vérifie $P_{u,x} = m_u$.

(4) Déduire des questions précédentes l'équivalence entre ($\star$) et ($\star\star$).

(5) Le but de cette question est de montrer que ($\star$) implique ($\star\star\star$). On suppose donc u cyclique, et on choisit $x \in E$ tel que E est engendré par les vecteurs $\{u^n(x) : n \in \mathbb{Z}_{\geq 0}\}$.
   (a) Montrer que si g est un endomorphisme de E, il existe $P \in \mathbb{K}[X]$ tel que $g(x) = P(u)(x)$.
   (b) Montrer que si g commute à u et si P est comme dans la question précédente, alors $g = P(u)$.
   (c) En déduire l'implication souhaitée.

(6) Dans cette question, on considère un endomorphisme u de E, et un vecteur $x \in E$ tel que $P_{u,x} = m_u$. On notera $E_x = \mathrm{Vect}(\{u^n(x) : n \in \mathbb{Z}_{\geq 0}\})$. Le but est de démontrer que E_x admet un supplémentaire stable par u.
   (a) Notons $k = \deg(m_u)$. Montrer que les vecteurs $x, u(x), \cdots, u^{k-1}(x)$ forment une base de l'espace vectoriel E_x.
   (b) On complète la famille de la question précédente en une base $e_1, \cdots, e_n$ de E, et on note $(e_1^*, \cdots, e_n^*)$ la base duale. On pose
   $$G = \bigcap_{i \geq 0} \ker(e_k^* \circ u^i).$$
   Montrer que G est un sous-espace vectoriel de E, stable par u, et tel que $E_x \cap G = \{0\}$.
   (c) Montrer que
   $$G = \bigcap_{i=0}^{k-1} \ker(e_k^* \circ u^i),$$
   et en déduire que $\dim(G) \geq \dim(E) - k$.
   (d) Conclure.

(7) Pour finir, on va montrer que ($\star\star\star$) implique ($\star$).
   (a) On continue avec le contexte de la question précédente : on considère un endomorphisme u de E, et $x \in E$ un vecteur tel que $P_{u,x} = m_u$. Montrer que le polynôme minimal de $u_{|E_x}$ est m_u.
   (b) On suppose à partir de maintenant que les endomorphismes qui commutent à u sont exactement les polynômes en u, et on note G un supplémentaire de E_x stable par u, et p la projection sur G parallèlement à E_x. Montrer qu'il existe $P \in \mathbb{K}[X]$ tel que $p = P(u)$.
   (c) Montrer que $P(u_{|E_x}) = 0$, et en déduire que $G = 0$.
   (d) Conclure.

Référence : `https://perso.univ-rennes1.fr/matthieu.romagny/agreg/dvt/endom_cycliques.pdf`, ou [Go, Chap. 4, §2.4, Exercices 3 et 6, et Annexe B, §3.2]. Les endomorphismes cycliques jouent un rôle crucial dans la théorie des invariants de similitude et la réduction de Frobenius. Pour plus de détails, voir [Go, Annexe B].

Exercice 13 (Endomorphismes semisimples et diagonalisabilité)**.** Une propriété classique affirme que si E est un espace vectoriel de dimension finie sur un corps $\mathbb{K}$ et u un endomorphisme, alors u est semisimple (c'est-à-dire que tout sous-espace de E stable par u admet un supplémentaire stable par u) si et seulement si son

polynôme minimal m_u n'a pas de facteurs carrés dans sa décomposition en produit d'irréductibles (dans $\mathbb{K}[X]$). Pour plus de détails, voir par exemple [CG, Chap. II, Proposition 1.6], ou [Go, Chap. 4, §5, Problème 19], ou encore `https://perso.univ-rennes1.fr/matthieu.romagny/agreg/dvt/endom_semi_simples.pdf`.

L'objectif de cet exercice est d'expliquer, pour une matrice A de $M_n(\mathbb{K})$, le lien entre la propriété que m_A n'a pas de facteur carré dans sa décomposition en produit d'irréductibles et la diagonalisabilité de A dans $M_n(\overline{\mathbb{K}})$, où $\overline{\mathbb{K}}$ est une clôture algébrique de $\mathbb{K}$.

(1) Montrer que si $A \in M_n(\mathbb{K})$ est diagonalisable dans $M_n(\overline{\mathbb{K}})$, alors m_A n'a pas de facteur carré dans sa décomposition en produit d'irréductibles (dans $\mathbb{K}[X]$). (*Indication* : on pourra utiliser la stabilité du polynôme minimal par extension de corps, cf. Exercice 7, et le critère classique de diagonalisabilité en termes du polynôme minimal.)

(2) Dans cette question on souhaite montrer que, si $\mathbb{K}$ est de caractéristique 0 ou s'il est de caractéristique $p > 0$ et de plus son endomorphisme de Frobenius (donné par $x \mapsto x^p$) est surjectif, alors si $A \in M_n(\mathbb{K})$ est telle que m_A n'a pas de facteur carré dans sa décomposition en produit d'irréductibles, la matrice A est diagonalisable dans $M_n(\overline{\mathbb{K}})$.

   (a) Pour $\mathbb{K}$ un corps quelconque, montrer que si P et Q sont deux éléments irréductibles distincts dans $\mathbb{K}[X]$ alors P et Q n'ont aucune racine commune dans $\overline{\mathbb{K}}$. (*Indication* : on pourra utiliser une relation de Bézout.)

   (b) On suppose à partir de maintenant que $\mathbb{K}$ est de caractéristique 0 ou qu'il est de caractéristique $p > 0$ et de plus son endomorphisme de Frobenius est surjectif. Si $P \in \mathbb{K}[X]$ est irréductible, montrer que P n'a pas de racine multiple dans $\overline{\mathbb{K}}$. (*Indication* : on pourra montrer que le polynôme dérivé P' est non nul, puis utiliser une relation de Bézout.)

   (c) Montrer qu'un produit de polynômes irréductibles distincts de $\mathbb{K}[X]$ n'admet pas de racine multiple dans $\overline{\mathbb{K}}$.

   (d) Conclure.

Référence : Voir les références citées dans l'exercice pour des versions (parfois plus faibles) de ces énoncés. On a démontré au passage que si $\mathbb{K}$ est de caractéristique 0 ou s'il est de caractéristique $p > 0$ et de plus son endomorphisme de Frobenius est surjectif, alors $\mathbb{K}$ est *parfait*, c'est-à-dire que tout polynôme irréductible sur $\mathbb{K}$ n'a que des racines simples dans une clôture algébrique de $\mathbb{K}$. La réciproque de cette implication est vraie également : si $\mathbb{K}$ est de caractéristique p et que son morphisme de Frobenius n'est pas surjectif alors il existe des polynômes irréductibles dans $\mathbb{K}[X]$ qui admettent des racines multiples dans $\overline{\mathbb{K}}$. Par exemple, si $a \in \mathbb{K}$ n'est pas une puissance p-ième d'un élément de $\Bbbk$, alors $X^p - a$ est irréductible (voir la fiche de la leçon 125, Exercice 5), mais il n'a qu'une seule racine (de multiplicité p) dans $\overline{\mathbb{K}}$.

4.6. **Un exercice plus anecdotique.**

Exercice 14. On rappelle qu'un anneau intègre commutatif A est dit *euclidien* s'il existe une application $\varphi : A \smallsetminus \{0\} \to \mathbb{N}$ telle que pour tout $(a, b) \in A \times (A \smallsetminus \{0\})$ il existe $(q, r) \in A^2$ tel que

$$a = bq + r \quad \text{et} \quad r = 0 \text{ ou } \varphi(r) < \varphi(b). \tag{1}$$

Remarquons que dans cette définition il n'y a *pas* de condition d'unicité sur q et r. Le but de cet exercice est de montrer que si A n'est pas un corps et si on suppose que pour tout (a, b) comme ci-dessus il existe un *unique* couple (q, r) vérifiant (1), alors $A \cong \mathbb{K}[X]$ pour un corps $\mathbb{K}$.

On suppose donc que A est un anneau euclidien dans lequel on a unicité de la division euclidienne.

(1) Montrer que si $a, b \in A \setminus \{0\}$ et si a divise b, alors $\varphi(a) \leq \varphi(b)$.

(2) En déduire que si $a, b \in A \setminus \{0\}$ sont associés,[7] alors $\varphi(a) = \varphi(b)$.

(3) On note $m_0 = \min(\varphi)$. Montrer que $A^\times = \{x \in A \setminus \{0\} : \varphi(x) = m_0\}$.

(4) Montrer que si $u \in A^\times \setminus \{-1\}$, alors $1 + u \in A^\times$.

(5) Montrer que $\mathbb{K} := A^\times \cup \{0\}$ est un sous-anneau de A qui est un corps.

(6) On note $m_1 = \min_{x \in A \setminus K} \varphi(x)$, et on choisit $X_0 \in A$ tel que $\varphi(X_0) = m_1$. On considère ensuite le morphisme d'algèbres

$$\Psi : \mathbb{K}[X] \to A$$

défini par $\Psi(P) = P(X_0)$. Montrer par récurrence sur n que si $P \in \mathbb{K}[X]$ est de degré n et si $\Psi(P) = 0$, alors $P = 0$.

(7) En déduire que Ψ est injective.

(8) Montrer que si $u \in A \setminus \mathbb{K}$, alors $\varphi(1 + u) = \varphi(u)$.

(9) En déduire que si $x \in A \setminus \mathbb{K}$ et $a \in \mathbb{K}$, alors $\varphi(x + a) = \varphi(x)$.

(10) Montrer que si $x \in A \setminus \{0\}$ alors $\varphi(xX_0) > \varphi(x)$.

(11) En utilisant les deux questions précédentes, montrer par récurrence sur n que si $x \in A \setminus \{0\}$ et $\varphi(x) \leq n$, alors $x \in \mathrm{Im}(\Psi)$.

(12) Conclure.

Référence : [FGN, Exercice 3.11].

5. Complément : équation de Ramanujan–Nagel

Référence : [FG, p. 166–173].

L'objectif de ce complément est de déterminer les solutions entières de l'équation

$$x^2 + 7 = 2^n,$$

en faisant intervenir la décomposition en facteurs irréductibles dans l'anneau principal $\mathbb{Z}[\frac{1+i\sqrt{7}}{2}]$.

5.1. **Étude de l'anneau $\mathbb{Z}[\frac{1+i\sqrt{7}}{2}]$.** Considérons tout d'abord le corps $\mathbb{Q}(i\sqrt{7})$. Tout élément x de ce corps s'écrit de manière unique $x = a + ib\sqrt{7}$ avec $a, b \in \mathbb{Q}$, et on pose

$$\sigma(x) = a - ib\sqrt{7}$$

(de sorte que σ est la restriction de la conjugaison complexe à $\mathbb{Q}(i\sqrt{7})$; en particulier c'est un automorphisme de ce corps) et

$$N(x) = x\sigma(x) = a^2 + 7b^2.$$

Les propriétés suivantes sont claires :

7. On rappelle que deux éléments d'un anneau sont dits *associés* s'ils diffèrent par multiplication par un inversible.

(1) $N(x) \geq 0$ pour tout $x \in \mathbb{Q}(i\sqrt{7})$;

(2) $N(x) = 0$ ssi $x = 0$;

(3) $N(xy) = N(x)N(y)$ pour tous $x, y \in \mathbb{Q}(i\sqrt{7})$.

On pose maintenant

$$\alpha := \frac{1 + i\sqrt{7}}{2},$$

et on considère l'anneau $\mathbb{Z}[\alpha]$ (c'est-à-dire le sous-anneau de $\mathbb{C}$ engendré par α). On remarque que $\alpha + \overline{\alpha} = 1$ et $\alpha\overline{\alpha} = 2$, de sorte que α est racine du polynôme

$$X^2 - X + 2.$$

En d'autres termes on a $\alpha^2 = \alpha - 2$, ce qui montre que $\mathbb{Z}[\alpha]$ est l'ensemble des nombres complexes qui s'écrivent $a + b\alpha$ avec $a, b \in \mathbb{Z}$, ou de façon équivalente qui s'écrivent sous la forme $a + ib\sqrt{7}$ avec a et b soit tous deux dans $\mathbb{Z}$, soit tous deux dans $\mathbb{Z} + \frac{1}{2}$. Il n'est pas difficile de voir que σ préserve $\mathbb{Z}[\alpha]$, et que $N(x)$ appartient à $\mathbb{Z}$ si $x \in \mathbb{Z}[\alpha]$.

Remarque. Ici σ est l'unique élément non trivial du groupe de Galois de $\mathbb{Q}(i\sqrt{7})$ sur $\mathbb{Q}$ (qui est d'ordre 2, donc isomorphe à $\mathbb{Z}/2\mathbb{Z}$), et N est la "norme" au sens de la théorie de Galois. Mais il n'est pas nécessaire de le savoir pour la suite.

Proposition 1. L'anneau $\mathbb{Z}[\alpha]$ est euclidien pour le stathme N. En particulier, il est principal, et donc factoriel.

Démonstration. Remarquons que pour tout $x \in \mathbb{Q}(i\sqrt{7})$ il existe $x_0 \in \mathbb{Z}[\alpha]$ tel que $N(x - x_0) < 1$. En effet, écrivons $x = a + ib\sqrt{7}$ avec $a, b \in \mathbb{Q}$. Notons d un entier tel que $|d - 2b|$ est minimal (parmi tous les entiers d), et c un entier tel que $|a - \frac{d}{2} - c|$ est minimal. On a alors

$$N\left(x - (c + d\frac{1 + i\sqrt{7}}{2})\right) = N\left((a - c - \frac{d}{2}) + i\sqrt{7}(b - \frac{d}{2})\right)$$
$$= (a - c - \frac{d}{2})^2 + 7(b - \frac{d}{2})^2 \leq \frac{1}{4} + \frac{7}{16} < 1$$

puisque $b - \frac{d}{2} \leq \frac{1}{4}$ et $a - c - \frac{d}{2} \leq \frac{1}{2}$, de sorte que $x_0 = c + d\frac{1+i\sqrt{7}}{2}$ convient.

Si maintenant x, y sont dans $\mathbb{Z}[\alpha]$ avec $y \neq 0$, d'après le résultat démontré ci-dessus il existe $a \in \mathbb{Z}[\alpha]$ tel que $N(\frac{x}{y} - a) < 1$. On a alors $N(x - ay) < N(y)$, de sorte que $x = ay + (x - ay)$ est une division euclidienne de x par y dans $\mathbb{Z}[\alpha]$. □

La propriété de $\mathbb{Z}[\alpha]$ qui va être utilisée dans la suite est la factorialité. Pour pouvoir déterminer si un élément est irréductible, et contrôler la "non unicité" de la décomposition en produit d'irréductibles, il faut connaitre les éléments inversibles de $\mathbb{Z}[\alpha]$. Ceux-ci sont décrits dans le lemme suivant.

Lemme 1. (1) Les éléments inversibles de l'anneau $\mathbb{Z}[\alpha]$ sont 1 et -1.

(2) L'élément α est irréductible dans $\mathbb{Z}[\alpha]$.

(3) Une décomposition de 2 en produit de facteurs irréductibles dans $\mathbb{Z}[\alpha]$ est donnée par :

$$2 = \alpha \cdot \sigma(\alpha).$$

Démonstration. (1) Il est clair que 1 et -1 sont inversibles dans $\mathbb{Z}[\alpha]$. Réciproquement, si $x \in \mathbb{Z}[\alpha]$ est inversible alors on a $N(x)N(x^{-1}) = N(xx^{-1}) = 1$, ce qui montre que $N(x)$ est inversible dans $\mathbb{Z}$. Comme il est positif, on a donc $N(x) = 1$. Écrivons maintenant $x = a + ib\sqrt{7}$. Si $b \neq 0$, alors $b^2 \geq \frac{1}{4}$, ce qui implique que

$$N(x) \geq \frac{7}{4} > 1,$$

contredisant le fait que $N(x) = 1$. On a donc $b = 0$, puis $a^2 = 1$, et donc $a = \pm 1$.

(2) Supposons que $\alpha = z'z''$ avec z' et z'' dans $\mathbb{Z}[\alpha]$. Alors

$$2 = N(\alpha) = N(z')N(z'').$$

Comme 2 est premier, ceci implique que $N(z') = 1$ ou $N(z'') = 1$. D'après la preuve de (1) on en déduit que z' ou z'' est inversible.

(3) On a déjà observé que $2 = N(\alpha) = \alpha\sigma(\alpha)$. Comme α est irréductible et comme σ se restreint en un automorphisme d'anneau de $\mathbb{Z}[\alpha]$, $\sigma(\alpha)$ est également irréductible, et ceci est donc une décomposition de 2 en produit de facteurs irréductibles. □

5.2. **Résolution de l'équation $x^2 + 7 = 2^n$.** Notre but est maintenant de démontrer le résultat suivant.

Théorème 1. Les seules solutions $(x, n) \in \mathbb{Z}_{\geq 0} \times \mathbb{Z}_{\geq 0}$ de l'équation $x^2 + 7 = 2^n$ sont les paires suivantes :

$$(1, 3), \quad (3, 4), \quad (5, 5), \quad (11, 7), \quad (181, 15).$$

Remarque. Les solutions de l'équation avec $x < 0$ s'obtiennent à partir de celles considérées ci-dessus en remplaçant x par $-x$.

On commence par remarquer que la valeur $x = 0$ ne fournit pas de solution. Dans la suite on ne considérera donc que le cas $x > 0$.

Commençons par le cas facile où n est pair : on écrit alors $n = 2p$. Et si $x \in \mathbb{Z}_{>0}$ satisfait $x^2 + 7 = 2^n$, on a alors $7 = 2^{2p} - x^2$, et donc

$$7 = (2^p - x)(2^p + x).$$

Puisque 7 est premier et $2^p + x > 2^p - x$, ceci implique que $2^p + x = 7$ et $2^p - x = 1$, et donc $p = 2$ (c'est-à-dire $n = 4$) et $x = 3$.

Le cas n impair va être plus difficile, mais aussi plus intéressant. On suppose donc que n est impair, que $x^2 + 7 = 2^n$, et que $x > 0$. Le cas $n = 1$ est impossible, donc $n \geq 3$. Notre équation se réécrit donc

$$\frac{x^2 + 7}{4} = 2^{n-2},$$

c'est-à-dire

$$\frac{x + i\sqrt{7}}{2} \cdot \frac{x - i\sqrt{7}}{2} = \alpha^{n-2} \cdot \sigma(\alpha)^{n-2}. \tag{2}$$

Ici x est nécessairement impair (puisque $x^2 + 7$ est pair), et donc les deux facteurs à gauche appartiennent à $\mathbb{Z}[\alpha]$.

Lemme 2. Il existe $\varepsilon \in \{\pm 1\}$ tel que $\alpha^{n-2} - \sigma(\alpha)^{n-2} = \varepsilon i\sqrt{7}$.

Démonstration. L'élément α ne peut diviser à la fois $\frac{x+i\sqrt{7}}{2}$ et $\frac{x-i\sqrt{7}}{2}$, car sinon il diviserait $i\sqrt{7}$, ce qui est impossible puisque $N(\alpha)=2$ ne divise par $N(i\sqrt{7})=7$. De même, $\sigma(\alpha)$ ne peut diviser à la fois $\frac{x+i\sqrt{7}}{2}$ et $\frac{x-i\sqrt{7}}{2}$. Par "unicité" de l'écriture comme produit d'irréductibles appliquée à (2), on a donc soit

$$\frac{x+i\sqrt{7}}{2}=\pm\alpha^{n-2}, \quad \text{et} \quad \frac{x-i\sqrt{7}}{2}=\pm\sigma(\alpha)^{n-2},$$

soit

$$\frac{x+i\sqrt{7}}{2}=\pm\sigma(\alpha)^{n-2} \quad \text{et} \quad \frac{x-i\sqrt{7}}{2}=\pm\alpha^{n-2}.$$

Dans les 2 cas, en faisant la différence on obtient la condition cherchée. □

Lemme 3. Supposons que l'élément ε du Lemme 2 vaut 1. Alors $n=3$ et $x=1$.

Démonstration. Puisque $\alpha+\sigma(\alpha)=1$ on a

$$\alpha^2+2\alpha\sigma(\alpha)+\sigma(\alpha)^2=1,$$

et donc

$$\alpha^2+\alpha^2\sigma(\alpha)^2+\sigma(\alpha)^2=1.$$

Ceci montre que $\sigma(\alpha)^2$ divise α^2-1, et donc $\alpha^{n-2}-\alpha$ (puisque $n-2$ est impair). Si $n-2>1$, en remarquant que

$$\alpha^{n-2}-\sigma(\alpha)^{n-2}=i\sqrt{7}=\alpha-\sigma(\alpha)$$

on obtient que $\sigma(\alpha)^2$ divise $\sigma(\alpha)^{n-2}-\sigma(\alpha)$, et donc $\sigma(\alpha)$, ce qui est absurde. On a donc nécessairement $n=3$, puis $x=1$. □

On suppose maintenant que l'élément ε du Lemme 2 vaut -1, et donc que

$$\alpha^{n-2}-\sigma(\alpha)^{n-2}=-i\sqrt{7}.$$

Lemme 4. (1) On a $n-2\equiv -2^{n-3} \mod 7$.

(2) n est congru à 5, 7 ou 15 modulo 21. [8]

Démonstration. (1) D'après la formule du binôme de Newton on a

$$\begin{aligned}\alpha^{n-2}-\sigma(\alpha)^{n-2} &= \left(\frac{1+i\sqrt{7}}{2}\right)^{n-2}-\left(\frac{1-i\sqrt{7}}{2}\right)^{n-2}\\ &= \frac{1}{2^{n-2}}\sum_{k=0}^{n-2}\binom{n-2}{k}\cdot\left((i\sqrt{7})^k-(-i\sqrt{7})^k\right)\\ &= \frac{i\sqrt{7}}{2^{n-3}}\sum_{\substack{p\in\mathbb{Z}\\ 0\le 2p+1\le n-2}}\binom{n-2}{2p+1}\cdot(-7)^p.\end{aligned}$$

On obtient donc que

$$-2^{n-3}=\sum_{\substack{p\in\mathbb{Z}\\ 0\le 2p+1\le n-2}}\binom{n-2}{2p+1}\cdot(-7)^p,$$

et finalement que $n-2\equiv -2^{n-3} \mod 7$.

8. Dans [FG] il est montré que ces congruences ont même lieu modulo 42. L'argument n'est pas difficile, mais cela n'est pas utile pour la suite de la démonstration.

(2) Puisque $2^3 \equiv 1 \mod 7$, les puissances de 2 modulo 7 sont données par :

$$2^{3k} \equiv 1 \mod 7, \quad 2^{3k+1} \equiv 2 \mod 7, \quad 2^{3k+2} \equiv 4 \mod 7$$

pour tout $k \in \mathbb{Z}_{\geq 0}$.

Si $n = 3k+2$ avec $k \in \mathbb{Z}_{>0}$, en utilisant (1) on a alors $3k \equiv 3 \mod 7$, donc $k \equiv 1 \mod 7$, puis $n \equiv 5 \mod 21$. De même, si $n = 3k$ avec $k \in \mathbb{Z}_{>0}$, on a $3k-2 \equiv 6 \mod 7$, donc $3k \equiv 1 \mod 7$, puis $k \equiv 5 \mod 7$, puis $n \equiv 15 \mod 21$. Enfin, si $n = 3k+1$ avec $k \in \mathbb{Z}_{>0}$, on a $3k-1 \equiv 5 \mod 7$, donc $3k \equiv 6 \mod 7$, puis $k \equiv 2 \mod 7$, puis $n \equiv 7 \mod 21$. □

La preuve du lemme suivante est fastidieuse, et expliquée au paragraphe suivant.

Lemme 5. Si m et m' sont deux entiers positifs congrus modulo 21 et tels que

$$\alpha^m - \sigma(\alpha)^m = \alpha^{m'} - \sigma(\alpha)^{m'},$$

alors $m = m'$.

On peut finalement conclure la preuve.

Preuve du théorème 1. On a déjà vu que les paires $(1,3)$ et $(3,4)$ sont solutions, et que si (x,n) est une autre paire solution alors n est impair, supérieur ou égal à 3, et qu'on a

$$\alpha^{n-2} - \sigma(\alpha)^{n-2} = -i\sqrt{7}.$$

D'après le Lemme 4, n est alors congru soit à 5, soit à 7, soit à 15 modulo 21, et d'après le Lemme 5 il existe au plus une solution pour chacune de ces possibilités. En observant que

$$5^2 + 7 = 2^5, \quad 11^2 + 7 = 2^7 \quad \text{et} \quad 181^2 + 7 = 2^{15},$$

ceci conclut la preuve. □

5.3. **Preuve du lemme restant.** On commence par un (autre) lemme.

Lemme 6. Pour tout $k \geq 0$:

(1) 7^{k+1} divise

$$(1 + i\sqrt{7})^{7^k} - (1 + i7^k\sqrt{7})$$

dans $\mathbb{Z}[\alpha]$;

(2) si $a \in \mathbb{Z}$ vérifie $a \equiv 1 \mod 7$, alors $a^{7^k} \equiv 1 \mod 7^{k+1}$ (dans $\mathbb{Z}$).

Démonstration. Les deux preuves s'obtiennent par récurrence sur k. Le deuxième cas est similaire au premier ; on ne traitera donc que celui-ci. Pour $k = 0$ il n'y a rien à démontrer. Si l'énoncé est connu pour $k \geq 0$, on écrit

$$(1 + i\sqrt{7})^{7^k} = (1 + i7^k\sqrt{7}) + 7^{k+1}c$$

avec $c \in \mathbb{Z}[\frac{1+i\sqrt{7}}{2}]$, et on remarque que

$$(1 + i\sqrt{7})^{7^{k+1}} = \left((1 + i\sqrt{7})^{7^k}\right)^7 = (1 + i7^k\sqrt{7} + 7^{k+1}c)^7.$$

En utilisant la formule du binôme de Newton on obtient que

$$(1 + i\sqrt{7})^{7^{k+1}} = 1 + i7^{k+1}\sqrt{7} + 7^{k+2}c + \sum_{j=2}^{7} \binom{7}{j} (i7^k\sqrt{7} + 7^{k+1}c)^j.$$

Ici dans les termes de droite, si $j < 7$ le coefficient binomial est divisible par 7, de sorte que le terme est divisible par 7 à la puissance

$$j(k+\frac{1}{2})+1 \geq k+2.$$

Pour $j = 7$ le terme est divisible par 7 à la puissance

$$7(k+\frac{1}{2}) \geq k+2.$$

On obtient donc bien le résultat au rang $k+1$. □

Preuve du Lemme 5. Par l'absurde on suppose que $m \neq m'$. Quitte à échanger m et m', on peut alors supposer que $m < m'$. On note k le plus grand entier tel que 7^k divise $m'-m$ (dans $\mathbb{Z}$), et par

$$\pi : \mathbb{Z}[\alpha] \to \mathbb{Z}[\alpha]/7^{k+1} \cdot \mathbb{Z}[\alpha]$$

le morphisme (d'anneaux) quotient. Notre hypothèse implique que $k \geq 1$. Avec cette notation le Lemme 6(1) affirme que

$$\pi((1+i\sqrt{7})^{7^k}) = \pi((1+i7^k\sqrt{7})). \tag{3}$$

Notons également que l'idéal $7^{k+1} \cdot \mathbb{Z}[\alpha]$ est stable par l'action de l'automorphisme σ, de sorte qu'il induit un automorphisme du quotient $\mathbb{Z}[\alpha]/7^{k+1} \cdot \mathbb{Z}[\alpha]$, qu'on notera $\overline{\sigma}$. (Ici, "induit" signifie que $\pi \circ \sigma = \overline{\sigma} \circ \pi$.)

On a

$$(1+i\sqrt{7})^{m'-m} = ((1+i\sqrt{7})^{7^k})^{\frac{m'-m}{7^k}},$$

de sorte que d'après (3)

$$\pi((1+i\sqrt{7})^{m'-m}) = \pi(1+i7^k\sqrt{7})^{\frac{m'-m}{7^k}},$$

et donc

$$\pi((1+i\sqrt{7})^{m'-m}) = \pi(1+i(m'-m)\sqrt{7})$$

en utilisant la formule du binôme de Newton (et le fait que $k \geq 1$).

On remarque ensuite que

$$2^{m'}\alpha^{m'} = 2^m\alpha^m(1+i\sqrt{7})^{m'-m},$$

de sorte que

$$\pi(2^{m'}\alpha^{m'}) = \pi(2^m\alpha^m \cdot (1+i(m'-m)\sqrt{7})).$$

Or 7 divise $2^m\alpha^m - (1+im\sqrt{7}) = (2\alpha)^m - (1+im\sqrt{7})$ dans $\mathbb{Z}[\alpha]$ d'après la formule du binôme de Newton, et 7^k divise $(m'-m)$ par définition de k, donc

$$\pi(2^m\alpha^m(m'-m)i\sqrt{7}) = \pi((m'-m)i\sqrt{7}),$$

ce qui implique que

$$\pi(2^{m'}\alpha^{m'}) = \pi(2^m\alpha^m + (m'-m)i\sqrt{7}).$$

En appliquant $\overline{\sigma}$ puis en faisant la différence on en déduit que

$$\pi\big(2^{m'}(\alpha^{m'} - \sigma(\alpha)^{m'})\big) = \pi\big(2^m(\alpha^m - \sigma(\alpha)^m) + 2(m'-m)i\sqrt{7}\big).$$

Ici, par hypothèse on a

$$\alpha^{m'} - \sigma(\alpha)^{m'} = \alpha^m - \sigma(\alpha)^m,$$

et d'après le Lemme 6(2) l'entier $2^{m'-m} = 8^{\frac{m'-m}{3}}$ est congru à 1 modulo 7^{k+1}, d'où $2^{m'} \equiv 2^m \mod 7^{k+1}$. On a donc

$$\pi\big(2^{m'}(\alpha^{m'} - \sigma(\alpha)^{m'})\big) = \pi\big(2^m(\alpha^m - \sigma(\alpha)^m)\big),$$

et finalement

$$\pi(2(m'-m)i\sqrt{7}) = 0.$$

Ceci implique que

$$\frac{2(m'-m)}{7^{k+1}} i\sqrt{7} \in \mathbb{Z}[\alpha],$$

ce qui n'est possible que si 7^{k+1} divise $m' - m$, ce qui contredit la définition de k. □

5.4. **Quelques remarques complémentaires.** Les corps de la forme $\mathbb{Q}(i\sqrt{d})$ avec d entier positif sans facteur carré sont les *corps quadratiques imaginaires*, c'est-à-dire les extensions de degré 2 de $\mathbb{Q}$ non contenues dans $\mathbb{R}$. Certaines de leurs propriétés sont étudiées dans [FG, p. 166–170]. En particulier on peut décrire leur *anneau des entiers*, c'est-à-dire l'anneau formé des éléments de $\mathbb{Q}(i\sqrt{d})$ qui sont entiers sur $\mathbb{Z}$. La réponse est $\mathbb{Z}[\frac{1+i\sqrt{d}}{2}]$ si $d \equiv -1 \mod 4$ (comme le cas $d = 7$ considéré ci-dessus), et $\mathbb{Z}[i\sqrt{d}]$ sinon.

Les propriétés de ces anneaux jouent un rôle crucial dans la résolution des équations diophantiennes faisant intervenir un carré. Mais de façon plus élémentaire, il peuvent également servir à donner des exemples ou des contre-exemples pour les propriétés classiques des anneaux. Il est par exemple montré dans [Pe] que $\mathbb{Z}[\frac{1+i\sqrt{19}}{2}]$ est principal mais non euclidien.

On a vu ci-dessus que $\mathbb{Z}[\frac{1+i\sqrt{7}}{2}]$ est un anneau euclidien. La même preuve montre que c'est également le cas pour l'anneau des entiers quand d vaut 1, 2, 3, 7 ou 11. Ces valeurs sont en fait les seules pour lesquelles cette propriété est vérifiée. Cet énoncé est beaucoup plus difficile à démontrer, mais on peut le voir sur des exemples. Par exemple, le cas $d = 19$ est expliqué ci-dessus. Pour un autre exemple, on peut voir que l'anneau $\mathbb{Z}[i\sqrt{5}]$ n'est pas factoriel : on a

$$6 = 2 \cdot 3 = (1 + i\sqrt{5}) \cdot (1 - i\sqrt{5}),$$

et on peut vérifier (en utilisant la norme, définie ici par $N(a + ib\sqrt{5}) = a^2 + 5b^2$) que 2, 3, $1 + i\sqrt{5}$ et $1 - i\sqrt{5}$ sont irréductibles. Il n'y a donc pas unicité de la décomposition en facteurs irréductibles dans cet anneau.

Références

[CG] P. Caldero, J. Germoni, *Histoires hédonistes de groupes et de géométries, Tome II*, Calvage & Mounet, 2015.

[FG] S. Francinou, H. Gianella, *Exercices de mathématiques pour l'agrégation – Algèbre 1*, Masson, 1994.

[FGN] S. Francinou, H. Gianella, S. Nicolas, *Oraux X-ENS, algèbre 1, troisième édition*, Cassini, 2014.

[Go] X. Gourdon, *Les maths en tête - Algèbre*, 2ème édition, Ellipses, 2009.

[Pe] D. Perrin, *Cours d'algèbre*, Ellipses, 1996.