Anneaux Z[w]. Anneaux intègres et factoriels

Première partie : les anneaux $\mathbb{Z}[\omega]$

Dans cette partie, α est un entier relatif qui n'est le carré d'aucun élément de $\mathbb{Z}$.

– Si $\alpha > 0$, on pose $\omega = \sqrt{\alpha}$ (c'est un réel strictement positif et irrationnel.)
– Si $\alpha < 0$, on pose $\omega = i\sqrt{-\alpha}$ (c'est un nombre complexe non réel, d'argument $\frac{\pi}{2}$.)

On a donc $\omega^2 = \alpha$.

On pose $\mathbb{Q}[\omega] = \{a + b\omega, (a, b) \in \mathbb{Q}^2\}$. Ainsi $\begin{cases} \text{Si } \alpha = -1, & \mathbb{Q}[i] = \{a + bi,\ (a, b) \in \mathbb{Q}^2\}. \\ \text{Si } \alpha = 2, & \mathbb{Q}[\sqrt{2}] = \{a + b\sqrt{2},\ (a, b) \in \mathbb{Q}^2\}. \\ \text{Si } \alpha = -2, & \mathbb{Q}[i\sqrt{2}] = \{a + ib\sqrt{2},\ (a, b) \in \mathbb{Q}^2\}. \end{cases}$

1. (a) Soit $z = a + b\omega$ dans $\mathbb{Q}[\omega]$ avec $(a, b) \in \mathbb{Q}^2$.
   Montrer que l'écriture de z sous cette forme est unique.
   On pose alors $N(z) = (a + b\omega)(a - b\omega) = a^2 - \alpha b^2$, qui est élément de $\mathbb{Q}$.
   Montrer que $N(z) = 0 \Leftrightarrow z = 0$. [S]

   (b) Montrer que $\mathbb{Q}[\omega]$ est muni d'une structure de corps. [S]

2. (a) Soit $z = a + b\omega$ dans $\mathbb{Q}[\omega]$ avec $(a, b) \in \mathbb{Q}^2$. On pose $z^\star = a - b\omega$.
   Montrer que $z \mapsto z^\star$ est un automorphisme du corps $\mathbb{Q}[\omega]$. [S]

   (b) Soient z, z' dans $\mathbb{Q}[\omega]$. Montrer que $N(zz') = N(z)N(z')$. [S]

3. On pose $\mathbb{Z}[\omega] = \{a + b\omega, (a, b) \in \mathbb{Z}^2\}$. L'ensemble $\mathbb{Z}[\omega]$ est donc une partie de $\mathbb{Q}[\omega]$.
   Pour tout $z = a + b\omega$ de $\mathbb{Z}[\omega]$, avec $(a, b) \in \mathbb{Z}^2$, on a donc $\begin{cases} z^\star = a - b\omega \in \mathbb{Z}[\omega] \\ N(z) = zz^\star = a^2 - \alpha b^2 \in \mathbb{Z} \end{cases}$

   (a) Montrer que $\mathbb{Z}[\omega]$ est un anneau intègre. [S]

   (b) Montrer que z est inversible dans $\mathbb{Z}[\omega]$ si et seulement si $N(z) = \varepsilon$ avec $\varepsilon = \pm 1$.
   Montrer qu'alors l'inverse de z dans $\mathbb{Z}[\omega]$ est $z^{-1} = \varepsilon z^\star$. [S]

4. Montrer que les éléments inversibles de l'anneau $\mathbb{Z}[i]$ sont 1, i, -1 et i.
   Quels sont ceux de $\mathbb{Z}[i\sqrt{m}]$ si $m \geq 2$ (m entier non carré bien sûr) ? [S]

5. Dans cette question, on cherche les éléments inversibles de l'anneau $\mathbb{Z}[\sqrt{2}]$.

   (a) Soit ε dans $\{-1, 1\}$ et m dans $\mathbb{Z}$. On pose $z = \varepsilon(1 + \sqrt{2})^m$.
   Montrer que z est un élément inversible de $\mathbb{Z}[\sqrt{2}]$, et que $z^{-1} = \varepsilon(-1 + \sqrt{2})^m$. [S]

   (b) Réciproquement, Soit $z = a + b\sqrt{2}$ un élément inversible de $\mathbb{Z}[\sqrt{2}]$.
   Dans un premier temps, on suppose $a \in \mathbb{N}^*$ et $b \in \mathbb{N}$.

      i. Vérifier que si $b = 0$, alors $z = 1$. [S]

Tous droits de l'auteur des œuvres réservés. Sauf autorisation, la reproduction ainsi que toute utilisation des œuvres autre que la consultation individuelle et privée sont interdites.

Extrait gratuit de document, le document original comporte 14 pages.

ii. Si $b > 0$, montrer qu'on a les inégalités $0 < b \leq a < 2b$. [S]

iii. Toujours si $b > 0$, on définit $z_1 = a_1 + b_1\sqrt{2}$ par $z_1 = (\sqrt{2} - 1)z$.
Montrer que z_1 est inversible dans $\mathbb{Z}[\sqrt{2}]$ et que $0 < a_1 \leq a$ et $0 \leq b_1 < b$. [S]

iv. En déduire qu'il existe un entier naturel n tel que $z = (1 + \sqrt{2})^n$.
(On pourra imaginer de construire $z_2 = (\sqrt{2} - 1)z_1$ si $b_1 > 0$, etc.) [S]

(c) Montrer z est inversible dans $\mathbb{Z}[\sqrt{2}] \;\Leftrightarrow\; z = \varepsilon(1 + \sqrt{2})^m$, avec $\begin{cases} \varepsilon = \pm 1 \\ m \in \mathbb{Z} \end{cases}$ [S]

Dans toute la suite de ce problème :

– A est un anneau intègre (donc commutatif). Ses lois sont notées $(a, b) \mapsto a + b$ et $(a, b) \mapsto ab$.
On note 0 le neutre additif et 1 le neutre multiplicatif de A.

– On note A' le groupe multiplicatif des éléments de A qui sont inversibles pour le produit.
Les éléments de A' seront appelés *unités* de A. L'inverse d'une unité a sera noté a^{-1}.

Deuxième partie : divisibilité dans un anneau intègre

Soient a, b deux éléments quelconques de l'anneau A.
On dit que a *divise* b, et on note $a \mid b$, s'il existe q dans A tel que $b = aq$.
Une telle relation est bien sûr réflexive et transitive.
Quand a divise b, on dit aussi que b est un *multiple* de a, ou que a est un *diviseur* de b.
On note $\mathcal{D}(a)$ l'ensemble des diviseurs de a, et $aA = \{ax, x \in A\}$ l'ensemble de ses multiples.
Pour tous a, b de A, on a : $\quad a \mid b \;\Leftrightarrow\; b \in aA \;\Leftrightarrow\; a \in \mathcal{D}(b) \;\Leftrightarrow\; \mathcal{D}(a) \subset \mathcal{D}(b) \;\Leftrightarrow\; bA \subset aA$.

1. Soient a, b deux éléments de A. On suppose que a est non nul et qu'il divise b.
Montrer qu'il existe un *unique* élément q de A tel que $b = aq$.
On peut donc parler de l'unicité du quotient exact de b par a. [S]

2. Identifier les ensembles $0A$, $1A$, $\mathcal{D}(0)$ et $\mathcal{D}(1)$. [S]

3. On dit que deux éléments a, b de A sont *associés* si : $\exists u \in A',\ b = au$.
Montrer qu'on définit ainsi une relation d'équivalence sur A.
On notera $\widetilde{a} = \{ax, x \in A'\}$ la classe de a, donc l'ensemble des associés de a. [S]

Bien entendu, on a les égalités $\widetilde{0} = \{0\}$ et $\widetilde{1} = A'$.
Par exemple, si $A = \mathbb{Z}$, on a $A' = \{-1, 1\}$ et $\widetilde{a} = \{-a, a\}$ pour tout a.

4. Pour tous a, b de A, montrer l'équivalence : $(a \mid b \text{ et } b \mid a) \;\Leftrightarrow\; b \in \widetilde{a}$.
Ainsi on a : $\quad (a \mid b \text{ et } b \mid a) \;\Leftrightarrow\; \mathcal{D}(a) = \mathcal{D}(b) \;\Leftrightarrow\; aA = bA \;\Leftrightarrow\; b \in \widetilde{a}$. [S]

5. Pour tout a de A, montrer que $A' \cup \widetilde{a}$ est inclus dans $\mathcal{D}(a)$.
Ainsi tout élément de A est divisible par ses associés et par les unités de A. [S]

6. On reprend les notations de la partie I, et on se place dans l'anneau $\mathbb{Z}[\omega]$.

Tous droits de l'auteur des œuvres réservés. Sauf autorisation, la reproduction ainsi que toute utilisation des œuvres autre que la consultation individuelle et privée sont interdites.

Extrait gratuit de document, le document original comporte 14 pages.

(a) Soient z, z' deux éléments de $\mathbb{Z}[\omega]$. On suppose que z' divise z dans $\mathbb{Z}[\omega]$.
Montrer qu'alors l'entier $N(z')$ divise l'entier $N(z)$ dans $\mathbb{Z}$.
Prouver que si de plus $|N(z')| = |N(z)|$ alors z et z' sont associés. [S]

(b) Trouver les 16 diviseurs de $4 + 7i$ dans $\mathbb{Z}[i]$. [S]

Troisième partie : pgcd, ppcm dans un anneau intègre

Soient a et b deux éléments de l'anneau intègre A.

– On dit que a et b ont un *pgcd* s'il existe d dans A tel que $\mathcal{D}(a) \cap \mathcal{D}(b) = \mathcal{D}(d)$.
Cela équivaut à dire qu'il existe un élément d tel que : $(x \mid a \text{ et } x \mid b) \;\Leftrightarrow\; x \mid d$.
D'après II.3, on a alors $\mathcal{D}(a) \cap \mathcal{D}(b) = \mathcal{D}(d') \;\Leftrightarrow\; d' \in \widetilde{d}$.
On dira alors que chaque d' de $\widetilde{d}$ est *un* pgcd de a et b, et on pourra noter $\text{pgcd}(a, b) = d'$.
Il est clair qu'un pgcd de a et b est en particulier un diviseur commun de a et b.

– On dit que a et b de A sont *étrangers* si $\mathcal{D}(a) \cap \mathcal{D}(b) = A'$.
Cela signifie que les seuls diviseurs communs de a et b sont les unités de A.
Puisque $A' = \widetilde{1}$, cela équivaut à dire que 1 est un pgcd de a et b.

– On dit que a et b ont un *ppcm* s'il existe m dans A tel que $aA \cap bA = mA$.
Cela équivaut à dire qu'il existe un élément m tel que : $(a \mid x \text{ et } b \mid x) \;\Leftrightarrow\; m \mid x$.
D'après II.3, on a alors $aA \cap bA = m'A \;\Leftrightarrow\; m' \in \widetilde{m}$.
On dira alors que chaque m' de $\widetilde{m}$ est *un* ppcm de a et b, et on pourra noter $\text{ppcm}(a, b) = m'$.
Il est clair que si $\text{ppcm}(a, b) = m$, alors $a \mid m$, $b \mid m$ et $m \mid ab$.

– On notera que dans le cas général, deux éléments a, b de l'anneau intègre A peuvent fort bien ne pas posséder de pgcd et/ou ne pas posséder de ppcm. Quand on écrira $\text{pgcd}(a, b) = d$, par exemple, cela signifiera donc "a et b possèdent un pgcd, et d est l'un d'eux".
On a bien sûr les égalités $\text{pgcd}(a, b) = \text{pgcd}(b, a)$ et $\text{ppcm}(a, b) = \text{ppcm}(b, a)$.

1. (a) Vérifier que pour tout a de A, on a $\text{pgcd}(a, 0) = a$ et $\text{ppcm}(a, 0) = 0$. [S]

   (b) Plus généralement, montrer que $\begin{cases} \text{pgcd}(a, b) = 0 \Leftrightarrow a = b = 0 \\ \text{ppcm}(a, b) = 0 \Leftrightarrow (a = 0 \text{ ou } b = 0) \end{cases}$ [S]

   (c) Montrer les équivalences : $\text{pgcd}(a, b) = a \;\Leftrightarrow\; \text{ppcm}(a, b) = b \;\Leftrightarrow\; a \mid b$. [S]

2. Soient a et b deux éléments non nuls de A, possédant un ppcm m.
En particulier m est non nul et il existe un élément d de A tel que $ab = md$.
Montrer alors que l'élément d est un pgcd de a et b. [S]

3. Soient a, b deux éléments non nuls de A. On considère les propriétés :

$$\mathcal{P}_1 : \text{pgcd}(a, b) = 1 \qquad \mathcal{P}_2 : \forall x \in A,\ a \mid bx \Rightarrow a \mid x$$
$$\mathcal{P}_3 : \text{ppcm}(a, b) = ab \qquad \mathcal{P}_4 : \exists (u, v) \in A^2,\ au + bv = 1$$

Montrer les résultats suivants :

Tous droits de l'auteur des œuvres réservés. Sauf autorisation, la reproduction ainsi que toute utilisation des œuvres autre que la consultation individuelle et privée sont interdites.

Extrait gratuit de document, le document original comporte 14 pages.

(a) La propriété $\mathcal{P}_4$ implique la propriété $\mathcal{P}_3$. [S]

(b) La propriété $\mathcal{P}_3$ implique la propriété $\mathcal{P}_2$. [S]

(c) La propriété $\mathcal{P}_2$ implique la propriété $\mathcal{P}_3$. [S]

(d) La propriété $\mathcal{P}_3$ implique la propriété $\mathcal{P}_1$. [S]

En conclusion : $\mathcal{P}_4 \Rightarrow \mathcal{P}_3$, $\mathcal{P}_3 \Leftrightarrow \mathcal{P}_2$ et $\mathcal{P}_2 \Rightarrow P_1$.

– On exprime $\mathcal{P}_4$ en disant que a et b satisfont à une *identité de Bezout*.

– On exprime $\mathcal{P}_2$ en disant que a et b satisfont à la *propriété de Gauss*.

– L'équivalence $\mathcal{P}_2 \Leftrightarrow \mathcal{P}_3$ montre que $\mathcal{P}_2$ est symétrique par rapport à a et b.

Quatrième partie : éléments irréductibles ou premiers

Soit p un élément non nul et non inversible de l'anneau intègre A.

– On dit que p est *irréductible* si $\mathcal{D}(p)$ se réduit à $A' \cup \widetilde{p}$.
Autrement dit, p est irréductible si ses seuls diviseurs sont ses associés et les unités de A.

– Un élément p non inversible de A est dit *premier* si : $\forall (a,b) \in A^2,\ p \mid ab \Rightarrow (p \mid a \text{ ou } p \mid b)$.

NB : 0 et les unités de A ne sont pas considérés comme irréductibles ou premiers.

Il est clair que dans l'anneau $\mathbb{Z}$, un élément p est irréductible si et seulement si il est premier, et plus précisément si et seulement si l'entier $|p|$ est premier (au sens usuel) dans $\mathbb{N}$.

Il est immédiat que si p est irréductible (resp. premier) et si p' est associé à p, alors p' est irréductible (resp. premier). Autrement dit les notions d'élément irréductible ou premier sont invariantes par association (c'est-à-dire par produit par un élément inversible.)

1. Montrer que si p est premier dans A, alors p est irréductible. [S]

2. On va montrer que la réciproque de la propriété précédente est fausse.
Pour cela on se place dans l'anneau $\mathbb{Z}[i\sqrt{5}]$.
   (a) Montrer que 2 est irréductible dans $\mathbb{Z}[i\sqrt{5}]$ (utiliser II-5-a) [S]
   (b) Montrer que 2 n'est pas premier dans l'anneau $\mathbb{Z}[i\sqrt{5}]$.
   Pour cela on observera que 2 ne divise ni $1 - i\sqrt{5}$ ni $1 + i\sqrt{5}$. [S]

3. On se place dans l'anneau $\mathbb{Z}[\omega]$, au sens de la partie I. Soit z un élément de cet anneau.
   (a) On suppose que l'entier $N(z)$ est premier dans l'anneau $\mathbb{Z}$.
   (Cela signifie donc que $|N(z)|$ est un entier naturel premier au sens usuel.)
   Montrer que z est un élément irréductible de $\mathbb{Z}[\omega]$. [S]
   (b) En utilisant la question IV-2, montrer que la réciproque est fausse. [S]

4. (a) On se place à nouveau dans $\mathbb{Z}[\omega]$. Soit z un élément non nul et non inversible.
   Montrer que z s'écrit au moins d'une façon comme un produit d'éléments irréductibles.
   Indication : raisonner par récurrence sur la valeur de $|N(z)|$. [S]

Tous droits de l'auteur des œuvres réservés. Sauf autorisation, la reproduction ainsi que toute utilisation des œuvres autre que la consultation individuelle et privée sont interdites.

Extrait gratuit de document, le document original comporte 14 pages.

(b) On se place plus particulièrement dans $\mathbb{Z}[i]$, et on considère $z = 19 + 61i$.
On remarque que $N(z) = 19^2 + 61^2 = 4082 = 2 \cdot 13 \cdot 157$.
Trouver une factorisation de z en produit d'éléments irréductibles. [S]

5. Soient a, p, p' deux éléments de A. On suppose que p et p' sont irréductibles.
   (a) Montrer que si p ne divise pas a, alors p et a sont étrangers. [S]
   (b) Montrer que si p et p' ne sont pas associés, alors ils sont étrangers. [S]

Cinquième partie : anneaux factoriels

Soit A un anneau intègre. On dit que A est *factoriel* si tout élément non nul et non inversible s'écrit de manière *essentiellement unique* comme un un produit d'éléments irréductibles.

Cette *unicité essentielle* doit être comprise à l'ordre près et à l'association près des facteurs.

De façon plus précise, soit z un élément non nul et non inversible de A.

Supposons $\begin{cases} z = p_1 p_2 \cdots p_n \\ z = q_1 q_2 \cdots q_m \end{cases}$ avec $n \geq 1$, $m \geq 1$, les p_k et les q_k étant irréductibles.

Alors $m = n$, et il existe une permutation σ de $\{1, \ldots, n\}$ telle que : $\forall k \in \{1, \ldots, n\},\ q_k \in \widetilde{p}_k$.

Il est clair que l'anneau $\mathbb{Z}$ est factoriel. On sait que dans $\mathbb{Z}$ on a $\widetilde{z} = \{z, -z\}$ pour tout z.

Dans $\mathbb{Z}$, l'entier $z = 30$ peut par exemple s'écrire : $z = 2 \cdot 3 \cdot 5 = (-5) \cdot (-3) \cdot 2$.

1. Soit A un anneau factoriel, et p un élément irréductible de A.
   Montrer que p est premier dans A (c'est donc une réciproque de la question IV-1.)
   Ainsi, dans un anneau factoriel : "z est irréductible" équivaut à "z est premier".
   Remarque : la question IV-2 montre que l'anneau $\mathbb{Z}[i\sqrt{5}]$ n'est pas factoriel. [S]
2. On reprend ici les notations de la question III-3.
   Montrer que dans un anneau factoriel A, la propriété $\mathcal{P}_1$ implique la propriété $\mathcal{P}_2$.
   Le th. de Gauss $\begin{cases} \text{pgcd}(a, b) = 1 \\ a \mid bc \end{cases} \Rightarrow a \mid c$ est donc vrai dans un anneau factoriel. [S]

Soit A un anneau factoriel.

Dans toute décomposition en facteurs irréductibles, on peut grouper les facteurs associés.

Tout élément $a \neq 0$ et non inversible de A s'écrit alors $a = u p_1^{k_1} p_2^{k_2} \cdots p_n^{k_n}$ où :

– L'élément u est inversible.

– Les éléments $p_1, p_2, \ldots, p_n$ sont irréductibles et deux à deux non associés.

– Les entiers $k_1, k_2, \ldots, k_n$ sont strictement positifs.

Une telle écriture est là encore *essentiellement unique*.

Si on accepte que les exposants soient seulement positifs ou nuls, on peut utiliser cette écriture pour tout élément inversible de A, ou pour "synchroniser" (c'est-à-dire utiliser les mêmes p_k) les décompositions de deux éléments a et b de A. On va voir que dans un anneau factoriel, deux éléments quelconques ont toujours un pgcd et un ppcm. Compte tenu du résultat de la question III-1-a, on peut se limiter au cas où ces deux éléments sont non nuls.

Tous droits de l'auteur des œuvres réservés. Sauf autorisation, la reproduction ainsi que toute utilisation des œuvres autre que la consultation individuelle et privée sont interdites.

Extrait gratuit de document, le document original comporte 14 pages.