Licence de Mathématiques

Mémoire EM45
Anneaux euclidiens, principaux, factoriels et applications

Théo Deturck, Louis Loiseau

Janvier › Mars 2020

Table des matières

1 Définitions et résultats préliminaires

1.1 Structure d'anneau

Définition 1 (Anneau)

Un anneau est un triplet $(A, +, \cdot)$ qui satisfait les conditions suivantes :

1. $(A, +)$ est un groupe abélien de neutre 0. L'opération $+$ est appellée addition.
2. L'opération $\cdot$ est appellée multiplication. Elle est associative et de neutre 1.
3. La multiplication est distributive par rapport à l'addition.

Un anneau dont l'opération de multiplication est commutative est appelée un anneau commutatif.

Par abus de notation, nous noterons parfois seulement A pour $(A, +, \cdot)$ lorsqu'il n'y a pas de confusion possible. Sauf mention du contraire, tout les anneaux dans ce document seront considérés comme commutatifs.
L'ensemble $\mathbb{Z}$ muni des opérations d'addition et de multiplication usuelles forme un anneau commutatif.

Définition 2 (Anneau intègre)

Soit A un anneau commutatif non trivial. A est dit intègre s'il vérifie les trois propriétés équivalentes suviantes :

1. A ne possède pas de diviseur de 0 (autrement dit, le produit de deux éléments non nul de A est non nul).
2. La règle du produit nul s'applique dans A :

$$\forall a, b \in A,\ ab = 0 \implies (a = 0 \ ou \ b = 0)$$

3. Si $a, b, c \in A$ avec $a \neq 0$, alors $ab = ac \implies b = c$

Tout corps commutatif est un anneau intègre. $\mathbb{Z}/6\mathbb{Z}$ n'est pas intègre.

1.2 Idéaux d'un anneau

Définition 3 (Idéal dans un anneau)

Soit A un anneau. Un ensemble $I \subset A$ est appelé idéal à gauche (resp. idéal à droite) si :

1. I est un sous-groupe additif.
2. Pour tout a de A et pour tout x de I, on a $a \cdot x \in I$. (resp. $x \cdot a \in I$).

Lorsque I est un idéal à gauche et à droite, on dit que c'est un idéal bilatère. Dans ce qui suit, lorsque nous parlerons d'idéal d'un anneau sans précision, nous parlerons d'idéal bilatère.
Nous donnerons une caractérisation des idéaux un peu plus loin dans cette partie.

Proposition 1 (Idéal dans un anneau commutatif)

Dans un anneau commutatif, tout idéal est bilatère (c'est-à-dire tout idéal à droite et un idéal à gauche et vice-versa).

Démonstration. Soit A un anneau commutatif.
Pour tout sous-ensemble I de A, pour tout a et pour tout $x \in I, x \cdot a \in I \Leftrightarrow a \cdot x \in I$ par commutativité.
En particulier :

I est un idéal à droite
$\Leftrightarrow$ I est un sous-groupe additif et : $\forall a \in A, \forall x \in I, xa \in I$
$\Leftrightarrow$ I est un sous-groupe additif et : $\forall a \in A, \forall x \in I, ax \in I$
$\Leftrightarrow$ I est un idéal à gauche

□

Proposition 2 (Intersection d'idéaux)

Soit A un anneau, alors pour tout famille $(I_k)_{k\in E}$ non vide d'idéaux à gauche de A, $\bigcap_{k\in E} I_k$ est un idéal à gauche de A.

Démonstration. Posons $I = \bigcap_{k\in E} I_k$.

1. I est un sous-groupe additif de A.
   Pour tout $k \in I, 0 \in I_k$, donc $0 \in I$.
   Soient $x, y \in I$, alors, pour tout $k \in I, x, y \in I_k$, donc $x + y \in I_k$.
   On en déduit que $x + y \in I$.
   De plus, pour tout $k \in I, -x \in I_k$, donc $-x \in I$.
   I est donc un sous-groupe additif de A.
2. Pour tout $a \in A$ et pour tout $x \in I$, on a $ax \in I$.
   Soient $a \in A$ et $x \in I$, alors pour tout $k \in E, x \in I_k$ donc $ax \in I_k$.
   On en déduit que $ax \in I$.
   Donc I est un idéal à gauche de A.

□

Proposition 3 (Plus petit idéaux contenant une partie)

Soit A un anneau commutatif et P une partie de A, alors il existe un plus petit idéal I de A contenant P, qui est l'intersection des idéaux de A contenant P.

Démonstration. D'après la proposition précédente, l'intersection des idéaux de A contenant P est un idéal de A, et il est évidemment inclus dans tout idéal de A contenant P. □

Définition 4 (Idéal engendré par une partie)

Soit A un anneau commutatif et P une partie de A.
On appelle idéal engendré par P le plus petit idéal de A contenant P, noté (P).
On pourra enlever les accolades ($\{\}$) définissant P au besoin (Ex : $P = \{a, b\}$, alors $(P) = (a, b)$).

Définition 5 (Idéal principal)

Soit A un anneau commutatif.
On appelle idéal principal de A tout idéal de A engendré par un élément de A (c'est-à-dire par le singleton qui le contient).

Proposition 4 (Forme explicite d'un idéal engendré par une partie)

Soit A un anneau commutatif et P une partie de A.
Alors :

$$(P) = \left\{ \sum_{i=1}^{n} a_i x_i \mid n \in \mathbb{N}, a_1, ..., a_n \in A \text{ et } x_1, ..., x_n \in P \right\}$$

Démonstration. Notons :

$$(P) = \left\{ \sum_{i=1}^{n} a_i x_i \mid n \in \mathbb{N}, a_1, ..., a_n \in A \text{ et } x_1, ..., x_n \in P \right\}$$

1. I est un idéal de A.
   0 est égal à la somme vide (pour $n = 0$), et donc $0 \in I$.
   Soient $x = \sum_{i=1}^{n} a_i x_i$ et $y = \sum_{i=1}^{p} b_i y_i$ (avec : $a_1, ..., a_n \in A$ *et* $x_1, ..., x_n \in P$ et $b_1, ..., b_p \in A$ *et* $y_1, ..., y_p \in P$). Alors, en notant $a_{n+1} = b_1, ..., a_{n+p} = b_p$ et $x_{n+1} = y_1, ..., x_{n+p} = y_p$, on a :

   $$x + y \ = \ \sum_{i=1}^{n+p} a_i x_i$$

   et donc $(x + y) \in I$. Soit a ∈ A. Alors :

   $$-x \ = \ \sum_{i=1}^{n} (-a_i) x_i$$

   et donc $-x \in I$.
   I est donc un sous-groupe additif. Soit $a \in A$. Alors :

   $$ax \ = \ \sum_{i=1}^{n} (a a_i) x_i$$

   et donc $ax \in I$.
   I est donc un idéal de A.
2. P $\subseteqq$ I.
   Soit $x \in P$, alors $x = \cdot x$, donc $x \in I$ (somme à un terme).
3. $(P) \subseteq I$.
   I est un idéal de A contenant P, donc par définition, $(P) \subseteqq I$.

4. I $\subsetneqq$ (P).
   (P) est un idéal et $P \subsetneqq$ (P), donc pour tout $a \in A$ et tout $x \in Pax \in (P)$.
   De plus, (P) est un sous-groupe additif de A, donc toute somme finie d'élément de (P) est dans (P), donc tout élément de I est dans (P).
   D'où I $\subsetneqq (P)$.

Enfin, d'après 3) et 4), $I = (P)$ □

Proposition 5 (Forme explicite d'un idéal principal)

Soient A un anneau commutatif et $a \in A$.
Alors (a) est l'ensemble des multiples de a.

Démonstration. C'est un cas particulier du théorème précédent : il est clair que tout multiple de a est dans (a) (somme à 1 terme), et on peut factoriser la somme finie par a pour avoir un multiple de a, ce sont donc les seuls éléments de (a). □

Proposition 6 (Idéal principal et anneau entier)

Soient A un anneau et $a \in A$.
Alors $(a) = A$ si et seulement si A est inversible.

Démonstration. Si $(a) = A$, alors 1 est un multiple de a. Autrement dit, a est inversible.
Si a est inversible d'inverse u, alors pour tout $b \in A, b = a(ub)$, donc b est dans A. □

Définition 6 (Diviseur)

Soient A un anneau et $a, b \in$ A.
On dit que b divise a, noté $b|a$, s'il existe $k \in A$ tel que $a = bk$.

Les diviseurs positifs de 6 sont $1, 2, 3, 6$

Proposition 7 (Lien entre diviseur et idéal)

Soient A un anneau et $a, b \in A$.
Alors $b|a$ si et seulement si $(a) \subsetneqq (b)$.

Démonstration. D'après la proposition sur la forme explicite d'un idéal engendré par un ensemble, on a :
$(a) = \{ac \mid c \in A\}$ et $(b) = \{bc \mid c \in A\}$
Donc :

$b|a$
$\Leftrightarrow$ il existe $k \in (a)$ tel que $a = bk$
$\Leftrightarrow$ $a \in (b)$
$\Leftrightarrow$ $(a) \subsetneqq (b)$ (par définition de (a))

□

Proposition 8 (Divisibilité et relation d'ordre)

Soit A un anneau.
Alors la relation $|$ (divise) sur A est réflexive et transitive.

Démonstration. Soient $a, b, c \in A$.

1. Réflexivité :
   $a = a \cdot 1$, donc $a|a$.
2. Transitivité :
   Supposons que $a|b$ et $b|c$, alors il existe $p, q \in A$ tel que $b = ap$ et $c = bq$.
   Alors $c = a(pq)$, donc $a|c$.

□

Proposition 9

Soient A un anneau intègre et $a, b, c \in A$ non nuls et c non inversible.
Si $a = bc$ alors $(a) \subsetneq (b)$.

Démonstration. $(a) \subseteq (b)$ car $b|a$.
Supposons $(a) = (b)$.
Alors $b \in (a)$ donc il existe $k \in A$ tel que $b = ak$.
Alors $a = akc$, donc $kc = 1$ et c est inversible. Absurde.
Donc $(a) \neq (b)$. □

2 Anneaux euclidiens, principaux et factoriels

2.1 Définitions et liens entre les différents types

Définition 1 (Stathme)

Soit A un anneau intègre. Un stathme euclidien sur A est une application $\varphi : A \setminus \{0\} \mapsto \mathbb{N}$ telle que :

1. Pour tout a, b de A, b non nul, il existe q, r de A de sorte que $a = bq + r$, avec r $= 0$ ou $\varphi(r) < \varphi(b)$.
2. Pour tout a, b de $A \setminus \{0\}$, $\varphi(a) \leq \varphi(ab)$.

On a assez intuitivement la définition suivante :

Définition 2 (Anneau euclidien)

Un anneau euclidien est un anneau qui admet un stathme euclidien.

[Division euclidienne usuelle]
Le stathme utilisé est la valeur absolue. [Anneau des polynômes]
Si $K = \mathbb{Q}, \mathbb{R}, \mathbb{C}$, alors l'anneau des polynômes $K[X]$ est euclidien.
Son stathme est l'application qui à un polynome lui associe son degré.

Définition 3 (Anneau principal)

On appelle anneau principal tout anneau intègre dont tous les idéaux sont principaux.

$\mathbb{Z}/6\mathbb{Z}$ n'est pas principal, car il n'est pas intègre.
Néanmoins, tout idéal de cet anneau est principal. $\mathbb{Z}[i\sqrt{5}]$ n'est pas principal.

Théorème 1 (Euclidien implique principal)

Tout anneau euclidien est principal.

Démonstration. Soient A un anneau euclidien et φ son stathme euclidien.
Pour montrer que A est principal, il suffit de montrer que tout idéal de A est principal.
Soit I un idéal de A.
Alors $\varphi(I \setminus \{0\})$ est un sous-ensemble de $\mathbb{N}$, donc posséde un plus petit élément noté n_0.
Il existe donc $n \in I \setminus \{0\}$ tel que $\varphi(n) = n_0$.
Soit $a \in I$.
Alors il existe $q, r \in A$ tel que $a = qn + r$, avec $r = 0$ ou $\varphi(r) < \varphi(n)$.
Mais $r = a - qn$, donc $r \in I$.
Si $r \neq 0$, alors $\varphi(r) \geq \varphi(n)$. Impossible car $\varphi(r) < \varphi(n)$.
Donc $r = 0$ et $a = qn$.
On en déduit que $I = (n)$. □

Définition 4 (Elément irréductible)

Soit A un anneau intègre.
On dit qu'un élément de A est irréductible s'il n'est ni inversible, ni produit de deux éléments non inversibles.

Dans $\mathbb{Z}$, 7 est irréductible.

Proposition 1 (Produit d'un inversible et d'un irréductible)

Soient A un anneau intègre et p un élément irréductible de A.
Alors pour tout u inversible de A, pu est irréductible.

Démonstration. Supposons que pu n'est pas irréductible.
pu n'est pas inversible, car sinon, si $pui = 1$, alors p serai inversible.
pu est non nul car u et p sont non nuls.
Donc pu doit être produit de deux éléments non inversibles a, b.
Donc $p = a(bu^{-1})$ et bu^{-1} n'est pas inversible (de la même façon que pu).
Donc p n'est pas irréductible. Absurde.
Donc pu est irréductible. □

Définition 5 (Eléments associés)

Soient A un anneau intègre et $a, b \in A$ non nuls.
On dit que a et b sont associés s'il existe un élément inversible u de A tel que $a = ub$.

Dans $K[X]$, deux polynômes P, Q sont associés si et seulement si il existe $\lambda \in K^*$ tel que $P = \lambda Q$

Proposition 2 (Eléments associés et idéal)

Soient A un anneau intègre et $a, b \in A$ non nuls.
Alors $(a) = (b)$ si et seulement si a et b sont associés.

Démonstration. Supposons a et b associés.
Soit $u \in A$ inversible tel que $a = ub$.
Alors $b|a$, donc $(a) \subseteqq (b)$.
Et $b = u^{-1}a$, donc $a|b$ et $(b) \subseteqq (a)$.
On en déduit $(a) = (b)$.
Supposons $(a) = (b)$.
Alors, il existe $n, m \in A$ tel que $a = nb$ et $b = ma$.
Donc $a = nma$, par intégrité de A, on a : $1 = nm$.
Donc n et m sont inversibles, et a et b sont associés. □

Définition 6 (Anneau factoriel)

On appelle anneau factoriel tout anneau intègre A tel que :

1. Pour tout élément a de A non nul et non inversible, il existe une suite finie $p_1, ..., p_n$ d'éléments irréductibles de A tel que :

$$a = p_1 \cdots p_n$$

2. Si, pour un tel élément a, on a deux telles suites $p_1, ..., p_n$ et $q_1, ..., q_m$, alors $m = n$ et il existe une permutation σ de l'ensemble $\{1, ..., n\}$ ainsi que des éléments inversibles $u_1, ..., u_n$ tels que $p_i = u_i q_{\sigma(i)}$ pour tout i (la décomposition de a est unique à l'ordre des facteurs et à association près).

$\mathbb{Z}[i\sqrt{3}]$ n'est pas factoriel.

2.2 Propriétés des anneaux principaux

Donnons maintenant quelques propriétés intéressantes des anneaux principaux. On pourra régulièrement faire l'analogie avec les résultats et démonstrations d'arithmétique connus.

Proposition 3 (PGCD et "théorème de Bézout")

Soit A un anneau principal.
Alors, pour tout $a, b \in A$, il existe $d \in A$ tel que $d|a, d|b$, et si $c \in A$ est tel que $c|a$ et $c|b$ alors $c|d$.
De plus, il existe $u, v \in A$ tel que $au + bv = d$.

Démonstration. A est principal, donc il existe $d \in A$ tel que $(a, b) = (d)$.
Et il existe donc $u, v \in A$, tels que $au + bv = d$.
Alors, si $c|a$ et $c|b$, alors $c|(au + bv)$ donc $c|d$. □

Définition 7 (Entiers premiers entre eux)

Soient A un anneau principal et $a, b \in A$.
On dit que a et b sont premiers entre eux si $(a, b) = A$.

3 et 5 sont premiers entre eux.

Proposition 4 (Irréductibles et premiers entre eux)

Soient A un anneau principal, p un élément irréductible de A et $a \in$ A.
Alors $p|a$ si et seulement si a et p ne sont pas premier entre eux.

Démonstration. Supposons que $p|a$.
Alors $a \in (p)$ donc $(p, a) = (p) \neq A$.
Donc a et p ne sont pas premiers entre eux.
Supposons que p ne divise pas a.
Alors $(p, a) = (d)$ pour un certain $d \in A$.
Et d n'est pas associé à p car $a \notin (p)$ (qui serait alors égal à (d)).
Donc d divise p, on peut écrire, pour un entier k, $p = dk$.
Comme p et d ne sont pas associés, k n'est pas inversible.
Mais p est irréductible, donc n'est pas produit de deux éléments non inversibles.
Donc d est inversible, et $(d) = A$.
Donc a et p sont premiers entre eux. □

Proposition 5 (Irréductibles premiers entre eux)

Soient A un anneau principal et p, q deux éléments irréductibles de A.
Alors p et q sont premiers entre eux si et seulement si ils ne sont pas associés.

Démonstration. S'ils sont associés alors ils ne sont pas premiers entre eux d'après la proposition précédente.
S'ils ne sont pas premiers entre eux, alors $p|q$ et $q|p$ d'après la proposition précédente, donc ils sont associés.

□

Proposition 6 (Lemme de Gauss)

Soit A un anneau principal.
Alors pour tout $a, b, c \in A$:

$$(a|bc \text{ et } (a,b) = A) \implies a|c.$$

Démonstration. $(a,b) = A$, donc il existe $u, v \in A$ tel que $au + bv = 1$.
Et $a|bc$ donc il existe $k \in A$ tel que $bc = ak$.
Donc $a(cu + kv) = auc + bvc = c$.
Donc $a|c$. □

Proposition 7 (Suite croissante d'idéaux)

Soit A un anneau principal.
Alors, toute suite croissante d'idéaux de A (au sens de l'inclusion) est stationnaire.

Démonstration. Soit $(I_n)_{n\in\mathbb{N}}$ une telle suite.
Alors, pour tout $n \in \mathbb{N}$, il existe $g_n \in A$ tel que $I_n = (g_n)$.
Posons $P = \{g_n \mid n \in \mathbb{N}\}$.
Alors il existe $p \in A$ tel que $(P) = (p)$.
Donc il existe une somme finie tel que :

$$p = \sum_{n=1}^{N} a_n g_n$$

avec $a_1, ..., a_N \in A$.
Or, pour tout $n \in \{1, ..., N\}, g_n \in (g_n) \subseteqq (g_N)$ (par croissance).
Donc $p \in (g_N)$.
Et, pour tout $n \geq N g_n) \subseteqq (p) \subseteqq (g_N)$ et $(g_N) \subseteqq (g_n)$.
Donc $(g_N) = (g_n)$ et la suite est stationnaire. □

Proposition 8 (Existence d'un diviseur irréductible)

Soit A un anneau principal.
Alors, pour tout $a \in A$ non nul et non inversible, il existe $p \in A$ irréductible tel que $p|a$.

Démonstration. Posons $a_0 = a$.
Ensuite, en supposant que a_n est définie, non nul et non inversible, on définit a_{n+1} de la façon suivante :

Si a_n est irréductible, on pose $a_{n+1} = a_n$.
Sinon, a_n étant non nuls, non inversibles et non irréductibles, il est produit de deux éléments b, c de A non nul et non inversible.
On pose alors $a_{n+1} = b$.

On a ainsi créé une suite $(a_n)_{n\in\mathbb{N}}$.
Remarquons que, pour tout $n \in \mathbb{N}$, $(a_{n+1})|(a_n)$.
Donc la suite des idéaux $((a_n))_{n\in\mathbb{N}}$ est croissante donc stationnaire.
Il existe donc $N \in \mathbb{N}$ tel que, pour tout $n \geq N$, $((a_n)) = ((a_N))$.
Or, si a_N n'est pas irréductible, alors $a_N = a_{N+1}c$ pour un certain c de A non inversible, donc (a_{N+1}) $\neq (a_N)$. Absurde.
Donc a_N est irréductible et divise a. □

Proposition 9 (Produit d'irréductible)

Soit A un anneau principal.
Alors, pour tout $a \in A$ non nul, non inversible, il existe une suite finie $p_1, ..., p_n$ d'élément irréductible de A tel que :

$$a = p_1 \cdots p_n$$

Démonstration. Soit a ∈ A.
Posons $a_0 = a$.
Ensuite, en supposant que a_n est défini, non nul et non inversible, on pose p_n un diviseur irréductible de a_n, et on pose $a_n = a_{n+1}p_n$.
a_{n+1} est non nul, car a_n est non nul.
Si a_{n+1} est inversible, alors on s'arrête. Sinon, on continue l'algorithme.
Supposons que l'algorithme ne finisse pas.
Alors, on crée ainsi une suite $(a_n)_{n\in\mathbb{N}}$.
Et de plus $a_{n+1}|a_n$, donc la suite des idéaux $(a_n)_{n\in\mathbb{N}}$ est croissante, donc stationnaire.
Mais, on déduit de la relation $a_n = a_{n+1}p_n$ que $(a_n) \neq (a_{n+1})$ pour tout $n \in \mathbb{N}$ (car p est irréductible).
Absurde, donc l'algorithme s'arrête.
Soit $n \in \mathbb{N}$ tel que a_n soit définie mais pas a_{n+1} (donc a_n inversible).
Alors $a = a_1p_0 = \cdots = a_np_0 \cdots p_{n-1}$.
Et a_np_0 est irréductible, on a donc bien écrit a comme produit d'une suite finie de terme irréductible.
□

Théorème 2 (Principal implique factoriel)

Tout anneau principal est factoriel.

Démonstration. Soit A un anneau principal.
Soit $a \in A$ non nul et non inversible.
Alors, il existe une suite finie $p_1, ..., p_n$ d'éléments irréductibles de A telle que :

$$a = p_1 \cdots p_n$$

Supposons qu'il existe une autre suite finie $q_1, ..., q_m$ d'éléments irréductibles de A telle que :

$$a = q_1 \cdots q_m$$

On peut supposer, quite à échanger les deux suites que $n \geq m$.
On va montrer que $m = n$ et qu'il existe une permutation σ de l'ensemble $\{1, \ldots, n\}$ ainsi que des éléments inversibles $u_1, \ldots, u_n$ tels que $p_i = u_i q_{\sigma(i)}$ pour tout i (la décomposition de a est unique à l'ordre des facteurs et à association près) par récurrence sur n.
Initialisation : pour $n = 1$.
Alors $n = 1 \geq m \geq 1$, donc $m = n = 1$.
Et $a = p_1 = q_1$.
La propriété est initialisée (la permutation est l'identité et $u_1 = 1$).
Hérédité : On suppose la propriété vraie au rang n. Montrons la au rang $n + 1$.

$$a = p_1 \cdots p_{n+1} = q_1 \cdots q_m$$

Donc $p_{n+1} | q_1 \cdots q_m$.
p_{n+1} est irréductible, donc premier avec tout irréductible qui ne lui ait pas associé.
Donc d'après le lemme de Gauss, il divise un q_i qui lui est donc associé (on enlève tous ce qui ne lui sont pas associés, et on prend un qui reste).
Il existe donc $1 \leq i \leq m$ et $u_{n+1} \in$ A inversible tel que $p_{n+1} = u_{n+1} q_i$.
Posons t la transposition qui échangent i et m.
Alors, après simplification :

$$u_{n+1} p_1 \cdots p_n = q_{t(1)} \cdots q_{t(m-1)}$$

Par hypothèse de récurrence $m - 1 = n$ (donc $m = n + 1$), et il existe une permutation σ de l'ensemble $\{1, \ldots, n\}$ ainsi que des éléments inversibles $u_1, \ldots, u_n$ tels que $p_i = u_i q_{t(\sigma(i))}$ pour tout i.
Etendons σ sur $\{1, \ldots, n + 1\}$ en laissant fixe $n + 1$ (donnant ainsi une permutation).
Alors, pour tout i entre 1 et $n + 1$, $p_i = u_i q_{t(\sigma(i))}$, et la composé de t et σ est une permuation.
On en déduit que la propriété est vraie au rang $n + 1$.
La propriété est héréditaire, donc d'après le principe de récurrence, elle est vraie quelque soit $n \in \mathbb{N}$.
L'anneau est intègre et vérifie donc la définition d'un anneau factoriel.
A est donc un anneau factoriel. □

3 Application : Entiers de Gauss et théorème des deux carrés

3.1 Entiers de Gauss

Définition 1 (Entier de Gauss)

On appelle entier de Gauss tout nombre complexe sous la forme $a + ib$ où a,b sont des entiers.
On note l'ensemble de ces entiers $\mathbb{Z}[i]$.

Proposition 1 (Structure d'anneau intègre)

L'ensemble $\mathbb{Z}[i]$ est un anneau intègre.

Démonstration. La structure d'anneau se vérifie directement.
Montrons rapidement que $\mathbb{Z}[i]$ est intègre.
Soient $x = a + ib$ et $y = c + id$ deux entiers de Gauss. Alors $x \times y \in \mathbb{Z}[i] \subset \mathbb{C}$. Or, $\mathbb{C}$ est un corps et donc la règle du produit nul est vérifiée.
$\mathbb{Z}[i]$ est donc un anneau intègre. □

Proposition 2 (Stathme euclidien sur l'anneau de Gauss)

L'application $\varphi : \mathbb{Z}[i] \setminus \{0\} \to \mathbb{N}$ qui à $a + ib$ associe $a^2 + b^2$ est un stathme euclidien sur $\mathbb{Z}[i]$.

Démonstration. Pour a et b entiers, $\varphi(a + ib)$ est un entier.
Prolongeons φ sur $\mathbb{C}$ en gardant la même formule.
Soient a et b des nombres complexes.
Alors on obtient par un simple calcul : $\varphi(ab) = \varphi(a)\varphi(b)$.
C'est en particulier vrai pour $a, b \in \mathbb{Z}[i] \setminus \{0\}$.
Soient $a \in \mathbb{Z}[i)$ et $b \in \mathbb{Z}[i] \setminus \{0\}$.
Si $a/b \in \mathbb{Z}[i]$, alors $a = (a/b)b + 0$.
Sinons, posons $a/b = c_1 + ic_2$.
Alors $|c_1 - E(c_1)| \leq 1/2$ ou $|c_1 - (E(c_1) + 1)| \leq 1/2$.
Donc il existe un entier q_1 tel que $|c_1 - q_1| \leq 1/2$.
De même, il existe un entier q_2 tel que $|c_2 - q_2| \leq 1/2$.
Posons $q = q_1 + iq_2$.
Alors $\varphi(a/b - q) = |c_1 - q_1|^2 + |c_2 - q_2|^2 < 1$.
Donc $\varphi(a - bq) < \varphi(b)$.
Et $a = bq + (a - bq)$.
Dans tous les cas, il existe $q, r \in \mathbb{Z}[i]$ tel que $a = bq + r$ et r=0 ou $\varphi(r) < \varphi(b)$.
On en déduit que φ est un stathme euclicien.

□

Proposition 3

$\mathbb{Z}[i]$ est un anneau euclidien.

Remarque 1. *D'après la proposition (1), il est donc principal.*

3.2 Théorème des deux carrés

Proposition 4

Tout nombre premier p de la forme $4n+1$ avec $n \in \mathbb{N}$ peut s'écrire sous la forme d'une somme de deux carrés.

Démonstration. On a vu en cours que pour un tel nombre premier p, il existe $m \in \mathbb{N}$ tel que $m^2 \equiv -1[p]$.
Il existe donc un entier $q \in \mathbb{N}$ tel que $m^2 + 1 = pq$.
Donc $pq = (m+i)(m-i)$.
Mais $(m+i)/p$ et $(m-i)/p$ ont pour partie imaginaire $\pm 1/p$ qui n'est pas un entier, et donc p ne divise ni $m+i$ ni $m-i$.
Donc p n'est pas irréductible (sinon, il serait premier avec $m+i$, et d'après le lemme de Gauss, il devrait diviser $m-i$).
Il existe donc $x, y \in \mathbb{Z}[i]$, non inversible, tel que $p = xy$.
Donc $p^2 = \varphi(p) = \varphi(x)\varphi(y)$ et $\varphi(x), \varphi(y)$ sont des entiers naturels différent de 1.
Ils doivent donc être égal à p.
Donc $p = \varphi(x)$ est bien somme de deux carrés. □

Proposition 5

Une somme de trois carrés est divisible par 4 si et seulement si les trois carrés sont divisibles par 4.

Démonstration. Il est évident que si les trois carrés sont divisibles par 4, leur somme l'est aussi.
Montrons la réciproque.
Soient $x, y, z \in \mathbb{Z}$ tel que 4 divise $x^2 + y^2 + z^2$.
Remarquons que le reste par la division par 4 d'un carré est soit 0 soit 1 (simple calcul).
Alors, il faut que les trois soient nuls pour que leur somme soit divible par 4.
C'est à dire que les trois carrés doivent être divisibles par 4. □

Proposition 6

Tout nombre de la forme $4n+3$ ne peut pas s'écrire comme somme de deux carrés.

Démonstration. Soit p un tel nombre.
Il peut s'écrire sous la forme $4n-1$.
Supposons que $p = x^2 + y^2$ avec $x, y \in \mathbb{N}$.
Alors $4n = x^2 + y^2 + 1^2$.
Donc, par la proposition précédente, 4 divise 1, absurde.
Donc p ne peut pas s'écrire comme somme de deux carrés. □

Proposition 7

Le produit de deux nombres exprimables comme somme de deux carrés est exprimable comme somme de deux carrés.

Démonstration. Simple conséquence de l'identité :

$$(x_1 + x_2)^2 + (y_1 + y_2)^2 = (x_1y_1 - x_2y_2)^2 + (x_1y_2 + x_2y_1)^2$$

□

Proposition 8

Tout nombre dont la décomposition en nombre premier vérifie que l'exposant de chaque nombre premier de la forme $4n+3$ soit pair est exprimable comme somme de deux carrés.

Démonstration. Simple conséquence des propositions précédentes car :

1. Un nombre au carré est exprimable comme somme de deux carrés (lui-même au carré + 0^2).
2. $2 = 1^2 + 1^2$.
3. Tout les nombres de la forme $4n + 1$ sont exprimable comme somme de deux carrés.
4. Tout nombre premier est soit 2, soit de la forme $4n + 1$, soit de la forme $4n + 3$.

□

Proposition 9

Soient p un nombre premier de la forme $4n + 3$ et a, b des nombres non divisibles par p. Alors p ne divise pas $a^2 + b^2$. (Par contraposée, si p divise la somme des deux carrés, il divise a et b).

Démonstration. Par le petit théorème de Fermat, p divise $a^{p-1} - b^{p-1}$.
Donc p ne divise pas $a^{p-1} + b^{p-1}$ (car sinon il diviserait la somme des deux et donc diviserait a).
Or $p - 2 = 2(2n - 1)$, donc on a :

$$a^{p-1} + b^{p-1} = (a^2 + b^2) \sum_{k=0}^{2n} (-1)^k a^{2n-1-k} b^k$$

Donc p ne divise pas $a^2 + b^2$.
Par contraposée, si p divise $a^2 + b^2$, alors p divise a ou b, et on en déduit facilement que p divise a et b. □

Théorème 1 (Des deux carrés)

Si un nombre peut s'écrire comme somme de deux carrés, alors tous les nombres premiers de la forme $4n + 3$ dans sa décomposition ont un exposant pair.

Démonstration. Soient $a = x^2 + y^2$ et p un nombre premier de la forme $4n + 3$ de sa décomposition en facteurs premiers.
p divise la somme des deux carrés, donc ses racines et p^2 divise donc x^2 et y^2.
En divisant par p^2, on trouve que a/p^2 s'écrit aussi comme somme de deux carré et est donc entier.
Si a/p^2 est aussi divisible par p, le même raisonnement donne que a/p^4 est entier et s'écrit comme somme de deux carré.
Et ainsi de suite jusqu'a ce que a/p^{2b} ne soit plus divisible par p.
Alors l'exposant de p dans la décomposition de a est $2b$ et est donc pair. □

Références

Xavier Gourdon "Les maths en tête - Algèbre" p28 Daniel Perrin "Cours d'aglèbre" p41-59 Patrice Tauvel "Algèbre agrégation" p225-232