

Anneau principal non euclidien

Lemme: Si (A, S) euclidien, alors $\exists x \in A \setminus A^*$ tel que $A/\langle x \rangle$ corps

Si A est un corps, $x=0$ convient. Sinon, soit $x \in A \setminus (0 \cup A^*)$ de norme minimale. Alors, $\forall z \in (A/\langle x \rangle)^*$, $\exists y \in A^*$ tel que $\pi(y) = z$ où $\pi: A \rightarrow A/\langle x \rangle$ par division euclidienne, $\exists q, r \in A$ tels que $y = xq + r$, $S(r) < S(x)$ ou $r=0$. Donc $z = \pi(y) = \pi(r)$ et $r \neq 0$. Par définition de x , on a $r \in A^*$ et $z \in (A/\langle x \rangle)^*$ d'inverse $\pi(r^{-1})$. Alors $A/\langle x \rangle$ corps.

Théorème: Soit $w = \frac{1}{2}(1+i\sqrt{5})$, $A = \mathbb{Z}[w]$. Alors A intègre, non euclidien, principal.

- ① A non euclidien ② $\langle 2 \rangle \subset A$ maximal ③ A principal.

① Puisque $A \subset \mathbb{C}$ sous anneau, A intègre. Supposons (A, S) euclidien. Par le lemme, $\exists x \in A \setminus A^*$ tel que $K := A/\langle x \rangle$ corps. Puisque $A^* = \{-1, 1\}$, par surjectivité de π , $|K| \leq 3$. Or, w est racine de $P = X^2 - X + 5$ et $\pi(w)$ aussi. Cependant, P n'a pas de racines sur $\mathbb{F}_2$ ou $\mathbb{F}_3$ ($P(0) = 5 \neq 0$, $P(1) = 5 \neq 0$, $P(2) = 7 \neq 0$). C'est absurde, donc A non euclidien.

② Par théorème d'isomorphisme, on a $A/\langle 2 \rangle \cong (\mathbb{Z}[X]/\langle 2, X^2 - X + 5 \rangle)_{\langle 2 \rangle} \cong \mathbb{Z}[X]/\langle 2, X^2 - X + 5 \rangle \cong \mathbb{F}_2[X]/\langle X^2 - X + 1 \rangle \cong \mathbb{F}_2[X]/\langle X^2 + X + 1 \rangle \cong \mathbb{F}_4$. Puisque $P = X^2 + X + 1 \in \mathbb{F}_2[X]$ est irréductible, on a $\mathbb{F}_2[X]/\langle P \rangle$ corps et $\langle 2 \rangle \subset A$ maximal.

③ Soit $I \subset A$ idéal non nul, et $b \in I \setminus \{0\}$ de norme N minimale. Montrons que $I = \langle b \rangle$.

On a $\forall a \in I$ par pseudo-division euclidienne, $\exists q, r \in A$ tels que

* $a = bq + r$, $N(r) < N(b)$ ou $r=0$. Par définition de b , on a $r=0$ et $a = bq \in \langle b \rangle$.

* $2a = bq + r$, $N(r) < N(b)$ ou $r=0$. On a aussi $r=0$ et $2a = bq$.

Puisque $2 \nmid bq$, où 2 est premier dans A car $\langle 2 \rangle$ maximal, on a 2 cas

- $2 \nmid q$ et $\exists q' \in A$ tel que $2q = q'$; donc $a = bq' \in \langle b \rangle$

- $2 \nmid q$, $2 \mid b$ et $\exists b' \in A^*$ tel que $2b = b'$; donc $a = bq'$

Puisque $q \notin \langle 2 \rangle$, on a $\langle 2 \rangle \subsetneq \langle 2, q \rangle$ et puisque $\langle 2 \rangle$ maximal, on a $\langle 2, q \rangle = A$.

Alors $\exists \lambda, \mu \in A$ tel que $1 = 2\lambda + q\mu$, et $b = 2\lambda b' + q\mu b = \lambda b' + \mu a \in I$.

Or, $b' \neq 0$ donc $N(b) < N(b')$ et $N(b) = N(2)N(b') > 2N(b')$, absurde. On en déduit que $I = \langle b \rangle$ et A est principal.

Lemme: $N: z \in A \mapsto |z|^2 = z\bar{z} \in \mathbb{N}$ est multiplicative, et $N(z) > 0$ si $z \neq 0$

Puisque $A \subset \mathbb{C}$, on a $\forall z = a + ib \in A$, $N(z) = z\bar{z} = a^2 + b^2 = (a + \frac{1}{2}b)^2 + \frac{19}{4}b^2 \in \mathbb{N}$.

Donc N bien défini, et $\forall z, z' \in A$ $N(zz') = zz' \overline{zz'} = z\bar{z} z'\bar{z'} = N(z)N(z')$

Et $N(z) = (a + \frac{1}{2}b)^2 + \frac{19}{4}b^2 = 0 \Leftrightarrow a = b = 0 \Leftrightarrow z = 0$

Lemme: On a $A^\times = \{-1, 1\}$

Soit $u \in A^\times$, alors $1 = N(uu^{-1}) = N(u)N(u^{-1})$, et $N(u) = (a + \frac{1}{2}b)^2 + \frac{19}{4}b^2 = 1$. Donc

$\frac{19}{4} \leq b^2$, $b^2 \leq \frac{4}{19}$ et $b = 0$, alors $a^2 = 1$, d'où $a \in \{-1, 1\}$. Réciproquement, $A^\times = \{-1, 1\}$.

Lemme (pseudo division euclidienne): Soit $a \in A, b \in A^\times$, alors $\exists q, r \in A$ tels que

$a = bq + r$ ou $2a = bq + r$ et $N(r) < N(b)$ ou $r = 0$

Soit $\frac{a}{b} = u + wv \in \mathbb{Q}(w)$, on pose $n = \lfloor v \rfloor$, et $v \in [n, n+1[$

* Si $v \in [n, n + \frac{1}{3}[\cup [n + \frac{2}{3}, n+1[$, on prend $s, r \in \mathbb{Z}$ tels que $|u-s| \leq \frac{1}{2}, |v-r| \leq \frac{1}{3}$

Alors, $q := s + wt \in A$, $r := a - bq \in A$ et $N(r) = N(b)N(\frac{a}{b} - q) < N(b)$ car

$N(\frac{a}{b} - q) = N((u-s) + w(v-r)) = (u-s)^2 + (u-s)(v-r) + 5(v-r)^2 \leq (\frac{1}{2})^2 + (\frac{1}{2})(\frac{1}{3}) + 5(\frac{1}{3})^2 = \frac{35}{36}$

* Sinon, $v \in [n + \frac{1}{3}, n + \frac{2}{3}[$, on pose $m = \lfloor 2v \rfloor$. Alors $2v \in [2n + \frac{2}{3}, 2n + 1 + \frac{1}{3}[$ donne:

* $2v \in [2n + \frac{2}{3}, 2n + 1[$ et $m = 2n$, alors $2v \in [m + \frac{2}{3}, m + 1[$

* $2v \in [2n + 1, 2n + 1 + \frac{1}{3}[$ et $m = 2n + 1$, alors $2v \in [m, m + \frac{1}{3}[$

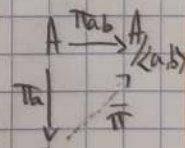
$\Rightarrow$ Alors $2v \in [m, m + \frac{1}{3}[\cup [m + \frac{2}{3}, m + 1[$ et le cas précédent avec $\frac{2a}{b} = 2u + w(2v)$

donne $q, r \in A$ tels que $2a = bq + r$, $N(r) < N(b)$

Lemme: Pour $a, b \in A$ anneau, on a $A_{\langle a, b \rangle} \simeq (A_{\langle a \rangle})_{\langle [b]_a \rangle}$

On note $\pi_a: A \rightarrow A_{\langle a \rangle}$, $\pi_b: A \rightarrow A_{\langle a, b \rangle}$. On a $\langle a \rangle \subset \langle a, b \rangle = \text{Ker } \pi_b$

donc $\exists \bar{\pi}: A_{\langle a \rangle} \rightarrow A_{\langle a, b \rangle}$ tel que $\bar{\pi} \circ \pi_a = \pi_b$, ie le diagramme



surj

* Puisque π_b surj, $\bar{\pi}$ surj ($\forall y \in A_{\langle a, b \rangle}, \exists x \in A, y = \pi_b(x) = \bar{\pi}(\pi_a(x))$)

Ker $\bar{\pi}$

* On a $[a]_a = \pi_a(x) \in \text{Ker } \bar{\pi} \Leftrightarrow x \in A, \bar{\pi}([a]_a) = \pi_b(x) = 0 \Leftrightarrow x \in \langle a, b \rangle$.

Donc $\text{Ker } \bar{\pi} = \pi_a(\langle a, b \rangle) = \langle [b]_a \rangle$. Alors $A_{\langle a, b \rangle} \simeq \text{Im } \bar{\pi}$, ie $A_{\langle a, b \rangle} \simeq (A_{\langle a \rangle})_{\langle [b]_a \rangle}$.

Théorème: Soit A, B anneaux, $f: A \rightarrow B$, $I \subset A$ idéal tel que $I \subset \text{Ker } f$.

Alors, $\exists \bar{f}: A/I \rightarrow B$ tel que $\bar{f} \circ \pi_I = f$, ie

