Anneaux

1) Exemple d'anneau euclidien

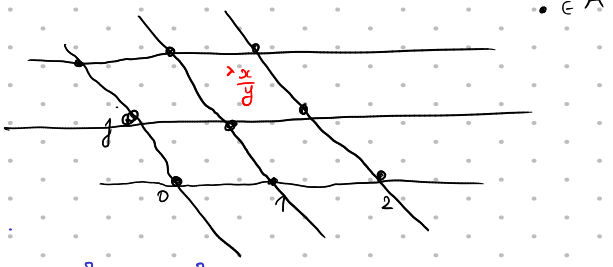
$A = \mathbb{Z}[j] = \mathbb{Z} + \mathbb{Z}j$ où $j = e^{\frac{2i\pi}{3}} = -\frac{1}{2} + i\frac{\sqrt{3}}{2}$

$(j^2 + j + 1 = 0)$

A est un sous-anneau de $\mathbb{C}$ donc intègre

Proposition L'anneau A est euclidien pour $N : A \to \mathbb{N}$, $x \mapsto |x|^2$

$(N(a+bj) = |a+bj|^2 = (a+bj)(a+bj^2) = a^2 + b^2 - ab)$



démo. Soit $x \in A$. Soit $0 \neq y \in A$

$\frac{x\bar{y}}{y\bar{y}} = \frac{x}{y} = \alpha + \beta j \qquad \alpha, \beta \in \mathbb{R}$

Soient $a, b \in \mathbb{Z}$, Soit $z = a + jb \in A$.

$$N\left(z - \frac{x}{y}\right) = N\left(a - \alpha + j(b-\beta)\right) = (a-\alpha)^2 + (b-\beta)^2 - (a-\alpha)(b-\beta)$$
$$= \left((a-\alpha) - \frac{(b-\beta)}{2}\right)^2 + \frac{3}{4}(b-\beta)^2$$

on choisit $b \in \mathbb{Z}$ tq $|b-\beta| \leq \frac{1}{2}$

on choisit $a \in \mathbb{Z}$ tq $|a - (\alpha + \frac{b-\beta}{2})| \leq \frac{1}{2}$

Alors $N\left(z - \frac{x}{y}\right) \leq \frac{1}{4} + \frac{3}{4} \times \frac{1}{4} = \frac{7}{16} < 1$

Alors $N(yz - x) = N(y)\, N\left(z - \frac{x}{y}\right) < N(y)$

Or $x = \underbrace{yz}_{\in A} - \underbrace{(yz - x)}_{r \in A}$ et $N(r) < N(y)$ (division euclidienne).

Corollaire $A = \mathbb{Z}[j]$ est principal.

Ex: 2 est premier dans A car $A/(2) \simeq \mathbb{Z}[X]/(2, X^2+X+1) \simeq \mathbb{Z}/2\mathbb{Z}[X]/(X^2+X+1)$ corps

3 n'est pas premier dans A car $3 = (2+j)(2+j^2)$.

De plus $A^* = \{\pm 1, \pm j, \pm j^2\}$

$= \{\pm 1, \pm j, \pm(1+j)\}$

En effet si $x = a + bj \in A^*$ alors $\exists x^{-1} \in A$, $x x^{-1} = 1$

$\Rightarrow N(x x^{-1}) = 1 = \underbrace{N(x)}_{\in \mathbb{N}} \underbrace{N(x^{-1})}_{\in \mathbb{N}}$

$\Rightarrow N(x) = 1$

Réciproquement $N(x) = 1 \Rightarrow x \in A^*$ car alors $x^{-1} = \bar{x} \in A$

donc $x \in A^* \Leftrightarrow |x|^2 = 1 \Leftrightarrow a^2 + b^2 - ab = 1$

$\Leftrightarrow (a - \frac{b}{2})^2 + \frac{3b^2}{4} = 1 \Rightarrow b^2 \leq \frac{4}{3} \Rightarrow b = \pm 1$ ou 0

Si $b=0$ $\quad a^2=1 \iff a=\pm 1$ donc $a+bj=\pm 1$

si $b=1$ $\quad \left(a-\frac{1}{2}\right)^2+\frac{3}{4}=1 \iff \left(a-\frac{1}{2}\right)^2=\frac{1}{4} \iff a-\frac{1}{2}=\pm\frac{1}{2}$

$\iff a=0$ ou 1

donc $x=j$ ou $1+j$

si $b=-1$ $\quad \left(a+\frac{1}{2}\right)^2+\frac{3}{4}=1 \iff x=-j$ ou $-1-j$.

Réciproquement, $\pm 1, \pm j, \pm(1+j)$ $(1+j=-j^2)$ $\in A^*$.

2) Corps des fractions

Théorème. Soit A anneau intègre.

Il existe un corps $A \subset K$ tel que $K=\left\{\frac{a}{b} : a\in A, b\in A\setminus\{0\}\right\}$

On appelle K le corps des fractions de A.

démo: On pose $K=\{(a,b)\in A\times A\setminus\{0\}\}/\sim$

où $(a,b)\sim(a',b')$ si $ab'=a'b$. $\quad (\iff \ll \frac{a}{b}=\frac{a'}{b'} \gg)$

C'est une relation d'équivalence c-à-d: $(a,b)\sim(a,b)$, $(a,b)\sim(a',b') \iff (a',b')\sim(a,b)$, $(a,b)\sim(a',b')\sim(a'',b'')$

$\Longrightarrow (a,b)\sim(a'',b'')$

on pose $[a,b]_\sim$ la classe d'équivalence de (a,b).

Remarque: $\forall a\in A, b\in A\setminus\{0\}$, $[a,b]_\sim=[a',b']_\sim \iff ab'=a'b$.

Voici des opérations sur K:

$\cdot$: $[a,b]_\sim\cdot[c,d]_\sim := [ac,bd]_\sim$ bien défini

$+$: $[a,b]_\sim+[c,d]_\sim := [ad+bc,bd]_\sim$ bien défini (*)

(*): en effet: si $[a,b]_\sim=[a',b']_\sim$ si $[c,d]_\sim=[c',d']_\sim$ alors $[ad+bc,bd]_\sim=[a'd'+b'c',b'd']_\sim$

ou: $ab'=a'b$, $cd'=c'd \Rightarrow (ad+bc)b'd' = ab'dd'+bb'cd'$

$= a'bdd'+bb'c'd$

$= (a'd'+b'c')bd \Rightarrow [ad+bc,bd]_\sim=[a'd'+b'c',b'd']_\sim$.

Pour ces opérations $(K,+,\cdot)$ est un corps.

En effet $0_K=[0,1]_\sim=[0,b]_\sim$ $(\forall 0\neq b\in A)$

$1_K=[1,1]_\sim=[a,a]_\sim$ $(\forall 0\neq a\in A)$

et $\forall a\neq 0$, $[a,b]_\sim^{-1}=[b,a]_\sim$.

et $\forall a\in A, \forall b\in A\setminus\{0\}$ $\quad [a,b]_\sim=[a,1]_\sim[b,1]_\sim^{-1}$

et $A\to K$, $a\mapsto[a,1]_\sim$ morphisme injectif d'anneaux.

Cas particulier si $A\subset L$ (L corps) alors le corps des fractions de A «est» (quotient dans L) $\left\{\frac{a}{b} : a\in A, b\in A^*\right\}$

$\underbrace{\text{Frac}(A)}$

ex $\text{Frac}(\mathbb{Z})=\mathbb{Q}$, $\text{Frac}(\mathbb{Z}[i])=\mathbb{Q}[i]=\mathbb{Q}+\mathbb{Q}i$

$\text{Frac}(\mathbb{Z}[\sqrt{2}])=\mathbb{Q}[\sqrt{2}]$, etc., $\text{Frac}(K[X])=K(X)$ (K corps)

3) Polynômes irréductibles sur un corps

a) sur $\mathbb{C}$

$P \in \mathbb{C}[X]$ irréductible $\Leftrightarrow \deg P = 1$ $\quad (P = aX+b,\ a \in \mathbb{C}^*,\ b \in \mathbb{C})$

(d'Alembert-Gauss : Si $P \notin \mathbb{C}$, $\exists z \in \mathbb{C}$, $P(z)=0 \Leftrightarrow X-z \mid P \Rightarrow P = \lambda(X-z)$ pour un $\lambda \in \mathbb{C}^*$ car P irréductible)

b) sur $\mathbb{R}$

$P \in \mathbb{R}[X]$ irréductible $\Leftrightarrow \deg P = 1$ ou $\deg P = 2$ et P n'a pas de racine réelle.

$\Leftrightarrow \deg P = 1$ ou $\deg P = 2$ et $\Delta_P < 0$.

démo : $\Rightarrow$: P a une racine dans $\mathbb{C}$: z.

Si $z \in \mathbb{R}$, $P = \lambda(X-z)$ $\lambda \in \mathbb{R}^*$ et $\deg P = 1$

Si $z \in \mathbb{C}\setminus\mathbb{R}$, $P(\bar{z})=0 \Rightarrow (X-z)(X-\bar{z}) \mid P$ dans $\mathbb{C}[X]$

($(X-z)$ et $(X-\bar{z})$ premiers entre eux)

or $(X-z)(X-\bar{z}) = X^2 - 2\mathrm{Re}(z) + |z|^2 \in \mathbb{R}[X]$

donc $P = \lambda (X-z)(X-\bar{z})$, $\lambda \in \mathbb{R}^*$ (P n'a pas de racine réelle).

ex : $X^4+1 = \underbrace{(X-e^{i\pi/4})(X-e^{-i\pi/4})}\ \underbrace{(X-e^{3i\pi/4})(X-e^{-3i\pi/4})}$

$= \underbrace{(X^2-\sqrt{2}X+1)}\ \underbrace{(X^2+\sqrt{2}X+1)}$

irréductibles sur $\mathbb{R}$ (deg 2 et pas de racine réelle)

exo : Conséquence X^4+1 irréductible sur $\mathbb{Q}$.

[Indication : un facteur irréductible sur $\mathbb{Q}$ est un produit de facteurs irréductibles sur $\mathbb{R}$ or $X^2 \pm \sqrt{2}X + 1 \notin \mathbb{Q}[X]$]

c) Sur K quelconque

Proposition : Si $P \in K[X]$ et si $\deg P = 2$ ou 3 alors P irréductible sur K

$\Leftrightarrow$ P n'a pas de racine dans K.

Rem. Contre-exemple si $\deg P = 4$: X^4+1 réductible sur $\mathbb{R}$ bien que sans racine réelle.

démo. $\Rightarrow$: Si $P(x)=0$ alors $X-x \mid P$ absurde.

$\Leftarrow$: si P n'a pas de racine si $P = P_1 P_2$

alors $\deg P_1 > 0$ et $\deg P_2 > 0$

$\Rightarrow \deg P_1$ ou $\deg P_2 = 1$.

$\Rightarrow P_1$ ou P_2 a une racine

$\Rightarrow P$ a une racine absurde.

Ex : sur $K = \mathbb{Z}/2\mathbb{Z}$ X^2+X+1 est le seul irréductible de degré 2.

X^3+X+1 et X^3+X^2+1 sont les irréductibles de degré 3

Sur $K=\mathbb{Z}/3\mathbb{Z}$: X^2+1, X^2-X+1 et X^2-X-1 sont irréductible

$\{0,\pm1\}$ X^3-Y^2-X-1 irréductible

sur $\mathbb{Q}$ X^3-3X+1 est irréductible.

[si $r=\frac{a}{b}$ $a,b\in\mathbb{Z}$, $a\wedge b=1$, $r^3-3r+1=0 \Leftrightarrow \frac{a^3}{b^3}-\frac{3a}{b}+1=0$

$\Leftrightarrow a^3-3ab^3+b^3=0$

$\Rightarrow b\mid a$ ($\Leftrightarrow b=\pm1$)

$\Rightarrow \frac{a}{b}=r\in\mathbb{Z}$

$\Rightarrow r\mid 1 \Rightarrow r=\pm1$

$r^3-3r=-b \Leftrightarrow r(r^2-3r)=-1$

Mais ±1 ne sont pas racine

d) sur $\mathbb{Q}$

Lemme: A intègre $\Rightarrow A[X]$ intègre

(démo: si $0\neq P,Q\in A[X]$, $\deg(PQ)=\deg P+\deg Q\geq 0$.

$\Rightarrow PQ\neq 0$ dans $A[X]$)

Lemme de Gauss.

Soit $P=a_0+\dots+a_dX^d\in A[X]$

Si A factoriel on pose $c(P)=\text{pgcd}(a_0,\dots,a_d)\in A$ (= CONTENU de P)

(défini à multiplication par un $u\in A^*$ près).

$\forall P,Q\in A[X]$, $c(PQ)=c(P)c(Q)$.

démo ($A=\mathbb{Z}$)

Il suffit de montrer que $c(P)=c(Q)=1$

alors $c(PQ)=1$.

Démo soit p nombre premier. Si par l'absurde, p divise tous les coefficients de PQ, alors $\overline{PQ}=0$ dans $\mathbb{Z}/p\mathbb{Z}[X]$

où si $F(X)=f_0+\dots+f_dX^d\in\mathbb{Z}[X]$, on pose $\overline{F}(X)=\overline{f_0}+\dots+\overline{f_d}X^d\in\mathbb{Z}/p\mathbb{Z}[X]$

Alors $\overline{P}\,\overline{Q}=0$ dans $\mathbb{Z}/p\mathbb{Z}[X]$

or $\mathbb{Z}/p\mathbb{Z}$ intègre $\Rightarrow \mathbb{Z}/p\mathbb{Z}[X]$ aussi $\Rightarrow \overline{P}$ ou $\overline{Q}=0$

$\Rightarrow p\mid c(P)$ ou $p\mid c(Q)$

absurde.

Donc $c(PQ)=1$.

Définition (factoriel)

On dit qu'un anneau A est factoriel si A intègre et si dans A « il y a existence et unicité de la factorisation en produit d'irréductibles »

c-à-d : i) $\forall a \in A^*$, $\exists u \in A^\times$, $\exists p_1, \dots, p_d \in A$ irréductibles, $a = u p_1 \cdots p_d$

ii) si $u p_1 \cdots p_d = v q_1 \cdots q_e$ avec $u, v \in A^\times$, p_i, q_j irréductibles alors $d = e$ et $\exists \sigma \in \mathfrak{S}_d$, $\forall 1 \le i \le d$, $p_i = u_i q_{\sigma(i)}$ pour des $u_i \in A^\times$.

ex : Principal $\Rightarrow$ Factoriel

contre-ex de la réciproque : $\mathbb{Z}[X]$ est factoriel mais non principal.

exo : $(2, X)$ n'est pas un idéal principal.

Contre-ex : $\mathbb{Z}[i\sqrt{5}] = \mathbb{Z} + \mathbb{Z} i\sqrt{5}$ est un anneau non factoriel

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

irréductible, 2 à 2 non associés

Définition Soit A factoriel

si $a, b \in A \setminus \{0\}$, on définit le pgcd noté $a \wedge b$:

si $a = u p_1^{\alpha_1} \cdots p_d^{\alpha_d}$ $u \in A^*$

$b = v p_1^{\beta_1} \cdots p_d^{\beta_d}$ $v \in A^*$ où p_i irréd 2 à 2 non associés ($\forall i \neq j$ $\frac{p_i}{p_j} \notin A^*$)

$\alpha_i, \beta_i \in \mathbb{N}$

$a \wedge b = p_1^{\delta_1} \cdots p_d^{\delta_d}$ où $\delta_j = \min\{\alpha_j, \beta_j\}$

Le ppcm : $a \vee b = p_1^{\delta_1} \cdots p_d^{\delta_d}$ où $\forall j$ $\delta_j = \max\{\alpha_j, \beta_j\}$

Théorème : A factoriel $\Rightarrow A[X]$ factoriel

de plus si $K = \mathrm{Frac}(A)$ corps des fractions.

$P \in A[X]$ irréductible $\iff$ $\begin{cases} \deg P = 0, P \in A \text{ irréductible} \\ \text{ou} \\ \deg P > 0 \text{ et } c(P) = 1 \text{ et } P \text{ irréductible sur } K \end{cases}$

ex : $X^3 - 3X + 1$ de contenu 1 irréductible sur $\mathbb{Z}$

$2X + 4$ de contenu 2 est irréductible sur $\mathbb{Q}$ mais non sur $\mathbb{Z}$.

Proposition (critère de la réduction modulo p).

Soit $P \in \mathbb{Z}[X]$. Soit p premier (dans $\mathbb{Z}$) tq $p \nmid$ coeff dominant de P

si $\overline{P} \in \mathbb{Z}/p\mathbb{Z}[X]$ est irréductible, alors P est irréductible sur $\mathbb{Q}$.

démo si $P = P_1 P_2$ $\quad P_1, P_2 \in \mathbb{Q}[X]$

soient $a_1, a_2 \neq 0$, entiers tq $a_1 P_1, a_2 P_2 \in \mathbb{Z}[X]$

Alors $a_1 a_2 P = a_1 P_1 \, a_2 P_2 \Rightarrow a_1 a_2 c(P) = c(a_1 P_1)\, c(a_2 P_2)$

$$\Rightarrow \frac{P}{c(P)} = \underbrace{\frac{a_1 P_1}{c(a_1 P_1)}}_{\in \mathbb{Z}[X]} \underbrace{\frac{a_2 P_2}{c(a_2 P_2)}}_{\in \mathbb{Z}[X]}$$

$$\Rightarrow \frac{\overline{P}}{c(P)} = \frac{\overline{a_1 P_1}}{c(a_1 P_1)} \frac{\overline{a_2 P_2}}{c(a_2 P_2)}$$

et $\deg \dfrac{\overline{a_i P_i}}{c(a_i P_i)} = \deg \dfrac{a_i P_i}{c(a_i P_i)}$

Or $\overline{P}$ irréductible $\Rightarrow \deg \dfrac{\overline{a_i P_i}}{c(a_i P_i)} = 0$ pour $i = 1$ ou 2 $\Rightarrow \deg P_i = 0$ pour $i = 1$ ou 2.

$\Rightarrow P_1$ ou P_2 constant.

Ex: $P = X^3 - 3X + 1$ $\mod 2$: $\overline{P} = X^3 + X + 1$ irréductible sur $\mathbb{Z}/2\mathbb{Z}$

donc P irréductible sur $\mathbb{Q}$.

$P = X^4 + X^3 + X^2 + X + 1$

Mod 2 : $\overline{P} = X^4 + X^3 + X^2 + X + 1$ irréductible sur $\mathbb{Z}/2\mathbb{Z}$

car pas de racine et $X^2 + X + 1 \nmid X^4 + X^3 + X^2 + X + 1$

$(X^2 + X + 1)^2 = X^4 + X^2 + 1$ (!!)

donc P irréductible sur $\mathbb{Q}$.

Contre-ex: $P = X^4 + 1$ est irréductible sur $\mathbb{Q}$.

mais $\overline{P}$ est réductible mod p ($\forall p$ premier)

$X^4 + 1 = (X+1)^4 \mod 2$

$X^4 + 1 = X^4 - 2X^2 + 1 + 2X^2 = (X^2 - 1)^2 - X^2 \mod 3$

$= (X^2 - X - 1)(X^2 + X + 1) \mod 3$

$X^4 + 1 = (X^2 + 2)(X^2 - 2) \mod 5.$

etc

Pause 5'