Arithmétique

1) Dans $\mathbb{Z}$: diviseurs, multiples, Bezout.
2) Dans un anneau principal : idéal, Bezout.
3) Irréductibles.

$n \in \mathbb{Z}$ $\qquad \mathrm{Div}(n) = \{k \in \mathbb{Z} \mid k \mid n\}$

$$\mathrm{Div}(12) = \{\pm 1, \pm 2, \pm 3, \pm 4, \pm 6, \pm 12\}$$

$$n\mathbb{Z} = \mathbb{Z}n = \{k.n,\ k \in \mathbb{Z}\}.$$

$a, b \in \mathbb{Z} \setminus \{0\}$ $\qquad \mathrm{Div}(a) \cap \mathrm{Div}(b)$

$$\mathrm{pgcd}(a,b) = \max(\mathrm{Div}(a) \cap \mathrm{Div}(b))$$

$$\mathrm{pgcd}(7, 27) = 1$$

$$\mathrm{pgcd}(156, 84) = 12$$

$27 = 3 \times 7 + 6$

$7 = 1 \times 6 + 1$

r	q
27	
7	3
6	1
$\boxed{1}$	6
0	

156	
84	1
72	1
$\boxed{12}$	6
0	

$$\mathrm{Div}(27) \cap \mathrm{Div}(7) \overset{?}{=} \mathrm{Div}(7) \cap \mathrm{Div}(27 - 3 \times 7)$$
$$= \mathrm{Div}(6) \cap \mathrm{Div}(7)$$
$$= \mathrm{Div}(6) \cap \mathrm{Div}(6+1)$$
$$= \mathrm{Div}(6) \cap \mathrm{Div}(1)$$
$$= \mathrm{Div}(1) = \{\pm 1\}$$

$$\mathrm{pgcd}(27, 7) = 1$$

$$\{27k + 7l,\ k, l \in \mathbb{Z}\} = 27\mathbb{Z} + 7\mathbb{Z} \overset{?}{=} 7\mathbb{Z} + (27 - 3 \times 7)\mathbb{Z}$$
$$= 7\mathbb{Z} + 6\mathbb{Z}$$
$$= (6+1)\mathbb{Z} + 6\mathbb{Z}$$
$$= 1\mathbb{Z} + 6\mathbb{Z}$$
$$= \mathbb{Z}$$

$$\mathrm{Div}(156) \cap \mathrm{Div}(84) = \mathrm{Div}(72) \cap \mathrm{Div}(84)$$
$$= \mathrm{Div}(12) \cap \mathrm{Div}(72)$$
$$= \mathrm{Div}(12)$$

$$156\mathbb{Z} + 84\mathbb{Z} = 72\mathbb{Z} + 84\mathbb{Z}$$
$$= 12\mathbb{Z} + 72\mathbb{Z}$$
$$= 12\mathbb{Z}$$

$\left[\begin{array}{ll} \exists\, k, \ell \in \mathbb{Z} \text{ tq. } & 1 = 27 \times k + 7 \times \ell \\ \exists\, m, n \in \mathbb{Z} \text{ tq. } & 12 = 156 \times k + 84 \times \ell \end{array}\right.$ identité de Bezout

$$27 = 3 \times 7 + 6 \qquad 27 - 3 \times 7 = 6$$
$$7 = 1 \times 6 + 1 \qquad 7 - 6 = 1$$
$$\underline{1} = 7 - (27 - 3 \times 7)$$
$$= 4 \times \underline{7} - \underline{27}$$
$$\mathbb{Z} = 7\mathbb{Z} + 27\mathbb{Z}$$

$(A, +, 0, \times, 1)$ anneau. $\qquad (A, +)$ gpe comm.

$(\mathbb{K}, +, 0, \times, 1)$ corps $\qquad (\mathbb{K}, +)$ gpe com.
$(\mathbb{K}^*, \times)$ gpe

A anneau commutatif et intègre
$(a \neq 0, b \neq 0 \Rightarrow ab \neq 0)$

__Ex__ : $\mathbb{Z}$, $\mathbb{K}[X]$ $\mathbb{K}$ corps $\qquad \mathbb{Z}/6\mathbb{Z}$ non intègre
$\bar{2} . \bar{3} = \bar{0}$

$a \in A \setminus \{0\}$ $\qquad \mathrm{Div}(a) = \{k \in A \text{ tq. } k \mid a\}$
$\Updownarrow$
$\exists \ell \in A$ tq $a = k.\ell$

$$aA = Aa = \{ka,\ k \in A\}$$

si $a, b \in A$, $\quad \mathrm{Div}(a) \cap \mathrm{Div}(b)$?

$$Aa + Ab = \{ka + \ell b,\ k, \ell \in A\}$$

__déf__ $I \subset A$ est un idéal de A __si__

- $0 \in I$
- (1) $\left[\begin{array}{l} \bullet\ \forall a, b \in I \quad a + b \in I \\ \bullet\ \forall a \in I\ \forall k \in A \quad k.a \in I \end{array}\right.$

(1) $\forall a, b \in I \quad \forall k, \ell \in A \qquad ka + \ell b \in I$

I est stable par C.L. à coef. dans A.

E $\mathbb{K}$-ev	A an.
F sev de E si	I idéal de A si
$\forall u, v \in F \ \forall \lambda, \mu \in \mathbb{K} \ \ \lambda u + \mu v \in F$	$\forall u, v \in I \ \forall a, b \in A \ \ au + bv \in I$
$u, v \in E \quad \mathrm{vect}(u,v) \to = \bigcap_{\substack{F \text{ sev de } E \\ u, v \in F}} F$	$u, v \in A$
	$\mathrm{Ideal}(u,v) = (u,v)$
$\to$ = p.p. sev de E contenant u, v (pmc)	$\to = \bigcap_{\substack{I \text{ id. de } A \\ u, v \in I}} I$
$\to = \{\lambda u + \mu v,\ \lambda, \mu \in \mathbb{K}\}$	$\to$ = p.p. idéal de A contenant u, v
$= \mathbb{R}u + \mathbb{R}v$	$\to = \{au + bv,\ a, b \in A\}$
	$= Au + Av$

Aa s'appelle un idéal principal.

Thm La division euclidienne dans $\mathbb{Z}$ (et dans $\mathbb{K}[X]$) fait que tout idéal de $\mathbb{Z}$ (et de $\mathbb{K}[X]$) est principal.

idée de la preuve: I idéal
a le "+ petit élt" de $I \setminus \{0\}$
$I = Aa$ ⊠

Théorème $a, b \in A$ principal, $\exists d \in A$
$\mathrm{ideal}(a,b) = Aa + Ab = Ad$.
On a alors $\mathrm{Div}(a) \cap \mathrm{Div}(b) = \mathrm{Div}(d)$

$\subseteq$ $d \in Ad$ $\exists u, v$ $d = au + bv$
$\supseteq$ car $Aa + Ab = Ad$

d s'appelle un pgcd de a et b.

$d \in Ad = Aa + Ab$

$\exists u, v \in A$ tq. $d = ua + vb$

identité de Bezout.

Soit A un anneau principal
($ex: A=\mathbb{Z}$ et $A=\mathbb{K}[X]$)

$\forall a,b\in A \quad \exists d\in A \quad Aa+Ab=Ad$
et $Div(a)\cap Div(b)=Div(d)$

$\boxed{A=\mathbb{Z}}$

$27\mathbb{Z}+7\mathbb{Z}=\mathbb{Z}$

$Div(27)\cap Div(7)=Div(1)=\{\pm 1\}$

$1=pgcd(27,7)$

$-27+4\times 7=1$

$-2\times 27+8\times 7=2$

$156\mathbb{Z}+84\mathbb{Z}=12\mathbb{Z}$

$12=pgcd(156,84)$

$Div(156)\cap Div(84)=Div(12)$

$-156+2\times 84=12$

$-2\times 156+4\times 84=24$

$\nexists k,l\in\mathbb{Z} \quad k\times 156+l\times 84=6$

$\boxed{A=\mathbb{K}[X]}$

$\mathbb{K}=\mathbb{R}$

$$\begin{aligned} A(X-1)+A(X+1) &= A(X-1)+A(X+1-(X-1)) \\ &= A(X-1)+2A \\ &= A(X-1)+A \\ &= A \end{aligned}$$

$pgcd(X-1,X+1)=1$

$pgcd(X-1,X+1)=2$

$Div(X-1)\cap Div(X+1)=Div(1)$

$-\frac{1}{2}(X-1)+\frac{1}{2}(X+1)=1$

$-(X-1)+(X+1)=2 \quad (\in Div(1))$

$Div(1)=Div(2)$

$-\frac{X}{2}(X-1)+\frac{X}{2}(X+1)=X$

$P=X^3+X-2=(X-1)(X^2+X+2)$

$Q=X^2-1=(X-1)(X+1)$

$$\begin{array}{r|l} X^3+X-2 & \\ X^2-1 & X \\ \hline \boxed{2(X-1)} & \frac{1}{2}(X+1) \\ 0 & \end{array}$$

un $pgcd(X^3+X-2,X^2-1)=2(X-1)$

$pgcd(X^3+X-2,X^2-1)=X-1$

$$\mathbb{R}[X](X^3+X-2) + \mathbb{R}[X](X^2-1) = \dots = \mathbb{R}[X]\, 2(X-1)$$
$$= \mathbb{R}[X](X-1)$$

$$\mathrm{Div}(X^3+X-2) \cap \mathrm{Div}(X^2-1) = \mathrm{Div}(X-1)$$

A qcq. $\quad \mathrm{Div}(1) = \{ a \in A \mid \exists b \in A \quad 1 = a.b \}$
$= \{ a \in A$ inversibles par $\times \}$
$=: A^\times = U(A)$

$A = \mathbb{Z} \quad \mathrm{Div}(1) = \{\pm 1\} = \mathbb{Z}^\times$

$A = \mathbb{K}[X] \quad \mathrm{Div}(1) = \{ P \in \mathbb{K}[X] \mid \exists Q \in \mathbb{K}[X] \quad 1 = P(X)Q(X) \}$

$\Downarrow$
$0 = \deg P + \deg Q$
$\Downarrow$
$\deg P = \deg Q = 0$
$\Downarrow$
$P \in \mathbb{K}^*$

$= \mathbb{K}^*$

$\underline{A = \mathbb{Z}} \quad \mathrm{Div}(6) = \{\pm 1, \pm 2, \pm 3, \pm 6\}$

$\underline{A = \mathbb{R}[X]} \quad \mathrm{Div}(X^2-1) = \{ \lambda, \lambda(X-1), \lambda(X+1), \lambda(X^2-1), \lambda \in \mathbb{R}^* \}$

$$X^2-1 = \lambda(X-1) \cdot \tfrac{1}{\lambda}(X+1)$$

A principal (ex : $\mathbb{Z}$, $\mathbb{K}[X]$ ...)

$a, b \in A \quad \exists d \in A \quad Aa + Ab = Ad$

Donc $\exists\, u, v \in A \quad \underline{ua + bv = d}$ $\quad$ Bezout.

Si $\exists\, u, v \in A \quad ua + vb = 1$, alors $\mathrm{pgcd}(a,b) = 1$

$Aa + Ab = A1 = A \qquad (\mathrm{Div}(a) \cap \mathrm{Div}(b) = \mathrm{Div}(1))$

On dit que a et b sont premiers entre eux.

Lemme de Gauss $\forall a, b, c \in A \quad a \wedge b = 1 \quad (\text{pgcd}(a,b)=1)$

$$a \mid bc \Rightarrow a \mid c$$

$$\left(A = \mathbb{Z} \qquad \underbrace{2^2 \times 3 \times 7} \mid \underbrace{5 \times 11} \times \underbrace{2^3 \times 3 \times 7^2} \right)$$

démo : Comme $\text{pgcd}(a,b) = 1$,

$\exists u, v \in A$ tq. $ua + vb = 1$

On a alors $\underline{uac} + v\underline{bc} = c$.

Si $a \mid bc$ $\quad a \mid u\underline{ac} + v\underline{bc} = c \quad \square$

Autres applications

- surjectivité $\mathbb{Z}/nm\mathbb{Z} \longrightarrow \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}$

lorsque $n \wedge m = 1$.

i.e. $\forall a, b \in \mathbb{Z} \quad \left| \begin{array}{l} x \equiv a\ [n] \\ x \equiv b\ [m] \end{array} \right.$

a une infinité de solution en $x \in \mathbb{Z}$, unique mod nm.

- $-27 + 4 \times 7 = 1$

Donc $4 \times 7 \equiv 1 \ [27]$

Donc $\bar{4} \times \bar{7} = \bar{1}$ dans $\mathbb{Z}/27\mathbb{Z}$.

Donc $\bar{7}$ est inversible dans $\mathbb{Z}/27\mathbb{Z}$, d'inverse 4.

Réciproquement $\forall a \in \mathbb{Z}$, $(\exists b \in \mathbb{Z}$ tq. $ab \equiv 1\ (27))$

$$\Updownarrow$$

$$\exists b, k \in \mathbb{Z} \quad ab + 27k = 1$$

$$\Updownarrow$$

$$a \wedge 27 = 1$$

Ex $3 \wedge 27 = 3$ Donc $\bar{3}$ n'est pas inversible dans $\mathbb{Z}/27\mathbb{Z}$

$\bar{3}.\bar{9} = \bar{0}$

si $\bar{3}\bar{a} = \bar{1}$ alors $\bar{3}.\bar{9}.\bar{a} = \bar{0} = \bar{9}$ impossible

$6 \wedge 27 = 3$ $\quad \bar{6}$ n'est pas inv. dans $\mathbb{Z}/27\mathbb{Z}$

$$\left(\mathbb{Z}/27\mathbb{Z}\right)^\times = \{\bar{1}, \bar{2}, \bar{4}, \bar{5}, \bar{7}, \bar{8}, \bar{10}, \bar{11}, \bar{13}, \bar{14}, \bar{16}, \bar{17}, \bar{19}, \bar{20}, \bar{22}, \bar{23}, \bar{25}, \bar{26}\}$$