Anneaux

1) Isomorphisme chinois

Théorème. Soit A anneau

Soient $I_1, \dots, I_n$ idéaux de A 2 à 2 étrangers

(c-à-d : $\forall i \neq j,\ I_i + I_j = A$)

Alors l'application $A/I_1 \cap \dots \cap I_n \xrightarrow{\simeq} A/I_1 \times \dots \times A/I_n$

$a + I_1 \cap \dots \cap I_n \longmapsto (a+I_1, \dots, a+I_n)$

est un isomorphisme d'anneaux.

De plus dans ce cas, $I_1 \cap \dots \cap I_n = I_1 \dots I_n = \{\text{idéal engendré par les } x_1 x_2 \dots x_n \text{ où } \forall i\ x_i \in I_i\}$

Exemple : si $m \wedge n = 1$ alors $\mathbb{Z}/mn\mathbb{Z} \xrightarrow{\simeq} \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$

$\Leftrightarrow m\mathbb{Z} + n\mathbb{Z} = \mathbb{Z}$ $\qquad a + mn\mathbb{Z} \longmapsto (a+m\mathbb{Z}, a+n\mathbb{Z})$

$\Rightarrow m\mathbb{Z} \cap n\mathbb{Z} = mn\mathbb{Z}$

démo (surjectivité)

Notation $\forall i,\ \widetilde{I_i} = \bigcap_{\substack{j=1 \\ j \neq i}}^{n} I_j$

Lemme : $\forall i\ \widetilde{I_i} + I_i = A$.

[En effet. $\forall j \neq i,\ \exists x_j \in I_j,\ y_j \in I_i,\ x_j + y_j = 1$

$\Rightarrow 1 = \prod_{\substack{j=1 \\ j \neq i}}^{n} (x_j + y_j) = \underbrace{\prod_{\substack{j=1 \\ j \neq i}}^{n} x_j}_{\in \widetilde{I_i}} + \underbrace{\dots}_{\in I_i}$]

$\forall 1 \leq i \leq n$ soient $X_i \in \widetilde{I_i}$, $Y_i \in I_i$ tq $X_i + Y_i = 1$

$\Rightarrow \forall i,\ X_i = 1 + I_i$ (dans A/I_i) et $X_i = 0 + I_j$ $(\forall j \neq i)$

Soient $\alpha_1, \dots, \alpha_n \in A$. Soit $x = \sum_{i=1}^{n} \alpha_i X_i$

Alors $x = \alpha_i + I_i$ $\quad (\forall i)$

c-à-d : $(x+I_1, x+I_2, \dots, x+I_n) = (\alpha_1 + I_1, \dots, \alpha_n + I_n)$ dans $A/I_1 \times \dots \times A/I_n$ □

Montrons de plus $I_1 \cap \dots \cap I_n = I_1 \dots I_n$

on a toujours $I_1 \dots I_n \subset I_1 \cap \dots \cap I_n$

si $n=2$ si $I+J=A$, alors $1 = x+y$ avec $x \in I$, $y \in J$.

Si $z \in I \cap J$, alors $z = z \cdot 1 = \underbrace{zx}_{\in IJ} + \underbrace{zy}_{\in IJ} \in IJ$.

de même pour n quelconque.

Exemple : Résoudre $\begin{cases} x = 3\,[5] \\ x = 2\,[6] \\ x = 9\,[23] \end{cases}$ $x \in \mathbb{Z}$

$5 \wedge 6 = 1$, $5 \wedge 23 = 1$, $6 \wedge 23 = 1$ } donc d'après le théorème chinois : $\mathbb{Z}/5\times6\times23\mathbb{Z} \xrightarrow{\sim} \mathbb{Z}/5\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z} \times \mathbb{Z}/23\mathbb{Z}$

$5 \times 6 \times 23 = 690$

$I_1 = 5\mathbb{Z}$, $I_2 = 6\mathbb{Z}$, $I_3 = 23\mathbb{Z}$

$\widehat{I}_i = b_i\mathbb{Z}$

$23 \times 6 = b_1 = 138$

$5 \times 23 = b_2 = 115$

$5 \times 6 = b_3 = 30$

$b_1 = -2\,[5] \Rightarrow b_1^{-1} = 2\,[5]$

$b_2 = 1\,[6] \Rightarrow b_2^{-1} = 1\,[6]$

$b_3 = 7\,[23] \Rightarrow b_3^{-1} = 10\,[23]$

} soit $x_0 = \underbrace{3 \times 138 \times 2}_{1\,[5]} + \underbrace{2 \times 115 \times 1}_{1\,[6]} + \underbrace{9 \times 30 \times 10}_{1\,[23]}$ $\quad 3 \times b_1 \times b_1^{-1} + 2 \times b_2 \times b_2^{-1} + 9 \times b_3 \times b_3^{-1}$

$x_0 = 3\,[5]$, $x = 2\,[6]$, $x = 9\,[23]$

Donc $\begin{cases} x = 3\,[5] \\ x = 2\,[6] \\ x = 9\,[3] \end{cases} \Leftrightarrow x = x_0\,[690] = 308\,[690]$.

Application : Calcul de $\varphi(n)$, Indicatrice d'Euler

Définition : Si $n \geq 1$, $\varphi(n) = \left|\{1 \leq k \leq n : k \wedge n = 1\}\right|$

Proposition a) $\forall m \wedge n = 1$, $\varphi(mn) = \varphi(m)\varphi(n)$

b) $\forall p$ premier, $\forall \alpha \in \mathbb{N}_{>0}$, $\varphi(p^\alpha) = p^\alpha - p^{\alpha-1} = p^{\alpha-1}(p-1)$

$\{p, 2p, \dots, p^{\alpha-1}p\}$ = multiples de p dans $[\![1, p^\alpha]\!]$

Ex : $\varphi(24) = \varphi(2^3 \times 3) = \varphi(2^3) \times \varphi(3) = (2^3 - 2^2) \times (3-1) = 12$

demo : a) $\mathbb{Z}/mn\mathbb{Z} \simeq \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$ isomorphisme d'anneaux

$(\mathbb{Z}/mn\mathbb{Z})^* \simeq (\mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z})^* = (\mathbb{Z}/m\mathbb{Z})^* \times (\mathbb{Z}/n\mathbb{Z})^*$ isomorphisme de groupes

$\Rightarrow |(\mathbb{Z}/mn\mathbb{Z})^*| = |(\mathbb{Z}/m\mathbb{Z})^*| \cdot |(\mathbb{Z}/n\mathbb{Z})^*|$

Or $\forall q$, $|(\mathbb{Z}/q\mathbb{Z})^*| = \varphi(q)$ $\quad (\mathbb{Z}/q\mathbb{Z})^* = \{\bar{k} : 1 \leq k \leq q, k \wedge q = 1\}$

$\Rightarrow \varphi(mn) = \varphi(m)\varphi(n)$

Propriétés de φ : 1) $\sum_{d \mid n} \varphi(d) = n$

2) $\varphi(n) = \sum_{d \mid n} d\,\mu\left(\frac{n}{d}\right)$ où $\mu(k) = \begin{cases} (-1)^s \text{ si } k = p_1 \cdots p_s \\ 0 \text{ sinon} \end{cases}$ (μ de Möbius), p_i premiers distincts

demo 1) $\Rightarrow$ 2) fait général

1) : $\left\{\frac{1}{n}, \frac{2}{n}, \dots, \frac{n}{n}\right\} = \bigsqcup_{d \mid n} \left\{\frac{k}{d} : 1 \leq k \leq d, k \wedge d = 1\right\}$ ($\varphi(d)$ éléments)

Ex. $\mathbb{C}[X]/(X^2+1) \simeq \mathbb{C}[X]/(X+i) \times \mathbb{C}[X]/(X-i)$

$\simeq \mathbb{C} \times \mathbb{C}$

(car par ex. $\mathbb{C}[X] \to \mathbb{C}$, $P(X) \mapsto P(i)$ surjectif de noyau $(X-i) \overset{\text{1er thm d'iso}}{\Longrightarrow} \mathbb{C}[X]/(X-i) \simeq \mathbb{C}$)

2) Anneaux principaux

Définition. A est un anneau principal si A est intègre et $\forall I \leq A$ idéal, $\exists x \in A$, $I = (x) = Ax$

ex $A = \mathbb{Z}$ (*), $A = K[X]$ (K corps) (**), $A = \mathbb{D}$ (décimaux), ~~$A = \mathbb{Z}[i] = \{a+ib : a,b \in \mathbb{Z}\}$~~, etc

(*) : si $0 \neq I \subset \mathbb{Z}$ idéal, soit $x \in I$ tq $0 < |x|$ minimale. Alors $I = (x)$

(**) : Si $0 \neq I \leq K[X]$ soit $P \in I$ tq $\deg P$ minimal, alors $I = (P)$

Contre-exemples : $\mathbb{Z}[X]$, $\mathbb{R}[X,Y]$, $\mathbb{Z}[i\sqrt{5}]$ ne sont pas principaux

car $(2,X)$ n'est pas principal dans $\mathbb{Z}[X]$ (exo)

(X,Y) n'est pas principal dans $\mathbb{R}[X,Y]$ (exo)

$(2, 1+i\sqrt{5})$ n'est pas principal dans $\mathbb{Z}[i\sqrt{5}] = \mathbb{Z} + i\sqrt{5}\mathbb{Z}$ (*)

(*) on pose $\forall \alpha \in \mathbb{C}$, $N(\alpha) = |\alpha|^2$

$\forall \alpha = x + i\sqrt{5}y \in \mathbb{Z} + i\sqrt{5}\mathbb{Z}$, $N(\alpha) = x^2 + 5y^2 \in \mathbb{N}$

$\forall \alpha, \beta \in A = \mathbb{Z}[i\sqrt{5}]$, $N(\alpha\beta) = N(\alpha)N(\beta)$, $N(1) = 1$

donc $A^* = \{\pm 1\}$ si $\alpha \in A^*$, $\underbrace{N(\alpha)}_{\in \mathbb{N}} \underbrace{N(\alpha^{-1})}_{\in \mathbb{N}} = N(1) = 1$

$\Rightarrow N(\alpha) = 1$

On $x^2 + 5y^2 = 1$, $x, y \in \mathbb{Z} \Rightarrow y = 0$, $x = \pm 1$.

si (par l'absurde) $(\alpha) = (2, 1+i\sqrt{5})$ alors $\alpha \mid 2 \Rightarrow N(\alpha) \mid N(2) = 4$

$\Rightarrow N(\alpha) = 1$ ou 2 ou ~~3~~

or $N(\alpha) = 1 \Rightarrow \alpha \in A^* \Rightarrow (2, 1+i\sqrt{5}) = (1)$ IMPOSSIBLE (***)

$N(\alpha) = 2$ impossible ($x^2 + 5y^2 = 2$ n'a pas de solution)

On $\alpha \mid 1+i\sqrt{5} \Rightarrow N(\alpha) \mid N(1+i\sqrt{5}) = 6 \Rightarrow N(\alpha) = 1$ ou 2 ou ~~3~~.

(***) $\mathbb{Z}[i\sqrt{5}]/(2, 1+i\sqrt{5}) \simeq \mathbb{Z}/2\mathbb{Z}$

car $\mathbb{Z}[i\sqrt{5}] \to \mathbb{Z}/2\mathbb{Z}$, $a + ib\sqrt{5} \mapsto a+b \bmod 2$ morphisme d'anneaux

a pour noyau $(2, 1+i\sqrt{5})$

$\Rightarrow 14 (2, 1+i\sqrt{5})$.

Définition. Soit A anneau intègre.
On dit que A est <u>euclidien</u> s'il existe
$N : A \setminus \{0\} \longrightarrow \mathbb{N}$ (stathme)
tq : $\forall a \in A, \forall\, 0 \neq b \in A, \exists q, r \in A,\ a = bq + r$ avec $r = 0$ ou $r \neq 0$ et $N(r) < N(b)$.

ex : Pour $\forall x \in \mathbb{Z},\ N(x) = |x|$
$\forall P \in K[X],\ N(P) = \deg P$
$\forall \alpha \in \mathbb{Z}[i],\ N(\alpha) = |\alpha|^2$
$\forall x \in \mathbb{D},\ N(x) = \min \{ |10^n x| : 10^n x \in \mathbb{Z} \}$.

Théorème : euclidien $\Rightarrow$ principal

<u>démo</u> Soit $0 \neq I \lhd A$ idéal
Soit $x \in I$ tq $x \neq 0$ et $N(x)$ minimal
Si $z \in I$, $z = xq + r$ avec $r = 0 \Rightarrow z \in (x)$
ou $r \neq 0$ et $N(r) < N(x)$
On $r = z - xq \in I$ CONTRADICTION. □

Contre-exemples de la réciproque : $\mathbb{Z}\left[\frac{1+i\sqrt{19}}{2}\right]$, $\mathbb{R}[X,Y]/(X^2+Y^2+1)$ } anneaux principaux non euclidiens.

Pgcd et Ppcm dans les anneaux principaux.

Définition. Soient $a_1, \dots, a_n \in A$ anneau principal
a) il existe $d \in A$ tq $(d) = (a_1) + \dots + (a_n)$ noté $d = a_1 \wedge \dots \wedge a_n$
($x, y \neq 0$) (défini à multiplication par un $u \in A^*$ près)
$(x) = (y) \Leftrightarrow \exists u \in A^*,\ y = ax$
$d = a_1 \wedge \dots \wedge a_n$ est le pgcd de $a_1, \dots, a_n$
c-à-d : si $x \in A$, alors $\forall i\ x | a_i \Leftrightarrow x | d$
[Car $d = a_1 x_1 + \dots + a_n x_n$ pour des $x_i \in A$]

b) il existe $q \in A$ tq $(q) = (a_1) \cap \dots \cap (a_n)$ noté $q = a_1 \vee \dots \vee a_n$
· $q = a_1 \vee \dots \vee a_n$ est le ppcm de $a_1, \dots, a_n$
c-à-d : si $x \in A$, alors $\forall i\ a_i | x \Leftrightarrow q | x$ □

Proposition : $\forall a,b \in A^*$, $(a \wedge b)\cdot(a \vee b) = (ab)$

c-à-d : $\exists u \in A^*$, $a \wedge b \cdot a \vee b = uab$

démo : il suffit de le faire si $a \wedge b = 1$

si $a \wedge b = 1$ alors $\exists u, v \in A$, $au + bv = 1$

si $a|q$ et $b|q$ alors $q = q.1 = qau + qbv$

$a|q \to ab|qb \Rightarrow ab|qbv$
$b|q \Rightarrow ab|aq|aqu \Rightarrow ab|aqu$
$\Big\} \Rightarrow ab|q$. □

Lemme de Gauss : Soit A principal

si $a, b, c \in A$, alors $a|bc$ et $a \wedge b = 1 \Longrightarrow a|c$.

démo : $1 = au + bv$ $\quad u, v \in A$

$\Rightarrow c = c.1 = (au+bv)c = \underbrace{auc}_{a|} + \underbrace{bcv}_{a|} \Rightarrow a|c$. □

3) Algorithme d'Euclide

Soit A euclidien

Soient $a, b \in A$, $0 \neq b$

on pose $a_0 = a$, $a_1 = b$ et $\forall n$, $a_n \neq 0$, $a_{n-1} = q_n a_n + a_{n+1}$ $\quad q_n \in A$ (division euclidienne)

$a_{n+1} = 0$ ou $N(a_{n+1}) < N(a_n)$

Comme $(N(a_n))_n \downarrow$ décroit strictement « ça s'arrête ».

Le dernier terme $a_N \neq 0$ est le pgcd de a et b.

Démo : $a_{n-1} = q_n a_n + a_{n+1} \Longrightarrow a_{n-1} \wedge a_n = a_n \wedge a_{n+1}$.

Rem. Si $\forall n$ $u_n a + v_n b = a_n$

alors $u_N a + v_N b = a \wedge b$.

Il suffit de poser $u_0 = 1$, $v_0 = 0$, $u_1 = 0$, $v_1 = 1$

et $u_{n+1} = u_{n-1} - q_n u_n$, $v_{n+1} = v_{n-1} - q_n v_n$

---

ex $a = 214$, $b = 147$

n	$a_{n-1} = q_n a_n + a_{n+1}$	u_n	v_n
0		1	0
1		0	1
2	$214 = 147 \times 1 + 67$	1	−1
3	$147 = 67 \times 2 + 13$	−2	3
4	$67 = 13 \times 5 + 2$	11	−16
5	$13 = 2 \times 6 + 1$	−68	99

$\Rightarrow \underline{1 = -68 \times 214 + 99 \times 147}$

Pause = 5'.