Chap 12 : Anneaux

A est un anneau (unitaire)

I. Généralités

Revoir : élts inversibles / diviseurs de 0 / nilpotents, intégrité, morphismes, noyaux, produits, unités

On dit que l'élément $a \in A$ est régulier à gauche lorsque : $\forall (x,y) \in A^2, ax = ay \Rightarrow x = y$

On définit de même la régularité à droite

a est régulier à gauche $\Leftrightarrow \forall b \in A, ab = 0 \Rightarrow b = 0$ (*i.e* : a n'est pas diviseur de 0 à gauche)

A intègre $\Rightarrow$ Tout élément non nul est régulier. Si a est inversible, il est régulier

II. Idéaux

$I \subset A$ est
- Un idéal à gauche de A lorsque $(I,+)$ est un ss-gpe de A et : $\forall (a,x) \in A \times I, ax \in I$
- Un idéal à droite de A lorsque $(I,+)$ est un ss-gpe de A et : $\forall (a,x) \in A \times I, xa \in I$
- Un idéal bilatère de A lorsque I est un idéal à droite et à gauche

A commutatif $\Rightarrow$ Notions équivalentes || I idéal [] de A, $1 \in I \Leftrightarrow I = A$

$\{0\}, A, \ker f$ (où f morphisme d'anneaux) sont des idéaux bilatères

$f : A \to B$ morphisme d'anneaux, J idéal de $B \Rightarrow f^{-1}(J)$ idéal de A (FAUX pour l'image directe)

Dans toute la suite, A sera commutatif

L'intersection d'une famille d'idéaux de A est un idéal de A || $\forall X \subset A, \mathcal{I}(X) = \bigcap_{\substack{I \text{ idéal} \\ X \subset I}} I$ est l'idéal engendré par X

I, J idéaux de A. $I + J = \{x + y / (x,y) \in I \times J\}$ est un idéal, c'est le plus petit contenant I et J

L'idéal de A de I est dit principal lorsque : $\exists a \in A, I = \mathcal{I}(a) = aA$

A (commutatif) est un corps *ssi* ses seuls idéaux sont $\{0\}$ et A

On dit qu'un idéal I de A est premier lorsque : $\forall (x,y) \in A^2, xy \in I \Rightarrow x \in I$ ou $y \in I$

Un idéal I de A est dit maximal lorsque : $I \neq A$ et $\forall J$ idéal de A, $(I \subset J \Rightarrow I = J$ ou $J = A)$

A intègre $\Rightarrow \{0\}$ est premier (maximal si A est un corps) || p premier $\geq 2 \Rightarrow p\mathbb{Z}$ est maximal

I maximal et $x \notin I \Rightarrow I + Ax = A$

I idéal maximal de $A \Rightarrow I$ est premier (P.abs $\to I + Ax = A \to 1 \in I$)

III. Divisibilité

A commutatif et intègre

$(a,b) \in A^2$. On dit que a divise b $(a \mid b)$ lorsqu'il existe $c \in A$ tel que $b = ac$ Cette relation est transitive

$\forall a \in A, a \mid 0$ $0 \mid b \Rightarrow b = 0$

$^{(I)} a \mid b \Leftrightarrow bA \subset aA$ || $a \mid b$ et $b \mid a \Leftrightarrow aA = bA \Leftrightarrow a$ et b sont associés : $\exists u \in U(A), b = au$

$(a,b)\in A^2$. On dit que $d\in A$ est un pgcd de (a,b) lorsque : $\forall c\in A,(c\mid d\Leftrightarrow(c\mid a \text{ et } c\mid b))$

$(a,b)\in A^2$, d un pgcd de (a,b). $d'\in A$ est un pgcd de (a,b) *ssi* d et d' sont associés

L'anneau A est principal lorsqu'il est commutatif, intègre, et tout idéal de A est principal $(\forall I,\exists a\in A, I=aA)$

$\mathbb{Z}$ est principal. $\mathbb{K}$ corps commutatif $\Rightarrow\mathbb{K}[X]$ est principal (si l'on impose P_0 normalisé, il est unique)

Dans la suite, A est principal

$(a,b)\in A^2$. Il existe $d\in A$ qui est un pgcd de (a,b)

a est b sont premiers entre eux lorsque leurs seuls diviseurs communs sont les éléments inversibles

$(a,b)\in A^2$ a et b sont premiers entre eux $\Leftrightarrow\exists(u,v)\in A^2, au+bv=1$

Gauss : $(a,b,c)\in A^2$ avec a et b premiers entre eux : $a\mid bc\Rightarrow a\mid c$ || a premier avec b et $c\Rightarrow$ avec bc

$p\in A\setminus\{0\}$ est irréductible lorsque p est non inversible et ($p=ab\Rightarrow a$ ou b inversible)

p irréductible dans A $\forall a\in A$, on a soit $p\mid a$, soit p premier avec a || $\forall(a,b)\in A^2, p\mid ab\Rightarrow p\mid a$ ou $p\mid b$
Si p et q sont irréductibles non associés, ils sont premiers entre eux

Tout anneau principal est noethérien : Si (I_n) est une suite croissante d'idéaux de A, elle est constante apcr

$\cup I_n$ est un idéal, il est donc de la forme aA, il existe un rang à partir duquel $a\in I_n$

A anneau principal, $a\in A\setminus\{0\}.\exists\varepsilon\in U(A)$ et $p_1...p_r$ irréductibles tq : $a=\varepsilon p_1...p_r$

P.abs : a ni inv, ni irréd, ni prod d'irréd $\Rightarrow a=a_1b_1$ où a_1 et b_1 non inv, l'un des deux n'est pas prod. d'irréd
$...a_n=a_{n+1}b_{n+1}\Rightarrow aI\subsetneq a_1I\subsetneq a_2I\subsetneq...\subsetneq a_nI\subsetneq...\Rightarrow$ suite croissante strictement croissante : non

$(u,v)\in U(A)^2, p_1...p_r, q_1...q_s$ éléments irréd. de A. $up_1...p_r=vp_1...p_s\Rightarrow r=s$ et $\exists\sigma\in\mathfrak{S}_r, \forall i, p_i$ et $q_{\sigma(i)}$ associés

On choisit un ensemble $\mathcal{P}$ de représentants des irréductibles de A : $\forall q$ irred, $\exists p\in\mathcal{P}$, p associé à q

Tout élément $a\in A\setminus\{0\}$ s'écrit de manière unique $a=u\prod_{i=1}^{r}p_i^{\alpha_i}$, $p_1...p_r\in\mathcal{P},\alpha_1...\alpha_r\in\mathbb{N}, u\in U(A)$

a et $b\in A\setminus\{0\}$, avec $a=u\prod_{i=1}^{r}p_i^{\alpha_i}, b=v\prod_{i=1}^{r}p_i^{\beta_i}$ $a\mid b\Leftrightarrow\forall i\in\ 1,r\ ,\beta_i\geq\alpha_i$

$$\text{ppcm}(a,b)=\prod_{i=1}^{r}p_i^{\max(\alpha_i,\beta_i)} \qquad \text{pgcd}(a,b)=\prod_{i=1}^{r}p_i^{\min(\alpha_i,\beta_i)}$$

IV. Anneaux de polynômes

$\mathbb{K}$ corps commutatif. $\mathbb{K}[X]$ est principal.

$\Rightarrow\mathbb{K}[X]$ est factoriel : si $\mathcal{P}=\{P\in\mathbb{K}[X]$ irréductible normalisé$\}$, tout $P\in\mathbb{K}[X]$ s'écrit de manière unique

$$P=u\prod_{i=1}^{r}\pi_i^{\alpha_i} \quad \text{où } u\in\mathbb{K}^*,\ \pi_1...\pi_r\in\mathcal{P} \text{ et } \alpha_1...\alpha_r\in\mathbb{N}^*$$

Si A est un anneau (intègre, comm), $A[X]$ n'est PAS TOUJOURS principal

Les irréductibles de $\mathbb{C}$ sont de degré 1 car $\mathbb{C}$ est algébriquement clos

Les irréductibles de $\mathbb{R}$ sont de degré 1 ou 2

> ${}^{(I)}P \in \mathbb{R}[X]$ scindé $\Rightarrow P'$ est scindé dans $\mathbb{R}[X]$ (extrema entre 2 racines)

Les irréductibles de $\mathbb{Q}[X]$ sont de tous degrés ($\forall n \geq 1, X^n - 2$ est irréductible dans $\mathbb{Q}[X]$)

> P irréd de $\mathbb{Q}[X] \Rightarrow$ racines complexes simples $(\text{pgcd}(P,P') = 1, UP + VP' = 1 \Rightarrow V(\alpha)P(\alpha) = 1)$
>
> $P \in \mathbb{Q}[X]$ $\deg P = 5$ Racine double complexe $\Rightarrow \exists$racine rationnelle $(P = QR, Q \wedge R \to 2^e$ racine)