II Anneaux

§1 Rappels sur la théorie des anneaux

Rappelons la définition d'un anneau:

Déf. Un anneau A est un ensemble muni de deux lois notées $+$ et $\cdot$ vérifiant les conditions suivantes:
1) $(A,+)$ est un groupe abélien
2) la loi $\cdot$ est distributive par rapport à $+$
3) la loi $\cdot$ est associative

Un anneau A est unitaire si de plus
4) il existe un élt neutre pour la loi $\cdot$.

Un anneau A est commutatif si
5) la loi $\cdot$ est commutative.

Dans la suite, on considérera surtout des anneaux unitaires commutatifs

Exemples: 1) $(\mathbb{Z},+,\cdot)$ est un anneau unitaire commutatif

2) Si A est un anneau unitaire commutatif l'ensemble de matrices carrées $n\times n$ $M_{n\times n}(A)$ muni des lois d'addition et multiplication matricielles, est un anneau unitaire

3) Si A est un anneau, l'ensemble des polynômes en X (une indéterminée) et à coefficients dans A est un anneau sous les lois polynomiales: $A[X]$. Par itération, on obtient

$$A[X_1,\dots,X_n] = (A[X_1,\dots,X_{n-1}])[X_n]$$

4) $A[X_1,\dots,X_n,X_{n+1},\dots] = \bigcup_{n=0}^{\infty} A[X_1,\dots,X_n]$ est un anneau.

Dans la suite on dira simplement "anneau" au lieu de "anneau commutatif unitaire" sauf cas exceptionnel.

Déf. Soit A un anneau. A est intègre si
1) $A \neq \{0\}$
2) si $a, b \in A$ avec $ab = 0$, alors $a = 0$ ou $b = 0$

A est un corps
1) $A \neq \{0\}$
2) tout élt $a \in A^* = A \setminus \{0\}$ est inversible multiplicativement

Un corps est intègre, mais la réciproque est fausse.

Déf. Soit A un anneau. Un idéal de A est un sous-ensemble I de A ayant les propriétés suivantes:
1) $0 \in I$
2) $x, y \in I \Rightarrow x + y \in I$
3) $a \in A, x \in I \Rightarrow ax \in I$

L'exemple motivant d'un idéal est le noyau d'un morphisme d'anneaux. En fait, tout idéal est le noyau d'un morphisme. C'est la construction de l'anneau quotient qui le prouve.

Prop. Soit $\mathcal{J}$ un ensemble d'idéaux d'un anneau A. Alors, l'intersection

$$\bigcap \mathcal{J} = \{x \in A \mid \forall I \in \mathcal{J}, x \in I\}$$

est un idéal de A.

Démo: exo

Corollaire. Soit $S \subseteq A$ un sous-ensemble d'un anneau A. Alors, il existe un plus petit idéal I de A contenant S.

Déf. Soit $S \subseteq A$. Le plus petit idéal I de A contenant S est l'idéal engendré par S et est noté (S)

Plus explicitement :

Prop Soit $S \subseteq A$ un sous-ensemble. Alors

$$(S) = \left\{ \sum_{i=1}^{n} a_i s_i \;\middle|\; a_i \in A,\ s_i \in S,\ n \in \mathbb{N} \right\}$$

Déf. Soit I un idéal de A. Une <u>famille génératrice</u> de I est un sous-ens S de A tq $(S) = I$ (on a forcément $S \subseteq I$). On dit que I est de <u>type fini</u> s'il admet une famille génératrice finie.

Exemple 1) $(X_1, X_2, \dots) \subseteq \mathbb{Z}[X_1, X_2, \dots]$ n'est pas de type fini (exo)

2) Un idéal est forcément un sous-groupe abélien de l'anneau. Donc les idéaux de $\mathbb{Z}$ sont les sous-ensembles de la forme $n\mathbb{Z} = (n)$. Tous les idéaux de $\mathbb{Z}$ peuvent être engendrés par un seul élément (idéal principal). Ils sont donc tous de type fini

3) De même pour $K[X]$, K un corps.

4) $K[X,Y] \supseteq (X,Y)$ n'est pas principal (exo) mais clairement de type fini

5) $\mathbb{Z}[X] \supseteq (2, X)$ n'est pas principal (exo) mais encore clairement de type fini.

Déf Un anneau est <u>noethérien</u> si tous ses idéaux sont de type fini.

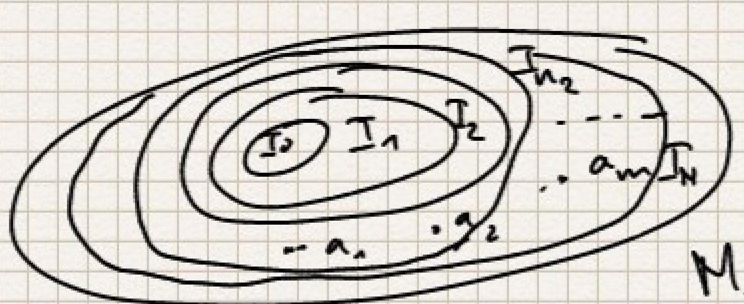
Un anneau principal est noethérien, mais la classe des anneaux noethériens est bien plus vaste que celle des anneaux principaux comme on verra.

Prop. Soit A un anneau. Alors A est noethérien si et seulement si toute chaîne croissante d'idéaux de A

$$I_0 \subseteq I_1 \subseteq I_2 \subseteq \dots \subseteq I_n \subseteq I_{n+1} \subseteq \dots$$

est stationnaire, i.e, il existe $N \in \mathbb{N}$ tq. $\forall k \in \mathbb{N}$: $I_{N+k} = I_N$.

Démo : Supposons que A est noethérien.
Soit $I_0 \subseteq I_1 \subseteq I_2 \subseteq \dots$ une chaîne croissante d'idéaux de A. Soit $I = \bigcup_{n=0}^{\infty} I_n$ la réunion de tous ces idéaux.
I est un idéal de A, $I = \{x \in A \mid \exists n \in \mathbb{N}\ x \in I_n\}$
Comme A est noethérien, I est de type fini. Il existe donc $a_1, \dots, a_m \in I$ tels que
$$I = (a_1, \dots, a_m)$$
Comme $a_i \in I$, il existe $n_i \in \mathbb{N}$: $a_i \in I_{n_i}$ pour $i = 1, \dots, m$



I Soit $N = \max\{n_1, \dots, n_m\}$
$$a_i \in I_{n_i} \subseteq I_N$$
Montrons que $I_N = I$
Comme $I = \bigcup I_n$, $I \supseteq I_N$
Réciproquement
$$I = (a_1, \dots, a_m) \subseteq I_N$$
car $a_1, \dots, a_m \in I_N$. D'où $I = I_N$
Pour $k \in \mathbb{N}$:
$$I = I_N \subseteq I_{N+k} \subseteq I$$
et $I_{N+k} = I_N$, c-à-d la chaîne est stationnaire.
Supposons maintenant que toute chaîne croissante d'idéaux de A est stationnaire, et montrons que A est noethérien. Soit I un idéal de A. On montre que I est de type fini par l'absurde. Supposons donc que I n'est pas de type fini.
Construisons une chaîne croissante d'idéaux de A non stationnaire par récurrence.
Soit $a_0 \in I$ et posons $I_0 = (a_0)$
Comme I n'est pas de type fini
$$I_0 = (a_0) \subsetneq I$$
Soit $a_1 \in I \setminus I_0$ et posons $I_1 = (a_0, a_1)$
On a $I_0 \subseteq I_1 = (a_0, a_1) \subsetneq I$.
Soit $a_2 \in I \setminus I_1$ et posons $I_2 = (a_0, a_1, a_2)$

On construit ainsi par récurrence une chaîne croissante d'idéaux de A

$$(a_0) \subseteq (a_0, a_1) \subseteq (a_0, a_1, a_2) \subseteq \dots$$

telle que $a_{n+1} \in I \setminus (a_0, \dots, a_n) = I_n$
Comme toute chaîne croissante d'idéaux de A est stationnaire, il existe $N \in \mathbb{N}$ tel que

$$a_{N+1} \in (a_0, \dots, a_N)$$

ce qui contredit la construction de la chaîne d'idéaux car $a_{N+1} \in I \setminus (a_0, \dots a_N)$ ⊠

<u>Déf.</u> Soit A un anneau. Soit $P \in A[X]$
Écrivons $P = a_0 + a_1 X + \dots + a_d X^d$
où $a_d \neq 0$ si $P \neq 0$. Le <u>degré</u> de P est défini par

$$\deg(P) = \begin{cases} d & \text{si } P \neq 0 \\ -\infty & \text{si } P = 0 \end{cases}$$

On a les règles de calcul suivantes :

1) $\deg(P+Q) \leq \max\{\deg(P), \deg(Q)\}$
2) $\deg(PQ) \leq \deg(P) + \deg(Q)$

<u>Théorème de la base d'Hilbert</u>

Soit A un anneau noethérien. Alors $A[X]$ est noethérien.

<u>Démo</u> : Par l'absurde : supposons que I est un idéal de $A[X]$ non de type fini.
On va construire par récurrence une suite de polynômes $P_1, P_2, P_3, \dots \in I$.
Comme $I \neq (0) = \{0\}$, soit $P_1 \in I \setminus (0)$ du plus bas degré. Comme $(P_1) \subsetneq I$, il existe $P_2 \in I \setminus (P_1)$ de plus bas degré.
En itérant on choisit $P_{n+1} \in I \setminus (P_1, \dots, P_n)$ de plus bas degré.
Soit $d_i = \deg P_i \in \mathbb{N}$ car $P_i \neq 0$
Soit a_i le coeff. dominant de P_i.
Considérons la chaîne croissante d'idéaux de A

$$(a_1) \subseteq (a_1, a_2) \subseteq (a_1, a_2, a_3) \subseteq \dots$$

Comme A est noethérien, cette chaîne est stationnaire d'après la prop précédente. Il existe donc $n \in \mathbb{N}$ tel que

$$a_{n+1} \in (a_1, \dots, a_n)$$

Il existe donc $b_1, \dots, b_n \in A$ tels que

$$a_{n+1} = b_1 a_1 + b_2 a_2 + \dots + b_n a_n$$

Soit

$$Q = P_{n+1} - \sum_{i=1}^{n} b_i X^{d_{n+1} - d_i} P_i \in A[X]$$

car $d_{n+1} \geq d_i$ $i = 1, \dots, n$. De plus $Q \in I$ et $Q \notin (P_1, \dots, P_n)$, sinon on aurait $P_{n+1} \in (P_1, \dots, P_n)$.

Quel est le coefficient de Q devant $X^{d_{n+1}}$? Il vaut

$$a_{n+1} - \sum_{i=1}^{n} b_i a_i = 0.$$

Du coup, $\deg(Q) < d_{n+1} = \deg P_{n+1}$. Cela contredit la construction de P_{n+1}. Par conséquent I est de type fini. ☐

<u>Corollaire</u> Soit A un anneau noethérien. Alors $A[X_1, \dots X_n]$ est noethérien

Exemples:

1) $\mathbb{Z}[X_1, \dots, X_n]$ est noethérien, $n \in \mathbb{N}$
2) $K[X_1, \dots, X_n]$ est noethérien, $n \in \mathbb{N}$. où K est un corps