Anneaux et Idéaux

Dans toute la suite un anneau est supposé commutatif et unitaire. On notera 1 ou 1_A l'élément unité de A (et on notera 0 l'élément neutre pour l'addition).

On dit que $a \in A$ est inversible (ou est une unité de A) s'il existe $b \in A$ tel que $ab = 1$. Si $b = a\alpha$ avec α inversible on dit que a et b sont associés.

On dit que A est un corps si tout élément non nul de A est inversible.

On dit que A est intègre si $ab = 0 \Rightarrow a = 0$ ou $b = 0$. Tout anneau intègre qui n'a qu'un nombre fini d'éléments est un corps.

Morphisme

Un morphisme f d'un anneau A dans un anneau B est une application f de A dans B telle que
$f(x + y) = f(x) + f(y)$
$f(xy) = f(x)f(y)$
$f(1) = 1$
Un isomorphisme est un morphisme bijectif.

Eléments inversibles

Les éléments inversibles d'un anneau A forment un groupe pour la multiplication noté $U(A)$ ou $A^\times$. Si A et B sont isomorphes les groupes $U(A)$ et $U(B)$ sont isomorphes.

On a $U(A[X]) = U(A)$.

Sous-anneau

On dit qu'un sous-ensemble A d'un anneau B est un sous-anneau de B si pour tous x et y dans A on a
$x + y \in A$
$xy \in A$
$1 \in A$

Anneau produit

Si A et B sont deux anneaux, l'anneau produit $A \times B$ est défini par les lois
$(a, b) + (c, d) = (a + c, b + d)$
$(a, b)(c, d) = (ac, bd)$
On a $U(A \times B = U(A) \times U(B)$

Idéaux

Les seules relations d'équivalence sur un anneau A compatibles avec les lois de A sont du type

$$x \sim y \Leftrightarrow x - y \in I$$

où $I \subset A$ est un idéal de A c'est à dire:
$0 \in I$
$x \in I, y \in I \Rightarrow x + y \in I$
$x \in I, a \in A \Rightarrow ax \in I$
On notera aussi $x - y \in I$ par $x = y \bmod I$.
L'ensemble des classes d'équivalence est $A/I = \{\widehat{a} | a \in A\}$, il est muni d'une structure d'anneau par les opérations

$$\begin{array}{rcl} (\widehat{a}, \widehat{b}) & \mapsto & \widehat{a + b} \\ (\widehat{a}, \widehat{b}) & \mapsto & \widehat{ab} \end{array}$$

La projection canonique $p_I : A \to A/I$ est un morphisme d'anneaux.

Remarques

a) $\{0\}$ et A sont des idéaux de A
b) Si un idéal I contient un élément inversible de A alors il contient 1 et donc il est égal à A.
c) L'intersection d'idéaux de A est un idéal de A.

Propriétés

1) Soit A un sous-anneau de B. Si I est un idéal de B avec $I \subset A$ alors I est un idéal de A.
Mais il peut y avoir des idéaux de A qui ne sont pas des idéaux de B.
2) Soit f un morphisme de A dans un anneau B
a) si J est un idéal de B alors $f^{-1}(J) = \{x \in A | f(x) \in J\}$ est un idéal de A.
En particulier $Ker(f) = f^{-1}(0) = \{x \in A | f(x) = 0\}$ est un idéal de A et on a le diagramme

$$\begin{array}{ccc} A & \to & B \\ \downarrow & & \uparrow \\ A/Ker(f) & \longleftrightarrow & f(A) \end{array}$$

b) si I est un idéal de A alors $f(I) = \{y \in B | y = f(x), x \in I\}$ est un idéal de $f(A)$

3) Si A et B sont des anneaux, les idéaux de l'anneau produit $A \times B$ sont les $I \times J$ où I est un idéal de A et J un idéal de B.

4) Si I est un idéal de A les idéaux de A/I sont du type

$$J/I = \{\widehat{x} \in A/I | x \in J\} \text{ où } J \text{ est un idéal de } A \text{ contenant } I$$

5) Si I est un idéal de A alors $I[X]$ est un idéal de $A[X]$ et on a l'isomorphisme

$$(A/I)[X] \leftrightarrow A[X]/I[X]$$

Idéal engendré

Soit C une partie quelconque de l'anneau A on appelle idéal engendré par C le plus petit idéal de A (au sens de l'inclusion) qui contient C. C'est l'idéal

$$(C) = \{x_1c_1 + ... + x_kc_k | k \in \mathbb{N}, x_i \in A, c_i \in C\}$$

Idéal de type fini

On dit qu'un idéal I de A est de type fini si il existe un nombre fini a_1,...,a_n d'éléments de tels que $I = (a_1, ..., a_n)$. Un anneau dans lequel tout idéal est de type fini est dit noethérien.

On a l'équivalence

$$A \text{ noethérien} \Leftrightarrow \text{ toute suite croissante d'idéaux } I_1 \subset I_2 \subset ... \subset I_n \subset ... \text{ est stationnaire}$$

et aussi

$$A \text{ noethérien} \Leftrightarrow \text{ toute famille (non vide) d'idéaux } \{I_\alpha | \alpha \in X\} \text{ possède un élément maximal}$$

Idéal principal

On dit qu'un idéal I de A est principal s'il est engendré par un élement, c'est-à-dire s'il existe a tel que $I = (a)$.
On a $(1) = A$ et

$$d \text{ est inversible} \Leftrightarrow (d) = (1)$$

Divisibilité et idéaux

Si a et b sont deux éléments d'un anneau A on définit a divise b et on note $a|b$ par

$$a|b \Leftrightarrow \text{ il existe } c \in A \text{ tel que } b = ac$$

du point de vue des idéaux on a

$$a|b \Leftrightarrow (b) \subset (a)$$

Si a et b sont deux éléments d'un anneau A. On a a et b sont associés si et seulement si
$(a) = (b)$.
Autrement dit

$$(a) = (b) \Leftrightarrow \ b = \alpha a \text{ avec } \alpha \text{ inversible}$$

Sommes et produits d'idéaux

Si I et J sont deux idéaux de A on définit l'idéal noté $I + J$ comme étant le plus petit idéal contenant $I \cup J$, donc l'idéal engendré par $I \cup J$, c'est l'idéal

$$I + J = \{x + y | x \in I, y \in J\}$$

Si I et J sont deux idéaux de A on définit l'idéal noté IJ comme étant le plus grand idéal inclus dans $I \cap J$ c'est l'idéal

$$IJ = \{x_1y_1 + ... + x_ky_k | k \in \mathbb{N}, x_i \in I, y_i \in J\}$$

Si $I_1, I_2, ..., I_k$ sont des idéaux de A on définit de même $I_1 + I_2 + ... + I_k$ et $I_1I_2...I_k$.

Idéaux étrangers

On dit que deux idéaux I et J de A sont étrangers (entre eux) si $I + J = A$.
Dans ce cas on a $IJ = I \cap J$ et on a le "théorème des restes chinois": l'application

$$\begin{array}{ccc} A & \rightarrow & A/I \times A/J \\ x & \mapsto & (p_I(x), p_J(x)) \end{array}$$

est surjective et son noyau est IJ, elle donne donc un isomorphisme

$$A/IJ \leftrightarrow A/I \times A/J$$

Ce qui se traduit pratiquement par: pour tous a, b de A il existe x dans A tel que

$$\begin{aligned} x &= a \bmod(I) \\ x &= b \bmod(J) \end{aligned}$$

et y satisfait les mêmes relations si et seulement si $y = x \bmod(IJ)$.
Si $I_1, I_2, ..., I_k$ sont des idéaux deux à deux étrangers on a de même un isomorphisme

$$A/I_1I_2...I_k \leftrightarrow A/I_1 \times A/I_2 \times ... \times A/I_k$$

Idéaux maximaux et premiers
On dit qu'un idéal I de A est maximal si $I \neq A$ et s'il n'existe pas d'idéal J de A, distinct de A, qui contient strictement I.
C'est équivalent à dire que pour tout $a \notin I$ on a:

pour tout $b \in A$ il existe $c \in A$ tel que $b - ac \in I$.

On a

$$I \text{ maximal} \Leftrightarrow A/I \text{ est un corps}$$

On dit qu'un idéal I de A est premier si $I \neq A$ et si

$$x \notin I \text{ et } y \notin I \Rightarrow \ xy \notin I$$

On a

$$I \text{ premier} \Leftrightarrow A/I \text{ est intègre}$$

P.G.C.D et éléments premiers entre eux
Soit A un anneau intégre.
Soient a et b dans A, on dira que $d \in A$ est *un* p.g.c.d. de a et b si $d|a$ et $d|b$ et si on a

$$c|a \text{ et } c|b \Rightarrow c|d$$

Ce qui se traduit par: (d) est le plus petit idéal principal contenant a et b donc (d) est le plus petit idéal principal tel que

$$(a) + (b) \subset (d)$$

On a: d' est un autre p.g.c.d. de a et b si et seulement si $(d) = (d')$.

La définition d'un p.p.c.m. de a et b est semblable et se traduit par $(m) = (a) \cap (b)$
On dira que a et b sont premiers entre eux si

$$c|a \text{ et } c|b \Rightarrow c \text{ est inversible}$$

Elements irréductibles éléments premiers
Soit A un anneau intégre.
Un élément x de A est dit irréductible s'il n'est pas inversible et si

$$x = ab \Rightarrow a \text{ ou } b \text{ est inversible}$$

Ce qui se traduit par: il n'existe pas d'idéal principal (a) distinct de A qui contient strictement (x).
Remarques
Si x est irréductible alors αx est irréducible pour tout α inversible.
Si A est un sous-anneau d'un anneau intègre B un élément x irréductible dans A peut ne plus être irréductible dans B.
Si a est irréductible et si a ne divise pas b alors a est premier avec b.

Un élément x de A est dit premier s'il est non nul, non inversible et si

$$x|ab \Rightarrow x|a \text{ ou } x|b$$

Ce qui se traduit par: (x) est un idéal premier non nul de A.

Tout élément premier est irréductible, la réciproque est fausse.

Anneaux principaux

Un anneau principal est un anneau intègre dans lequel tout idéal est principal.

L'anneau $A[X]$ est principal si et seulement si A est un corps.

Remarque: Un sous-anneau d'un anneau principal n'est pas nécessairement principal. Exemple l'anneau $\mathbb{Z}[X]$ est un sous-anneau de $\mathbb{Q}[X]$ mais n'est pas principal; l'idéal $(2, X)$ n'est pas principal.

Soient a et b dans A, on a

$$d \in A \text{ est un p.g.c.d.de } a \text{ et } b \Leftrightarrow (a) + (b) = (d)$$

Soit A un anneau principal, a et b sont premiers entre eux si et seulement si $(a) + (b) = (1)$. Donc a et b sont premiers entre eux si et seulement si il existe u et v dans A tels que l'on ait la relation de Bezout:

$$1 = au + bv$$

Lemme de Gauss:

$$c|ab \text{ et } c \text{ premier avec } a \Rightarrow c|b$$

Dans un anneau principal on a

$$a \text{ est irréductible} \Leftrightarrow a \text{ est premier}$$

Anneaux euclidiens

Un anneau intègre A est euclidien si

a) il existe une application $v : A \setminus \{0\} \to \mathbb{N}$ telle que pour tous a et b on a $v(ab) \geq v(a)$ avec inégalité stricte si b est non inversible.

b) pour tous $a \in A$ et $b \in A \setminus \{0\}$ il existe $q \in A$ et $r \in A$

$$a = bq + r \text{ avec } v(r) < v(b) \text{ ou } r = 0$$

Un anneau euclidien est principal.

Anneaux factoriels.

Un anneau factoriel est un anneau intègre dans lequel tout élément x non inversible est produit d'un nombre fini d'éléments irréductibles

$$x = r_1 ... r_k$$

et si on a la propriété

$$c|ab \text{ et } c \text{ irréductible } \Rightarrow c|a \text{ ou } c|b$$

Si on a une autre décomposition de x en produit d'un nombre fini d'éléments irréductibles

$$x = r_1 ... r_k = s_1 ... s_l$$

alors $k = l$ et il existe une permutation σ des indices telle que pour tout i on ait

$$(s_i) = (r_{\sigma(i)})$$

Un anneau principal est factoriel. Si A est factoriel alors $A[X]$ est factoriel. Le lemme de Gauss reste valable dans un anneau factoriel mais non la relation de Bezout.

Exemple: Les éléments 2 et X sont premiers entre eux dans $\mathbb{Z}[X]$ car si $P(X)$ divise 2 on a $P(X) = 1$ ou $P(X) = -1$. Mais on ne peut trouver P et Q dans $\mathbb{Z}[X]$ tels que

$$2P(X) + XQ(X) = 1$$