Anneaux et corps

Soit $(A,+,\cdot)$ anneau commutatif unité

Définition. On dit que $I \subset A$ est un <u>idéal</u> de A si

1) $(I,+) \leq (A,+)$ sous-groupe
2) $\forall a \in A, \forall i \in I,\ a \cdot i \in I$

Ex. Si $n \in \mathbb{Z}$, $n\mathbb{Z}$ idéal de $\mathbb{Z}$

Exercice : Les idéaux de $\mathbb{Z}$ sont les $n\mathbb{Z}$, $n \in \mathbb{Z}$.

Définition (quotient)

Soit A anneau, Soit $I \leq A$ idéal, $I \neq A$

alors $A/I = \{x+I : x \in A\}$ où $x+I = \{x+i : i \in I\} \subset A$

est un anneau pour les opérations :

$+$: $\forall x,y \in A$, $(x+I)+(y+I) := (x+y)+I$

$\cdot$: $\forall x,y \in A$, $(x+I)\cdot(y+I) := xy+I$

Notations : $\forall x \in A$, $\overline{x} = x+I$

ou : $\overline{x} = \overline{y} \iff x-y \in I$

Remarque : c'est bien défini

car si $\overline{x_1} = \overline{x_2}$ $(x_1 - x_2 \in I)$

$\overline{y_1} = \overline{y_2}$ $(y_1 - y_2 \in I)$

alors $\overline{x_1+y_1} = \overline{x_2+y_2}$ car $x_1+y_1-(x_2+y_2) = \underbrace{x_1-x_2}_{\in I} + \underbrace{y_1-y_2}_{\in I} \in I$

de même $\overline{x_1 y_1} = \overline{x_2 y_2}$ car $x_1y_1 - x_2y_2 = \underbrace{(x_1-x_2)y_1}_{\in I} - \underbrace{x_2(y_2-y_1)}_{\in I} \in I$

Exercice $(A/I, +, \cdot)$ est un anneau

$0_{A/I} = 0+I = \overline{0}$, $1_{A/I} = 1+I = \overline{1}$

Proposition $\pi_I : A \to A/I$ est un morphisme d'anneaux surjectif

1) $a \longmapsto \overline{a} = a+I$

et $\ker \pi_I = I$

2) $\forall f : A \to B$ morphisme d'anneaux,

$\ker f = f^{-1}(0) = \{a \in A : f(a) = 0\}$ est un idéal de A.

1er Théorème d'isomorphisme : si $f : A \to B$ morphisme d'anneaux tq $f(1) \neq 0$

alors $A/\ker f \xrightarrow{\cong} f(A)$ $\overline{a} = a+\ker f \longmapsto f(a)$ isomorphisme

Ex : $\mathbb{R}[X]/(X^2+1) \simeq \mathbb{C}$ car $\mathbb{R}[X] \to \mathbb{C}$, $P(X) \mapsto P(i)$ morphisme d'anneaux surjectif de noyau (X^2+1)

(X^2+1) : idéal des polynômes divisibles par X^2+1

Définitions Soit A anneau

1) on dit que $a \in A$ est un diviseur de 0 si $\exists b \in A$, $ab = 0$
2) on dit que $a \in A$ inversible si $\exists b \in A$, $ab = 1$. Noté $b = a^{-1}$. $A^* = \{a \in A : a \text{ inversible}\}$
3) on dit que $a \in A$ est irréductible si a non inversible et si $a = bc$ avec $b, c \in A$ alors b ou c inversible
4) on dit que $a \in A$ est premier si $\forall b, c \in A$, alors $a \mid bc \Rightarrow a \mid b$ ou $a \mid c$.
5) A est intègre si $\forall a, b \in A$, $ab = 0 \Rightarrow a = 0$ ou $b = 0$
   ex : $\mathbb{Z}/p\mathbb{Z}$ intègre si p premier, $\mathbb{Z}/12\mathbb{Z}$ n'est pas intègre car $\bar{2} \cdot \bar{6} = \bar{0}$ ($\bar{2} \neq 0$, $\bar{6} \neq 0$)
6) A est un corps si $A^* = A \setminus \{0\}$

Remarque : inversible $\Rightarrow$ non diviseur de zéro, corps $\Rightarrow$ intègre

ex. $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ sont intègres, $\mathbb{Q}, \mathbb{R}, \mathbb{C}$ corps, $\mathbb{Z}$ non

$\mathbb{Z}+\mathbb{Z}\sqrt{2}/(3)$ est un corps (de cardinal 9)

(en effet : $A := \mathbb{Z}+\mathbb{Z}\sqrt{2}$ (sous-anneau de $\mathbb{R}$)

$A/3A = \{\bar{0}, \bar{1}, \bar{2}, \overline{\sqrt{2}}, \overline{2\sqrt{2}}, \overline{1+\sqrt{2}}, \overline{1+2\sqrt{2}}, \overline{2+\sqrt{2}}, \overline{2+2\sqrt{2}}\}$

inversibles

$(\overline{1+\sqrt{2}})(\overline{2+\sqrt{2}}) = \overline{2+\sqrt{2}+2\sqrt{2}+2} = \bar{1}$ ...)

Proposition. A intègre $\Rightarrow A[X]$ intègre

Démo. Si $P = a_0 + \dots + a_n X^n$, $Q = b_0 + \dots + b_k X^k \in A[X]$
($a_n \neq 0$, $b_k \neq 0$, $a_0 \neq 0$, $b_0 \neq 0$)

avec $a_n \neq 0$, $b_k \neq 0$, alors $PQ = a_0 b_0 + \dots + a_n b_k X^{n+k}$

donc $a_n b_k \neq 0$ (A intègre) $\Rightarrow \deg PQ = n+k$ et $PQ \neq 0$.

Exercice. Soit $A = \mathbb{Z}+\mathbb{Z}i\sqrt{5}$ sous-anneau de $\mathbb{C}$ (DONC intègre)

$A^* = \{\pm 1\}$, 2 est irréductible dans A mais non premier

Solution : $N : A \to \mathbb{N}$, $x \mapsto |x|^2$ ($x = a + ib\sqrt{5}$, $a, b \in \mathbb{Z}$ $\Rightarrow N(x) = a^2 + 5b^2 \in \mathbb{N}$)

$\forall x, y \in A$, $N(xy) = N(x)N(y)$. $N(1) = 1$

donc $x \in A^*$, alors $N(x) = 1$

(car $N(xx^{-1}) = \underbrace{N(x)}_{\in \mathbb{N}} \underbrace{N(x^{-1})}_{\in \mathbb{N}} = N(1) = 1$)

Remarque $x \in A^* \iff N(x) = 1$

($N(x) = 1 \Rightarrow x^{-1} = \overline{x}$)

On a si $x = a + ib\sqrt{5}$, $a, b \in \mathbb{Z}$, $N(x) = 1 \iff a^2 + 5b^2 = 1$

$\Rightarrow b = 0$ et $a = \pm 1$

$\Rightarrow x = \pm 1$.

$2 = xy$, $x, y \in A \Rightarrow N(2) = 4 = \underbrace{N(x)}_{\in \mathbb{N}} \underbrace{N(y)}_{\in \mathbb{N}}$ $\Rightarrow$ ($N(x) = 1$, $N(y) = 4$) $\Rightarrow x \in A^*$

~~$N(x) = 2 = N(y)$~~ impossible

($N(x) = 4$, $N(y) = 1$) $\Rightarrow y \in A^*$

car $a^2 + 5b^2 = 2$ n'a pas de solution $a, b \in \mathbb{Z}$.

Mais 2 n'est pas premier (dans A) car $2 \cdot 3 = 6 = (1 + i\sqrt{5})(1 - i\sqrt{5})$

$2 \mid (1 + i\sqrt{5})(1 - i\sqrt{5})$

et $2 \nmid 1 \pm i\sqrt{5}$

Définitions. Soient $I \leqslant A$ idéal tq $I \neq A$ (c-à-d. $1 \notin I$)

- on dit que I est premier si $\forall a, b \in A$, $ab \in I \Rightarrow a$ ou $b \in I$

  [ou : a et $b \notin I \Rightarrow ab \notin I$]

- on dit que I est maximal si $\forall$ $I \subset J \subset A$ idéal, $I = J$ ou $J = A$

Proposition. Soit $I \leqslant A$ idéal, $I \neq A$.

Alors 1) I premier $\iff$ A/I intègre

(I : idéal ; A/I : anneau)

2) I maximal $\iff$ A/I corps

Dém 2) si I maximal.

si $\overline{x} \neq \overline{0}$ (dans A/I) alors $x \in A \setminus I \Rightarrow I + (x) = A$ (idéal)

$\Rightarrow 1 \in I + (x)$

$\iff \exists\, i \in I, \lambda \in A$, $1 = i + \lambda x \Rightarrow \overline{1} = \overline{\lambda}\,\overline{x} \Rightarrow \overline{x}$ inversible.

si A/I corps. Si $I \subset J \subset A$ idéal alors soit $I = J$

soit $\exists\, x \in J \setminus I \Rightarrow \overline{x}$ inversible dans A/I

$\Rightarrow \exists\, y \in A,\ \overline{xy} = \overline{1}$

$\Rightarrow 1 - xy \in I$

$\Rightarrow \exists\, i \in I,\ 1 = \underbrace{xy}_{\in J} + \underbrace{i}_{\in I \subset J} \in J$

$\Rightarrow J = A.$

Exc - Dans $\mathbb{Z}$, les idéaux premiers sont 0 et les $p\mathbb{Z}$ p premier.
les idéaux maximaux sont les $p\mathbb{Z}$ p premier

- Dans A quelconque, maximal $\Rightarrow$ premier.

Pause = 5'