Anneau quotient

déf. 1) Un anneau (commutatif, unitaire) est un ensemble A muni de deux opérations $+, \cdot : A \times A \to A$ t.q.

1) $a+b = b+a$
2) $a+(b+c) = (a+b)+c$
3) $\exists e \in A$ t.q. $a+e = e+a = a$
4) pour $a \in A$, $\exists b \in A$ t.q. $a+b = e$.

1) $a \cdot b = b \cdot a$
2) $a \cdot (b \cdot c) = (a \cdot b) \cdot c$
3) $\exists u \in A$ t.q. $a \cdot u = u \cdot a = a$
4) $a \cdot (b+c) = a \cdot b + a \cdot c$.

2) Un anneau est un corps, si pour tout $a \in A \setminus \{e\}$, $\exists b \in A$ t.q. $ab = u$

(e : élément neutre pour la somme, u : élément neutre pour)

3) Un anneau est intègre si pour tout $a, b \in A \setminus \{e\}$ on a $a \cdot b \in A \setminus \{e\}$

4) Soit A un anneau. Un idéal de A est une partie $I \subseteq A$ t.q.

- $a, b \in I \Rightarrow b - a \in I$
- $a \in A$, $b \in I \Rightarrow a \cdot b \in I$

Exemples : 0) $e = u \iff A = \{e\}$

En effet, si $a \in A$, on $a = a \cdot u = a \cdot e = a(e+e) = a \cdot e + a \cdot e$

$= a \cdot u + a \cdot u = a + a$

$\Longrightarrow a = e$.

1) $A = \mathbb{Z}$ anneau des entiers : intègre, mais ce n'est pas un corps

2) $A = \mathbb{Q}$ corps

3) $A = \mathbb{Z}/n\mathbb{Z} = \{\text{entiers modulo } n\}$

$\mathbb{Z}/n\mathbb{Z}$ intègre $\Leftrightarrow$ n est premier

($\Rightarrow$) Si n n'est pas premier, $n = p \cdot q$ avec $p, q \in \mathbb{Z} \setminus \{\pm 1, 0\}$.

$\Rightarrow p, q$ ne sont pas des multiples de n

mais $p \cdot q = n \equiv 0 \pmod{n}$.

[e.g. $n = 6 = 2 \cdot 3$ $\quad 2, 3 \not\equiv 0 \ (6)$ mais $2 \cdot 3 \equiv 0 \pmod{6}$.]

($\Leftarrow$) plus tard (aussi cours d'Arithmétique).

4) $A = K[x] = \{$ polynômes à coefficients dans un corps $K\}$.

intègre mais ce n'est pas un corps $\left(\frac{1}{x} \notin A\right)$.

5) Tous les idéaux de $\mathbb{Z}$ sont de la forme $(n) = \{$ multiples de $n\}$ pour un certain $n \in \mathbb{N}$.

En effet, soit $I \subseteq \mathbb{Z}$ un idéal. Si $I = \{0\}$ on a fini.

Sinon, soit $x \in I \setminus \{0\}$ t.q.

$$x \geq 0$$

et $$x = \min \underbrace{\{|y| : y \in I \setminus \{0\}\}}_{\subseteq \mathbb{N}}.$$

Si $a \in I \setminus \{0\}$, alors

$$a = qx + r \quad \text{avec } q, r \in \mathbb{Z} \quad \text{et} \quad |r| < |x| = x.$$

mais $$r = \underbrace{a}_{\in I} - \underbrace{qx}_{\in I} \in I.$$

On a : $r \in I$ et $|r| < x \Longrightarrow r = 0$.

$$\Longrightarrow \quad a = qx.$$

□

6) Tous les idéaux de $K[x]$ sont de la forme

$(f) = \{gf : g \in K[x]\}$ pour un certain $f \in K[x]$.

Construction de l'anneau quotient : A anneau, $I \subseteq A$ idéal

$a, b \in A$ $\quad a \sim b$ si $b - a \in I$.

C'est une relation d'équivalence :

- réflexive : $a \sim a \Leftrightarrow a - a = 0 \in I$.
- symétrique : $a \sim b \Rightarrow b - a \in I \Rightarrow \underbrace{-(b-a)}_{a-b} \in I \Rightarrow b \sim a$.
- transitive : $a \sim b$ et $b \sim c$

$\Downarrow$ $\qquad$ $\Downarrow$

$b - a \in I$ $\qquad$ $c - b \in I$ $\Rightarrow$ $c - a = \underbrace{(c-b)}_{\in I} + \underbrace{(b-a)}_{\in I} \in I$.

$$\Rightarrow \quad c \sim a.$$

déf. Le quotient de A par I est l'ensemble des classes d'équivalence

de $\sim$.

$$A/I := A/\sim \ni \bar{a}, \quad a \in A.$$

Opérations : $a, b \in A$

$$\bar{a} \oplus \bar{b} = \overline{a+b} \qquad \bar{a} \odot \bar{b} = \overline{ab}.$$

Rmq: c'est bien défini.

démo. $a \sim a' \to a' - a \in I$
$b \sim b' \to b' - b \in I$

- $a' + b' = \underbrace{(a'-a)}_{\in I} + a + \underbrace{(b'-b)}_{\in I} + b \Rightarrow \overline{a'+b'} = \overline{a+b}.$

- $a' \cdot b' = ((a'-a)+a)((b'-b)+b)$

$$= \underbrace{(a'-a)}_{\in I}\underbrace{(b'-b)}_{\in I} + \underbrace{(a'-a)}_{\in I}\underbrace{b}_{\in A} + \underbrace{a}_{\in A}\underbrace{(b'-b)}_{\in I} + ab$$

$$\Longrightarrow \overline{a'b'} = \overline{ab}. \qquad \square$$

Exo: $(A/I, \oplus, \odot)$ est un anneau avec éléments neutres $\bar{0}$ pour $\oplus$, et $\bar{1}$ pour $\odot$.

Exemple: $A = \mathbb{Z}$, $I = n\mathbb{Z} = (n) \Rightarrow A/I = \mathbb{Z}/n\mathbb{Z}$.

Déf: Si A, B sont des anneaux, une application $\varphi : A \to B$ est dite une application d'anneaux (ou un homomorphisme) si

$$\varphi(a +_A a') = \varphi(a) +_B \varphi(a')$$

$$\varphi(a \cdot_A a') = \varphi(a) \cdot_B \varphi(a').$$

Exemple: Soit $I \subseteq A$ un ideal, alors la projection sur le quotient

$$\pi : A \longrightarrow A/I$$
$$a \mapsto \bar{a}$$

est une application d'anneaux.

Prop. Si $\varphi : A \to B$ est une application d'anneaux, alors

$\ker(\varphi) := \{a \in A : \varphi(a) = 0\}$ est un ideal.

De plus il existe une unique application d'anneaux $\tilde{\varphi} : A/I \to B$ t.q. $\varphi = \tilde{\varphi} \circ \pi$ où $\pi : A \to A/I$ est la projection sur le quotient.

Démo: (I idéal) : • $a, a' \in I \implies \varphi(a'-a) = \varphi(a') - \varphi(a) = 0 - 0 = 0.$

$\Rightarrow a' - a \in I.$

• $a \in A$, $a' \in I \Rightarrow \varphi(aa') = \varphi(a) \underbrace{\varphi(a')}_{0} = \varphi(a) \cdot 0 = 0.$

$\Longrightarrow I$ idéal.

(Définition de $\tilde{\varphi}$.) On pose $\tilde{\varphi}(\bar{a}) = \varphi(a)$.

C'est bien défini : $a' - a \in I \Rightarrow \varphi(a') = \varphi(a' - a + a) = \underbrace{\varphi(a'-a)}_{0} + \varphi(a)$

$= \varphi(a).$

• $\tilde{\varphi}(\overline{ab}) = \tilde{\varphi}(\bar{a}\bar{b})$ (=) $\varphi(ab) = \varphi(a)\varphi(b)$ $\Longrightarrow$ $\tilde{\varphi}(\bar{a}\bar{b}) = \tilde{\varphi}(\bar{a})\tilde{\varphi}(\bar{b})$.

• $\tilde{\varphi}(\bar{a} + \bar{b}) = \tilde{\varphi}(\overline{a+b}) = \varphi(a+b) = \varphi(a) + \varphi(b) = \tilde{\varphi}(\bar{a}) + \tilde{\varphi}(\bar{b})$.

$\Longrightarrow$ $\tilde{\varphi}$ est une application d'anneaux.

Par définition $\varphi(a) = \tilde{\varphi}(\bar{a}) = \tilde{\varphi}(\pi(a))$.

L'unicité en découle directement. □

Exo: Soit $I \subseteq A$ un idéal et $\varphi : A \to B$ une application d'anneaux t.q. $\varphi(a) = 0$ pour tout $a \in I$. Alors, il existe une unique application d'anneaux $\tilde{\varphi} : A/I \to B$ t.q. $\varphi = \tilde{\varphi} \circ \pi$.

Exemple: $\mathcal{C}$ = {suites de Cauchy rationnelles}

$\mathcal{N}$ = {suites négligeables rationnelles}

Alors $\mathcal{C}$ est un anneau :

$(x_n)_n \cdot (y_n)_n = (x_n y_n)_n$

$(x_n)_n + (y_n)_n = (x_n + y_n)_n$

et $\mathcal{N} \subseteq \mathcal{C}$ est un idéal et on a $\mathbb{R} := \mathcal{C}/\mathcal{N}$.

Extension de corps

$I \neq A$

Un idéal $I \subsetneq A$ est dit premier si $\forall$ pour tout $a, b \in A$ t.q

Déf: Un idéal $I \subsetneq A$ est premier si pour tout $a, b \in A$ tels que $ab \in I$, alors $a \in I$ ou $b \in I$.

Exemple: 1) $A = \mathbb{Z}$, $(n) = I$ avec $n \in \mathbb{N} \setminus \{0, 1\}$.

I est premier $\iff$ n est premier. (*)

$a, b \in \mathbb{Z}$. $ab \in I \iff n$ divise ab

$a \in I$ ou $b \in I \iff n$ divise a ou n divise b.

L'équivalence (*) revient à

n premier $\Leftrightarrow$ pour tout $a, b \in \mathbb{Z}$ t.q. $n \mid ab$ alors $n \mid a$ ou $n \mid b$.

Lemme: Soit $I \subsetneq A$ idéal. Alors I est premier $\iff$ A/I intègre.

démo: ($\Rightarrow$) On suppose I premier. Soient $a, b \in A$ t.q. $\bar{a}\bar{b} = \bar{0}$ dans A/I. Cela signifie que ab appartient à I.

$ab \in I \underset{I \text{ premier}}{\Longrightarrow} a \in I$ ou $b \in I \Longrightarrow \bar{a} = \bar{0}$ ou $\bar{b} = \bar{0}$.

($\Leftarrow$) On suppose A/I intègre. Soient $a, b \in A$ t.q. $ab \in I$

$\overline{ab} = \bar{0}$ dans $A/I \underset{A/I \text{ intègre}}{\Longrightarrow} \bar{a} = \bar{0}$ ou $\bar{b} = \bar{0} \Longrightarrow a \in I$ ou $b \in I$. $\Longrightarrow I$ premier $\square$

Idéaux premiers dans $K[x]$

On fixe un corps K. $K^* = K \setminus \{0\}$

déf: Un polynôme $f \in K[x]$ est :

- irréductible si pour tout $g, h \in K[x]$ t.q. $f = gh$, on a $g \in K \setminus \{0\}$ ou $h \in K \setminus \{0\}$.
- premier si pour tout $gh \in K[x]$ t.q. f divise gh, alors f divise g ou f divise h. ($f \notin K$)

Prop. Soit $f \in K[x] \setminus K$. Alors $(f) \subsetneq K[x]$ est premier ssi f est premier

démo. Exercice. $\square$

Prop (Factorisation unique.) Soit $f \in K[x]$. Il existe un unique $r \in \mathbb{N}$, $g_1, \dots, g_r \in K[x]$ et $d_1, \dots, d_r \in \mathbb{N} \setminus \{0\}$ (à permutation près) et $\lambda \in K^*$ t.q.

$$f = \lambda g_1^{d_1} \cdots g_r^{d_r}.$$

g_i unitaire (= coeff. dominant est 1)

démo. Soient $f = \lambda\, g_1^{d_1} \cdots g_r^{d_r} = \mu\, h_1^{e_1} \cdots h_s^{e_s}$ et premier, deux à deux distincts !

g_i, h_j unitaires et premiers

$d_i, e_j \in \mathbb{N} \setminus \{0\}$.

- g_i, h_j unitaires $\Rightarrow \lambda = \mu$.

$$g_i \mid h_1^{e_1} \cdots h_s^{e_s} \xrightarrow[g_i \text{ premier}]{} \exists\, \tau(i) = 1, \dots, r \text{ t.q. } g_i \mid h_{\tau(i)}$$

$$h_j \mid g_1^{d_1} \cdots g_r^{d_r} \xrightarrow[h_j \text{ premier}]{} \exists\, \tau(j) = 1, \dots, s \text{ t.q. } h_j \mid g_{\tau(j)}$$

$\Rightarrow$ g_i divise $h_{\tau(i)}$ qui divise $g_{\tau(\tau(i))}$.

[Lemme : F premier $\Rightarrow$ irréductible.

démo. Si $F = GH$, alors F divise GH. Donc F divise G ou F divise H, mais $\deg(G) \leq \deg(F)$, $\deg(H) \leq \deg(F)$.

Donc si F divise G, on a forcément $\deg(G) = \deg(F)$.

Donc H est constant (i.e. $\deg H = 0$). □]

Puisque $g_{\tau(\tau(i))}$ est irréductible (car premier)

$$g_{\tau(\tau(i))} = \alpha\, g_i \quad \text{avec } \alpha \in K^*$$

g_i, $g_{\tau(\tau(i))}$ unitaires $\Rightarrow \alpha = 1$. $\Longrightarrow$ $\tau(\tau(i)) = i$.

De manière analogue, on trouve $\tau(\tau(j)) = j$.

$\Longrightarrow$ $r = s$, $d_i = e_{\tau(i)}$, $h_{\tau(i)} = g_i$. □

Cor : Soit $f \in K[x] \setminus K$. Alors f est irréductible $\Leftrightarrow$ f est premier.

démo ($\Leftarrow$) : déjà fait ($\Rightarrow$) On écrit $f = \lambda\, f_1^{d_1} \cdots f_r^{d_r}$ avec f_i premiers et unitaires.

f irréductible $\Rightarrow$ $f = \lambda f_i$ pour un certain i. □

$\Rightarrow$ f premier

$\Rightarrow$ [illegible]

Cor: Soit $I \subsetneq K[x]$ un idéal premier. Alors ou bien $I = \{0\}$ ou bien $I = (f)$ où f irréductible.

Prop. Soit $f \in K[x] \setminus K$ irréductible. Alors $K[x]/(f)$ est un corps.

Rmq: Soit $f, g \in K[x]$. Le pgcd de f, g est l'unique polynôme unitaire d qui engendre l'idéal $(f,g) = \{ af + bg : a, b \in K[x] \}$.

Lemme: Soit f irréductible, et $g \in K[x]$. Alors

$$\text{pgcd}(f,g) = \begin{cases} 1 & \text{si } f \nmid g \\ f & \text{sinon} \end{cases}$$

(« et unitaire »)

démo. Si $f \mid g$ on a $(f,g) = (f) \Rightarrow \text{pgcd}(f,g) = f$.

Supposons que f ne divise pas g. Supposons par l'absurde $\text{pgcd}(f,g) \neq 1$. Alors, il existe un élément $d \in (f,g)$ de degré > 0 qui divise f et g.

$\Longrightarrow d = f \Rightarrow f$ divise g. $\lightning$

(f irréductible et unitaire)

$\Longrightarrow \text{pgcd}(f,g) = 1$. $\square$

démo de la Prop. Soit $g \in K[x]$ t.q. $\bar{g}$ est non nul dans $K[x]/(f)$.

Ceci signifie que g n'appartient pas à (f), i.e. f ne divise pas g

$\underset{\text{Lemme}}{\Longrightarrow} \text{pgcd}(f,g) = 1$.

Donc 1 appartient à l'idéal $(f,g) = \{ af + bg : a, b \in K[x] \}$.

Soient $a, b \in K[x]$ t.q. $af + bg = 1$. Alors, dans $K[x]/(f)$,

$$\bar{1} = \overline{af} + \bar{b}\bar{g} = \bar{b}\bar{g} \Rightarrow \bar{b} \text{ est l'inverse de } \bar{g}.$$

($af \in (f) \Rightarrow \overline{af} = 0$)

Tout élément non nul est inversible, donc $K[x]/(f)$ est un corps. $\square$

Prop. Soit $\varphi : A \to B$ une application d'anneaux. L'application induite

$\tilde{\varphi} : A/\mathrm{Ker}(\varphi) \longrightarrow B$ est injective.

démo. Soit $a, a' \in A$ t.q. $\varphi(a) = \varphi(a')$. On doit montrer que $\overline{a} = \overline{a'}$ dans $A/\mathrm{Ker}(\varphi)$, i.e. $a' - a \in \mathrm{Ker}(\varphi)$. Ceci est vrai:

$$\varphi(a') = \varphi(a) \iff \varphi(a' - a) = 0 \iff a' - a \in \mathrm{Ker}(\varphi). \quad \square$$

Lemme : Si $f \in K[x]$ est un polynôme de degré d, $K[x]/(f)$ est un K-espace vectoriel de dimension d.

démo. Une base du K-esp. vect. $K[x]$ est

$$1, x, x^2, x^3, \dots, x^d, x^{d+1}, \dots$$

Soit $f = \sum_{i=0}^{d} a_i x^i$. Dans $K[x]/(f)$ on a la relation linéaire suivante

$$a_0 + a_1 \overline{x} + a_2 \overline{x}^2 + \dots + a_d \overline{x}^d = \overline{0}$$

Ceci implique que $1, \overline{x}, \dots, \overline{x}^d$ sont lin. dépendants. On procède de cette manière

$$a_0 \overline{x} + a_1 \overline{x}^2 + \dots + a_d \overline{x}^{d+1} = \overline{0}$$

$$\Rightarrow \quad \overline{x}^{d+1} \in \mathrm{Vect}(1, \dots, \overline{x}^{d-1}).$$

En raisonnant par récurrence on trouve que

$$\overline{x}^n \in \mathrm{Vect}(1, \dots, \overline{x}^{d-1}) \quad \text{pour tout } n \geq d.$$

Il suffit de remarquer que $1, \overline{x}, \dots, \overline{x}^{d-1}$ sont lin. indép. Sinon on aurait une combinaison linéaire

$$b_0 + b_1 \overline{x} + \dots + b_{d-1} \overline{x}^{d-1} = \overline{0} \quad \text{dans } K[x]/(f)$$

$$g(x)$$

Cela signifie que le polynôme $b_0 + b_1 x + \dots + b_{d-1} x^{d-1}$ appartient à l'idéal (f). Puisque $\deg(g) = \deg(f) - 1 < \deg(f)$ on a $g = 0$

$$\text{donc} \quad b_0 = b_1 = \dots = b_{d-1} = 0.$$

$$\Longrightarrow \quad \dim K[x]/(f) = d. \qquad \square$$

Exemples : 0) $a \in K$ On considère l'application

$$\varphi : \begin{array}{ccc} K[x] & \longrightarrow & K \\ f(x) & \longmapsto & f(a) \end{array}$$

$$\operatorname{Ker}(\varphi) = \{ f \in K[x] : f(a) = 0 \} = (x-a)$$

L'application φ induit une application (injective) d'anneaux

$$\tilde{\varphi} : \underbrace{K[x]/(x-a)}_{\text{dim } 1} \xrightarrow{\text{inj}} \underbrace{K}_{\text{dim } 1}$$

Rmq : $\tilde{\varphi}$ application d'anneau $\Rightarrow$ K-linéaire

$\Longrightarrow$ $\tilde{\varphi}$ est bijective. $\quad K[x]/(x-a) \simeq K$.

i) $K = \mathbb{R}$ $\quad f = x^2 + 1$.

$$\begin{array}{ccc} \mathbb{R}[x] & \xrightarrow{\varphi} & \mathbb{C} \\ f(x) & \longmapsto & f(i) = f(\sqrt{-1}) \end{array}$$

$$\operatorname{Ker}(\varphi) = \{ f \in \mathbb{R}[x] : f(i) = 0 \} = (x^2+1)$$

↑ Comme il est de degré minimal, c'est un générateur.

$$\Longrightarrow \tilde{\varphi} : \underbrace{\mathbb{R}[x]/(x^2+1)}_{\text{dim } 2} \longrightarrow \underbrace{\mathbb{C}}_{\text{dim } 2}$$

application d'anneaux injective

$\Longrightarrow$ $\tilde{\varphi}$ est un isomorphisme.

Il faut penser au corps $K[x]/(f)$ comme le corps K auquel on a ajouté une racine de f : en effet, si $f = \sum_{i=0}^{d} a_i x^i$

$$f(\bar{x}) = a_0 + a_1 \bar{x} + a_2 \bar{x}^2 + \cdots + a_d \bar{x}^d = 0 \quad \text{dans } K[x]/(f(x)).$$

Donc $\bar{x} \in K[x]/(f(x))$ c'est une racine de f.

Exemple : $K = \mathbb{Q}$, $\alpha \in \mathbb{C}$ algébrique ($= \exists P \in \mathbb{Q}[x]$ $P \neq 0$ t.q. $P(\alpha) = 0$).

$$\varphi : \begin{array}{ccc} \mathbb{Q}[x] & \longrightarrow & \mathbb{C} \\ f & \longmapsto & f(\alpha) \end{array}$$

$$\operatorname{Ker}(\varphi) = \{ f \in \mathbb{Q}[x] : f(\alpha) = 0 \} = (P_\alpha)$$

↑ polynôme minimal de α.

On obtient une application injective d'anneaux :

$$\tilde{\varphi} : \mathbb{Q}[X]/(P_\alpha) \longrightarrow \mathbb{C}$$
$$\overline{X} \longmapsto \alpha$$