



DÉFINITION 3.1. Un anneau $(A, +, \cdot, 0_A, 1_A)$ est la donnée, d'un groupe commutatif $(A, +)$ (note additivement) d'élément neutre note 0_A , d'une loi de composition interne (dite de multiplication)

$$\bullet \bullet : \begin{array}{ll} A \times A & \mapsto A \\ (a, b) & \mapsto a \cdot b \end{array}$$

et d'un élément unité $1_A \in A$ ayant les propriétés suivantes

(1) Associativité de la multiplication:

$$\forall a, b, c \in A, (a \cdot b) \cdot c = a \cdot (b \cdot c) = a \cdot b \cdot c.$$

(2) distributivité:

$$\forall a, b, c \in A, (a + b) \cdot c = a \cdot c + b \cdot c, c \cdot (a + b) = c \cdot a + c \cdot b.$$

(3) Neutralité de l'unité:

$$\forall a \in A, a \cdot 1_A = 1_A \cdot a = a.$$

Un anneau est dit commutatif si de plus la multiplication est commutative:

$$\forall a, b \in A, a \cdot b = b \cdot a.$$

Examples: $\mathbb{Z} \subset \mathbb{Q} \subset \mathbb{R} \subset \mathbb{C}$

$$- (\mathbb{Z}/q\mathbb{Z}, +_q, \times_q, 0(\bmod q), 1(\bmod q))$$

$$- F(X; A) \quad X \text{ ens}, A \text{ anneau}$$

$$0_F = \underline{0}_A \quad 1_F = \underline{1}_A$$

- A commutatif:

$$M_2(A) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \mid a, b, c, d \in A \right\}$$

$$0_{M_2(A)} = 0_2 = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix} \quad 1_{M_2(A)} = Id_2 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$

- $(M, +)$ = gpe commutatif

$$(End_{Gr}(M), +, 0, 0_M, Id_M)$$

Elements Inversibles

Unités

DÉFINITION 3.2. Soit A un anneau. Un element $a \in A$ est inversible si il existe $b \in A$ tel que

$$a.b = b.a = 1_A.$$

On dit alors que b est un inverse (à gauche et à droite) de a (pour la multiplication).

NOTATION 3.1. Par la Proposition précédente si un element $a \in A$ est inversible son inverse est unique. On notera cet inverse

$$a^{-1}.$$

Notons que a^{-1} est également inversible et on a

$$(a^{-1})^{-1} = a.$$

On déduit de cette discussion que

PROPOSITION 3.2. Soit $A^\times$ l'ensemble des elements inversibles d'un anneau A , alors

$$(A^\times, \cdot, 1_A, \bullet^{-1})$$

forme un groupe: le groupe des elements inversibles de A .

Examples $\mathbb{Z}^* = \{\pm 1\} \neq \mathbb{Z} - \{0\}.$

$$\mathbb{Q}^* = \mathbb{Q}^\times = \mathbb{Q} - \{0\}$$

$$\mathbb{R}^* = \mathbb{R}^\times = \mathbb{R} - \{0\} \quad \mathbb{C}^* = \mathbb{C}^\times = \mathbb{C} - \{0\}.$$

$$= \{0\}^* = \{0\}$$

$$(\mathbb{Z}/_q \mathbb{Z})^* = \{ a(q) = a + q\mathbb{Z} \mid (a, q) = 1 \}$$

EXERCICE 3.2. Soit A un anneau commutatif et $M_2(A)$ l'anneau des matrices à coefficients dans A . Soit $M = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in M_2(A)$, la transposée de la matrice des *cofacteurs* de M est la matrice définie par

$$\text{tcof}(M) := \begin{pmatrix} d & -b \\ -c & a \end{pmatrix}.$$

(1) Montrer que

$$M \cdot \text{tcof}(M) = \text{tcof}(M) \cdot M = \det(M) \cdot \text{Id}_2 = \begin{pmatrix} \det(M) & 0 \\ 0 & \det(M) \end{pmatrix}$$

ou $\det(M)$ (le déterminant de M) est défini par

$$\det(M) := ad - bc \in A.$$

(2) En déduire que

$$M_2(A)^\times =: \text{GL}_2(A) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix}, a, b, c, d \in A, \det \begin{pmatrix} a & b \\ c & d \end{pmatrix} = ad - bc \in A^\times \right\}.$$

$$M_2(\mathbb{Z})^{\times} = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \mid a, b, c, d \in \mathbb{Z} \text{ tq } ad - bc = \pm 1 \right\}.$$

$M =$ gpe commutatif

$$\text{End}_{Gr}^{\times}(M) = \text{Aut}_{Gr}(M) = \text{ls morphismes. de } M \text{ vers } M \text{ bijectifs}$$

Sous - Anneau

DÉFINITION 3.4. Soit $(A, +, \cdot)$ un anneau. Un sous-anneau $B \subset A$ est un sous-groupe de $(A, +)$ qui est

- soit le sous-groupe trivial $\{0_A\}$,
- soit qui contient l'unité 1_A et qui est stable par multiplication:

$$\forall b, b' \in B, \quad b.b' \in B.$$

Ainsi $(B, +, \cdot, 0_A, 1_A)$ est un anneau.

PROPOSITION 3.3. (Critère de sous-anneau) Soit $(A, +, \cdot)$ un anneau et $B \subset A$ un sous-ensemble non-vidé; alors B est un sous-anneau ssi $B = \{0_A\}$, ou bien $1_A \in B$ et

$$(3.1.1) \quad \forall b, b', b'' \in B, \quad b.b' - b'' \in B$$

Preuve: Exercice.

□

Morphismes

DÉFINITION 3.5. Soient $(A, +_A, \cdot_A)$, $(B, +_B, \cdot_B)$ des anneaux. Un morphisme d'anneaux $\varphi : A \mapsto B$ est un morphisme de groupes commutatif $\varphi : (A, +_A) \mapsto (B, +_B)$ tel que

$$\varphi(1_A) = 1_B \text{ ou bien } \varphi(1_A) = 0_B,$$

$$\forall a, a' \in A, \varphi(a \cdot_A a') = \varphi(a) \cdot_B \varphi(a').$$

REMARQUE 3.1.4. Si $\varphi(1_A) = 0_B$ alors φ est l'application constante nulle $\underline{0}_B$:

$$\forall a \in A, \varphi(a) = \varphi(a) \cdot \varphi(1_A) = 0_B.$$

Exemple: Le morphisme canonique.

Soit A un anneau

$$\text{Can}_A: \mathbb{Z} \longrightarrow A$$

$$\begin{aligned} n &\longrightarrow n \cdot 1_A = \underbrace{1_A + \dots + 1_A}_{n \text{ fois}} \quad (n \geq 0) \\ &= \underbrace{(-1_A) + \dots + (-1_A)}_{\substack{n \text{ fois} \\ \text{si } n \leq 0}} \quad (n \leq 0) \end{aligned}$$

$$\ker(\text{Can}_A) = q_A \mathbb{Z} \quad q_A = \text{caractéristique de } A.$$

Exemple:

$$\begin{array}{ccc} \mathbb{Z} & \longrightarrow & \mathbb{Z}/q\mathbb{Z} \\ \pi_q = \bullet \pmod{q}: & & \\ a & \longrightarrow & a \pmod{q} = a + q\mathbb{Z} \end{array}$$

c'est un morphisme d'anneaux et
c'est le morphisme canonique de $\mathbb{Z}/q\mathbb{Z}$
et la caractéristique de $\mathbb{Z}/q\mathbb{Z}$ c'est q .

PROPOSITION 3.4. (Stabilité par morphismes) Soient $\varphi \in \text{Hom}_{\text{Ann}}(A, B)$ un morphisme alors $\varphi(A) \subset B$ est un sous-anneau. Par ailleurs le sous-groupe $\ker(\varphi)$ est un sous-groupe de $(A, +)$ qui est de plus stable par multiplication (à gauche et à droite) par A :

$$\forall a \in A, k \in \ker(\varphi), a.k, k.a \in \ker(\varphi).$$

et si $A' \subset A$ est un sous-anneau alors $\varphi(A')$ est un sous-anneau.

Preuve: deux cas. $\varphi(1_A) = 0_B$ alors
 $\forall a \quad \varphi(a) = 0_B \quad \varphi(A) = \{0_B\}$ l'anneau nul de B
 $\ker \varphi = A$

$$\text{Si } \varphi(1_A) = 1_B \neq 0_B$$

Alors $\varphi(A) \subset B$ est un sous-anneau de B

Soient $b, b', b'' \in \varphi(A)$ alors $b \cdot b' - b'' \in \varphi(A)$

$$b = \varphi(a) \quad b' = \varphi(a') \quad b'' = \varphi(a'')$$

$$\begin{aligned} b \cdot b' - b'' &= \varphi(a) \cdot \varphi(a') - \varphi(a'') \\ &= \varphi(a \cdot a') - \varphi(a'') = \varphi(aa' - a'') \end{aligned}$$

$$b \cdot b' - b'' = \varphi(aa' - a'') \in \varphi(A) \text{ car } aa' - a'' \in A$$

$$\ker(\varphi) = \varphi^{(-1)}(\{0_B\}) \text{ est un s.s.c.p.e de } (A, +_A)$$

$$\forall a \in A \quad k \in \ker(\varphi)$$

$$\begin{aligned} \varphi(a \cdot_A k) &= \varphi(a) \cdot_B \varphi(k) = \varphi(a) \cdot_B 0_B \\ &= 0_B \end{aligned}$$

$$\varphi(k.a) = \varphi(k) \cdot_B \varphi(a) = 0_B \cdot \varphi(a) \\ = 0_B$$



⚡ THE WARNING ⚡

$\ker \varphi = \varphi^{(-1)}(\{0_B\})$ n'est pas en
général un sous-espace de A .

- en général $\ker \varphi \not\ni 1_A$ en effet

$$\text{si } 1_A \in \ker \varphi \Rightarrow \varphi(1_A) = 0_B$$

$$\Rightarrow \varphi = \underline{0}_B$$

Un autre cas où $\ker \varphi$ est un sous-anneau
c'est si $\ker \varphi = \{0_A\}$ (l'anneau nul)
de A

PROPOSITION 3.5. Un morphisme d'anneaux $\varphi \in \text{Hom}_{\text{Ann}}(A, B)$ est injectif ssi $\ker(\varphi) = \{0_A\}$.

PROPOSITION 3.6. Soient $\varphi : A \mapsto B$ et $\psi : B \mapsto C$ des morphismes d'anneaux alors

- $\psi \circ \varphi : A \mapsto C$ est un morphisme d'anneaux.
- Soit $\varphi \in \text{Hom}_{\text{Ann}}(A, B)$ un morphisme d'anneaux bijectif, l'application reciproque $\varphi^{-1} : B \mapsto A$ est un morphisme d'anneaux. On dit que φ est un isomorphisme d'anneaux et on dit que A et B sont des anneaux isomorphes.

NOTATION 3.3. On note

$$\text{Hom}_{\text{Ann}}(A, B), \text{End}_{\text{Ann}}(A) := \text{Hom}_{\text{Ann}}(A, A)$$

$$\text{Isom}_{\text{Ann}}(A, B), \text{Aut}_{\text{Ann}}(A) := \text{Isom}_{\text{Ann}}(A, A)$$

l'ensemble des morphismes, endomorphismes, isomorphismes et automorphismes d'anneaux.

$(0, \text{Id}_A, \circ^{-1})$ est un spe.

est un anneau
/
 $(+, 0, 0_A, \text{Id}_A)$

DÉFINITION 3.6. Soit A un anneau pas forcément commutatif.

- Un idéal (à gauche) de A est un sous-groupe additif $(I, +) \subset (A, +)$ qui est stable par multiplication (à gauche) par les éléments de A :

$$\forall a \in A, b \in I, a.b \in I.$$

- Un idéal (à droite) de A est un sous-groupe additif $(I, +) \subset (A, +)$ qui est stable par multiplication (à droite) par les éléments de A :

$$\forall a \in A, b \in I, b.a \in I.$$

- Un idéal bilatère de A est un sous-groupe additif $(I, +) \subset (A, +)$ qui est un idéal à gauche et à droite:

$$\forall a \in A, b \in I, a.b, b.a \in I.$$

En particulier si A est commutatif les notions d'idéal à gauche, à droite ou bilatère sont toutes les mêmes.

Rmq: si $\varphi: A \rightarrow B$ un morphisme d'anneaux
alors $\ker \varphi$ est un idéal bilatère (m si A n'est pas commutatif)

Anneau Quotient

Exemple: $A = \mathbb{Z}$ $I = q\mathbb{Z}$ $q \geq 1$

alors $q\mathbb{Z}$ est un idéal de $\mathbb{Z}$.

(et tous les idéaux de $\mathbb{Z}$ sont de cette forme)

- $q\mathbb{Z}$ est un ssgr de $(\mathbb{Z}, +)$

- soit $m \in q\mathbb{Z}$ alors m est un multiple de q

$\forall n \in \mathbb{Z}$ $n.m$ est un multiple de q

$\Rightarrow q\mathbb{Z}$ est stable par $\times$ par
les elts de $\mathbb{Z}$.

$\Rightarrow$ on peut former un anneau

$$\mathbb{Z}/q\mathbb{Z} = \{a + q\mathbb{Z} \mid a \in \mathbb{Z}\}$$

(fini d'ordre q)

THÉORÈME 3.1. Soit $(A, +, \cdot, 0_A, 1_A)$ un anneau et $I \subset A$ un idéal bilatère et

$$A/I = \{a \pmod I = a + I, a \in A\}$$

l'ensemble des classes de congruences modulo I . En particulier on a

$$0_A \pmod I = I, 1_A \pmod I = 1_A + I.$$

(1) Il existe une (unique) structure d'anneau

$$(A/I, +_I, \cdot_I, 0_{A/I}, 1_{A/I})$$

telle que l'application

$$\pi_I := \bullet \pmod I : \begin{array}{ccc} A & \mapsto & A/I \\ a & \mapsto & a \pmod I \end{array}$$

soit un morphisme d'anneau surjectif de noyau

$$\ker(\pi_I) = I.$$

On appelle cet anneau l'anneau quotient de A par I et on appelle π_I morphisme canonique de A vers son quotient A/I .

(2) On a en particulier

$$(3.5.1) \quad 0_{A/I} = 0_A \pmod I = I, 1_{A/I} = 1_A \pmod I = 1_A + I$$

et pour tout $a, b \in A$

$$(3.5.2) \quad a \pmod I +_I b \pmod I = a + b \pmod I, a \pmod I \cdot_I b \pmod I = a \cdot b \pmod I.$$

(3) Soit $\varphi : A \rightarrow B$ un morphisme d'anneaux. On suppose que $I \subset \ker(\varphi)$. Alors il existe un unique morphisme d'anneaux

$$\varphi_I : A/I \rightarrow B$$

tel que

$$(3.5.3) \quad \forall a \in A, \varphi_I(a \pmod{I}) = \varphi(a).$$

En d'autres termes on a

$$(3.5.4) \quad \varphi = \varphi_I \circ \pi_I;$$

On dit que le morphisme φ se factorise par le morphisme canonique et on le note avec le diagramme suivant

$$\begin{array}{ccc} A & \xrightarrow{\varphi} & B \\ \pi_I \downarrow & \nearrow \varphi_I & \\ A/I & & \end{array}$$



Corps

Allemand: Koerper

Anglais: Field

"Le corps conditionne le raisonnement."

DÉFINITION 4.1. Un corps K est un anneau commutatif possédant au moins deux éléments $0_K \neq 1_K$ et tel que tout élément non-nul est inversible:

$$K^\times = K - \{0_K\} = K^*$$

Exemples: $\mathbb{Z}$ n'est pas un corps.

$\mathbb{Q}, \mathbb{R}, \mathbb{C}$ sont des corps.

THÉORÈME 4.1. Soit $q \geq 2$ un nombre premier (les seuls diviseurs de q sont 1 et q) alors l'anneau des classes de congruences modulo q ($\mathbb{Z}/q\mathbb{Z}, +, \cdot$) est un corps (fini de cardinal q).

Rmq: la réciproque est vraie: si $q=1$ ou est composé $q=q_1 q_2$ $q_1, q_2 > 1$ alors $\mathbb{Z}/q\mathbb{Z}$ n'est pas un corps.

$$q = q_1 q_2 \quad 1 < q_1, q_2 < q$$

$$q_1(q) \cdot q_2(q) = q_1 q_2(q) = 0(q)$$

on a 2 elts non nuls de $\mathbb{Z}/q\mathbb{Z}$ $q_1(q)$
et $q_2(q)$ dont le produit est nul.

Pourtant $q_1(q)$ n'est pas inversible
car les inversibles de $\mathbb{Z}/q\mathbb{Z}$ sont les
 $a(q)$ avec $(a, q) = 1$

$\Rightarrow \mathbb{Z}/q\mathbb{Z}$ n'est pas un corps. $\square$

Preuve: on veut mq si $q \geq 2$ est premier
alors $\mathbb{Z}/q\mathbb{Z}$ a au moins 2 elts (vrai
car $|\mathbb{Z}/q\mathbb{Z}| = q$)

- $\mathbb{Z}/q\mathbb{Z}$ est commutatif

- On veut mq $(\mathbb{Z}/q\mathbb{Z})^{\times q} \cong \mathbb{Z}/q\mathbb{Z} - \{0(q)\}$

On sait que

$$\left(\mathbb{Z}/q\mathbb{Z}\right)^{\times} = \{ a(q) = a + q\mathbb{Z} \mid (a, q) = 1 \}$$

On veut donc mq si q est premier

$$(a, q) = 1 \iff a(q) \neq 0(q)$$

$$(a, q) \neq 1 \iff a(q) = 0(q)$$

$$\implies (a, q) \neq 1 \quad (a, q) = r > 1 \quad \text{et } r \mid q$$

comme q est premier $r = q$ et $r = q \mid a \Rightarrow a \equiv 0(q)$

$$\Longleftarrow \text{ si } a \equiv 0(q) \Rightarrow q \mid a \Rightarrow (a, q) \geq q > 1$$

si q est premier

$\mathbb{Z}/q\mathbb{Z}$ est un corps a q elts noté $\mathbb{F}_q$

Rmq: pour q premier il n'existe a
isomorphisme pres qu'un seul corps
a q elts $\mathbb{F}_q$

PROPOSITION 4.1. Soit K un corps, B un anneau et $\varphi \in \text{Hom}_{\text{Ann}}(K, B)$ un morphisme d'anneaux. Alors si φ n'est pas nul ($\varphi \neq \underline{0}_B$) φ est injectif:

$$\varphi: K \hookrightarrow B.$$

Preuve: Soit $\varphi: K \rightarrow B$ tq $\varphi \neq \underline{0}_B$

On veut mq $\ker \varphi = \{0_K\}$

soit $k \in \ker \varphi$ si $k \neq 0_K$

alors k est inversible et il existe

$$k^{-1} \in K \text{ tq } k k^{-1} = 1_K$$

$$\varphi(kk^{-1}) = \varphi(1_K) = 1_B$$

$$\varphi(k)\varphi(k^{-1}) = 0_B \cdot \varphi(k^{-1}) = 0_B$$

Contradiction.

φ est injectif.

Prop: Soit K un corps et $I \subset K$ un idéal
alors ou bien $I = \{0_K\}$ ou bien $I = K$.

Preuve: Soit $I \subset K$ un idéal

Supposons $I \neq \{0_K\} \stackrel{?}{\Rightarrow} I = K$

Soit $k \in I - \{0_K\}$, il existe $k^{-1} \in K$ tq $k \cdot k^{-1} = 1_K$
comme I est un idéal et que $k \in I$

$$1_K = k k^{-1} \in I$$

$$\forall k' \in K \quad k' \cdot \underset{I}{1_K} \in I$$

$$\Rightarrow K \subset I \subset K \quad K = I$$



Caractéristique d'un corps

$$\begin{aligned} \text{Can}_K: \mathbb{Z} &\longrightarrow K \\ 1 &\longrightarrow 1_K \\ n \geq 0 &\longrightarrow n_K = 1_K + \dots + 1_K \text{ } n \text{ fois} \end{aligned}$$

$$\ker(\text{Can}_K) = q\mathbb{Z} \quad q \geq 0$$

$$\begin{aligned} q &= \text{caractéristique de } K \\ &= \text{Car}(K) \end{aligned}$$

Cas 1: $\text{Car } K = 0 \Leftrightarrow \text{Can}_K$ est injectif
(son noyau est $\{0\}$)

l'anneau $\mathbb{Z}$ un ssanneau de K
peut être vu comme
en identifiant $\mathbb{Z} \cong \text{Can}_K(\mathbb{Z})$
en particulier K est infini.

en plus K contient une copie
un corps $\mathbb{Q} = \left\{ \frac{a}{b} \mid a \in \mathbb{Z} \ b \in \mathbb{Z} - \{0\} \right\}$
en effet pour toute fraction $\frac{a}{b}$

on définir $\text{Can}_K\left(\frac{a}{b}\right) = \text{Can}_K(a) \cdot \text{Can}_K(b)^{-1}$

$\text{Can}_K(b) \neq 0_K$ il est inversible
et $\text{Can}_K(b)^{-1}$ existe

On vérifie que cette extension

$$\text{Can}_K: \mathbb{Q} \rightarrow K$$

$$\frac{a}{b} \mapsto \text{Can}_K(a) \cdot \text{Can}_K(b)^{-1}$$

$\parallel_{-1}$
 $a_K \cdot b_K$

est un morphisme d'anneau entre $\mathbb{Q}$ et K
qui est donc injectif (car $\neq 0_K$)

et donc K contient une copie
du corps $\mathbb{Q}$ comme sous-corps

$$\text{Can}_K(\mathbb{Q}) \subset K.$$

$$\text{Cor}(K) = p \geq 1$$

Thm: p est un nb premier.

Supposons $p = q_1 q_2$ avec $1 < q_1, q_2 < p$

on a que $p_K = 0_K = q_{1K} \cdot q_{2K}$

$\Rightarrow q_{1K}$ ou q_{2K} est un 1.

Pourquoi: si $q_{1K} \neq 0_K$ q_{1K} serait inversible

$$- q_{1K}^{-1} q_{1K} \cdot q_{2K} = q_{1K}^{-1} 0_K = 0_K$$

$$q_{2K} = 0_K$$

$\Rightarrow$ pas possible car alors $q_2 \in \ker(\text{Can}_K)$
ce qui n'est pas possible car $p \nmid q_2$



alors K contient un copie de $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$
comme sous-corps.

$$\text{Can}_K: \begin{array}{ccc} \mathbb{Z} & \longrightarrow & K \\ n & \longrightarrow & n_K \end{array}$$

$$\ker(\text{Can}_K) = p\mathbb{Z}$$

On va définir un morphisme d'anneau

$$\iota_K: \mathbb{Z}/p\mathbb{Z} \longrightarrow K$$

en posant $\iota_K(n \bmod p) := n_K \in K$

C'est bien défini: si $n' \bmod p = n \bmod p$

alors $n'_K = n_K$ ou a

$$n'(p) = n(p) \Leftrightarrow n' - n = pm \quad m \in \mathbb{Z}$$

$$\Rightarrow n'_K - n_K = p_K m_K = 0_K$$

l'application $i_K: \mathbb{Z}/p\mathbb{Z} \rightarrow K$
 $n(p) \rightarrow n_K$

est bien définie et est un morphisme
d'anneau (car $n \xrightarrow{\text{Can}_K} n_K$ est un
morphisme d'anneau)

i_K est non-nulle (car $\text{Can}_K \neq \underline{0}_K$)
donc est injective $\mathbb{Z}/p\mathbb{Z} = \mathbb{F}_p$ est un
corps.

THÉORÈME 3.1. Soit $(A, +, \cdot, 0_A, 1_A)$ un anneau et $I \subset A$ un idéal bilatère et

$$A/I = \{a \pmod I = a + I, a \in A\}$$

l'ensemble des classes de congruences modulo I . En particulier on a

$$0_A \pmod I = I, 1_A \pmod I = 1_A + I.$$

(1) Il existe une (unique) structure d'anneau

$$(A/I, +_I, \cdot_I, 0_{A/I}, 1_{A/I})$$

telle que l'application

$$\pi_I := \bullet \pmod I : \begin{array}{ccc} A & \mapsto & A/I \\ a & \mapsto & a \pmod I \end{array}$$

soit un morphisme d'anneau surjectif de noyau

$$\ker(\pi_I) = I.$$

On appelle cet anneau l'anneau quotient de A par I et on appelle π_I morphisme canonique de A vers son quotient A/I .

(2) On a en particulier

$$(3.5.1) \quad 0_{A/I} = 0_A \pmod I = I, 1_{A/I} = 1_A \pmod I = 1_A + I$$

et pour tout $a, b \in A$

$$(3.5.2) \quad a \pmod I +_I b \pmod I = a + b \pmod I, a \pmod I \cdot_I b \pmod I = a \cdot b \pmod I.$$

(3) Soit $\varphi : A \rightarrow B$ un morphisme d'anneaux. On suppose que $I \subset \ker(\varphi)$. Alors il existe un unique morphisme d'anneaux

$$\varphi_I : A/I \rightarrow B$$

tel que

$$(3.5.3) \quad \forall a \in A, \varphi_I(a \pmod{I}) = \varphi(a).$$

En d'autres termes on a

$$(3.5.4) \quad \varphi = \varphi_I \circ \pi_I;$$

On dit que le morphisme φ se factorise par le morphisme canonique et on le note avec le diagramme suivant

$$\begin{array}{ccc} A & \xrightarrow{\varphi} & B \\ \pi_I \downarrow & \nearrow \varphi_I & \\ A/I & & \end{array}$$



Corps des Fractions

et

$$(4.2.1)$$

Preuve: soient $a, b \in A$ tq $a.b = 0$

supposons $a \neq 0$ a admet un inverse
dans K note a^{-1} et on a

$$a^{-1} \cdot a \cdot b = a^{-1} \cdot 0 = 0$$

$$b = 0$$



DÉFINITION 4.2. Un anneau A non-nul, commutatif, tel que $\forall a, b \in A$ on ait

$$a.b = 0 \iff a = 0 \text{ ou } b = 0$$

est dit intègre.

Ex: anneau pas intègre

$$q = q_1 q_2 \quad q_1, q_2 > 1 \text{ alors}$$

$\mathbb{Z}/q_1 q_2 \mathbb{Z}$ n'est pas intègre

$$q_1(q) \neq 0(q), q_2(q) \neq 0(q)$$

$$q_1(q) \cdot q_2(q) = q_1 q_2(q) = q(1) = \alpha(q)$$



Ex: $\mathbb{Z}$ est intègre, un corps K est intègre, tout sous-anneau non nul d'un corps est intègre.

THÉORÈME 4.2. Soit A un anneau intègre (en particulier commutatif), alors il existe un corps K et un morphisme d'anneau injectif

$$\iota : A \hookrightarrow K$$

(de sorte qu'on peut considérer A comme un sous-anneau de K en identifiant A à son image $\iota(A) \subset K$) et tel que K a la propriété de minimalité suivante: pour tout corps K' et tout morphisme injectif

$$\iota' : A \hookrightarrow K',$$

il existe un morphisme (nécessairement injectif)

$$\iota'_K : K \hookrightarrow K'$$

prolongeant le morphisme ι' (ainsi A et K peuvent être vus comme des sous-anneaux de K').

 $\iota'_K \circ \iota = \iota'$

DÉFINITION 4.3. Le corps K s'appelle le corps des fractions ~~de~~ et se note $\text{Frac}(A)$.

de A

Preuve (Idée de la construction)

A intègre et on considère

$$A \times (A - \{0\}) = \{ (a, b) \mid a, b \in A \quad b \neq 0_A \}$$

$(a, b) \rightsquigarrow \frac{a}{b}$: fraction rationnelle

on définit sur $A \times (A - \{0\})$ une relation
d'équivalence

$$(a, b) \sim (a', b') \text{ ssi } ab' = a'b$$

$$\left(\text{Idée } \frac{a}{b}, \frac{a'}{b'} \in \mathbb{Q} \quad \frac{a}{b} = \frac{a'}{b'} \iff ab' = a'b \right)$$

On montre que $\sim$ est une relation d'équivalence
et pour $(a, b) \in A \times (A - \{0\})$ on note
 $\frac{a}{b} :=$ la classe d'équivalence à laquelle (a, b)
appartient.

On a donc $\frac{a}{b} = \frac{a'}{b'}$ ssi $ab' = a'b$

(Rmq: Cela utilise le fait que A est intègre)

on définit le corps $K = \text{Frac}(A)$

$$= \left\{ \frac{a}{b}, (a, b) \in A \times (A - \{0\}) \right\}$$
$$= A \times (A - \{0\}) / \sim$$

On définit sur K une addition et une multiplication

en posant $\frac{a}{b} + \frac{a'}{b'} := \frac{ab' + a'b}{bb'}$

$\nwarrow$
 éléments de A

$\frac{a}{b} \cdot \frac{a'}{b'} := \frac{aa'}{bb'}$ on vérifie que on obtient un anneau commutatif

avec $0_K = \frac{0_A}{1_A}$ $1_K = \frac{1_A}{1_A}$

on a un morphisme d'anneau (injectif)

$$i: A \hookrightarrow K$$

$$a \longmapsto \frac{a}{1_A}$$

— si on a un morphisme inj

$$i': A \hookrightarrow K'$$

on définit une extension de i'

en posant

$$i'_K: K \longrightarrow K'$$

$$\frac{a}{b} \longrightarrow i'_K(a) \cdot (i'_K(b))^{-1}$$

(car $i'_K(b) \neq 0_{K'}$, car $b \neq 0_A$
et i'_K est injectif)

...





Construction de Corps par quotient

On a "vu" que si $A =$ anneau commutatif
 et $I \subset A$ un idéal on peut fabriquer
 un anneau quotient $(\underline{A}, +, \times, 0, 1)$

$$\underline{A} = \{a(I) = a + I, a \in A\} \subset \mathcal{P}(A)$$

$$a + I = \{a + i \mid i \in I\}$$

en posant $a(I) = a + I \subset A$

$$a(I) +_I b(I) := a + b(I)$$

$$a(I) \times_I b(I) := a \cdot b(I).$$

On veut prendre I tel que A/I
soient un corps.

- Comme A est commutatif A/I est commutatif

- A/I possède au moins 2 elts

$$\Leftrightarrow I \neq A$$

si $I \neq A$ soit $a \in A - I$ alors

$$a(I) = a + I \neq I = 0(I) \text{ (sinon } a \in I)$$

DÉFINITION 4.4. soit A un anneau commutatif. Un idéal $I \subset A$ est maximal si $I \neq A$ et si I est maximal pour l'inclusion parmi tous les idéaux de A distincts de A :

$$\forall J \subset A, J \neq A \text{ idéal de } A, I \subset J \implies I = J.$$

THÉORÈME 4.3. L'anneau commutatif A/I est un corps ssi I est un idéal maximal.

Preuve: si I maximal $\implies A/I = \text{corps}$.

(si q est premier alors $q\mathbb{Z}$ est un idéal maximal de $\mathbb{Z}$)

Comme $I \subsetneq A$ A/I possède au moins 2 elts.

et A/I est commutatif.

Montrons que si $a(I) \neq 0(I)$
(ie $a \notin I$) alors $a(I)$ est inversible
dans $A/\underline{I}$.

on cherche $b(I) \neq 0$

$$a(I) \cdot b(I) = ab(I) = 1(I)$$

on cherche $b \in A$ tq $ab - 1 \in I$

Considérons J l'idéal engendré par
 a et I $J = \langle a, I \rangle =$ le plus petit
idéal de A contenant a et I
(l'intersection des idéaux de A contenant
 a et I)

Comme $a \notin I \Rightarrow I \subsetneq J$

Comme I est maximal $\Rightarrow J = A$

Donc $1 \in \langle a, I \rangle = A$

$1 \in \langle a, I \rangle \implies$ il existe

$b \in A$ et $i \in I$ tq

$$1 = ab + i$$

$$ab - 1 = -i \in I$$

$$ab(I) = 1(I) \implies \frac{A}{I} = \text{Caps.}$$

