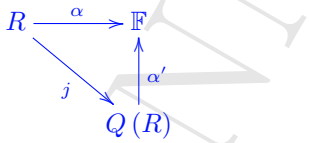
2.4 Le corps des quotients

Dans cette section, il s'agit de construire un corps à partir d'un anneau intègre

2.4.1 Théorème

Soit $(R,+,\times)$ un anneau unitaire commutatif intègre.
Il existe un corps $Q(R)$ et un monomorphisme d'anneau $j : R \longrightarrow Q(R)$ tel que :

1. Tout élément $x \in Q(R)$ soit de la forme $x = \dfrac{j(a)}{j(b)} = j(a)\,(j(b))^{-1}$ avec $a \in R$, $b \in R$ et $b \neq 0$
2. De plus, tout monomorphisme d'anneau $\alpha : R \longrightarrow \mathbb{F}$ où $\mathbb{F}$ est un corps peut se mettre sous la forme composée $\alpha = \alpha' \circ j$ où $\alpha' : Q(R) \longrightarrow \mathbb{F}$ est un monomorphisme unique de corps.
C'est à dire que nous obtenons alors le diagramme suivant :



Démonstration

Soit $(R,+,\times)$ un anneau unitaire commutatif intègre.

1. **On construit le corps** $Q(R)$
Soit R^* l'ensemble des éléments non nuls de R
(a) On définit une relation d'équivalence sur $R \times R^*$
On définit sur $R \times R^*$ la relation $\mathcal{R}$ suivante :

$$(a,b)\,\mathcal{R}\,(c,d) \iff ad = bc$$

Nous allons montrer que c'est une relation d'équivalence
→ La relation $\mathcal{R}$ est réflexive
En effet, pour tout $(a,b) \in R \times R^*$, nous avons $ab = ab$ et donc $(a,b)\,\mathcal{R}\,(a,b)$
→ La relation $\mathcal{R}$ est symétrique
Soient $(a,b) \in R \times R^*$ et $(c,d) \in R \times R^*$ tels que $(a,b)\,\mathcal{R}\,(c,d)$.
Alors $ad = bc \iff cb = da \iff (c,d)\,\mathcal{R}\,(a,b)$.
La relation $\mathcal{R}$ est donc symétrique
→ La relation $\mathcal{R}$ est transitive
Soient $(a,b) \in R \times R^*$, $(c,d) \in R \times R^*$ et $(e,f) \in R \times R^*$ tels que $(a,b)\,\mathcal{R}\,(c,d)$ et $(c,d)\,\mathcal{R}\,(e,f)$
Nous avons donc $ad = bc$ et $cf = de$
- Si $c = 0$, alors $ad = 0$, et comme $d \neq 0$, de l'intégrité de R, nous déduisons que $a = 0$; de la même manière, nous démontrons que $e = 0$. Nous avons alors :

$$(0,b)\,\mathcal{R}\,(0,d) \text{ et } (0,d)\,\mathcal{R}\,(0,f) \text{ et donc } (0,b)\,\mathcal{R}\,(0,f)$$

- Si $c \neq 0$, de $ad = bc$ et $cf = de$, nous déduisons par multiplication $adcf = bcde \iff dc\,(af) = dc\,(be)$. De la règle de simplification dans un anneau intègre vue en 2.3.1 et comme $dc \neq 0$, nous déduisons que $af = be$, c'est à dire $(a,b)\,\mathcal{R}\,(e,f)$

La relation $\mathcal{R}$ est bien transitive
La relation $\mathcal{R}$ est bien une relation d'équivalence sur $R \times R^*$
(b) On appelle $Q(R) = R \times R^*/\mathcal{R}$ l'ensemble quotient
Tout élément de $Q(R)$ est donc une classe d'équivalence modulo $\mathcal{R}$ d'un couple $(a,b) \in R \times R^*$.
Pour la commodité des calculs qui suivent, nous appelons $[a;b]$ cette classe.
Donc $[a;b] = [c;d] \iff ad = bc$

→ Définissons une addition sur $Q(R)$:

$$(\forall [a;b] \in Q(R))(\forall [c;d] \in Q(R))([a;b] \oplus [c;d]) = [ad+bc;bd]$$

Cette addition ne dépend pas des représentants choisis
En effet, soient $(a,b) \in R \times R^*$, $(c,d) \in R \times R^*$, $(x,y) \in R \times R^*$ et $(z,t) \in R \times R^*$ tels que $[a;b] = [x;y]$ et $[c;d] = [z;t]$.
Nous avons donc :

$$[a;b] = [x;y] \Longleftrightarrow ay = bx \text{ et } [c;d] = [z;t] \Longleftrightarrow ct = dz$$

Nous avons donc $[a;b] \oplus [c;d] = [ad+bc;bd]$ et $[x;y] \oplus [z;t] = [xt+yz;yt]$.
Il faut donc montrer que $[ad+bc;bd] = [xt+yz;yt]$. Or :

$$yt(ad+bc) = ytad+ytbc = (ay)\,dt+(ct)\,by = (bx)\,dt+(dz)\,by = bxdt+dzby = bd(tx+zy)$$

Nous avons bien $[ad+bc;bd] = [xt+yz;yt]$
L'addition est bien définie et ne dépend donc pas des représentants choisis.
Cette addition confère à $(Q(R), \oplus)$ la structure de groupe abélien

⋆ L'addition $\oplus$ est évidemment interne

⋆ L'addition $\oplus$ est associative
Soient $[a;b] \in Q(R)$, $[c;d] \in Q(R)$ et $[e;f] \in Q(R)$.
Alors :

$$\begin{aligned}[[a;b] \oplus [c;d]] \oplus [e;f] &= [ad+bc;bd] \oplus [e;f] \\ &= [(ad+bc)f + bde; bdf] \\ &= [adf + bcf + bde; bdf]\end{aligned}$$

Et

$$\begin{aligned}[a;b] \oplus [[c;d] \oplus [e;f]] &= [a;b] \oplus [cf+de;df] \\ &= [adf + b(cf+de); bdf] \\ &= [adf + bcf + bde; bdf]\end{aligned}$$

Nous avons donc $[[a;b] \oplus [c;d]] \oplus [e;f] = [a;b] \oplus [[c;d] \oplus [e;f]]$ et la loi $\oplus$ est bien associative.

⋆ La loi $\oplus$ admet un élément neutre : $[0;1]$.
En effet, pour tout $[a;b] \in Q(R)$, nous avons :

$$[a;b] \oplus [0;1] = [a \times 1 + 0 \times b; b \times 1] = [a;b] \text{ et } [0;1] \oplus [a;b] = [a;b]$$

⋆ Tout élément $[a;b] \in Q(R)$ admet, pour $\oplus$ un symétrique.
Soit $[a;b] \in Q(R)$; le symétrique de $[a;b]$ pour $\oplus$ est donné par $[-a;b]$. En effet :

$$[a;b] \oplus [-a;b] = \left[0;b^2\right]$$

Et nous avons $\left[0;b^2\right] = [0;1]$ puisque $0 \times 1 = b^2 \times 0$ et donc $[a;b] \oplus [-a;b] = [0;1]$. De la même manière, nous montrerions que $[-a;b] \oplus [a;b] = [0;1]$

⋆ La loi $\oplus$ est commutative.
Soient $[a;b] \in Q(R)$ et $[c;d] \in Q(R)$. Alors :

$$[a;b] \oplus [c;d] = [ad+bc;bd] \text{ et } [c;d] \oplus [a;b] = [cb+ad;bd]$$

La loi $\oplus$ est bien commutative

Nous venons de montrer que $(Q(R), \oplus)$ est un groupe abélien

→ Nous appelons $Q(R)^* = Q(R) \setminus \{[0;1]\}$.

De manière évidente, pour tout $b \in R^*$, $[0;1] = [0;b]$ et que si $a \in R$ et $a \neq 0$, $[0;1] \neq [a;b]$ et donc,

$$Q(R)^* = \{[a;b] \text{ où } a \in R^* \text{ et } b \in R^*\}$$

Nous définissons sur $Q(R)^*$ la multiplication suivante :

$$(\forall [a;b] \in Q(R))(\forall [c;d] \in Q(R))([a;b] \otimes [c;d]) = [ac;bd]$$

Cette multiplication ne dépend pas des représentants choisis
En effet, soient $(a,b) \in R \times R^*$, $(c,d) \in R \times R^*$, $(x,y) \in R \times R^*$ et $(z,t) \in R \times R^*$ tels que $[a;b] = [x;y]$ et $[c;d] = [z;t]$.
Nous avons donc :

$$[a;b] = [x;y] \iff ay = bx \text{ et } [c;d] = [z;t] \iff ct = dz$$

Nous avons donc $[a;b] \otimes [c;d] = [ac;bd]$ et $[x;y] \otimes [z;t] = [xz;yt]$.
Il faut donc montrer que $[ac;bd] = [xz;yt]$. Or :

$$yt(ac) = ytac = (ay)tc = (bx)tc = (bx)dz = bdxz$$

Nous avons bien $[ac;bd] = [xz;yt]$
La multiplication $\otimes$ est bien définie et ne dépend donc pas des représentants choisis.
Cette multiplication confère à $\left(Q(R)^*, \otimes\right)$ la structure de groupe abélien

- ⋆ La multiplication $\otimes$ est évidemment interne
- ⋆ La multiplication $\otimes$ est associative
  Soient $[a;b] \in Q(R)^*$, $[c;d] \in Q(R)^*$ et $[e;f] \in Q(R)^*$.
  Alors :
  $$[[a;b] \otimes [c;d]] \otimes [e;f] = [ac;bd] \otimes [e;f] = [ace;bdf]$$
  De même :
  $$[a;b] \otimes [[c;d] \otimes [e;f]] = [a;b] \otimes [ce;df] = [ace;bdf]$$
  Nous avons donc $[[a;b] \otimes [c;d]] \otimes [e;f] = [a;b] \otimes [[c;d] \otimes [e;f]]$ et la loi $\otimes$ est bien associative.
- ⋆ La loi $\otimes$ admet un élément neutre : $[1;1]$.
  En effet, pour tout $[a;b] \in Q(R)^*$, nous avons :
  $$[a;b] \otimes [1;1] = [a \times 1; b \times 1] = [a;b] \text{ et } [1;1] \otimes [a;b] = [a;b]$$
- ⋆ Tout élément $[a;b] \in Q(R)^*$ admet, pour $\otimes$ un inverse.
  Soit $[a;b] \in Q(R)^*$; l'inverse de $[a;b]$ pour $\otimes$ est donné par $[b;a]$, possible puisque $a \in R^*$ et $b \in R^*$. Donc :
  $$[a;b] \otimes [b;a] = [ab;ab]$$
  Et nous avons $[ab;ab] = [1;1]$ *(évident)* et donc $[a;b] \otimes [b;a] = [1;1]$. De la même manière, nous montrerions que $[b;a] \otimes [a;b] = [1;1]$
- ⋆ La loi $\otimes$ est commutative.
  Soient $[a;b] \in Q(R)^*$ et $[c;d] \in Q(R)^*$. Alors :
  $$[a;b] \otimes [c;d] = [ac;bd] \text{ et } [c;d] \otimes [a;b] = [ca;bd]$$
  La loi $\oplus$ est bien commutative

Nous venons de montrer que $\left(Q(R)^*, \otimes\right)$ est un groupe abélien

→ La loi $\otimes$ est distributive par rapport à la loi $\oplus$
Soient $[a;b] \in Q(R)^*$, $[c;d] \in Q(R)^*$ et $[e;f] \in Q(R)^*$. Alors :

$$[a;b] \otimes ([c;d] \oplus [e;f]) = [a;b] \otimes [cf + de;df] = [acf + ade;bdf]$$

Et

$$([a;b] \otimes [c;d]) \oplus ([a;b] \otimes [e;f]) = [ac;bd] \oplus [ae;bf] = \left[acbf + bdae;b^2df\right]$$

Nous avons $[acf + ade;bdf] = \left[acbf + bdae;b^2df\right]$ puisque $b^2df(acf + ade) = bdf(acbf + bdae)$
Et donc :

$$[a;b] \otimes ([c;d] \oplus [e;f]) = ([a;b] \otimes [c;d]) \oplus ([a;b] \otimes [e;f])$$

La loi $\otimes$ est donc distributive par rapport à la loi $\oplus$

Ainsi, $(Q(R), \oplus, \otimes)$ est un corps commutatif.

Ainsi, à partit d'un anneau unitaire, commutatif et intègre, nous avons pu construire un corps

2. **On construit un morphisme de R vers $Q(R)$**
   Soit $j : R \longrightarrow Q(R)$ défini par :
$$\begin{cases} j : R & \longrightarrow & Q(R) \\ a & \longmapsto & j(a) = [a;1] \end{cases}$$
   $\Rightarrow$ j est un homomorphisme d'anneau
   - ⋆ Soient $a \in R$ et $b \in R$. Alors :
$$j(a) \oplus j(b) = [a;1] \oplus [b;1] = [a \times 1 + 1 \times b; 1 \times 1] = [a+b;1] = j(a+b)$$
   - ⋆ Soient $a \in R$ et $b \in R$. Alors :
$$j(a) \otimes j(b) = [a;1] \otimes [b;1] = [ab;1] = [a+b;1] = j(ab)$$
   - ⋆ Et, de manière évidente, $j(1) = [1;1]$

   $\Rightarrow$ j est injectif
   En effet, soient $a \in R$ et $b \in R$ tels que $j(a) = j(b)$. Nous avons :
$$j(a) = j(b) \Longleftrightarrow [a;1] = [b;1] \Longleftrightarrow a = b$$
3. **Soit $x = [a;b]$ un élément quelconque de $Q(R)$**
   Alors, considérons l'expression $[b;1] \otimes x$
$$[b;1] \otimes x = [b;1] \otimes [a;b] = [ab;b] = [a;1]$$
   Ainsi, x est la solution de l'équation $j(b)\, x = j(a)$; comme $b \in R^*$, $(j(b))^{-1}$ existe dans $Q(R)$, et donc $x = j(a)(j(b))^{-1}$, et d'après la définition de quotient déjà rencontrée, nous avons $x = \dfrac{j(a)}{j(b)}$
4. **Soit $\mathbb{F}$ un corps et $\alpha : R \longrightarrow \mathbb{F}$ un morphisme d'anneaux**
   Si $\alpha' : Q(R) \longrightarrow \mathbb{F}$ telle que $\alpha = \alpha' \circ j$ existe, comme α' est un morphisme de corps (donc injectif) et j injective par construction, α est forcément injectif et α' doit vérifier :
$$\begin{aligned} \alpha'([a;b]) &= \alpha'\left(j(a)(j(b))^{-1}\right) \\ &= \alpha'(j(a))\,\alpha'\left((j(b))^{-1}\right) \\ &= \alpha'(j(a))\,(\alpha'(j(b)))^{-1} \\ &= \alpha(a)(\alpha(b))^{-1} \\ &= \frac{\alpha(a)}{\alpha(b)} \end{aligned}$$
   Ainsi, α' est-elle bien définie.

Remarque 17 :

Soit $(R, +, \times)$ un anneau unitaire commutatif intègre. Il est donc possible d'identifier chaque élément $a \in R$ avec son image $j(a) \in Q(R)$. Cette identification a pour effet de faire de $j : R \longrightarrow Q(R)$ un morphisme injectif d'insertion.
Ainsi, tout anneau intègre $(R, +, \times)$ est un sous-anneau d'un corps $(Q(R), \oplus, \otimes)$, les opérations $\oplus$ et $\otimes$ n'étant qu'un prolongement de l'addition $+$ et $\times$ dans R.

2.4.2 Corollaire

Si un anneau unitaire commutatif intègre $(R, +, \times)$ est un sous-anneau d'un corps $(\mathbb{F}, +, \times)$, dans lequel tout les éléments $x \in \mathbb{F}$ sont de la forme $x = \dfrac{a}{b}$ avec $a \in R$ et $b \in R^*$, alors $Q(R)$ est isomorphe à $\mathbb{F}$

Remarque 18 :

C'est par cette méthode que nous construisons $\mathbb{Q}$ à partir de l'anneau des entiers relatifs $\mathbb{Z}$