Anneau quotient d'un anneau commutatif

Considérons un anneau commutatif A et I un idéal de A.
Puisque I est un sous groupe de $(A,+)$ qui est commutatif, on peut associer à I la relation d'équivalence $\mathcal{R}$ définie pour tous $x,y \in A$ par la condition :

$$x \mathcal{R} y \iff x-y \in I$$

L'ensemble quotient A/I, muni de la loi

$$(x+I)+(y+I) = (x+y)+I$$

est donc un groupe abélien d'élément neutre $\overline{0} = I$.
On va définir une deuxième loi sur A/I appelée multiplication de sorte que A/I soit, avec l'addition précédente, muni d'une structure d'anneau commutatif.
Soient $x+I$ et $y+I$ deux éléments de A/I.
On définit la multiplication par la formule

$$(x+I)(y+I) = xy+I$$

Pour que cette définition ait du sens, il faut vérifier qu'elle ne dépend pas des représentants x et y de $x+I$ et $y+I$.
Soient $x', y' \in A$ tels que l'on ait $x+I = x'+I$ et $y+I = y'+I$
Il existe $r,t \in I$ tels que $x = x'+r$ et $y = y'+t$. On a

$$xy = x'y' + (x't + ry' + rt)$$

Puisque r et t sont dans I, il en est de même de $x't+ry'+rt$, par suite, $xy-x'y'$ appartient à I, ce qui établit notre assertion.

Théorème : L'ensemble A/I muni de l'addition et la multiplication définies précédemment est un anneau commutatif. On l'appelle l'anneau quotient de A par I.

Preuve : On sait déjà que $(A/I,+)$ est un groupe commutatif. La multiplication dans A étant associative et commutative, il en est de même dans A/I. Par ailleurs, $1+I$ est l'élément neutre multiplicatif de A/I.
Il reste à vérifier que la multiplication est distributive par rapport à l'addition. Soient $x,y,z \in A$, on a les égalités :

$$\begin{aligned}(x+I)\big((y+I)(z+I)\big) &= (x+I)\big((yz)+I\big)\\ &= x(yz)+I\\ &= (xy+xz)+I\\ &= (xy+I)(xz+I)\\ &= (x+I)(y+I)+(x+I)(z+I)\end{aligned}$$

La deuxième égalité dans la définition de la distributivité se vérifie de la même façon. D'où le résultat

■

L'anneau quotient $\mathbb{Z}/n\mathbb{Z}$:

Soit $n \geq 1$ un entier.

On a vu que $n\mathbb{Z}$ est un idéal de $\mathbb{Z}$. D'après le théorème précédent, l'ensemble $\mathbb{Z}/n\mathbb{Z}$ est donc muni d'une structure d'anneau commutatif pour laquelle l'addition et la multiplication sont données par les égalités :

$$\bar{a} + \bar{b} = \overline{a+b} \quad \text{et} \quad \bar{a}\bar{b} = \overline{ab} \qquad \forall\, a, b \in \mathbb{Z}$$

Rappelons que l'élément neutre additif est $\bar{0} = n\mathbb{Z}$. L'élément neutre multiplicatif est $\bar{1} = 1 + n\mathbb{Z}$.

L'anneau $\mathbb{Z}/n\mathbb{Z}$ s'appelle l'anneau des entiers modulo n.

Groupe des éléments inversibles / Corps :

Soit A un anneau

Définition : On dit qu'un élément $a \in A$ est inversible s'il possède un inverse pour la multiplication, autrement dit, s'il existe un élément $b \in A$ tels que l'on ait $ab = ba = 1$. On notera $A^\times$ l'ensemble des éléments inversibles de A.

Proposition : L'ensemble $(A^\times, \times)$ muni de la multiplication induite par celle de A, est un groupe. On l'appelle le groupe des éléments inversibles de A, ou le groupe des unités de A.

Exemple :

- $\mathbb{Z}^* = \{\pm 1\}$
- $A[X]^* = A^*$
- $M_n(A)^* = GL_n(A) = \{M \in M_n(A) \mid \det(M) \in A^*\}$

Lemme : Soient A et B deux anneaux. Le groupe des éléments inversibles de l'anneau produit $A \times B$ est $A^* \times B^*$. Autrement dit,

$$(A \times B)^* = A^* \times B^*$$

Preuve :

Si $(a,b) \in (A \times B)^*$, il existe $(c,d) \in A \times B$ tels que

$$(a,b)(c,d) = (c,d)(a,b) = (1_A, 1_B)$$

En d'autres termes, $ac = ca = 1_A$ et $bd = db = 1_B$.

donc $a \in A^\times$ et $b \in B^\times$. La réciproque se prouve similairement.

Lemme : Soit A un anneau commutatif et I un idéal de A. Alors $I = A$ s'il existe un élément inversible dans I.

Preuve :

Supposons qu'il existe $x \in I \cap A^*$. Dans ce cas, $x x^{-1} = 1$ est dans I. Par suite, $\forall y \in A$, l'élément $y \cdot 1 = y$ est aussi dans I, d'où $I = A$.

Définition : On dit que A est un corps si l'on a $1 \neq 0$ et si tout élément non nul de A est inversible, i.e., si l'on a

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

Exemple :

- Les anneaux $\mathbb{Q}$, $\mathbb{R}$ et $\mathbb{C}$ sont des corps commutatifs.

Homomorphisme d'anneaux

Définition : Soient A et B deux anneaux. On appelle morphisme d'anneaux de A dans B toute application $f : A \to B$ vérifiant les conditions suivantes :

1) $\forall\, x, y \in A$ $\quad f(x+y) = f(x) + f(y)$
$\qquad\qquad\qquad\qquad\quad f(xy) = f(x) f(y)$

2) On a $f(1_A) = 1_B$.

Exemple :

Pour $n \geq 1$ un entier, la surjection canonique $\pi : \mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$ définie par $\pi(x) = x + n\mathbb{Z}$ est un morphisme d'anneaux.

Lemme : Soient $f : A \to B$ un morphisme d'anneaux et A', B' des sous-anneaux de A et B respectivement.

1) L'image $f(A')$ est un sous-anneau de B.

2) L'image réciproque $f^{-1}(B')$ est un sous-anneau de A.

Preuve : Exercice.

De façon analogue aux morphismes de groupes, on démontre que la composée de deux morphismes d'anneaux est un morphisme d'anneaux, et que si un morphisme d'anneaux est une bijection, son application réciproque est aussi un morphisme d'anneaux.

Définition : Soient A et B deux anneaux. On appelle isomorphisme de A sur B tout morphisme d'anneaux bijectif de A sur B.
S'il existe un isomorphisme entre A et B, on dit que A et B sont isomorphes.

Lemme : Soient A et B deux anneaux commutatifs, $f : A \to B$ un morphisme, et I un idéal de B. Alors $f^{-1}(I)$ est un idéal de A.

Preuve : Considérons deux éléments $x \in A$ et $y \in f^{-1}(I)$, alors

l'élément $f(xy) = f(x)f(y)$ est dans I car $f(y) \in I$.
Donc $xy \in f^{-1}(I)$.
L'assertion en résulte puisque $f^{-1}(I)$ est un sous-groupe additif de A.

■

Remarque : L'image par un morphisme d'un idéal n'est pas en général un idéal, comme le montre l'injection $\mathbb{Z} \hookrightarrow \mathbb{Q}$.

Définition : Soient A et B deux anneaux et $f : A \to B$ un morphisme.
On appelle noyau de f et on note $\ker(f)$ l'idéal $f^{-1}(\{0\})$.
Le sous-anneau $f(A)$ de B s'appelle l'image de f.

Théorème : Soient A un anneau commutatif, B un anneau, et $f : A \to B$ un morphisme. Alors on a un isomorphisme d'anneaux

$$\varphi_f : A/\ker(f) \longrightarrow f(A)$$
$$x + \ker(f) \longmapsto f(x)$$

Preuve :
L'application est bien définie car si $x + \ker(f) = x' + \ker(f)$, il existe $y \in \ker(f)$ tels que $x = x' + y$ donc

$$\varphi_f(x) = \varphi_f(x'+y) = \varphi_f(x') + \varphi_f(y) = \varphi_f(x') + 0 = \varphi_f(x')$$

c'est un morphisme de groupes additifs. car

$$\varphi_f((x+\ker f)+(y+\ker f)) = \varphi_f((x+y)+\ker f)$$
$$= f(x+y)$$
$$= f(x)+f(y)$$
$$= \varphi_f(x+\ker f) + \varphi_f(y+\ker f)$$

φ_f est injectif car si $\varphi_f(x+\ker f) = 0$, alors $f(x) = 0$ donc $x \in \ker f$ et $x+\ker f = \ker f$.

φ_f est clairement surjective. Ainsi φ_f est bijective.

Par ailleurs, on a :

$$\varphi_f((x+\ker f)(y+\ker f)) = \varphi_f(xy+\ker f)$$
$$= f(xy)$$
$$= f(x)\,f(y)$$
$$= \varphi_f(x+\ker f)\,\varphi_f(y+\ker f)$$

De plus $\varphi_f(1_A+\ker f) = f(1_A) = 1_B$.

Donc φ_f est un isomorphisme d'anneaux. ∎

Théorème : Soit A un anneau et a, b deux éléments de A tels que $ab = ba$. Alors pour tout entier $n \geq 0$, on a

$$(a+b)^n = \sum_{k=0}^{n} \binom{n}{k} a^k b^{n-k}$$

Preuve : comme dans le cas classique. ∎