Chapitre 1

LOIS DE COMPOSITION INTERNES, GROUPES

2.1 Lois de composition internes

Définition 2.1.1 *Soit E un ensemble non vide. On appelle loi de composition interne sur E toute application de $E \times E$ dans E.*

Notation : Une loi de composition interne est généralement notée par $*, T, \perp, +, \times, \circ, \ldots$

Si E est muni d'une loi de composition interne $*$ alors, pour tout $(x, y) \in E \times E$,l'image de (x, y) est notée $x * y$ et est appelée le composé de x et y par la loi $*$.

Définition 2.1.2 *Une loi de composition interne $*$ définie sur un ensemble E est dite associative si et seulement si*

$$(x * y) * z = x * (y * z), \forall (x, y, z) \in E^3$$

et elle est dite commutative si et seulement si

$$x * y = y * x, \forall (x, y) \in E^2$$

Définition 2.1.3 *Soit $(E, *)$ un ensemble muni d'une loi de composition interne et $a \in E$. L'élément a est dit élément central si*

$$x * a = a * x, (\forall x \in E)$$

l'ensemble des élèment centraux de E est appelé centre de E on le note $C(E)$ ou $Z(E)$,

$$Z(E) = \{a \in E \mid a * x = x * a, \forall x \in E\}$$

Proposition 2.1.1 *Soit $(E,*)$ un ensemble muni d'une loi de composition interne. La loi $*$ est commutative si et seulement si $Z(E) = E$.*

Définition 2.1.4 *Soit $(E,*)$ un ensemble muni d'une loi de composition interne. On appelle translation à gauche (respectivement à droite) associée à l'élément a l'application γ_a (respectivement δ_a) définie par :*

$$\gamma_a : \begin{array}{ccc} E & \longrightarrow & E \\ x & \longmapsto & a*x \end{array}, \qquad \delta_a : \begin{array}{ccc} E & \longrightarrow & E \\ x & \longmapsto & x*a. \end{array}$$

Définition 2.1.5 *On dit qu'un élément a est régulier à gauche (respectivement à droite) si et seulement si la translation à gauche γ_a (respectivement la translation à droite δ_a) est injective.*

Théorème 2.1.1 *Soit $(E,*)$ un ensemble muni d'une loi de composition interne. S'il existe un élément $e \in E$ tel que*

$$e*x = x*e = x, (\forall x \in E)$$

alors e est unique, on l'appelle élément neutre de $(E,*)$.

Démonstration. Supposons qu'il existe deux éléments e et e' tels que, pour tout $x \in E$

$$e*x = x*e = x \text{ et } e'*x = x*e' = x.$$

$$\text{Donc } e*e' = e'*e = e = e' \blacksquare$$

Définition 2.1.6 *Soit $(E,*)$ un ensemble muni d'une loi de composition interne et possède un élément neutre e.*

On dit qu'un élément x est symetrisable ou inversible, par rapport à la loi $*$, s'il existe un élément $x' \in E$ tel que

$$x*x' = x'*x = e.$$

On dit que x' est le symétrique ou l'inverse de x et l'élément x est le symétrique ou l'inverse de x'.

2.2 Monoïdes

Définition 2.2.1 *Soit $(E,*)$ un ensemble muni d'une loi de composition interne. On dit que $(E,*)$ est un monoïde si la loi $*$ est associative. Si de plus $*$ admet un élément neutre $(E,*)$ est dit monoïde unitaire.*

Exemple 2.2.1 $(\mathbb{N},+),(\mathbb{N}^*,\times),(\mathbb{Z}^*,\times)$ *sont des monoïdes unitaires .*

Théorème 2.2.1 *Soit $(E;*)$ un monoïde unitaire d'élément neutre e et a E. Si a admet un symétrique a' alors a' est unique.*

Démonstration. Supposons que a admet deux symétriques a' et a'' , alors on a :

$a*a'=a'*a=e$ et $a*a''=a''*a=e$. Donc $a'*a*a''=(a'*a)*a''=e*a''=a''$ et $a'*a*a''=a'*(a*a'')=a'*e=a'$. On en déduit que $a'=a''$ ■

Proposition 2.2.1 *Soit $(E,*)$ un monoïde unitaire d'élément neutre e. Tout élément symetrisable est régulier à droite et à gauche.*

Démonstration. Soit a un élément symetrisable E de symétrique a'.

Si $a*x=a*y$, alors $a'*a*x=a'*a*y$. Donc $x=y$. De même si $x*a=y*a$ alors $x=y$.

D'où a est régulier ■

Proposition 2.2.2 *Soit $(E,*)$ un monoïde unitaire. Si $a,b\in E$ sont symetrisables de symétriques respectivement a' et b' alors $a*b$ est symetrisable de symétrique $b'*a'$.*

Démonstration. On a $(b'*a')*(a*b)=b'*(a'*a)*b=b'*b=e$

et $(a*b)*(b'*a')=a*(b*b')*a'=a*a'=e$. D'où le résultat ■

2.3 Groupes

2.3.1 Définitions et premières propriétés

Définition 2.3.1 *Un ensemble $(G,*)$ muni d'une loi de composition interne est dit un groupe si :*

1. *la loi $*$ est associative,*
2. *la loi $*$ possède un élément neutre,*
3. *tout élément de G est symetrisable.*

On peut dire qu'un groupe est un monoïde unitaire dont tous les éléments sont symetrisables. Si de plus la loi $*$ est commutative on dit que le groupe G est commutative ou abélien. Si le groupe G n'a qu'un nombre fini d'élément on dit que G est un groupe fini ou un groupe d'ordre fini.

Notation : Si la loi du groupe est notée multiplicativement on dit que le groupe est multiplicative et on le note $(G,\cdot)$, et si la loi du groupe est notée additivement on dit que le groupe est additive et on le note $(G,+)$.

Exemples 2.3.1 *1.* $(\mathbb{Z},+),(\mathbb{Q},+),(\mathbb{R},+),(\mathbb{C},+)$ *sont des groupes additives abéliens.*

2. $(\mathbb{Q}^*,\times),(\mathbb{R}^*,\times),(\mathbb{C}^*,\times)$ *sont des groupes multiplicatives abéliens.*

3. $(\mathbb{Z}/n\mathbb{Z},+)$ *est un groupe additive abélien* $(\forall n \in \mathbb{N})$.

4. Soit X *un ensemble non vide,* $(S(X),\circ)$ *l'ensemble des bijections de* X *dans* X *est un groupe. Si* $X=\{1,2,\ldots,n\}$ *on note* $S(X)$ *par* S_n, *et on l'appelle groupe des permutations de* X *ou groupe symétrique de* X.

5. Soit $n \in \mathbb{N}^*$, $(S_n,\circ)$ *est un groupe non abélien pour* $n \geq 3$. *Pour* $n=3$ *on a :*

$$S_3 = \{e = \begin{pmatrix}1&2&3\\1&2&3\end{pmatrix};\ t_1 = \begin{pmatrix}1&2&3\\1&3&2\end{pmatrix};\ t_2 = \begin{pmatrix}1&2&3\\3&2&1\end{pmatrix};\ t_3 = \begin{pmatrix}1&2&3\\2&1&3\end{pmatrix};\ c = \begin{pmatrix}1&2&3\\2&3&1\end{pmatrix};\ c^2 = \begin{pmatrix}1&2&3\\3&1&2\end{pmatrix}\}$$ et

$\circ$	e	t_1	t_2	t_3	c	c^2
e	e	t_1	t_2	t_3	c	c^2
t_1	t_1	e	c	c^2	t_2	t_3
t_2	t_2	c^2	e	c	t_3	t_1
t_3	t_3	c	c^2	e	t_1	t_2
c	c	t_3	t_1	t_2	c^2	e
c^2	c^2	t_2	t_3	t_1	e	c

Proposition 2.3.1 *pour tout élément* a *d'un groupe* G *les applications :*

$$\begin{cases} \gamma_a : & G \longrightarrow G \\ & x \longmapsto ax \\ \delta_a : & G \longrightarrow G \\ & x \longmapsto xa \end{cases}$$

sont bijectives.

Démonstration. Puisque dans un groupe tout élément est inversible, alors γ_a et δ_a sont bijectives ■

Proposition 2.3.2 *Soit* $(G,\cdot)$ *un groupe noté multiplicativement, alors on a :*

1. $(x^{-1})^{-1} = x, (\forall x \in E)$

2. $(x \cdot y)^{-1} = y^{-1} \cdot x^{-1}, (\forall x, y \in E)$

3. *Pour tout a et b éléments de G, les équations :*

$$a \cdot x = b \text{ et } x \cdot a = b$$

admettent des solutions uniques

4. *Pour tout $x \in G$ et pour tout $n, m \in \mathbb{N}$ on a*

$x^n \cdot x^m = x^{n+m}$

$(x^n)^m = x^{nm}$

$x^0 = e$ *(e élément neutre de G)*

2.3.2 Sous groupe d'un groupe

Définition 2.3.2 *Soit $(G, \cdot)$ un groupe noté multiplicativement et H une partie de G.*

On dit que H est une partie stable si et seulement si :

$$(\forall x, y \in H),\ x \cdot y \in H.$$

Définition 2.3.3 *On appelle sous groupe d'un groupe $(G, \cdot)$ toute partie H non vide de G stable tel que $(H, \cdot)$ muni de la loi induite de G est un groupe, on note $H \leq G$.*

Remarque 2.3.1 *Les sous groupes de G ont le même élément neutre que G.*

En effet, si e est l'élément neutre de G et si H est un sous-groupe de G d'élément neutre e', alors $ee' = e'e' = e'$. Or e' est régulier dans G, donc $e = e'$.

Remarque 2.3.2 *Soit H un sous groupe de G et $x \in H$, si x^{-1} est l'inverse de x dans G alors x^{-1} est aussi l'inverse de x dans H.*

En effet, si x' est l'inverse de x dans H , alors on a : $xx' = e = xx^{-1}$. Or x est régulier dans G donc $x = x'$.

Exemples 2.3.2

1. *$\{e\}$ et G sont des sous groupes de G, tout sous groupe de G différent de $\{e\}$ et de G est appelé sous groupe propre.*
2. *Pour tout $n \in \mathbb{N}$, $n\mathbb{Z}$ est un sous groupe de $\mathbb{Z}$.*
3. *Tout sous groupe de $\mathbb{Z}$ est de la forme $n\mathbb{Z}$.*

Théorème 2.3.1 *Pour qu'une partie non vide H de $(G,\cdot)$ soit un sous-groupe il faut et il suffit que :*

$$(\forall x, y \in H),\ xy^{-1} \in H$$

Démonstration. L'implication directe est claire.

Réciproquement, la loi dans H est associative, car elle l'est dans G. Soit $x \in H$ alors on a par hypothèse $xx^{-1} = e \in H$. De plus $ex^{-1} = x^{-1} \in H$. D'ou H est un groupe pour la loi induite de G , c'est-à-dire H est un sous groupe de G. ■

Exercice

1. Démontrer que le centre d'un groupe est un sous groupe.
2. Démontrer que toute partie H non vide d'un groupe est un sous groupe si et seulement si $HH^{-1} = H$

2.4 Homomorphismes et isomorphismes de groupes

Définition 2.4.1 *Soient $(G,*)$ et $(G',\perp)$ deux groupes et $f : G \longrightarrow G'$ une application. On dit que f est un homomorphisme de groupes si :*

$$(\forall x, y \in G),\ f(x * y) = f(x) \perp f(y)$$

Si de plus f est bijective on dit que f est un isomorphisme de groupes.

Si $(G,*) = (G',\perp)$ on dit que f est un endomorphisme de G, et il est dit automorphisme de G s'il est bijective.

Proposition 2.4.1 *Soit $f : (G,\cdot) \longrightarrow (G',\cdot)$ un homomorphisme de groupes. On notera e l'élément neutre de G et e' celui de G', alors on a :*

1. $f(e) = e'$,
2. $f(x^{-1}) = (f(x))^{-1}$, $(\forall x \in G)$,
3. *Si $H \leq G$ alors $f(H) \leq G'$,*
4. *Si $K \leq G'$ alors $f^{-1}(K) \leq G$,*
5. $\ker(f) = \{x \in G \ /\ f(x) = e'\} = f^{-1}(\{e'\}) \leq G$ *et* $Im(f) \leq G'$

Démonstration.

1. On a $f(ee) = f(e)f(e)$, donc $f(e) = f(e)f(e)$. Or tout élément de G' est régulier, donc $f(e) = e'$.

2. Pour tout $x \in G$, on a $f(xx^{-1}) = f(x)f(x^{-1})$ c'est-à-dire $f(e) = f(x)f(x^{-1})$. Or $f(e) = e'$, donc $f(x^{-1}) = (f(x))^{-1}$.

3.Puisque $H \neq \emptyset$ alors $f(H) \neq \emptyset$. Soit $x, x' \in H$, on a $f(x'x^{-1}) = f(x')\,(f(x))^{-1}$. Puisque H est un sous groupe, alors $x'x^{-1} \in H$. Donc $f(x'x^{-1}) = f(x')\,(f(x))^{-1} \in f(H)$, d'ou $f(H) \leq G'$.

5. On a $f(e) = e' \in K$ alors $e \in f^{-1}(K)$. Soit $x, x' \in f^{-1}(K)$. On a $f(x'x^{-1}) = f(x')f(x^{-1})$. Or $f(x')$ et $f(x^{-1}) \in K$ donc $f(x'x^{-1}) \in K$ c'est-à-dire $x'x^{-1} \in K$. D'ou $f^{-1}(K) \leq G$. ■

Proposition 2.4.2 *Soit $f : G \longrightarrow G'$ un homomorphisme de groupes, alors f est injective si et seulement si* $\ker(f) = \{e\}$.

Démonstration. Supposons que f est injective. Soit $x \in \ker(f)$, alors $f(x) = e' = f(e)$, donc $x = e$. Supposons que $\ker(f) = \{e\}$. Soit x et $x' \in G$ tel que $f(x) = f(x')$, alors $f(x'x^{-1}) = e'$. Or $\ker(f) = \{e\}$ donc $x'x^{-1} = e$ c'est-à-dire $x = x'$. D'ou f est injective. ■

Proposition 2.4.3 *Soit $f : G \longrightarrow G'$ un isomorphisme de groupes , alors l'application réciproque $f^{-1} : G' \longrightarrow G$ est un isomorphisme .*

Démonstration. Il suffit de montrer que f^{-1} est un homomorphisme de groupe. Soit x' et y' deux élément de G', alors il existe x et $y \in G$ tel que $x' = f(x)$ et $y' = f(y)$. Donc $f^{-1}(x'y') = f^{-1}(f(x)f(y)) = f^{-1}(f(xy)) = xy = f^{-1}(x')f^{-1}(y')$. ■

Proposition 2.4.4 *Soient $f : G \longrightarrow G'$ et $g : G' \longrightarrow G''$ deux homomorphismes de groupes. Alors $g \circ f : G \longrightarrow G'$ est un homomorphisme de groupes. Si de plus f et g sont des isomorphismes alors $g \circ f$ est également un isomorphisme.*

2.4.1 Sous groupe engendré par une partie d'un groupe

Proposition 2.4.5 *Soit G un groupe. L'intersection d'une famille quelconque de sous groupe de G est un sous groupe de G.*

Démonstration. Soit $(H_i)_{i \in I}$ une famille de sous-groupes de G. Montrons que $\bigcap_{i \in I} H_i$ est un sous-groupe de G.

L'élément neutre e de G appartient à $H_i (\forall i \in I)$ donc $e \in \bigcap_{i \in I} H_i$. Soit $x, y \in \bigcap_{i \in I} H_i$ alors $xy^{-1} \in H_i (\forall i \in I)$ car H_i est un sous-groupe de G, donc $xy^{-1} \in \bigcap_{i \in I} H_i$. ■

Définition 2.4.2 *Soit G un groupe et X une partie de G. Le sous groupe de G engendré par X est le plus petit sous groupe de G contenant X, on le note $\langle X \rangle$. Si $\langle X \rangle = G$ on dit que X est une partie génératrice de G.*

Cas particuliers :

1. Si $X = \emptyset$ alors $\langle X \rangle = \{e\}$
2. Si $X = \{e\}$ alors $\langle X \rangle = \{e\}$
3. Si $X = G$ alors $\langle X \rangle = G$.

Proposition 2.4.6 *Soit G un groupe et X une partie de G . Alors on a* $\langle X \rangle = \bigcap_{X \subset H \leq G} H$.

Exemples 2.4.1 *1. $G = (\mathbb{Z}, +)$*

Si $X = \{n\}$ alors $\langle X \rangle = n\mathbb{Z}$,

Si $X = \{n, m\}$ alors $\langle X \rangle = n\mathbb{Z} + m\mathbb{Z}$.

2. Soit G un groupe et $a \in G$

Si G est noté multiplicativement alors $\langle a \rangle = \{a^n \ / \ n \in \mathbb{Z}\}$

Si G est noté additivement alors $\langle a \rangle = \{na \ / \ n \in \mathbb{Z}\}$

Définition 2.4.3 *On appelle groupe monogène, tout groupe engendré par un seul élément.*

Si de plus G est fini alors G est dit cyclique.

Exemple 2.4.1 *$(\mathbb{Z}, +)$ et $(\mathbb{Z}/n\mathbb{Z}, +)$ sont des groupes cycliques.*

Définition 2.4.4 *soit $(G, \cdot)$ un groupe et $x \in G$. On dit que x est d'ordre fini s'il existe un entier n non nul tel que $x^n = e$. Le plus petit entier p tel que $x^p = e$ est appelé ordre de x, on le note $O(x)$.*

Remarque 2.4.1 *Si x est un élément d'ordre n alors $\langle x \rangle = \{e, x, x^2, \ldots, x^{n-1}\}$.*

Proposition 2.4.7 *Si G est un groupe d'ordre fini alors tout élément de G est d'ordre fini.*

Démonstration. Supposons qu'il existe un élément x de G tel que $O(x) = +\infty$, alors

$$\langle x \rangle = \{e, x, x^2, x^3, ...\}$$

est infini. Ceci est impossible, car G est fini.

2.5 Sous groupes distingués et groupes quotients

Proposition 2.5.1 *Soit $(G,\cdot)$ un groupe et H un sous groupe de G. Les relations binaires suivantes définies sur G par :*

1. $(\forall x,y\in G), x\mathcal{R}_d y \Longleftrightarrow xy^{-1}\in H$
2. $(\forall x,y\in G), x\mathcal{R}_g y \Longleftrightarrow x^{-1}y\in H$

sont des relations d'équivalences, et la classe d'équivalence à gauche (respectivement à droite) est égale à xH (respectivement Hx)

Démonstration. Montrons que $\mathcal{R}_d$ est une relation d'équivalence. $(\forall x\in G), xx^{-1}=e\in H$, donc $x\mathcal{R}_d x$

$(\forall x,y\in G)$ tel que $x\mathcal{R}_d y$ alors $xy^{-1}\in H$. Or H est un sous groupe de G, donc $(xy^{-1})^{-1}=yx^{-1}\in H$. D'ou $y\mathcal{R}_d x$.

$(\forall x,y,z\in G)$ tel que $x\mathcal{R}_d y$ et $y\mathcal{R}_d z$ alors $xy^{-1}\in H$ et $yz^{-1}\in H$. Or H est un sous groupe de H, donc $(xy^{-1})(yz^{-1})=xz^{-1}\in H$. D'ou $x\mathcal{R}_d z$.

$$\begin{aligned}\overline{x}^g &= \{y\in G \mid x^{-1}y\in H\}\\ &= \{y\in G \mid y\in xH\}\\ &= xH\end{aligned}$$

et $\overline{x}^d=\{y\in G \;/\; xy^{-1}\in H\}=Hx$. ■

Remarque 2.5.1 *Si $(G,\cdot)$ est un groupe abélien alors $\mathcal{R}_g=\mathcal{R}_d$.*

Proposition 2.5.2 *Les ensembles quotients $G/\mathcal{R}_g$ et $G/\mathcal{R}_g$ sont en bijection.*

Démonstration. Soit $f: G/\mathcal{R}_g \longrightarrow G/\mathcal{R}_d$ tel que $f(xH)=Hx^{-1}$. Soient xH et $yH\in G/\mathcal{R}_g$ alors on a :

$xH=yH \Longleftrightarrow x^{-1}y\in H \Longleftrightarrow x^{-1}(y^{-1})^{-1}\in H \Longleftrightarrow Hx^{-1}=Hy^{-1}$. Donc l'application f est bien définie et est injective. De plus f est surjective par construction. ■

Définition 2.5.1 *Soit G un groupe et H un sous groupe de G. On appelle indice de H dans G s'il existe le cardinal de l'ensemble quotient $G/\mathcal{R}_g$ (ou le cardinal de $G/\mathcal{R}_d$) , on le note*

$$[G:H]=card\,(G/\mathcal{R}_g)=card\,(G/\mathcal{R}_d)\,.$$

Exemple 2.5.1 *Soit $n \in \mathbb{N}^*$ alors $[\mathbb{Z} : n\mathbb{Z}] = card(\mathbb{Z}/n\mathbb{Z}) = n$.*

Théorème 2.5.1 *(de Lagrange) Soit $(G, \cdot)$ un groupe fini et H un sous groupe de G alors on a :*

$$| G | = [G : H] \times | H |$$

(ou $| G | = card(G)$ appelé ordre de G).

Démonstration. Soit $x \in G$ l'application qui à $h \longmapsto xh$ de H dans xH est une bijection .Donc toutes les classes d'équivalence (à gauche) ont le même cardinal que H.

Or les classes d'équivalences (à gauche) forment une partition de G donc $G = \bigcup_x xH$. par conséquent $card(G) = \sum_x card(xH)$. De plus $card(G/\mathcal{R}_g) = [G : H]$ donc $| G | = [G : H] \times | H |$ ■

Corollaire 2.5.1 *Si G est un groupe fini alors le cardinal de tout sou groupe de G divise le cardinal de G.*

Corollaire 2.5.2 *Soient H et K deux sous groupes d'un groupe G fini tels que $H \subset K$ alors :*

$$[G : H] = [G : K] \times [K : H]$$

Définition 2.5.2 *Soit G un groupe et H un sous groupe de G. On dit que H est un distingué dans G et on note $H \trianglelefteq G$ si :*

$$G/\mathcal{R}_g = G/\mathcal{R}_d$$

Remarque 2.5.2 *Si G est abélien alors tout sous groupe de G est distingue.*

Théorème 2.5.2 *Soit G un groupe et H un sous groupe de G. Alors les propriétés suivantes sont équivalentes :*

1. $H \trianglelefteq G$,
2. $(\forall x \in G), xH = Hx$,
3. $(\forall x \in G), xHx^{-1} = H$,
4. $(\forall x \in G), xHx^{-1} \subset H$,
5. $(\forall x \in G), xH \subset Hx$.

Démonstration.

1) $\Longrightarrow$ 2) Puisque H est distingué dans G alors $G/\mathcal{R}_g = G/\mathcal{R}_d$. Soit $x \in G$ alors il existe $y \in G$ tel que

$$xH = Hy \qquad (1)$$

on déduit de cette égalité qu'il existe $h \in H$ tel que $x = hy$ donc $xy^{-1} = h \in H$ c'est-à-dire $x\mathcal{R}_d y$ par quonséquent

$$Hy = Hx \qquad (2)\,.$$

On déduit de (1) et (2) que, pour tout $x \in G, xH = Hx$.

Les implications 2) $\Longrightarrow$ 3) $\Longrightarrow$ 4) $\Longrightarrow$ 5) sont claires.

5) $\Longrightarrow$ 1) On sait que, pour tout $x \in G, xH \subset Hx$ donc aussi $x^{-1}H \subset Hx^{-1}$ apr conséquent $Hx \subset xH$, on déduit que $xH = Hx$ c'est-à-dire $G/\mathcal{R}_g = G/\mathcal{R}_d$. D'où H est distingué. ■

Théorème 2.5.3 *Soit $(G, \cdot)$ un groupe et H un sous groupe distingué, on note l'ensemble quotient $G/\mathcal{R}_g = G/\mathcal{R}_d = G/H$.*

(*i*) *La correspondance $(xH, yH) \longmapsto xyH$ est une loi de composition interne sur G/H appelé loi quotient.*

(*ii*) *L'ensemble quotient G/H muni de la loi de composition interne définie ci-dessus est un groupe appelé groupe quotient de G par H.*

(*iii*) *La surjection canonique $p : G \longrightarrow G/H$ définie par $p(x) = xH$ est un homomorphisme de groupes.*

Démonstration.

(*i*) Soient $x, x', y, y' \in G$ tel que $xH = x'H$ et $yH = y'H$, alors on a $(x'y')(xy)^{-1} = x'y'y^{-1}x \in x'Hx^{-1}$, or $H \trianglerighteq G$ donc $x'Hx^{-1} = Hx'x^{-1} = H$. Par conséquent $(x'y')(xy)^{-1} \in H$ c-à-d $xyH = x'y'H$. D'où La correspondance $(xH, yH) \longmapsto xyH$ est une application bien définie de $G/H \times G/H \longrightarrow G/H$.

(*ii*) La loi de composition interne définie sur G/H est une loi de composition interne associative, d'élément neutre $eH = H$ et l'inverse de xH est $x^{-1}H$. Donc G/H est un groupe.

(*iii*) Par définition de la loi quotient on a, $p(xy) = xyH = xHyH = p(x)p(y)$, donc p est homomorphisme de groupes. ■

Théorème 2.5.4 *Soit $f : G \longrightarrow G'$ un homomorphisme de groupes*

1. Si $H \trianglerighteq G$ alors $f(H) \trianglerighteq f(G)$

2. Si $H' \trianglerighteq G'$ alors $f^{-1}(H') \trianglerighteq G$
3. $\ker(f) \trianglerighteq G$.

Remarque 2.5.3 *Tout sous groupe distingué d'un groupe est le noyau d'un homomorphisme de groupes.*

En effet , la surjection canonique $p : G \longrightarrow G/H$ est un homomorphisme de groupes et son noyau est H

2.5.1 Décomposition d'un homomorphisme de groupes

Théorème 2.5.5 *Soit $f : G \longrightarrow G'$ un homomorphisme de groupes. Alors il existe un homomorphisme surjectif $p : G \longrightarrow G/\ker(f)$, un isomorphisme $\bar{f} : G/\ker(f) \to Im(G)$ et un homomorphisme injectif $j : Im(G) \longrightarrow g'$ tels que $f = j \circ \bar{f} \circ p$ c'est-à-dire le diagramme suivant est commutatif*

$$\begin{array}{ccc} G & \xrightarrow{f} & G' \\ p \downarrow & & \uparrow j \\ G/\ker f & \xrightarrow{\bar{f}} & Imf \end{array}$$

Démonstration. Posons, pour tout $\bar{x} \in G/\ker f$, $\bar{f}(\bar{x}) = f(x)$ et montrons que $\bar{f}$ est bien définie et est un isomorphisme de groupes.

Soit $x_1, x_2 \in G$ tel que $\bar{x}_1 = \bar{x}_2$ alors $x_1 x_2^{-1} \in \ker f$, donc $f\left(x_1 x_2^{-1}\right) = e'$ c'est-à-dire $f(x_1) = f(x_2)$ d'où $\bar{f}$ est bien définie. De plus on a :

$$\bar{f}(\bar{x}_1 \bar{x}_2) = \bar{f}(\overline{x_1 x_2}) = f(x_1 x_2) = f(x_1) f(x_2) = \bar{f}(\bar{x}_1) \bar{f}(\bar{x}_2)$$

$\bar{f}$ est un homomorphisme de groupes.

Soit $x \in G$ tel que $\bar{f}(\bar{x}) = e'$, d'après la définition de $\bar{f}$ on a $x \in \ker f$ c'est-à-dire $\bar{x} = \bar{e}$. Donc $\bar{f}$ est injectif, par conséquent c'est un isomorphisme de $G/\ker f$ dans Imf.

Par définition de $\bar{f}$ on a, pour tout $x \in G$

$$j \circ \bar{f} \circ p(x) = \bar{f}(\bar{x}) = f(x)$$

ce qui achève la démonstration. ■

Corollaire 2.5.3 *(premier théorème d'isomorphisme) Si $f : G \longrightarrow G'$ est un homomorphisme de groupe alors*

$$G/\ker(f) \simeq Im(G).$$

Proposition 2.5.3 *Soit G un groupe monogène,*

1. *Si G est infini alors G est isomorphe à $\mathbb{Z}$,*
2. *Si G est fini d'ordre n alors G est isomorphe à $\mathbb{Z}/n\mathbb{Z}$.*

Théorème 2.5.6 *(2^{eme} théorème d'isomorphisme)*
Soient G un groupe et H, K deux sous-groupes de G tel que $K \trianglelefteq G$. Alors

$$H/H \cap K \simeq HK/K.$$

Théorème 2.5.7 *(3^{eme} théorème d'isomorphisme)*
Soient H et K deux sous-groupes distingués d'un groupe G. On suppose que $K \subset H$. Alors on a :

1. $H/K \trianglelefteq G/K$
2. $(G/K)/(H/K) \simeq G/H$.

2.6 Groupes symétriques

2.6.1 Groupe des permutations d'un ensemble E

On appelle *permutation* de E toute bijection de E sur lui même. L'ensemble de toutes les permutations de E est un groupe pour la composition des applications. Ce groupe est appelé *groupes des permutations* de E, ou *groupe symétrique* de E, on le note $S(E)$.

Remarque 2.6.1 *Si E et E' sont deux ensembles équipotents alors $S(E)$ et $S(E')$ sont isomorphes.*

En effet, soit $\varphi : E \longrightarrow E'$ une bijection. Alors l'application

$$\begin{array}{ccc} S(E) & \longrightarrow & S(E') \\ f & \longmapsto & \varphi \circ f \circ \varphi^{-1} \end{array}$$

est un isomorphisme de groupes.

2.6.2 Étude du groupe symétrique S_n.

Supposons que E est un ensemble fini de cardinal n, tous les groupes S_E sont isomorphe à S_n, groupe des permutations de $\{1, ..., n\}$. Tous ces groupes sont finis de cardinal $n!$.

Notation : une permutation σ de $\{1,...,n\}$ sera notée $i \longmapsto \sigma(i)$ ou encore

$$\begin{pmatrix} 1 & 2 & \cdots & n \\ \sigma(1) & \sigma(2) & \cdots & \sigma(n) \end{pmatrix}.$$

Si $n = 2$, $cardS_2 = 2$, donc on a :

$$S_2 = \left\{ e = \begin{pmatrix} 1 & 2 \\ 1 & 2 \end{pmatrix}, t = \begin{pmatrix} 1 & 2 \\ 2 & 1 \end{pmatrix} \right\}.$$

Si $n = 3$, $cardS_3 = 6$, et on a :

$$S_2 = \{e, t_1, t_2, t_3, c_1, c_2\}$$

avec $e = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}, t_1 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}, t_2 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}, t_3 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}, c_1 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}, c_2 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}$

Définition 2.6.1 *Soit $E = \{1,...,n\}$ et $I \subset E$. On dit qu'une permutation σ de E opère sur I ou de support I si σ permute tous les éléments de I et laisse invariant chaque élément de $E - I$.*

Une transposition t est une permutation qui opère sur une partie à deux éléments : il existe $i \neq j \in E$ tel que $\sigma(i) = j, \sigma(j) = i$ et pour tout $k \in E - \{i,j\}, \sigma(k) = k$. On la note $t = (i,j)$.

Un cycle de longueur k est une permutation c qui opère sur une partie de E à k éléments, autrement dit : il existe $\{i_1,...,i_k\} \subset E$ telle que

$$\begin{cases} \sigma(i_1) = i_2 \\ \sigma(i_2) = i_3 \\ \vdots \\ \sigma(i_k) = i_1 \\ \sigma(j) = j, \text{et pour } j \notin \{i_1,...,i_k\}. \end{cases}$$

On le note $c = (i_1,...,i_k)$.

Remarque 2.6.2

1. *Toute transposition est un cycle de longueur 2*
2. *Tout cycle de longueur k est un élément de S_n d'ordre k.*
3. *Deux cycle opérant sur deux parties disjointes, sont permutables.*

On montre facilement si c est un cycle de longueur k alors $c^k = e$.

Soient c_1 et c_2 deux cycles opérants respectivement sur $\Omega_1 = \{i_1, ..., i_p\}$ et $\Omega_2 = \{j_1, ..., j_q\}$ deux parties disjointes de E. Alors

$$c_1 \circ c_2(x) = \begin{cases} x = c_2 \circ c_1(x) & \text{si } x \notin \Omega_1 \cup \Omega_2 \\ c_1(x) = c_2 \circ c_1(x) & \text{si } x \in \Omega_1 \\ c_2(x) = c_2 \circ c_1(x) & \text{si } x \in \Omega_2 \end{cases}$$

On déduit que $c_1 \circ c_2 = c_2 \circ c_1$.

Proposition 2.6.1 *Pour $n \geqslant 3$, le groupe S_n n'est pas commutatif.*

Pour $n = 3$, on a : $(1,2) \circ (2,3) = (1,2,3)$ et $(2,3) \circ (1,2) = (1,3,2)$.

Proposition 2.6.2 *Toute permutation de S_n se décompose en produit de cycles deux à deux disjoints et dont la somme des ordres est égle à n. Autrement dit S_n est engendré par les cycles.*

Démonstration. Soit $\sigma \in S_n$ une permutation de support J de cardinal r. On raisonne par recurrence sur r, si $r = 0$ on a $\sigma = e$ donc c'est un cycle de longueur 0. Supposons que la propriété est vrai pour toute permutation de support de cardinal $s < r$. Soit $i_1 \in J$ tel que i_1 n'est pas invariant par σ on pose $J_1 = \{i_1, \sigma(i_1), \sigma^2(i_1), \ldots, \sigma^{r_1}(i_1)\}$ alors $J_1 \subset J$. Soit $c_1 = (i_1, \sigma(i_1), \sigma^2(i_1), \ldots, \sigma^{r_1}(i_1))$ alors $\sigma = c_1 \circ \rho$ où ρ est une permutation de support $J - J_1$ de cardinal $r' < r$. D'après l'hypothèse de recurrence on a $\rho = c_2 \circ \ldots \circ c_k$ où tous les cycles sont disjonits, donc $\sigma = c_1 \circ \ldots \circ c_k$. ■

Exemple 2.6.1 *Soit* $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 3 & 2 & 4 & 1 & 7 & 6 & 5 \end{pmatrix}$ *alors* $\sigma = (1,3,4) \circ (5,7)$.

Théorème 2.6.1 *Toute permutation est un produit de transpositions, c'est-à-dire S_n est engendré par les transpositions.*

Démonstartion. Comme toute permutation est un produit de cycles deux à deux disjoints, il suffit de montrer que tout cycle est un produit de transpositions. Soit $(i_1, \ldots, i_r)$ un cycle de longueur r. Alors on montre aisement que

$$(i_1, \ldots, i_r) = (i_1, i_r) \circ (i_1, i_{r-1}) \circ \ldots (i_1, i_2).$$

Lemme 2.6.1 *Pour toute permutation σ, le produit*

$$\varepsilon(\sigma) = \prod_{i<j} \frac{\sigma(i) - \sigma(j)}{i - j}$$

est égal à ± 1, appelé signature de σ.

Démonstartion. Comme σ est une bijection de l'ensemble $\{1,...,n\}$ alors tous les facteurs du dénominateur se retrouvent donc une fois et une seule dans le numérateur avec éventuellement un changement de signe, donc $\varepsilon(\sigma) = \pm 1$. ■

Une permutation de signature 1 est dite permutation *paire* et elle est dite *impaire* dans le cas contraire.

Remarque 2.6.3 *Toute transposition est une permutation impaire.*

Proposition 2.6.3 *L'application*

$$\begin{array}{rccc} \varepsilon: & (S_n, \circ) & \longrightarrow & (\{1,-1\}, \times) \\ & \sigma & \longmapsto & \varepsilon(\sigma) \end{array}$$

est un homomorphisme de groupes c'est-à-dire $\varepsilon(\sigma \circ \tau) = \varepsilon(\sigma) \times \varepsilon(\tau)$.

On en déduit la proposition suivante :

Proposition 2.6.4 *La signature d'une permutation σ est égale à $(-1)^r$ où r est le nombre de transpositions qui figure dans la décomposition de σ.*

Démonstration. Supposons que $\sigma = t_1 \circ \ldots \circ t_r$ alors $\varepsilon(\sigma) = \varepsilon(t_1)...\varepsilon(t_r) = (-1)^r$. ■

Proposition 2.6.5 *La signature d'un cycle de longueur r est égale à $(-1)^{r-1}$.*

2.7 Groupe opérant sur un ensemble

Définition 2.7.1 *Soient G un groupe et E un ensemble non vide. On dit que G opère sur E ou on a une action de G sur E si on peut définir une application*

$$\begin{array}{ccc} G \times E & \longrightarrow & E \\ (g,x) & \longmapsto & gx \end{array}$$

vérifiant :

1. $(g_1 g_2)\, x = g_1 (g_2 x)$
2. $ex = x$

pour tout $g_1, g_2 \in G$ et $x \in E$.

Exemple 2.7.1 *Soit G un groupe.*

1. *L'application*

$$\begin{array}{ccc} G \times G & \longrightarrow & G \\ (g,x) & \longmapsto & g.x = gxg^{-1} \end{array}$$

définit une opération de G sur lui même. On dit que G opère sur lui par conjugaison.

2. *G opère sur lui même par translation :*

$$\begin{array}{ccc} G \times G & \longrightarrow & G \\ (g,x) & \longmapsto & g.x = gx. \end{array}$$

3. *Soit E un ensemble et G un sous-groupe de $S(E)$. Alors G opère sur E par :*

$$\begin{array}{ccc} G \times E & \longrightarrow & E \\ (\sigma,x) & \longmapsto & \sigma(x). \end{array}$$

Théorème 2.7.1 *Soit G un groupe et E un ensemble non vide. Alors G opère sur E si et seulement s'il existe un homomorphisme de G dans $S(E)$.*

Démonstration. Supposons que G opère sur E. Pour tout $g \in G$, on désigne par t_g l'application

$$\begin{array}{rccc} t_g : & E & \longrightarrow & E \\ & x & \longmapsto & gx \end{array}$$

on a

$$t_g \circ t_{g'} = t_{gg'}$$
$$t_g \circ t_{g^{-1}} = Id_E$$

donc t_g est une permutation de E. Par conséquent l'application

$$\begin{array}{rccc} t : & G & \longrightarrow & S(E) \\ & g & \longmapsto & t_g \end{array}$$

est un homomorphisme de groupes.

Réciproquement : soit un homomorphisme de groupes $\varphi : G \longrightarrow S(E)$ alors on peut définir une action de G sur E par

$$g.x = \varphi(g)(x)$$

pour tout $g \in G$ et $x \in E$. ■

Définition 2.7.2 *Le noyau de l'homomorphisme T défini ci-dessus est appelé noyau de l'action.*

2.7.1 Orbites et stabilisateur d'un élément.

Soit G un groupe opérant sur un ensemble E no vide. On définit sur E une relation d'équivalence associé à l'action de G sur E par :

$$xRy \Longleftrightarrow (\exists g \in G) \text{ tel que } y = gx$$

Définition 2.7.3 *La classe de x modulo la relation R s'appelle l'orbite ou la trajectoire de x, on le note O_x :*

$$O_x = \{gx \mid g \in G\} = Gx.$$

Exemple 2.7.2 *Si G opère sur lui même par conjugaison alors on a*

$$O_x = \{gxg^{-1} \mid g \in G\}.$$

Proposition 2.7.1 *Soit G un groupe opérant sur un ensemble E no vide, l'ensemble des éléments de G qui laisse fixe l'élément x est un sous-groupe de G appelé stabiliosateur ou sous-groupe d'isotropie de x, on le note G_x.*

Démonstration. G_x est non vide car $ex = x$. Soit $g, g' \in G_x$ alors $(gg')\,x = g\,(g'x) = gx = x$ et $g^{-1}x = x$. Donc G_x est un sous-groupe de G. ■

Exemple 2.7.3 *Si G opère sur lui même par conjugaison alors*

$$G_x = \{g \mid gxg^{-1} = x\} = \{g \mid gx = xg\} = C_x$$

le centralisateur de x.

Définition 2.7.4 *On dit que G opère transitivement sur E si le nombre des orbites suivant E est égal à 1, autrement dit si, pour tout $x, y \in E$, il existe $g \in G$ tel que $y = gx$.*

Théorème 2.7.2 *Soient G un groupe qui opère sur un ensemble E et Ω une orbite suivant G. Si $a, b \in \Omega$ alors il existe $g \in G$ tel que*

$$G_b = g^{-1}G_a g.$$

Démonstration. Puisque $a, b \in \Omega$ alors il existe $g \in G$ tel que $b = ga$. Soit $x \in G_b$ alors $x\,(ga) = ga$ c'est-à-dire $(xg)\,a = ga$ donc $(g^{-1}xg)\,a = a$ on en déduit que $g^{-1}G_b g \subset G_a$.

Réciproquement : Soit $x \in G_a$ alors $(xg^{-1})\,b = g^{-1}b$ c'est-àdire $(gxg^{-1})\,b = b$ donc $gxg^{-1} \in G_b$ d'où $G_a \subset g^{-1}G_b g$. ■

Théorème 2.7.3 *Soit E un $G-$ensemble. Il existe une bijection de l'orbite de x sur l'ensemble des classes à gauche modulo G_x.*

Démonstration. Soit $x \in E$, considérons l'application

$$\begin{array}{rccc} f: & O_x & \longrightarrow & G/G_x \\ & gx & \longmapsto & gG_x \end{array}$$

où $\bar{g}$ est la classe de g modulo G_x.

Montrons que f est bien définie. Soit $g, g' \in G$ tel que $gx = g'x$ alors $g^{-1}g'x = x$ donc $g^{-1}g' \in G_x$ c'est-à-dire $g'G_x = gG_x$.

Soit $gx, g'x \in O_x$ tel que $g'G_x = gG_x$ alors $g^{-1}g' \in G_x$ c'est à dire $gx = g'x$. Donc f est injective et puisqu'elle est surjective par construction d'où f est bijective. ■

Corollaire 2.7.1 *Si G est fini alors toutes les orbites sont finies et pour tout $x \in G, card(O_x)$ divise $card(G)$. De plus on a :*

$$card(O_x) = [G : G_x].$$

Corollaire 2.7.2 *Soit E un $G-$ensemble fini et X une partie de E contenant un élément et un seul de chaque orbite, alors on a :*

$$card(E) = \sum_{x \in X} [G : G_x].$$

Théorème 2.7.4 *(équations des classes de Fröbenius). Soit G un groupe qui opère sur lui même par conjugaison, alors on a :*

$$card(G) = card(Z(G)) + \sum_{x \in X - Z(G)} [G : G_x].$$

Démonstration. Puisque G opère sur lui même par conjugaison alors $O_x = \{gxg^{-1} \mid g \in G\}$ et si $x \in Z(G)$ alors $O_x = \{x\}$. Le stabilisateur G_x de x est :

$$G_x = \{g \in G \mid gxg^{-1} = x\}$$

et si $x \in Z(G)$ alors

$$G_x = G.$$

Les orbites de G forment une partition de G alors $card(G) = \sum_{x \in X} O_x = \sum_{x \in Z(G)} O_x + \sum_{x \in X - Z(G)} O_x = card(Z)$

2.8 Exercices

Exercice 2.1 *On définit sur $\mathbb{Q}$ une loi de composition interne (L.C.I) par :*

$$x * y = \frac{x+y}{2}.$$

1. *Montrer que tout élément de $\mathbb{Q}$ est régulier pour la loi $*$.*
2. *Montrer que, pour tout $x, y, y \in \mathbb{Q}$, on a :*

$$x * (y * z) = (x * y) * (x * z).$$

3. *$\mathbb{Q}$ admet-il un élément neutre ?*
4. *$(\mathbb{Q}, *)$ est-il un groupe ?*

Exercice 2.2 *Soit $(G, .)$ un ensemble muni d'une L.C.I associative telle que, pour tout x les translations à gauche γ_x sont surjectives et il existe a tel que la translation à droite δ_a est surjective. Démontrer que $(G, .)$ est un groupe.*

Exercice 2.3 *Soit E un mnoïde non unitaire tel que tout élément est régulier à gauche.*

1. *Montrer que si $u \in E$ est idempotent ($u^2 = u$) alors $ux = x \ \ (\forall x \in E)$*
2. *Montrer que si u, v sont idempotent distincts alors il n'existe aucun couple $(x, y) \in E^2$ tel que $xu = yv$*
3. *Montrer que, si E admet un élément neutre e alors e est le seul élément idempotent.*

Exercice 2.4 *Soit E un monoïde tel qu'il existe $e \in E$ admet un élément neutre à droite et $(\forall x \in E) \ (x' \in E)$ tel que $xx' = e$. Montrer que E est un groupe.*

Exercice 2.5 *Soit E un mnoïde fini tel que tout élément est régulier (simplifiable à droite et à gauche). Montrer que E est un groupe.*

Exercice 2.6 *Soit G un groupe noté multiplicativement tel que $x^2 = e$, pour tout $x \in G$.*

1. *Démontrer que G est abélien*
2. *Démontrer que si G est fini alors $O(G)$ (ordre de G) est une puissance de 2.*

Exercice 2.7 *Soit $(G, .)$ un groupe et H un sous-groupe.*
Démontrer que si $[G : H] = 2$ alors H est un sous-groupe distingué de G.

Exercice 2.8 *Soit G un groupe et H, K sont deux sous-groupes de G. Montrer que les propriétés suivantes sont équivalentes :*

1. *HK est un sous groupe de G*
2. *$HK = KH$.*

Exercice 2.9 *Soit G un groupe, G_1 et G_2 deux sous groupes de G. Montrer que si $G_1 \cup G_2 = G$ alors $G_1 = G$ ou $G_2 = G$.*

Exercice 2.10 *On appelle sous-groupe dérivé du groupe G, et on note $D(G)$, le sous-groupe engendré par les éléments $xyx^{-1}y^{-1}, (x, y \in G)$.*

1. *Montrer que $D(G)$ est distingué dans G.*
2. *Etant donné H un sous-groupe distingué dans G, montrer que G/H est abélien si et seulement si $D(G) \subset H$.*

Exercice 2.11 *Soit H et K deux sous-groupes de G. On désigne par G' le sous-groupe de G engendré par $H \cup K$ et par HK l'ensemble des éléments de la forme hk où $(h, k) \in H \times K$.*

1. *Montrer que si H est distingué dans G alors $G' = HK$.*
2. *On suppose que si H et K sont distingués et $H \cap K = \{e\}$. Montrer que $hk = kh$, $\forall (h, k) \in HK$ et HK est isomorphe à $H \times K$.*

Exercice 2.12 *Soit $\alpha \in S_6$ et $\beta \in S_9$.*

1. *Décomposer en produit de cycles puis en produit de transpositions les permutations* $\alpha = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 3 & 6 & 1 & 4 & 2 & 5 \end{pmatrix}, \beta = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 3 & 7 & 8 & 9 & 4 & 5 & 2 & 1 & 6 \end{pmatrix}$
2. *Calculer*

Exercice 2.13 *Soit $n \in \mathbb{N}$ avec $n \geq 2$.*

1. *Montrer que S_n est engendré par les $n-1$ transpositions $(i, i+1)$.*
2. *Montrer que S_n est engendré par la transposition $(1, 2)$ et le cycle $(1, ..., n)$.*

Chapitre 2

ANNEAUX ET CORPS

3.1 Anneaux

3.1.1 Définitions et règles de calcul

Définition 3.1.1 *On appelle anneau tout ensemble non vide A muni de deux lois de composition internes une loi additive $(+)$ est une loi multiplicative $(\times$ ou $.)$ tel que :*

1. *$(A,+)$ est un groupe abélien*
2. *La multiplication est associative*

$$x(yz) = (xy)z, \forall x, y, z \in A.$$

3. *La multiplication est distributive à droite et à gauche par rapport à l'addition*

$$x(y+z) = xy + xz \text{ et } (y+z)x = yx + yz, \ \forall x, y, z \in A$$

4. *la multiplication possède un élément unité noté 1_A*

$$1_A x = x 1_A = x, \forall x \in A$$

Si de plus la multiplication est commutative l'anneau A est dit commutatif.

Exemples 3.1.1
1. *$(\mathbb{Z},+,\times),(\mathbb{Q},+,\times),(\mathbb{R},+,\times),(\mathbb{C},+,\times)$ sont des anneaux commutatifs.*
2. *Pour tout $n \in \mathbb{N}$, $(\frac{\mathbb{Z}}{n\mathbb{Z}},+,\times)$ est un anneau commutatif.*
3. *$\mathcal{F}(\mathbb{R},\mathbb{R}) = \{$fonctions de $\mathbb{R}$ dans $\mathbb{R}\}$, $(\mathcal{F}(\mathbb{R},\mathbb{R}),+,\circ)$ est un anneau non commutatif*

4. *Soit I un intervalle de $\mathbb{R}$, $\mathcal{F}(I,\mathbb{R}) = \{$fonctions de I dans $\mathbb{R}\}$, $(\mathcal{F}(I,\mathbb{R}),+,\times)$ est un anneau commutatif.*

Proposition 3.1.1 *(règles de calculs dans un anneau) Soit A un anneau. $(\forall x, y, \in A), (\forall n \in \mathbb{N})$, on a :*

1. $x \cdot 0_A = 0_A$
2. $x \cdot (-y) = (-x) \cdot y = -x.y$
3. $x \cdot (ny) = (nx) \cdot y = n(x \cdot y)$
4. $(-x) \cdot (-y) = x \cdot y$

Exercice. Soit A un anneau , a et $b \in A$ tel que $ab = ba$. Montrer que, pour tout $n \in \mathbb{N}$,

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

3.1.2 Eléments remarquables dans un anneau

Définition 3.1.2 *Soit A un anneau.*

1. *Un élément $x \in A$ est dit inversible dans A s'il existe $x' \in A$ tel que :*

$$xx' = x'x = 1_A.$$

2. *Un élément $a \in A$ est dit régulier si a est simplifiable à droite et à gauche par rapport à la multiplication.*
3. *Un élément $a \in A - \{0\}$ est dit diviseur de zéro s'il existe $b \in A - \{0\}$ tel que :*

$$ab = ba = 0$$

4. *Un élément $x \in A$ est dit nilpotent s'il existe $n \in \mathbb{N}^*$ tel que :*

$$x^n = 0,$$

le plus petit entier p tel que $x^p = 0$ est appelé indice de nilpotence de x.

Théorème 3.1.1 *L'ensemble $(U(A),.)$ des éléments inversibles de A muni de la multiplication est un groupe d'élément unité 1_A.*

Démonstration. $U(A)$ est stable par la multiplication : si $u, v \in U(A)$ alors $(uv)(v^{-1}u^{-1}) = 1_A$, donc $uv \in U(A)$, de plus si $u \in U(A)$ alors $u^{-1} \in U(A)$ et $1_A \in U(A)$, donc $U(A)$ est un groupe multiplicatif. ■

Définition 3.1.3 *Un anneau intègre est un anneau non nul commutatif sans diviseur de zéro.*

Exemple 3.1.1 *1.* $(\mathbb{Z},+,\times),(\mathbb{Q},+,\times),(\mathbb{R},+,\times),(\mathbb{C},+,\times)$ *sont des anneaux intègres.*

2. Si n *est un entier premier alors* $(\frac{\mathbb{Z}}{n\mathbb{Z}},+,\times)$ *est un anneau intègre.*

3.1.3 Sous anneaux et idéaux d'un anneau

Définition 3.1.4 *On appelle sous anneau d'un anneau* A *toute partie* B *de* A *telle que*

1. B *est stable pour l'addition*

$$\forall x,y\in B,\ x+y\in B$$

2. B *est stable par la multiplication*

$$\forall x,y\in B,\ x\times y\in B$$

3. B *est un anneau pour les deux lois induites.*

Définition 3.1.5 *(autre définition) Un sous anneau d'un anneau* A *est une partie* B *de* A *telle que :*

1. B *est un sous groupe de* $(A,+)$
2. B *est stable pour la multiplication*
3. $1_A\in B$.

Exemple 3.1.2 $\mathbb{Z}$ *est un sous anneaux de* $(\mathbb{Q},+,\times),\mathbb{Q}$ *est un sous anneaux de* $(\mathbb{R},+,\times),\mathbb{R}$ *est un sous anneaux de* $(\mathbb{C},+,\times)$. *Le seul sous anneau de* $\mathbb{Z}$ *est* $\mathbb{Z}$.

Proposition 3.1.2 *Soit* $(A,+,\times)$ *un anneau et* $B\subset A$. *La partie* B *est un sous anneau de* A *si et seulement si les propriétés suivantes sont satisfaites :*

1. $(\forall x,y\in B),\ x-y\in B$
2. $(\forall x,y\in B),\ xy\in B$
3. $1_A\in B$

Définition 3.1.6 *Soit* $(A,+,\times)$ *un anneau et* I *une partie non vide de* A. *On dit que* I *est un idéal à gauche (resp.à droite) de* A *si* $(I,+)$ *est un sous groupe de* $(A,+)$ *et* $(\forall x\in I,\forall a\in A)\ ax\in I$ *(resp.* $xa\in I$ *). Un idéal qui est à la fois idéal à gauche et à droite est appelé idéal bilatère.*

Remarque 3.1.1 *Si A est un anneau commutatif tout idéal à gauche est un idéal à droite.*

Proposition 3.1.3 *Soient A un anneau et $I \subset A$. La partie I est un idéal à gauche (resp. à droite) de A si et seulement si les propriétés suivantes sont satisfaites :*

1. $(\forall x, y \in I), x + y \in I$ *(stabilité pour la loi $+$)*
2. $(\forall a \in A; \forall x \in I), ax \in I$ *,(resp. $xa \in I$)*

Exemples 3.1.2 1. $(\forall n \in \mathbb{N})$, $n\mathbb{Z}$ *est un idéal de* $\mathbb{Z}$.

2. *Soit A un anneau, $\{0_A\}$ et A sont des idéaux bilatères de A.*
3. *Pour tout $a \in A$,*
$$aA = \{ax \,/\, x \in A\}$$
est un idéal à droite de A et
$$Aa = \{xa \,/\, x \in A\}$$
est un idéal à gauche de A.
4. *Soit B une partie non vide de A,*
$$Ann_g(B) = \{x \in A \,/\, xb = 0_A, \forall b \in B\}$$
est un idéal à gauche de A et
$$Ann_d(B) = \{x \in A \,/\, bx = 0_A, \forall b \in B\}$$
est un idéal à droite de A.

Remarque 3.1.2 *tout idéal à gauche ou à droite de A contenant 1_A est égal à A.*

3.2 Homomorphismes d'anneaux

Définition 3.2.1 *Soient A et A' deux anneaux et $f : A \longrightarrow A'$ une application . On dit que f est un homomorphisme d'anneaux si :*

1. $f(x + y) = f(x) + f(y)$
2. $f(xy) = f(x)f(y)$
3. $f(1_A) = 1_{A'}$

Si de plus f est bijective on dit que f est un isomorphisme d'anneaux.

Remarque 3.2.1 *Si $f : A \longrightarrow A'$ est un homomorphisme d'anneaux alors*

$$f(0_A) = 0_{A'}$$
$$f(-x) = -f(x) \quad (\forall x \in A)$$

Proposition 3.2.1 *Soient $f : A \longrightarrow A'$ un homomorphisme d'anneaux B et B' deux sous anneaux de A et A' respectivement alors on a :*

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

Démonstration. Soient $y, y' \in f(B)$, alors il existe $x, x' \in B$ tel que $y = f(x)$ et $y' = f(x')$. On a $y - y' = f(x) - f(x') = f(x - x')$. Puisque B est un anneau alors $x - x' \in B$ par conséquent $f(x - x') \in f(B)$ c'est-à-dire $y - y' \in f(B)$. Or $yy' = f(x) f(x') = f(xx')$ car f est un homomorphisme d'anneaux de plus $xx' \in B$ (B est un sous anneau de A), donc on déduit que $yy' \in f(B)$. Puisque B est un sous anneau de A alors $1_A \in B$ et $f(1_A) = 1_{A'} \in f(B)$. Donc B est un sous anneaux de A'.

Montrons la seconde assertion, $f^{-1}(B') = \{x \in A \mid f(x) \in B'\}$. On a $1_{A'} = f(1_A)$, donc $1_A \in f^{-1}(B')$, de plus si $x, x' \in f^{-1}(B')$ alors $f(xx') = f(x) f(x') \in B'$ car B' est un sous anneau de A', donc $xx' \in f^{-1}(B')$ c'est-à-dire $f^{-1}(B')$ est stable pour la multiplication. Or $f(x - x') = f(x) - f(x') \in B'$ car B' est un sous anneau de A', donc $x - x' \in f^{-1}(B')$. D'où $f^{-1}(B')$ est un sous anneau de A. ■

Proposition 3.2.2 *Soient $f : A \longrightarrow A'$ un homomorphisme d'anneaux I et I' deux idéaux de A et A' respectivement alors on a :*

1. *$f(I)$ est un idéal de $f(A')$*
2. *$f^{-1}(I')$ est un idéal de A.*

Proposition 3.2.3 *Soit $f : A \longrightarrow A'$ un homomorphisme d'anneaux alors on a :*

1. *$f(A)$ est un sous anneau de A', appelé image de f, et est noté $Im(f)$,*
2. *$f^{-1}(\{0_{A'}\})$ est un idéal de A, appelé noyau de f, et est noté $\ker(f)$.*

Proposition 3.2.4 *Soit $f : A \longrightarrow A'$ un homomorphisme d'anneaux, alors on a :*

1. *f est injective si et seulement si $\ker(f) = \{0_A\}$*
2. *f est surjective si et seulement si $Im(f) = A'$.*

3.3 Anneaux quotients

Théorème 3.3.1 *Soient A un anneaux, I un idéal bilatère de A et $(\frac{A}{I},+)$ le groupe quotient. Il existe une loi de composition interne unique notée aussi $\times$ telle que :*

1. *$(\frac{A}{I},+,\times)$ est un anneau*
2. *la surjection canonique $p : A \longrightarrow \frac{A}{I}$ est un homomorphisme d'anneaux.*

L'anneau $(\frac{A}{I},+,\times)$ est appelé anneau quotient, si de plus l'anneau A est commutatif $\frac{A}{I}$ est aussi commutatif.

Démonstration. Posons $\overline{x} \times \overline{y} = \overline{x \times y}$ et montrons que cette loi est bien définie.

Soient $\overline{x},\overline{x'},\overline{y},\overline{y'} \in \frac{A}{I}$ tels que $\overline{x} = \overline{x'}$ et $\overline{y} = \overline{y'}$, montrons que $\overline{x} \times \overline{y} = \overline{x'} \times \overline{y'}$. On a $xy - x'y' = (x-x')y + x'(y-y')$. Puisque $\overline{x} = \overline{x'}$ et $\overline{y} = \overline{y'}$ alors $x - x'$ et $y - y' \in I$. Donc $xy - x'y' \in I$, c-à-d $\overline{x \times y} = \overline{x' \times y'}$ c-à-d $\overline{x} \times \overline{y} = \overline{x'} \times \overline{y'}$. De plus la loi ainsi définie est unique telle que $(\frac{A}{I},+,\times)$ est un anneau et la surjection canonique $p : A \longrightarrow \frac{A}{I}$ est un homomorphisme d'anneau. ■

Théorème 3.3.2 *(décomposition canonique d'un homomorphisme d'anneaux)*

Soient $f : A \longrightarrow A'$ un homomorphisme d'anneaux , $p : A \longrightarrow \frac{A}{\ker f}$ la surjection canonique et $j : Im(f) \longrightarrow A'$ l'injection canonique. Alors il existe un isomorphisme unique $\bar{f} : \frac{A}{\ker f} \longrightarrow Im(f)$ tel que $f = j \circ \bar{f} \circ p$ c-à-d le diagramme suivant est commutatif

$$\begin{array}{ccc} A & \xrightarrow{f} & A' \\ p \downarrow & & \uparrow j \\ \frac{A}{\ker f} & \xrightarrow{\bar{f}} & Im(f) \end{array}$$

Corollaire 3.3.1 *(1er théorème d'isomorphisme) Soient $f : A \longrightarrow A'$ un homomorphisme d'anneaux, alors $A/\ker f$ est isomorphe à $Im(f)$.*

3.4 Idéaux d'un anneau commutatif

Proposition 3.4.1 *Soient A un anneau commutatif et $(I_i)_{i\in I}$ une famille quelconque d'idéaux.*
Alors $\bigcap_{i\in I} I_i$ est un idéal de A.

Démonstration. $\bigcap_{i\in I} I_i \neq \emptyset$ car $0_A \in I_i$, pour tout $i \in I$. Soient $a \in A$ et $x, y \in \bigcap_{i\in I} I_i$ alors $ax, x+y \in \bigcap_{i\in I} I_i$ car, pour tout $i \in I$, I_i est un idéal de A. Donc $\bigcap_{i\in I} I_i$ est un idéal de A. ■

Définition 3.4.1 *Soit A un anneau commutatif et X une partie de A . On appelle idéal engendré par X le plus petit idéal de A contenant X on le note (X). Si $X = \{a\}$ alors $(X) = (a)$ est dit idéal principal.*

Proposition 3.4.2 *Soit A un anneau commutatif et X une partie de A. Alors l'idéal engendré par X est l'intersection de tout les idéaux de A contenant X .*

Proposition 3.4.3 *Soit A un anneau commutatif*

1. *Si $X = \emptyset$ alors $(X) = \{e\}$*
2. *Si $X = \{x\}$ alors $(X) = Ax = \{ax \mid a \in A\}$*
3. *Si $X = \{x_1, ..., x_n\}$ alors $(X) = \{a_1x_1 + ... + a_nx_n \mid a_1, \ldots, a_n \in A\}$*
4. *Si X est une partie infinie de A alors*

$$(X) = \{x \in A \mid \exists n \in \mathbb{N}^* \text{ tel que } x = a_{i_1}x_{i_1} + ... + a_{i_n}x_{i_n} \text{ avec } x_{i_j} \in X, a_{i_j} \in A\}.$$

Théorème 3.4.1 *Soient A un anneau commutatif I et J deux idéaux de A. alors*

$$I + J = \{x + y \mid x \in I, y \in J\}$$

est idéal de A appelé idéal somme de I et J.

Démonstration. L'élément neutre $0_A \in I + J$ donc $I + J \neq \emptyset$. Soient $z, z' \in I + J$, alors il existe $x, x' \in I$ et $y, y' \in J$ tel que $z = x + y$ et $z' = x' + y'$. Donc $z + z' = (x + y) + (x' + y') = (x + x') + (y + y') \in I + J$. Et si $a \in A$ alors $az = a(x + y) = ax + ay \in I + J$. Donc $I + J$ est un idéal de A. ■

Remarque 3.4.1 *Si $X = \{a_1, ...a_n\}$ alors $(X) = (a_1) + ... + (a_n)$*

Définition 3.4.2 *(idéal produit) Soient A un anneau commutatif I et J deux idéaux de A. L'idéal engendré par $\{xy \mid x \in I \text{ et } y \in J\}$ est appelé idéal produit de I et J. On le note $I \cdot J$.*

Définition 3.4.3 *Soit A un anneau. L'application :*

$$\begin{array}{rccc} \varphi & : & \mathbb{Z} & \longrightarrow & A \\ & & n & \longmapsto & n1_A \end{array}$$

est un homomorphisme d'anneaux. L'entier p qui engendre $\ker\varphi$ est appelé caractéristique de A on la note $caract(A)$.

Si φ est injective alors $\ker\varphi = \{0\}$;donc $caract(A) = 0$

Si φ est non injective alors il existe un entier $p \neq 0$ tel que $Kerf = p\mathbb{Z}$,donc $caract(A) = p$.

Remarque 3.4.2 *Si $caract(A) = p$ alors $p1_A = 0_A$, donc $px = 0_A, \forall x \in A$.*

Proposition 3.4.4 *Un anneau A non nul sans diviseurs de zéro (en particulier un anneau intègre) est de caractéristique 0 ou un nombre premier.*

Démonstration. si $caract(A) = p \neq 0$ alors $Ker\varphi = p\mathbb{Z}$. Donc $\dfrac{\mathbb{Z}}{p\mathbb{Z}}$ est isomorphe à $Im\varphi = \mathbb{Z}1_A$ qui est un anneau intègre, donc p est un nombre premier. ■

Exemple 3.4.1 *1.* $ccaract(\mathbb{Z}) = caract(\mathbb{Q}) = caract(\mathbb{R}) = caract(\mathbb{C}) = 0$

2. $caract(\dfrac{\mathbb{Z}}{n\mathbb{Z}}) = n$.

3.5 Divisibilité dans les anneaux intègres

Définition 3.5.1 *Soit A un anneau et $(a, b) \in A^2$. On dit que a divise b si et seulement s'il existe $q \in A$ tel que $b = aq$, et on note $a \mid b$.*

Remarque 3.5.1 *1.* $\forall u \in U(A), \forall b \in A,\ u \mid b$

2. $\forall a \in A - \{0\},\ a \mid 0$.

Proposition 3.5.1 *Pour tout $(a, b) \in A^2$ on a :*

(i) $a \mid b \Longleftrightarrow (b) \subset (a)$

(ii) $(a) = (b) \Longleftrightarrow \exists u \in U(A)$, *tel que* $b = ua$, *on dit que a et b sont associés.*

Démonstration. (i) $a \mid b \iff \exists\ q \in A$ tel que $b = qa \iff b \in (a)$ i.e $(b) \subset (a)$.

(ii) On a d'après ce qui précède $(a) = (b) \iff \exists q, q' \in A$ tel que $a = qb$ et $b = q'a$. Donc $a = qq'a$, or l'anneau est intègre par conséquent $qq' = 1_A$. On pose $q = u \in U(A)$ donc $b = ua$. ■

Définition 3.5.2 *On appelle élément irréductible de A tout élèment non inversible $a \in A$, dont les seuls diviseurs sont les éléments inversibles ou les élèments associés à a.*

Exemple 3.5.1 *Les éléments irréductibles de $\mathbb{Z}$ sont les nombres premiers.*

Définition 3.5.3 *On appelle anneau principal tout anneau intègre tel que tout idéal est principal (i.e engendré par un seul élèment).*

Exemple 3.5.2 *$\mathbb{Z}$ est un anneau principal.*

Définition 3.5.4 *Soit A un anneau intègre et a, $b \in A$. Un élèment d est dit pgdc(a, b) s'il vérifie les conditions suivantes :*

1. *$d \mid a$ et $d \mid b$*
2. *Si $d' \in A$ tel que $d' \mid a$ et $d' \mid b$ alors $d' \mid d$.*

Un élèment $m \in A$ est dit ppmc(a, b)s'il vérifie les conditions suivantes :

1. *$a \mid m$ et $b \mid m$*
2. *Si $m' \in A$ tel que $a \mid m'$ et $b \mid m'$ alors $m \mid m'$.*

Théorème 3.5.1 *Soit A un anneau principal. Tout couple $(a, b) \in A^2$ admet un pgdcet un ppmc.*

Démonstration. Puisque A est un anneau principal alors $(a) + (b)$ est un idéal principal. Donc il existe $d \in A$ tel que $(a) + (b) = (d)$. d'où $d = p\gcd(a, b)m$.

De même on montre que $(a) \cap (b) = (ppmc(a, b))$. ■

Définition 3.5.5 *Soit A un anneau commutatif et P un idéal de A, l'idéal P est un idéal premier si :*

1. *$P \neq A$*
2. *$(\forall x, y \in A)\ xy \in P \Longrightarrow x \in P$ ou $y \in P$.*

Exemple 3.5.3 *$p\mathbb{Z}$ est un idéal premier de $\mathbb{Z}$ pour tout nombre premier p.*

$\{0_A\}$ est un idéal premier de $A \iff A$ est un anneau intègre.

Théorème 3.5.2 *Soit A un anneau commutatif. Les propriétés suivantes sont équivalentes :*

(i) *P est un idéal premier de A,*

(ii) *$A - P$ est une partie stable de A pour la loi $\times$,*

(iii) *$\frac{A}{P}$ est un anneau intègre..*

Démonstration.

$(i) \Longrightarrow (ii)$ Soit $x, y \in A - P$ alors $x \notin P$ et $y \notin P$ et d'après la définition de P on a $xy \notin P$ i.e $xy \in A - P$.

$(ii) \Longrightarrow (iii)$ Soit $\overline{x}, \overline{y} \in \frac{A}{P}$ tel que $\overline{x} \neq \overline{0}_A$ et $\overline{y} \neq \overline{0}_A$ alors $x \notin P$ et $y \notin P$ i.e $x \in A - P$ et $y \in A - P$. Comme $A - P$ est stable par $\times$ alors $xy \in A - P$. Donc $\overline{xy} \neq \overline{0}_A$ i.e $\frac{A}{P}$ est intègre.

$(ii) \Longrightarrow (iii)$ Soit $x, y \in A$ tel que $xy \in P$ alors $\overline{xy} = \overline{xy} = \overline{0}_A$. Puisque $\frac{A}{P}$ est intègre alors $\overline{x} = \overline{0}_A$ ou $\overline{y} = \overline{0}_A$ i.e $x \in P$ ou $y \in P$. ■

3.6 Corps

Définition 3.6.1 *Soit K un anneau non nul. On dit que K est un corps si tout élèment non nul de K est inversible; ou si $U(K) = K - \{0_K\}$.*

Exemple 3.6.1 *$\mathbb{Q}, \mathbb{R}, \mathbb{C}$ sont des corps commutatifs.*

Proposition 3.6.1 *Soit K un anneau non nul. K est un corps si et seulement si les seuls idéaux de K sont $\{0_K\}$ et K.*

Lemme 3.6.1 *Si I est un idéal d'un anneau A contenant un élèment inversible alors $I = A$.*

Démonstration. Soit $u \in U(A)$ tel que $u \in I$ alors $1_A = uu^{-1} \in I$. Donc $I = A$. ■

La démonstration de la proposition découle immédiatement du lemme.

Définition 3.6.2 *Soit K un corps et $L \subseteq K$. On dit que L est un sous corps de K si L muni des lois induites de K est un corps.*

Proposition 3.6.2 *Soit K un corps et $L \subseteq K$. L est un sous corps de K si L vérifie les propriétés suivantes :*

1. $(\forall x, y \in L)\ x - y \in L$
2. $(\forall x, y \in L)\ xy \in L$
3. $(\forall x \in L)\ x^{-1} \in L$.

Définition 3.6.3 *Soit A un anneau commutatif. $\mathcal{M}$ un idéal de A est dit maximal si :*

1. $\mathcal{M} \neq A$
2. Si J est un idéal de A tel que $\mathcal{M} \subseteq J$ alors $J = A$ ou $j = \mathcal{M}$.

Exemple 3.6.2 *Si p est un nombre premier alors $p\mathbb{Z}$ est idéal maximal de $\mathbb{Z}$.*

Théorème 3.6.1 *Soit A un anneau commutatif. $\mathcal{M}$ est un idéal maximal de A si et seulement si $\frac{A}{\mathcal{M}}$ est un corps.*

Démonstration.

$\Longrightarrow$) Soit I un idéal de $\frac{A}{\mathcal{M}}$, $p^{-1}(I)$ est un idéal de A contenat $\mathcal{M}$ (où p est la surjection canonique). Or $\mathcal{M}$ est maximal, donc $p^{-1}(I) = \mathcal{M}$ ou $p^{-1}(I) = A$. Puisque p est surjective alors $I = p(\mathcal{M}) = \{0_A\}$ ou $I = p(A) = \frac{A}{\mathcal{M}}$. Donc d'après la proposition 6.1 $\frac{A}{\mathcal{M}}$ est un corps.

$\Longleftarrow$) Soit J un idéal de A tel que $\mathcal{M} \subseteq J$ alors $p(J)$ est un idéal de $\frac{A}{\mathcal{M}}$. Or $\frac{A}{\mathcal{M}}$ est un corps donc $p(J) = \{\overline{0}_A\}$ ou $P(J) = \frac{A}{\mathcal{M}}$ i.e $J = \mathcal{M}$ ou $J = A$. Donc $\mathcal{M}$ est maximal ■

Corollaire 3.6.1 *Un idéal maximal est un idéal premier.*

Théorème 3.6.2 *(théorème de Krull) Tout élément d'un anneau commutatif est contenu dans un idéal maximal.*

Démonstration. Soient A un anneau commutatif et $x \in A$. Considérons $\mathcal{F}$ l'ensemble des idéaux propres de A contenant x. L'ensemble $\mathcal{F}$ partiellement ordonné par l'inclusion est un ensemble inductif (c'est-à-dire toute partie totalement ordonnée est majorée) ; en effet, soit $(I_j)_{j\in J}$ une partie de $\mathcal{F}$ totalement ordonnée. Montrons que $\bigcup_{j\in J} I_j$ est un idéal propre de A contenant x

3.6.1 Corps de fraction d'un anneau intègre

Position du problème. Etant donné un anneau intègre $(A, +, \times)$, on se propose de montrer qu'il existe un corps commutatif K vérifiant les deux conditions :

1. K admet un sous-anneau isomorphe à A.
2. K est minimal pour la condition 1) ce qui signifie que tout corps contenant un sous-anneau isomorphe à A admet un sous-corps isomorphe à K.

Il en résulte que si deux corps répondant à la question alors ils sont isomorphes.

Existence d'une solution. Posons $E = A \times (A - \{0_A\})$, sur E la relation $\mathcal{R}$ définie par :

$$(a,b)\,\mathcal{R}\,(c,d) \Longleftrightarrow ad - bc = 0$$

est une relation d'équivalence .

Posons $K = \dfrac{E}{\mathcal{R}}$ l'ensemble quotient, on note par $\dfrac{a}{b}$ la classe d'équivalence de (a,b), et on définit sur K les deux lois suivantes :

$$\frac{a}{b} + \frac{c}{d} = \frac{ad - bc}{bd}$$
$$\frac{a}{b} \times \frac{c}{d} = \frac{ac}{bd}$$

Ces deux lois sont bien définies :

Soit $\dfrac{a'}{b'}\ \dfrac{c'}{a'} \in K$ tel que $\dfrac{a}{b} = \dfrac{a'}{b'}$ et $\dfrac{c}{a} = \dfrac{c'}{a'}$ montrons que $\dfrac{a}{b} + \dfrac{c}{a} = \dfrac{a'}{b'} + \dfrac{c'}{a'}$ et $\dfrac{a}{b} \times \dfrac{c}{d} = \dfrac{a'}{b'} \times \dfrac{c'}{d'}$. On a

$$\begin{aligned} b'd'\,(ad - bc) &= ab'dd' - cd'bb' \\ &= dd'\,(ab' - a'b) - bb'\,(cd' - c'd) + bd\,(a'd' - b'c') \\ &= bd\,(a'd' - b'c') \end{aligned}$$

donc

$$\frac{a}{b} + \frac{c}{d} = \frac{a'}{b'} + \frac{c'}{d'}$$

et

$$acb'd' - a'c'bd = a'b\,(cd' - c'd) = 0$$

donc

$$\frac{a}{b} \times \frac{c}{d} = \frac{a'}{b'} \times \frac{c'}{d'}$$

c'est-à-dire les deux lois $+$ et $\times$ sont bien définies sur K.

Théorème 3.6.3 $(K,+,\times)$ *est un corps commutatif.*

Proposition 3.6.3 *Considérons l'application*

$$\begin{array}{rccc} \varphi: & A & \longrightarrow & K \\ & a & \longmapsto & \varphi(a)=\dfrac{a}{1_A} \end{array}$$

φ *est un homomorphisme d'anneau injectif.*

Démonstration. $\varphi(a+b)=\dfrac{a+b}{1}=\dfrac{a}{1}+\dfrac{b}{1}=\varphi(a)+\varphi(b)$ (d'après la définition de la loi $+$). $\varphi(ab)=\dfrac{ab}{1}=\dfrac{a}{1}\times\dfrac{b}{1}=\varphi(a)\times\varphi(b)$ (d'après la définition de $\times$), et $\varphi(1_A)=\dfrac{1_A}{1_A}=1_K$.

Montrons que φ est injectif. Soit $a\in A$ tel que $\varphi(a)=\dfrac{a}{1}=0_K$, or $0_K=\dfrac{0_A}{1}$ donc $\dfrac{a}{1}=\dfrac{0_A}{1}$ donne $a=0_A$ c'est-à-dire φ est injectif. On peut donc identifier A au sous anneau $\varphi(A)=\left\{\dfrac{a}{1}\mid a\in A\right\}$ de K. ■

Proposition 3.6.4 *Soit L un corps tel qu'il existe un morphisme injectif $\omega: A\longrightarrow L$ alors il existe un morphisme injectif $\bar{\omega}: K\longrightarrow L$.*

Définition 3.6.4 *le corps* $K=\dfrac{E}{\mathcal{R}}=\left\{\dfrac{a}{b}\mid a\in A \text{ et } b\in A-\{0_A\}\right\}$ *est appelé corps de fraction de l'anneau A et on le note $Fr(A)$ ou $K(A)$.*

Exercice. Montrer que le corps de fractions de l'anneau $\mathbb{Z}$ est $\mathbb{Q}$.

3.7 Anneux factoriels

Définition 3.7.1 *On appelle anneau factoriel tout anneau A intègre possédant les propriétés suivantes :*

1) tout élément non nul x de A admet une décomposition :

$$x=up_1^{n_1}...p_r^{n_r} \tag{3.1}$$

où u est un élément inversible, $p_1,...,p_r$ sont des éléments irréductibles de A distincts deux à deux et $n_1,...,n_r$ sont des entiers naturels.

2) Si x admet une autre décomposition de la même forme

$$x=vq_1^{m_1}...q_s^{m_s}$$

alors $r=s$ et il existe une permutation $\sigma\in S_r$ telle que, pour tout $i\in\{1,...,r\}$, p_i est associé à $q_{\sigma(i)}$ et $n_i=m_{\sigma(i)}$.

Exemple 3.7.1 *$\mathbb{Z}$ est un anneau factoriel.*

Si K est un corps commutatif alors $K[X]$ est un anneau factoriel.

Proposition 3.7.1 *Soient A un anneau factoriel et x, y deux éléments non nuls et non inversibles de A. Avec les notations, $x = up_1^{n_1}...p_r^{n_r}$ et $y = vq_1^{m_1}...q_s^{m_s}$, pour que x divise y il faut et il suffit que, pour tout $i \in \{1,...,r\}$ il existe un unique $j \in \{1,...,s\}$ tel que $p_i = q_j$ et $n_i \leq m_j$.*

Proposition 3.7.2 *Soient A un anneau factoriel et x, y deux éléments non nuls de A, alors (x, y) admet un pgcd et un ppcm.*

Si de plus $x = up_1^{n_1}...p_r^{n_r}$ et $y = vq_1^{m_1}...q_s^{m_s}$. Alors on a :

$$p\gcd(x,y) = p_{i_1}^{\alpha_{i_1}}...p_{i_k}^{\alpha_{i_k}},$$

$$ppcm(x,y) = p_{i_1}^{\beta_{i_1}}...p_{i_k}^{\beta_{i_k}},$$

où $p_{i_1},...,p_{i_k}$ sont les éléments irréductibles en commun dans la décomposition de x et de y, et pour tout $1 \leq j \leq k$, $\alpha_{i_j} = \min(n_{i_j}, m_{i_j})$, $\beta_{i_j} = \max(n_{i_j}, m_{i_j})$.

Théorème 3.7.1 *(de Gauss). Soient un anneau factoriel et $a, b, c \in A^*$ alors si a et b sont premiers entre eux et divise bc alors a divise c.*

Théorème 3.7.2 *Soient un anneau factoriel et $a, b_1, b_2 \in A^*$ tel que b_1 et b_2 sont premier entre eux. Si a est divisible par b_1 et b_2 alors a est divisible par le produit $b_1 b_2$.*

Théorème 3.7.3 *Tout anneau principal est factoriel.*

Démonstration. Supposons qu'il $x_1 \in A$ n'admettant pas de décomposition (1) en élément irrédictuble, alors x_1 n'est ni inversible n'est irréductible. Il existe $x_2, y_2 \in A$ tel que $x_1 = x_2 y_2$; puisque x_1 n'ayant pas de décomposition il en est de même de x_2 ou de y_2, supposons que ce soit x_2, on a donc $(x_1) \subsetneq (x_2)$. On reprend le même raisonnement pour x_2, on voit qu'on peut construire par récurrence une suite strictement croissante $(x_1) \subsetneq (x_2) \subsetneq ... \subsetneq (x_n)...$ d'idéaux de A. Il est clair que $\bigcup_{i=\mathbf{N}} (x_i)$ est un idéal de A. L'anneau A étant principal il existe $d \in A$ tel que $\bigcup_{i=\mathbf{N}} (x_i) = (d)$, il existe $i_p \in I$ tel que $d \in (x_p)$ donc $(d) \subset (x_p)$, par conséquent $(x_p) = (d)$. La suite est donc stationnaire à partir de p, ce qui est en contradiction avec l'hypothèse. ■