Chapitre 3

STRUCTURES ALGEBRIQUES

La formalisation des structures algébriques (groupes, anneaux, corps, espaces vectoriels) est relativement récente ; elle n'apparait qu'en début du XIX siècle, mais l'idée est présente partout dans les sciences, en particulier les mathématiques.

Il s'agit grosso modo d'extraire des règles opératoires, valables indépendamment de la nature des objets considérés. Par exemple la somme de deux nombres, la somme de deux vecteurs du plan ou la composition de deux relations ont des propriétés similaires.

.

Définition 29 *Soit E un ensemble. Une loi de composition interne sur E est une application de $E \times E$ dans E.*$\mathbb{N}$

Notation

$$\begin{array}{rll} T: & E \times E & \to E \\ & (x,y) & \mapsto T(x,y) = xTy \end{array}$$

Exemples :

L'addition dans $\mathbb{N}$ est une loi de compostion interne

La multiplication dans $\mathbb{R}$ est une loi de compostion interne

Par contre la soustraction n'est pas une loi de compostion interne dans $\mathbb{N}$

On peut aussi définir une loi de composition interne par un tableau. Par exemple, $T : \{a,b,c\} \to \{a,b,c\}$ définie par :

T	a	b	c
a	c	a	c
b	b	a	c
c	b	c	a

.

Définition 30 *On appelle magma tout ensemble muni d'une loi de composition interne.*

Exemple 32 $(\mathbb{N},+)$, $(\mathbb{Z},+)$, $(\mathbb{Q},+)$, $(\mathbb{R},+)$, $(\mathbb{C},+)$, $(\mathbb{N},\times)$, $(\mathbb{Z},\times)$, $(\mathbb{Q},\times)$,

$(\mathbb{R},\times)$, $(\mathbb{C},\times)$ sont des magmas.

3.1 Groupes

frametitleGroupes

Définition 31 *Un magma $(G, *)$ est un groupe si il vérifie les trois conditions suivantes :*

i) *La loi $*$ est associative c'est-à-dire : $\forall x, y, z \in G,\ x * (y * z) = (x * y) * z$.*

ii) *La loi $*$ admet un élément neutre c'est-à-dire : $\exists e \in G / \ \forall x \in G,\ x * e = e * x = x$*

iii) *Tout élément admet un symétrique c'est-à-dire : $\forall x \in G\ \exists x' \ \in G / \ x * x' = x' * x = e$*

Si, de plus, la loi $*$ est commutative, on dit que le groupe est commutatif ou abélien.

3.1.1 Exemoles et contre -exemples

frametitleExemples et contre-exemples

Les magmas suivants sont des groupes :
- $(\mathbb{Z}, +)$ où $+$ est l'addition usuelle.
- $(C^*, \times)$ où $\times$ est la multiplication usuelle.
- $\{0, 1\}$ muni d'une loi $+$ définie par le tableau suivant :

$+$	0	1
0	0	1
1	1	0

- Soit E un ensemble et soit $S(E)$ l'ensemble des bijections de E sur E, soit $\circ$ la loi définie par la composition de deux bijections. On vérifie facilement que $(S(E), \circ)$ est un groupe, et qu'il est non abélien si E a au moins trois éléments. En particulier pour $n \in \mathbb{N}^*$, soit $E = \{1, 2, ...n\}$. Alors $S(E)$ est noté S_n. S_n est un groupe de cardinal $n!$. On l'appelle le groupe des permutations sur n éléments ou groupe symétrique.

Les magmas suivants ne sont pas des groupes :
- $(\mathbb{Z}, \times)$ où $\times$ est la multiplication usuelle.
- $(\mathbb{R}, \times)$ où $\times$ est la multiplication usuelle.

Remarques :

- Lorsque la loi est notée $+$ et $(G, +)$ un groupe, on parle d'opposé à la place de symétrique et on note
$$x + (-x) = (-x) + x = e = 0_G$$
Par convention $0_G.x = 0_G$, $1.x = x$, $n.x = x + x + ... + x$ (n fois) et $(-n)x = -(n.x)$.
- Lorsque la loi est notée $\times$, on parle d'inverse à la place de symétrique et on note
$$x \times x^{-1} = x^{-1} \times x = e = 1_G.$$
- Par convention $x^0 = 1_G$, $x^1 = x$, $x^n = x \times x \times ... \times x$ (n fois) et $x^{-n} = (x^n)^{-1}$.
- Dans le reste du cours, nous utiliserons de préférence la notation multiplicative.

3.1.2 Quelques propriétés des groupes

frametitleQuelques propriétés des groupes

Proposition 31 *Soit $(G,*)$ un groupe et soit x un élément de G.*

1. *L'élément neutre est unique,*
2. *L'inverse $x^{'}$ d'un élément x est unique,*
3. *L'inverse de l'inverse de x est x, i.e. $(x^{'})^{'} = x$.*

Preuve :

1. Soit $e^{'} \in G$ un autre élément neutre. Puisque e est un élément neutre , on a $e^{'} * e = e * e^{'} = e'$. De même, puisque $e^{'}$ est un élément neutre , on a $e * e^{'} = e^{'} * e = e$ et par conséquent $e^{'} = e$.
2. Soient x' et $x"$ deux éléments symétriques de x.
   Donc $x" * x = e$ On a alors $x" * x * x' = e * x' = x'$
   Mais on a aussi $x * x' = e$ donc $x" * x * x' = x" * e = x''$
   Par conséquent $x" = x'$.
3. On a $x * x' = x' * x = e$ donc x est l'inverse de x' ; d'apès 2. on a $x = (x')'$.

Remarque :

- Si une loi $*$ est commutative, alors pour vérifier qu'un élément e est l'élément neutre, il suffit de vérifier que, $\forall x \in G$, on a $x * e = x$ (ou $e * x = x$). L'autre relation étant obtenue par la commutativité. De même, pour vérifier qu'un élément x' est le symétrique de x, il suffit que l'on ait soit $x * x' = e$ soit $x' * x = e$
- Si $(G,*)$ est juste un magma, on a :

$$a = b \Rightarrow a * c = b * c \text{ et } a = b \Rightarrow c * a = c * b$$

Mais si, de plus, $(G,*)$ est un groupe, on a alors la réciproque. car

$$\begin{array}{rcl} a * c = b * c & \Rightarrow & (a * c) * c' = (b * c) * c' \text{ o } c' \text{ est le symtrique de } c \\ & \Rightarrow & a * (c * c') = b * (c * c') \text{ car } * \text{ est associative} \\ & \Rightarrow & a = b \end{array}$$

De même :
$c * a = c * b \Rightarrow a = b$

.

- On a : $(\mathbb{R},+)$ est un groupe donc $a + c = b + c \Leftrightarrow a = b$
- Mais : $(\mathbb{R},\times)$ n'est pas un groupe (car 0 n'est pas inversible) et donc $a \times c = b \times c \not\Rightarrow a = b$

Proposition 32 *Soit $(G,*)$ un groupe, pour tous les éléments a et b de G, on a :*

$$(a * b)^{-1} = b^{-1} * a^{-1}$$

Démonstration :
$(a*b)^{-1}$ est par définition l'unique élément de G qui vérifie

$$(a*b)^{-1}*(a*b)=(a*b)*(a*b)^{-1}=e$$

Or

$$(b^{-1}*a^{-1})*(a*b)=b^{-1}*(a^{-1}*a)*b=b^{-1}*e*b=b^{-1}*b=e$$

et

$$(a*b)*(b^{-1}*a^{-1})=a*(b*b^{-1})*a^{-1}=a*e*a^{-1}=a*a^{-1}=e$$

Donc $(a*b)^{-1}=b^{-1}*a^{-1}$

Remarque :

Dans le cadre de lois non commutatives, les définitions d'élément neutre, de symétrique, d'élément simplifiable (et autres) peuvent être données en séparant les cas à gauche et à droite.

Par exemple : $a*c=b*c\Leftrightarrow a=b$ signifie que c est simplifiable à droite.

.

Proposition 33 *Soit $(G,*)$ un groupe.*

$$\forall n,p\in\mathbb{Z},\ \forall x\in G,\ x^n*x^p=x^{n+p}\ \textit{et}\ x^{n\times p}=(x^n)^p$$

Preuve :

– Si n et p strictement positifs :

$$x^n*x^p=\underbrace{(x*x*...*x)}_{n\text{ fois}}*\underbrace{(x*x*..*x)}_{p\text{ fois}}=x^{n+p}$$

– Si n et p strictement negatifs :

$$\begin{aligned}x^n*x^p &= \underbrace{((x^{-1})*(x^{-1})*...*(x^{-1}))}_{|n|\text{ fois}}*\underbrace{((x^{-1})*(x^{-1})*..*(x^{-1}))}_{|p|\text{ fois}}\\ &= (x^{-1})^{|n|+|p|}=(x)^{-(|n|+|p|)}=x^{n+p}\end{aligned}$$

.

– Si n positif et p négatif :
  – Si $n=-p$

$$x^n*x^p=\underbrace{(x*x*...*x)}_{n\text{ fois}}*\underbrace{((x^{-1})*(x^{-1})*..*(x^{-1}))}_{n\text{ fois}}=e=1_G=x^0$$

  – Si $|p|>n$

$$\begin{aligned}x^n*x^p &= \underbrace{(x*x*...*x)}_{n\text{ fois}}*\underbrace{((x^{-1})*(x^{-1})*..*(x^{-1}))}_{p\text{ fois}}\\ &= \underbrace{(x^{-1}*x^{-1}*...*x^{-1})}_{|p|-n\text{ fois}}=(x^{-1})^{|p|-n}=(x)^{-(|p|-n)}=x^{n+p}\end{aligned}$$

– Si $|p| < n$

$$\begin{aligned} x^n * x^p &= \underbrace{(x * x * ... * x)}_{n \text{ fois}} * \underbrace{((x^{-1}) * (x^{-1}) * .. * (x^{-1}))}_{|p| \text{ fois}} \\ &= \underbrace{(x * x * ... * x)}_{n-|p| \text{ fois}} = (x)^{n-|p|} = x^{n+p} \end{aligned}$$

.

– Si n négatif et p positif : Idem

Remarque

En notation additive, cela donne :

$$\forall n, p \in \mathbb{Z},\ \forall x \in G : \quad (n+p)x = (nx) + (px) \text{ et } (n \times p)x = n(px)$$

3.1.3 Sous groupes

frametitleSous groupes

Définition 32 *Soit $(G, *)$ un groupe. Soit $H \subset G$ et $H \neq \emptyset$. On dit que H est un sous-groupe de $(G, *)$ si et seulement si H est un groupe pour la loi $*$ induite.*

Exemples

– Si G est un groupe, G et $\{e\}$ sont des sous-groupes de G. On les appelle les sous-groupes "triviaux".
– T $= \{z \in \mathbb{C} \text{ tel que } |z| = 1\}$ est un sous-groupe de $(\mathbb{C}^*, \times)$
– Les inclusions $\mathbb{Z} \subset \mathbb{Q} \subset \mathbb{R} \subset \mathbb{C}$ sont des inclusions de sous-groupes pour l'addition et $\{-1, 1\} \subset \mathbb{Q}^* \subset \mathbb{R}^* \subset \mathbb{C}^*$ sont des sous-groupes pour la multiplication
– $(\mathbb{R}_+^*, \times)$ est un sous-groupe de $(\mathbb{R}^*, \times)$ mais Attention, $(\mathbb{R}_-^*, \times)$ n'est pas un sous-groupe de $(\mathbb{R}^*, \times)$ car $(-2) \times (-3) \notin \mathbb{R}_-^*$
– Soit $n \in \mathbb{N}^*$; posons $n\mathbb{Z} := \{kn, k \in \mathbb{Z}\}$. Alors $(n\mathbb{Z}, +)$ est un sous groupe de $(\mathbb{Z}, +)$.

.

Proposition 34 *Soit $(G, .)$ un groupe noté multiplicativement. Soit $H \subset G$. Les propriétés suivantes sont équivalentes :*

1. *H est un sous-groupe de G.*
2. *$H \neq \emptyset,\ \forall x, y \in H\ x.y \in H$ et $\forall x \in H,\ x^{-1} \in H$*
3. *$H \neq \emptyset,\ \forall x, y \in H\ x.y^{-1} \in H$*

– **Démonstration**

(1) $\Rightarrow$ (2) évident
(2) $\Rightarrow$ (3) évident
(3) $\Rightarrow$ (1) En effet
– Associativité : elle découle de celle de G.
– Elément neutre : $\forall x \in H\ x.x^{-1} \in H \Rightarrow e \in H$

– Symétrique :$\forall x \in H\ e.x^{-1} \in H \Rightarrow x^{-1} \in H$
– Loi de composition interne :$\forall x, y \in H$ on a $y^{-1} \in H$ et donc $x.y = x(y^{-1})^{-1} \in H$

Remarques
- Soit H un sous-groupe de G. L'élément neutre de H est le même que celui de G.
- Le symétrique d'un élément de H est le même dans H que dans G.
- Si la loi de G est une loi notée additivement, on a :

Proposition 35 *Soit $H \subset G$. Les propriétés suivantes sont équivalentes :*

1. H est un sous-groupe de G.
2. $H \neq \emptyset,\ \forall x, y \in H,\ x + y \in H$ et $\forall x \in H,\ -x \in H$
3. $H \neq \emptyset,\ \forall x, y \in H\ x - y \in H$.

3.1.4 Homomorphisme de groupes

frametitleHomomorphisme de groupes

Soient $(G, *)$ et $(G', \top)$ deux groupes. On dit qu'une application f de G vers G' est un homomorphisme (ou simplement morphisme) de groupe si et seulement si :

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

Exemples

$$\begin{array}{rccc} f: & (\mathbb{R}, +) & \to & (\mathbb{R}^*, \times) \\ & x & \mapsto & e^x \end{array}$$

$$\begin{array}{rccc} g: & (\mathbb{R}^*, \times) & \to & (\mathbb{R}, +) \\ & x & \mapsto & \ln|x| \end{array}$$

$$\begin{array}{rccc} h: & (\mathbb{C}^*, \times) & \to & (\mathbb{C}^*, \times) \\ & z & \mapsto & \overline{z} \end{array}$$

Remarques
Un homomorphisme d'un ensemble dans lui-même est appelé un endomorphisme.
Un homomorphisme bijectif est appelé un isomorphisme.
Un endomorphisme bijectif est appelé un automorphisme.

Proposition 36 *Soient $(G, \perp)$ et $(G', \top)$ deux groupes d'éléments neutres respectif e et e'. Soit f un homomorphisme de groupe de G vers G'. Alors :*

1. $f(e) = e'$
2. $\forall x \in G,\ f(x^{-1}) = [f(x)]^{-1}$.
3. $\forall x \in G,\ \forall n \in \mathbb{Z}\ f(x^n) = [f(x)]^n$.

Preuve :

1. $f(x) = f(x * e) = f(x) \top f(e) = f(e * x) = f(e) \top f(x)$ C'est-à-dire $f(e) = e'$ à cause de l'unicité de l'élément neutre.
2. $e' = f(x * x^{-1}) = f(x) \top f(x^{-1}) = f(x^{-1} * x) = f(x^{-1}) \top f(x)$ C'est-à-dire $f(x^{-1}) = [f(x)]^{-1}$ à cause de l'unicité du symétrique.
3. 1ère étape : si $n \geq 0$, on utilise une démonstration par récurrence :
   - c'est vrai au rang 0 : par convention $x^0 = e$
   - on suppose vrai au rang n
   $-f(x^{n+1}) = f(x^n * x) = f(x^n) \top f(x) = [f(x)]^n \top f(x) = [f(x)]^{n+1}$

   2ème étape : si $n < 0$
   $-f(x^n) = f((x^{-1})^{-n}) = [f(x^{-1}))]^{-n} = [f(x)]^n$

Remarque
En notation additive, cela donne :

1. – $\forall x \in G,\ f(-x) = -f(x)$.
   – $\forall x \in G,\ \forall n \in \mathbb{Z}\ f(nx) = nf(x)$.

.

1. **Proposition 37** *La composée de deux morphismes est un morphisme. La composée de deux isomorphismes est un isomorphisme*

Démonstration :
Soient $(G_1, *_1), (G_2, *_2)$ et $(G_3, *_3)$ trois groupes.
$\forall a, b \in G_1$,

$$\begin{array}{rcll} (f \circ g)(a *_1 b) & = & f[g(a *_1 b)] & \\ & = & f[g(a) *_2 g(b)] & \text{car } g \text{ est un morphisme} \\ & = & f[g(a)] *_3 f[g(b)] & \text{car } f \text{ est un morphisme} \end{array}$$

.

Définition 33 *Soit $(G_1, *_1)$ un groupe d'élément neutre e_1 et soit $(G_2, *_2)$ un groupe d'élément neutre e_2. Soit f un morphisme de groupe de G_1 vers G_2. On appelle image de f et on note Im f l'ensemble image de f c'est-à-dire :*

$$f(G_1) = Imf = \{y \in G_2 / \exists x \in G_1; y = f(x)\}.$$

On appelle noyau de f et on note Ker f l'image réciproque de $\{e_2\}$ c'est-à-dire :

$$Kerf = \{x \in G_1 / f(x) = e_1\}.$$

Exemples :

$$\begin{array}{rcll} f: & (\mathbb{Z}, +) & \to (\{0, 1\}, +) & \\ & p & \mapsto 0 & \text{si } p = 2k \quad k \in \mathbb{Z} \\ & p & \mapsto 1 & \text{si } p = 2k + 1 \quad k \in \mathbb{Z} \end{array}$$

$$Ker f = 2\mathbb{Z}$$

.

$$\begin{aligned} f : \ (\mathbb{R}, +) &\to (\mathbb{R}^*, \times) \\ x &\mapsto \exp x \end{aligned}$$

$$Im f = \mathbb{R}_+^*$$

Proposition 38 *Soit $(G_1, *_1)$ un groupe d'élément neutre e_1 et soit H_1 un sous-groupe de G_1. Soit $(G_2, *_2)$ un groupe d'élément neutre e_2 et soit H_2 un sous-groupe de G_2. Soit f un morphisme de groupe de G_1 vers G_2. Alors $f(H_1)$ est un sous-groupe de G_2 et $f^{-1}(H_2)$ est un sous-groupe de G_1. En particulier, Im f est un sous-groupe de G_2 et Ker f est un sous-groupe de G_1.*

Preuve :
$f(H_1)$ sous-groupe de G_2 En effet :
$e_1 \in H_1$ donc $f(e_1) = e_2 \in f(H_1)$ Donc $f(H_1) \neq \emptyset$.
Soient b_1 et b_2 deux éléments de $f(H_1)$.

$$\exists a_1 \in H_1 / \ b_1 = f(a_1) \text{ et } \exists a_2 \in H_1 / \ b_2 = f(a_2)$$

$b_1 *_2 (b_2)^{-1} = f(a_1) *_2 (f(a_2))^{-1} = f(a_1) *_2 f(a_2^{-1}) = f(a_1 *_1 a_2^{-1})$
Or $a_1 *_1 a_2^{-1} \in H_1$ car H_1 est un sous-groupe de G_1, Donc $b_1 *_2 (b_2)^{-1} \in f(H_1)$.
$f^{-1}(H_2)$ sous-groupe de G_1 En effet :
$e_2 \in H_2$ et $f(e_1) = e_2$ donc $e_1 \in f^{-1}(H_2)$. Donc $f^{-1}(H_2) \neq \emptyset$.
Soient a_1 et a_2 deux éléments de $f^{-1}(H_2)$.

$$\exists b_1 \in H_2 / b_1 = f(a_1) \text{ et } \exists b_2 \in H_2 / b_2 = f(a_2)$$

$f(a_1 *_1 a_2^{-1}) = f(a_1) *_2 f(a_2^{-1}) = f(a_1) *_2 (f(a_2))^{-1} = b_1 *_2 (b_2)^{-1}$
Or $b_1 *_2 (b_2)^{-1} \in H_2$ car H_2 est un sous-groupe de G_2, Donc $a_1 *_1 a_2^{-1} \in f^{-1}(H_2)$.

Sous-groupes engendrés

frametitleSous-groupes engendrés

Proposition 39 *Soit $\{H_i\}_{i \in I}$ une famille quelconque (c'est-à-dire I quelconque) de sous-groupes d'un groupe G. Alors leur intersection est encore un sous-groupe de G.*

Preuve : On vérifie sans problème les deux assertions qui caractérisent un sous groupe.

.

Proposition 40 *Soit A une partie de G. On note H_A l'ensemble des sous-groupes de G contenant A et on pose $Gr(A) = \{H \ / H \in H_A\}$*

Alors $Gr(A)$ est un sous-groupe de G contenant A et c'est le plus petit possédant cette propriété. On dit que c'est le sous-groupe engendré par A.

Preuve : La proposition précédente permet de dire que $Gr(A)$ est un sous-groupe de G. Il contient A puisque $\forall H \in H_A$, $A \subset H$, et donc $A \subset \{H \ \ / H \in H_A\} = Gr(A)$.

Réciproquement, soit H_0 un sous-groupe de G contenant A, i.e. H_0 est un élément de l'ensemble H_A. Donc $\underset{H\in H_A}{} H \subset H_0$, puisque l'intersection est incluse dans l'une des parties qui est H_0. Or $\underset{H\in H_A}{} H$ est par définition égal à $Gr(A)$, d'où la conclusion.

La proposition suivante permet de mieux préciser $Gr(A)$

.

Proposition 41 *Soit A une partie d'un groupe G. Alors :*
$Gr(A) = \left\{g_1 * g_2 * ...g_n, \quad n \geq 1 \quad g_i \in A \text{ ou } g_i^{-1} \in A\right\}$

Preuve : On désigne par K le membre de droite de la proposition. On a successivement
– K est un sous-groupe de G contenant A, donc il contient $Gr(A)$.
– Soit H un sous-groupe de G contenant A. Contenant A, il contient les inverses des éléments de A, leurs produits (puisque c'est un groupe), donc contient K. Donc K est inclus dans tout sous-groupe H contenant A, il est donc inclus dans leur intersection, qui est $Gr(A)$.

Remarque : Il y a en général deux façons de voir un sous-groupe de G engendré par une partie de G : par "l'extérieur", c'est le choix de la définition donnée au départ ou par "l'intérieur", c'est la proposition précédente.

3.1.5 Groupes monogènes

frametitleGroupes monogènes

Pour avoir des notations plus simple, on adopte la notation a^{-1} pour le symétrique de a et e reste l'élément neutre pour bien indiquer qu'on reste dans le cas général.

Définition 34 *On dit qu'un groupe $(G; *)$ est monogène si il est engendré par un singleton $\{a\}$ et a est dit générateur de G. Un groupe monogène fini est dit un groupe cyclique.*

.

Proposition 42 *Soit a un élément du groupe G ; alors*

$$Gr(a) = \left\{a^k; k \in \mathbb{Z}\right\}$$

où

$$a^k = \begin{cases} \underset{k \text{ fois}}{a * a... * a} & \text{si } k > 0 \\ \underset{|k| \text{ fois}}{a^{-1} * a^{-1}... * a^{-1}} & \text{si } k < 0 \\ e & \text{si } k = 0 \end{cases}$$

Preuve : La partie $\left\{a^k; k \in \mathbb{Z}\right\}$ est un sous groupe contenant a et donc contient $Gr(a)$ et tout sous groupe de G contenant a contient a^{-1} et est stable pour $*$ donc contient $\left\{a^k; k \in \mathbb{Z}\right\}$. En particulier $Gr(a)$ contient $\left\{a^k; k \in \mathbb{Z}\right\}$

.

Définition 35 *Un sous groupe d'ordre fini est un sous groupe ayant un nombre fini d'élément et on appelle ordre d'un groupe le cardinal de ce groupe. Un élément a est dit d'ordre fini s'il existe un entier k tel que $a^k = e$ et on appelle ordre de a le plus petit entier $n \geq 1$ tel que $a^n = e$.*

Remarque : Si $a \neq e$ est d'ordre fini, l'ensemble $\{n \in \mathbb{N} \ / \ a^n = e\}$ est non vide et l'ordre de a est le plus petit élément de $\{n \in \mathbb{N} \ / \ a^n = e\}$

Remarque : Un groupe monogène est toujours commutatif.

On suppose dans cette partie que G est un groupe fini.

Proposition 43 *Tout sous-groupe H de $(\mathbb{Z}, +)$ est de la forme $H =< n >$ où n est un entier positif.*

Preuve : Soit H un sous-groupe de $(\mathbb{Z}, +)$.

Si $H = 0$ alors $H =< 0 >$.

Si $H = \mathbb{Z}, H =< 1 >$

On suppose que H est un sous-groupe propre de $(\mathbb{Z}, +)$. Soit n le plus petit élément strictement positif de H.

Montrons que $< n >= H$:

n appartient à H sous-groupe de $\mathbb{Z}$ donc $< n >$ est inclus dans H (car $< n >$ est le plus petit sous-groupe de $\mathbb{Z}$ contenant n).

Réciproquement montrons que H est inclus dans $< n >$:

soit $x \in H$. D'après la division euclidienne, il existe un couple d'entiers (i, j) avec $0 \leq j < n$ tel que $x = in + j$.

Si i est positif, $in = n + ... + n$ appartient à H car n appartient à H et H sous groupe de $\mathbb{Z}$. Si i est négatif, $in = (-n) + ... + (-n)$ appartient à H car n appartient à H et H sous groupe de $\mathbb{Z}$.

Comme $x \in H$ sous-groupe de $\mathbb{Z}$, $j = x - in$ appartient à H.

Or j est positif et strictement inférieur à n et n est le plus petit entier strictement positif appartenant à H donc j= 0.

D'où, $x = in$ et x appartient donc à $< n >$. H est donc inclus dans $< n >$.

Conclusion : $H =< n >$.

Notation : $< n >$ est noté $n\mathbb{Z}$.

3.1.6 Groupes symétriques

frametitleGroupes symétriques

Définition 36 *Les bijections d'un ensemble E sur lui-même sont appelées permutations ou substitutions de E, et sont notées $S(E)$.*

Pour $E_n = \{1, 2, ..., n\}$, on note $S_n = S(E_n)$.

Notation : Si $E = \{x_1, x_2, ..., x_n\}$, on écrit un élément s de $S(E)$

sous la forme :

$$s = \begin{pmatrix} x_1 & x_2 & ... & x_n \\ s(x_1) & s(x_2) & ... & s(x_n) \end{pmatrix}$$

Exemple : Soit $s \in S_6$ définie par :
$s(1) = 2$; $s(2) = 4$; $s(3) = 5$; $s(4) = 6$; $s(5) = 3$; $s(6) = 1$:
s se note alors :

$$s = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 4 & 5 & 6 & 3 & 1 \end{pmatrix}$$

Le produit st de deux éléments s et t de S_n n'est autre que la composée $s \circ t$. Ce produit n'est donc pas commutatif en général, il s'effectue de droite à gauche.
Exemple : Dans S_5,

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 5 & 3 & 1 & 4 \end{pmatrix}\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 5 & 2 & 1 & 4 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 4 & 5 & 2 & 1 \end{pmatrix}$$
$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 5 & 2 & 1 & 4 \end{pmatrix}\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 5 & 3 & 1 & 4 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 5 & 4 & 2 & 3 & 1 \end{pmatrix}$$

Remarque : On peut omettre d'écrire les points fixes, c-à-d. les k tels que $s(k) = k$. Il faut alors préciser la valeur de n, surtout si n est un point fixe.
Exemple : Dans S_5,

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 4 & 1 & 3 & 2 & 5 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 4 \\ 4 & 1 & 2 \end{pmatrix}$$

Proposition 44 *$(S(E), \circ)$ forme un groupe, appelé groupe symétrique de E*

Preuve :
- $\circ$ est un loi de composition interne car le composé de deux bijections sur E est une bijection sur E ;
- on sait dejà que $\circ$ est associative ;
- l'aplication identité sur E est un élément de $S(E)$, c'est l'élement neutre de la loi $\circ$ sur $S(E)$.
- Tout élément s de $S(E)$, admet un symétrique $s' \in S(E)$ qui est s^{-1}.

Dans tout ce qui suit, E désignera un ensemble fini de cardinal n.
frametitleOrbite d'un élément

Définition 37 *Soient $s \in S_n$ et $i \in E_n$. On appelle orbite de i suivant s l'ensemble :*

$$O_s(i) = \left\{ s^k(i);\ k \in \mathbb{Z} \right\}$$

Remarque : on peut se limiter à des exposants entre 0 et $p = \text{card}(O_s(i)) \leq n$, car on ne peut obtenir plus de n éléments différents dans E_n.
Exemple : Soit $s \in S_7$ définie par :

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 2 & 4 & 5 & 7 & 3 & 6 & 1 \end{pmatrix}$$

$O_s(1) = \{1, 2, 4, 7\}$, $\quad O_s(3) = \{3, 5\}$, $\quad O_s(6) = \{6\}$.
Remarque : $O_s(1) = O_s(2) = O_s(4) = O_s(7)$, $O_s(3) = O_s(5)$.
frametitleDécomposition en cycles disjoints

Définition 38 *On appelle cycle toute permutation $s \in S_n$ admettant exactement une orbite qui ne soit pas réduite à un seul élément. Cette orbite est appelée le support du cycle ; son cardinal est dit longueur du cycle. Un cycle de longueur l est aussi appelé l–cycle.*

Remarque : On pourrait remplacer "exactement" par "au plus", ainsi l'application identité serait également un cycle, de longueur 1 par définition (voir plus bas) ; mais elle n'a bien sûr aucune orbite non-triviale.

Exemple : Soit $s \in S_6$ définie par :

$$s = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 4 & 3 & 6 & 5 & 1 \end{pmatrix}$$

$O(1) = \{1, 2, 4, 6\}, \quad O(3) = \{3\}, \quad O(5) = \{5\}.$

C'est donc un cycle, de support $O(1)$ et de longueur 4.

Notation : Soit s un cycle de S_n de longueur l. Soit i un élément du support de s. Alors s se note $(i\ s(i)\ s^2(i)...s^{l-1}(i))$.

C'est-à-dire, on écrit entre parenthèses les éléments de l'orbite dans l'ordre qu'on les obtient, en commençant avec l'un quelconque d'entre eux, et en appliquant $l-1$ fois la permutation, afin de parcourir l'ensemble de l'orbite.

Exemple : Dans l'exemple précédent, s se note

$$s = (1\ 2\ 4\ 6)$$

Il est évident que la longueur l d'un l-cycle s est égale à l'ordre $|s|$ de cet élément du groupe S_n : toute puissance inférieure du cycle est différente de l'application identité (sur les éléments de son support), mais lorsque la puissance est égale à la longueur, on obtient bien l'application identité, élément neutre de S_n. (C'est donc compatible avec la convention que id_E est un 1–cycle).

Plus généralement, on a l'importante proposition :

.

Proposition 45 *Tout élément s de S_n s'écrit de façon unique (à l'ordre des facteurs près) comme produit de cycles disjoints (c-à-d. à supports disjoints). Ces cycles commutent entre eux et le ppcm des longueurs de ces derniers est égal à l'ordre de la permutation.*

Remarque : Ici il faut bien sûr faire abstraction des 1–cycles, sinon il n'y a pas d'unicité, car on peut toujours composer par id_E un nombre arbitraire de fois. L'identité elle-même s'écrit comme un produit vide, par définition égal à l'élément neutre du groupe.

Cependant, il arrive qu'on rajoute dans cette écriture les points fixes x^* sous forme de 1–cycles (x^*) à la fin du produit, pour mettre en évidence ces points fixes et en même temps l'ensemble de toutes les orbites.

Exemple : Dans S_8,

$$s = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 4 & 8 & 7 & 3 & 5 & 6 & 1 & 2 \end{pmatrix} = (1\ 4\ 3\ 7)(2\ 8) = (2\ 8)(1\ 4\ 3\ 7)$$

L'ordre de s est $O(s) = ppcm(2, 4) = 4$.

frametitleTranspositions

Définition 39 *On appelle transposition tout* 2*–cycle, c-à-d. toute permutation qui échange deux éléments* i *et* $j \neq i$ *en laissant fixe chacun des* $n-2$ *autres ; on la note aussi* τ_{ij}*,*

$$\tau_{ij} = (ij) = \begin{pmatrix} 1 & 2 & ... & i & ... & j & ... & n \\ 1 & 2 & ... & j & ... & i & ... & n \end{pmatrix}$$

Exemple : Dans S_4,

$$s = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 4 & 3 & 2 \end{pmatrix} = (2\ 4) \text{ est la transposition } \tau_{24}.$$

Proposition 46 *Tout élément de* S_n *est produit de transpositions.*

Démonstration : Avec la proposition concernant la décomposition en cycles disjoints, c'est une conséquence immédiate du Lemme suivant.

.

Lemme 47 *Soit* s *un* k*–cycle de* S_n*,*
$s = (a_1\ a_2 ... a_k)$;
alors s *se décompose en produit de* $k-1$ *transpositions :*
$s = (a_1\ a_2)(a_2\ a_3)...(a_{k-1}\ a_k)$.

Rappellons que la multiplication de transpositions est la composition, le facteur à droite est donc celui qui agit en premier sur l'élément auquel on applique ce produit.

Preuve : Notons τ le produit dans le membre de gauche. On vérifie explicitement que $\forall i < k : \tau(a_i) = a_{i+1} = s(a_i)$ (seule la transposition $(a_i\ a_{i+1})$ a un effet non–trivial sur cet élément), et $\tau\ (a_k) = a_1 = s(a_k)$.

Remarque : Attention, l'ordre des transpositions est important : si on l'inverse, on obtient la permutation inverse s^{-1}. (Exercice : pourquoi ?)

Par contre, il y a d'autres décompositions tout aussi bonnes , telle que $s = \tau_{a_1,a_k}\tau_{a_1,a_{k-1}}...\tau_{a_1,a_2}$ (exercice : vérifier ceci !), où les indices doivent être pris dans l'ordre décroissant.

En général, la décomposition d'une permutation en un produit de transpositions n'est donc pas unique.

Exercice : Trouver une décomposition en transpositions de la permutation

$$s = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 \\ 3 & 10 & 6 & 4 & 2 & 1 & 7 & 5 & 8 & 9 \end{pmatrix}$$

Solution : On écrit d'abord s sous forme de produit de cycles à supports disjoints :

$$s = (1\ 3\ 6)(2\ 10\ 9\ 8\ 5)(4)(7)$$

On applique ensuite le Lemme pour décomposer chacun des cycles en produit de transpositions :

$$s = (1\ 3)(3\ 6)(2\ 10)(10\ 9)(9\ 8)(8\ 5)$$

frametitleSignature d'une permutation

Définition 40 *On appelle signature d'une permutation $s \in S_n$, et on note $\varepsilon(s)$, l'entier $(-1)^{n-m}$, où m est le nombre d'orbites suivant s.*

Exemple :

a) $\varepsilon(Id) = (-1)^{1-1} = 1$.
b) Soit τ une transposition de S_n ; alors $\varepsilon(\tau) = (-1)^{n-(n-1)} = -1$.
c) Soit s un cycle de longueur l ; alors $\varepsilon(s) = (-1)^{n-(n-l+1)} = (-1)^{l-1}$.
Exemple : (Suite de l'exercice précédent.)
Trouver la signature de s, permutation de S_{10} définie par :

$$s = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 \\ 3 & 10 & 6 & 4 & 2 & 1 & 7 & 5 & 8 & 9 \end{pmatrix}$$

On avait trouvé les 4 orbites :
$O_s(1) = \{1\ 3\ 6\}$ $O_s(2) = \{2\ 10\ 9\ 8\ 5\}$ $O_s(4) = \{4\}$ $O_s(7) = \{7\}$
La signature de s est donc : $\varepsilon(s) = (-1)^{10-4} = 1$

3.1.7 Théorème de Lagrange

frametitleThéorème de Lagrange

Proposition 48 ***Théorème de Lagrange***
L'ordre d'un sous groupe de G divise l'ordre de G. En particulier l'ordre d'un élément de G divise l'ordre de G.

Preuve. : Considérons la relation dite de congruence modulo H sur G définie par :
Pour x et y dans G, $x \equiv y\ [H] \Leftrightarrow x^{-1}y \in H$.
On a $x^{-1}x = e \in H$ donc la relation est réfléxive ;
$x^{-1}y \in H \Rightarrow (x^{-1}y)^{-1} = y^{-1}x \in H$ donc la relation est symétrique ;
$x^{-1}y \in H$ et $y^{-1}z \in H \Rightarrow x^{-1}z = (x^{-1}y)(y^{-1}z) \in H$ donc la relation est transitive.
Donc la congruence modulo H est une relation d'équivalence et on a :
$\overline{x} = xH = \{xh; h \in H\}$.
En effet $y \in \overline{x} \Leftrightarrow x^{-1}y \in H \Leftrightarrow \exists z \in H\ /\ z = x^{-1}y \Leftrightarrow \exists z \in H\ /\ y = xz$
Donc $y \in \overline{x} \Leftrightarrow y \in xH$
Par conséquent
$\overline{x} = xH = \{xh; h \in H\}$
D'autre part L'application $H \longrightarrow xH$ $y \longrightarrow xy$ est une bijection En effet $xy_1 = xy_2 \Longrightarrow y_1 = y_2$ donc l'application est injective et elle est par construction surjective donc bijective.
Donc toutes les classes ont le même nombre d'éléments qui est exactement le cardinal de H
Comme les classes forment une partition de G ona :
$card(G) = n\ card(H)$
où n est le nombre de classes d'équivalence distinctes.
ce qui finit la démonstration du Théorème de Lagrange.
.

Corollaire 49 *Si G un groupe dont le cardinal est un nombre premier. Alors G ne possède pas d'autres sous-groupes que ses sous-groupes triviaux.*

Proposition 50 $\forall x \in G \quad x^{cardG} = e$

Preuve. Si n est l'ordre de x ; alors $cardG = np$ et donc
$x^{cardG} = (x^n)^p = e^p = e$.

3.2 Anneaux

frametitleAnneaux

Définition 41 *Soit A un ensemble muni de deux lois de composition interne $\top$ et $\perp$. On dit que $(A, \top, \perp)$ est un anneau si et seulement si :*
i) $(A, \top)$ est un groupe abélien.
ii) La loi $\perp$ est associative.
iii) La loi $\perp$ est distributive par rapport à la loi $\top$, c'est-à-dire :

distributive à gauche : $\forall x, y, z \in A, x \perp (y \top z) = (x \perp y) \top (x \perp z)$
et distributive à droite : $\forall x, y, z \in A, (y \top z) \perp x = (y \perp x) \top (z \perp x)$.
Si en plus $\perp$ a un élément neutre on dit que A est un anneaux unitaire
Dans toute la suite, et sauf mention contraire, nous ne considérons que des anneaux unitaires.

Remarques :
- Un anneau n'est jamais vide
- Généralement la loi donnant la structure de groupe est notée additivement et l'autre est notée multiplicativement
- Un anneau est donc un triplet $(A, \top, \perp)$, l'ensemble A s'appelle l'ensemble sous-jacent à l'anneau ; toutefois on parle souvent de l'anneau A en sous-entendant les lois $\top$ et $\perp$ quand il est clair dans le contexte de quelles lois il s'agit.

Exemples d'anneaux :
- $(\mathbb{Z}, +, \times)$ où $+$ et $\times$ sont l'addition usuelle et la multiplication usuelle.
- $(\{0, 1\}, +, \times)$ où $+$ et $\times$ sont les lois définis par les tableaux suivants :

+	0	1
0	0	1
1	1	0

et

x	0	1
0	0	0
1	0	1

- $(\{0\}, +, \times)$ où $+$ et $\times$ sont l'addition usuelle et la multiplication usuelle. Cet anneau est appelé un anneau nul.
- Soit $E = \{$ fonctions numériques définies sur $\mathbb{R}\}$
$(E, +, \times)$ où $+$ et $\times$ sont les lois usuelles :
$(f + g)(x) = f(x) + g(x)$ et $(f \times g)(x) = f(x) \times g(x)$ pour tout réel x (f et g étant deux éléments de E)

Notation

Soit $(A,+,\times)$ un anneau.
On note généralement 0 ou 0_A l'élément neutre de $(A,+)$ et 1 ou 1_A l'élément neutre de $(A,\times)$.
On note $A^* = A\backslash\{0_A\}$

Définition 42 *Un anneau $(A,+,\times)$ est dit commutatif si la loi $\times$ et commutative.*

Exemples
- Les précédents exemples d'anneaux sont des anneaux commutatifs.
- Soit $(G,+)$ un groupe abélien. Soit End$(G) = \{$ endomorphismes de $G\}$. $+$ et $\circ$ étant l'addition et la composition usuelle des fonctions. (End $(G),+,\circ)$ est un anneau qui n'est généralement pas commutatif.

Règles de calcul dans les anneaux. Soit $(A,+,\times)$ un anneau.
a- $\forall x \in A \qquad 0 \times x = x \times 0 = 0.$
b- $\forall x,y \in A \qquad (-x)\times y = x \times (-y) = -(x\times y).$
c- $\forall x,y \in A \qquad (-x)\times(-y) = x \times y.$

Démonstration
a. $\forall x \in A,\ 0 \times x = (0+0)\times x = 0\times x + 0 \times x.$
Donc $0 \times x = 0$. Idem pour l'autre égalité.

$$0 \times y = (x+(-x))\times y = xy + (-x)y = 0 \quad \text{donc}(-x)y\text{est le symétrique de } xy.$$

b. $\forall x,y \in A\ 0\times y = 0$ $\quad x \times 0 = 0$

$$x \times 0 = x \times (y+(-y)) = xy + x(-y) = 0 \quad \text{donc } x(-y) \text{ est aussi le symétrique}$$

c.$\forall x,y \in A \qquad (-x)\times(-y) = -(x\times(-y)) = -(-xy) = xy$

Remarque importante
Soit $(A,+,\times)$ un anneau. Si l'élément neutre de la multiplication est le même que celui de l'addition c'est-à-dire $1 = 0$
alors $\forall x \in A$, $1.x = x$ car 1 élément neutre de la multiplication. et $1.x = 0.x = 0$ d'après la propriété précédente.
Donc $\forall x \in A, x = 0$ c'est-à-dire A est l'anneau nul.
Les anneaux non nuls seront dit unifères.

Définition 43 *Soit $(A,+,\times)$ un anneau unifère. On dit qu'un élément est inversible si et seulement si il admet un symétrique par rapport à la loi $\times$ c'est-à-dire $x \in A$ et x inversible $\Leftrightarrow \exists x' \in A/\ x\times x' = x'\times x = 1$. On note $u(A)$ l'ensemble des éléments inversibles de A (qui sont appelés aussi des unités).*

Exemple
- $u(\mathbb{Z}) = \{-1;1\}$ et $u(\mathbb{Q}) = \mathbb{Q}^*$.
- $(E,+,\times)$ où $E = \{$fonctions numériques définies sur $\mathbb{R}\}$, $+$ et $\times$ sont l'addition et la multiplication usuelles des fonctions. $u(E) = \{$ fonctions numériques qui ne s'annulent pas sur $\mathbb{R}\}$.
- (End$(G),+,\circ)$ où $(G,+)$ est un groupe, $+$ et $\circ$ sont l'addition et la composition usuelles des fonctions. $u(\text{End}(G)) = \text{Aut}(G) = \{$automorphismes de $G\}$.

.

Proposition 51 *Soit $(A,+,\times)$ un anneau unifère. L'ensemble $u(A)$ des unités est un groupe pour la loi $\times$ de A (loi induite).*

Démonstration
– Stabilité : évident $\forall x, y \in u(A)\ (xy^{-1})(yx^{-1}) = 1$
– Associativité : évident $\times$ est associative
– Elément neutre : évident $1.1 = 1$
– Elément symétrique : évident par définition de $u(A)$
Exemple
– $(\mathbb{R}, +, \times)$ est un anneau dont les éléments inversibles sont les réels non nuls donc $(\mathbb{R}^*, \times)$ est un groupe.
– $(\mathbb{Z}, +, \times)$ est un anneau dont les éléments inversibles sont -1 et 1 donc $(\{-1; 1\}, \times)$ est un groupe.

.
– **Définition 44** *Soit $(A, +, \times)$ un anneau unifère. Soit $a, b \in A^*$.*
Si $ab = 0$, on dit que a est un diviseur de zéro à gauche et que b est un diviseur de zéro à droite.
Exemples
– $(E, +, \times)$ où $E = \{$fonctions numériques définies sur $R\}, +$ et $\times$ sont l'addition et la multiplication usuelles des fonctions. Soient f et g les fonctions de E définies par :
$$\begin{cases} f(x) = 0 \text{ si } x < 0 \\ \quad\ = 1 \text{ sinon} \end{cases} \quad \text{et} \quad \begin{cases} g(x) = 1 \text{ si } x < 0 \\ \quad\ = 0 \text{ sinon} \end{cases}$$
On a $f \times g = 0$
– Dans $\mathbb{Z}/6\mathbb{Z}$, on a $\overline{2} \times \overline{3} = \overline{0}$

.
– **Définition 45** *On dit qu'un anneau non nul est intègre si et seulement si il ne possède pas de diviseur de zéro.*
c-à-d $ab = 0 \Rightarrow a = 0$ *ou* $b = 0$
Exemples
$(\mathbb{C}, +, \times)$ est un anneau intègre .
$(\mathbb{Z}, +, \times)$ est un anneau intègre.

3.2.1 Homomorphisme d'anneaux

frametitleHomomorphisme d'anneaux

Définition 46 *Soit $(A, +, \times)$ et $(A', +, \times)$ deux anneaux. On appelle morphisme d'anneaux toute application de A dans A' qui vérifie :*

$$\forall x, y \in A, f(x + y) = f(x) + f(y)$$

et

$$\forall x, y \in A, f(x \times y) = f(x) \times f(y)$$

Exemple

$$\begin{array}{rccc} f: & (\mathbb{C}, +, \times) & \to & (\mathbb{C}, +, \times) \\ & z & \mapsto & \overline{z} \end{array}$$

Remarque

– L'élément unité de A n'est pas forcement transformé en l'élément unité de A'.

$$\begin{array}{rccc} f: & A & \to & A' \\ & x & \mapsto & 0 \end{array}$$

f est bien un morphisme d'anneaux et on a $f(1) = 0$.

Soient A et B deux anneaux.

$$\begin{array}{rccc} i: & A & \to & A \times B \\ & x & \mapsto & (x, 0) \end{array}$$

i est bien un morphisme d'anneaux et on a $i(1) = (1, 0) \neq (1, 1)$

Si A et A' sont unifères et que l'on a $f(1) = 1$, on dit que f est unitaire.

3.2.2 sous anneau

frametitlesous anneau

Définition 47 *Soit $(A, +, \times)$ un anneau. On dit qu'une partie B de A est un sous anneau de A si et seulement si :*
(i) $(B, +)$ est un sous-groupe de A.
(ii) B est stable pour la loi $\times$ c'est-à-dire $\forall x, y \in B, x \times y \in B$

Exemples
$(\mathbb{Z}, +, \times)$ est un sous anneau de $(\mathbb{R}, +, \times)$.
$(2\mathbb{Z}, +, \times)$ est un sous anneau de $(\mathbb{Z}, +, \times)$.
. **Remarques**
- Soit $(A, +, \times)$ un anneau et B un sous anneau de A.

- A unifère $\not\Rightarrow B$ unifère. Par exemple, $\{0_A\}$ est un sous anneau de tout anneau unifère.
- $(2\mathbb{Z}, +, \times)$ est un sous anneau de $\mathbb{Z}$ mais ne possède pas d'élément neutre pour la multiplication.

Définition 48 *On dit qu'un sous anneau B d'un anneau A est unitaire s'il possède le même élément unité que A.*

Exemple : $\mathbb{Z}$ est le seul sous anneau unitaire de $(\mathbb{Z}, +, \times)$.

.

Proposition 52 *Soit $(A, +, \times)$ un anneau. Soit $(B_i)_{i \in I}$ une famille non vide de sous anneaux (resp. sous anneaux unitaires) de A. Alors $\bigcap_{i \in I} B_i$ est un sous anneau (resp. sous anneau unitaire) de A.*

– **Démonstration**
– $\forall i \in I, B_i$ est un sous-groupe de A donc $\bigcap_{i \in I} B_i$ est un sous-groupe de A.

– Stable par multiplication

$$x, y \in \bigcap_{i\in I} B_i \Leftrightarrow \forall i \in I, x \in B_i \text{ et } y \in B_i$$

$$\Rightarrow \forall i \in I, x \times y \in B_i \Rightarrow x \times y \in \bigcap_{i\in I} B_i$$

– $\forall i \in I, 1_A \in B_i$. Donc $1_A \in \bigcap_{i\in I} B_i$

3.2.3 Sous anneau engendré

frametitleSous anneau engendré

Définition et proposition : Soit $(A, +, \times)$ un anneau et soit C une partie de A. On appelle sous anneau engendré par C, le plus petit (en terme d'inclusion) sous anneau de A qui contient le sous-ensemble C.

Démonstration

Soit $(B_i)_i \in I$ l'ensemble des sous anneaux de A qui contiennent C. Cette famille n'est pas vide car A appartient à cette famille. $\bigcap_{i\in I} B_i$ est le plus petit sous anneau de A qui contient C.

.

– **Proposition 53** *Soient $(A, +, \times)$ et $(A', +, \times)$ deux anneaux. Soit f un morphisme unitaire d'anneaux de A vers A'. L'image directe d'un sous anneau (resp. unitaire) de A est un sous anneau (resp. unitaire) de A'. L'image réciproque d'un sous anneau (resp. unitaire) de A' est un sous anneau (resp. unitaire) de A.*

Démonstration

– Sous-groupe déjà fait.

– Stabilité par multiplication évidente.

3.2.4 Définition et propriétés d'un idéal

frametitleDéfinition et propriétés d'un idéal

Dans la partie qui concerne les idéaux, nous considérerons uniquement les anneaux unifères commutatifs.

Définition 49 *Soit $(A, +, \times)$ un anneau et soit I une partie de A. On dit que I est un idéal de A si et seulement si*
(i) $(I, +)$ est un sous-groupe de A.
(ii) $\forall x \in I, \forall a \in A, a \times x \in I$.

Exemples

$(2\mathbb{Z}, +, \times)$ est un idéal de $(\mathbb{Z}, +, \times)$

De façon plus général $(p\mathbb{Z}, +, \times)$ est un idéal de $(\mathbb{Z}, +, \times)$ pour tout $p \in \mathbb{N}$.

A et $\{0_A\}$ sont des idéaux de A

.

– **Remarques**
– Tout idéal est un sous anneau.
– Si A est unifère le seul idéal de A qui contienne l'élément unité est A
– $\mathbb{Z}$ est un sous anneau de $(\mathbb{R}, +, \times)$ mais n'est pas un idéal de ce même anneau.

.

– **Proposition 54** *Soient $(A, +, \times)$ et $(A', +, \times)$ deux anneaux. Soit f un morphisme d'anneaux de A vers A'. L'image réciproque d'un idéal de A' est un idéal de A. En particulier, Ker f est un idéal de A. Mais en général, c'est faux pour l'image directe d'un idéal de A.*

Démonstration
– 1. Image réciproque
  – Sous-groupe déjà fait.
  – Stabilité par multiplication par un élément de A
  Soit I un idéal de$A', x \in f^{-1}(I) \Leftrightarrow f(x) \in I$
  $\forall a \in A, f(ax) = f(a)f(x)$ or $f(a) \in A'$ et $f(x) \in I$ donc $f(a)f(x) \in I$.
  C'est-à-dire $ax \in f^{-1}(I)$
2. Ker$f = f^{-1}(\{0_{A'}\})$, $\{0_{A'}\}$ est bien un idéal de A'.
3. Image directe : Il faudrait que f soit surjective pour espérer que cela marche (voir série n^{0}3)

.

– **Définition 50** *Soit $(A, +, .)$ un anneau. On définit l'indice d'un élément a de A (noté $i(a)$) par :*
Si $\forall n \in \mathbb{N}^*, n.a \neq 0$ alors $i(a) = +\infty$. Sinon $i(a)$ est le plus petit entier non nul p tel que $p.a = 0$

Exemple
Dans $\mathbb{Z}/12\mathbb{Z}$, $i(2) = 6$ et $i(3) = 4$.
Définition 51 *Soit $(A, +, \times)$ un anneau. Soit J l'ensemble des indices des éléments de A.*
Si J est majoré, le ppcm de ces indices est appelé caractéristique de l'anneau A et est noté $\mathcal{X}(A)$.
Si J est non majoré, on dit que l'anneau est de caractéristique nulle.
Exemples
$\mathcal{X}(\mathbb{R}) = 0$.
$X(\mathbb{Z}/n\mathbb{Z}) = n$.car $(n.\overline{1} = \underbrace{(\overline{1} + \overline{1} + ... + \overline{1})}_{n \text{ fois}} = \overline{n} = \overline{0})$

3.2.5 Idéal engendré par une partie. Idéal principal. Anneau principal

frametitleIdéal engendré par une partie. Idéal principal. Anneau principal

Proposition 55 *Soit $(A, +, \times)$ un anneau et soit $(I_j)_{j \in J}$une famille quelconque (c'est-à-dire J quelconque) d'idéaux de A. Alors $\bigcap_{j \in J} I_j$ est un idéal de A.*

Démonstration

– – $\forall j \in J, I_j$ est un sous-groupe de A donc $\bigcap_{j\in J} I_j$ est un sous-groupe de A

– Stable par multiplication par un élément de A

$$x \in \bigcap_{j\in J} I_j \Leftrightarrow \forall j \in J, x \in I_j$$

$$\Rightarrow \forall j \in J, x \times a \in I_j \quad \forall a \in A \Rightarrow x \times a \in \bigcap_{j\in J} I_j$$

La dernière proposition légitime la définition suivante.

.

Définition 52 *Soit X une partie de A. On note I_X l'ensemble des idéaux de A contenant X et on pose $< X >= \{I,\ I \in I_X\}$*

Alors $< X >$ est un idéal de A contenant X et c'est le plus petit possèdant cette propriété. On dit que c'est l'idéal engendré par X.

On se place dans le cas d'un anneau commutatif A. Soit $a \in A$. On pose $M = \{a.x, x \in A\}$.

On vérfie facilement que M est un idéal de A contenant a et que de plus c'est le plus petit idéal de A contenant a.

Soit en effet J un idéal de A contenant a et soit m un élément de M. L'élément m est donc de la forme $a.x$ où $x \in A$.

Alors, par définition de l'idéal, $a.x \in J$ car $a \in J$. Donc $M \subset J$.

C'est donc l'idéal engendré par a. On le note souvent $< a >$ ou (a). On a prouvé :

$$< a >= \{a.x, x \in A\}$$

.

Définition 53 *On appelle idéal principal tout idéal engendré par un singleton $X = \{a\}$.*

Définition 54 *On appelle anneau principal tout anneau A tel que*

1. A est intègre,

2. tout idéal de A est principal.

L'arithmétique se fonde en partie sur le théorème suivant :

Proposition 56 *L'anneau $(\mathbb{Z}, +, \times)$ des entiers relatifs munis des lois usuelles est un anneau principal.*

Preuve : on a deja vu que Les seuls sous-groupes de $(\mathbb{Z}; +)$ sont $n\mathbb{Z}$ pour n entier et que $n\mathbb{Z} =< n >$

$n\mathbb{Z}$ est bien un idéal de $\mathbb{Z}$. Donc les seuls ideaux de $\mathbb{Z}$ sont $n\mathbb{Z} =< n >$

3.2.6 Groupes, anneaux et relation d'équivalence compatible

frametitleGroupes, anneaux et relation d'équivalence compatible

Compatibilité d'une relation d'équivalence avec une loi de composition interne $*$ sur E

Définition 55 *Soit $*$ une loi de composition interne sur E, et R une relation d'équivalence ;*
On dit que R est compatible avec $*$ si pour tout a, b dans E on a

$$aRb \Longrightarrow \begin{cases} (a* \ x)R(b* \ x) \\ \quad et \qquad \text{pour tout } x \in E. \\ (x* \ a)R(x* \ b) \end{cases}$$

.

Définition 56 *Si R est compatible avec $*$, on peut définir sur E/R la loi de composition interne $\dot{*}$ de la façon suivante :*
$\overline{x} \dot{*} \overline{y} = \overline{x * y}$
où, x est un représentant de la classe $\overline{x}$ et y un représentant de la classe $\overline{y}$.

Preuve : Pour prouver que loi $\dot{*}$ est bien définie, il faut vérifier que cette définition ne dépend pas du choix des représentants x et y.
Soient $x^{'} \in \overline{x}$ et $y^{'} \in \overline{y}$ deux autres représentants respectifs de $\overline{x}$ et $\overline{y}$ Alors
$x^{'}Rx \Longrightarrow (x^{'} * y)R(x * y)$.
$y^{'}Ry \Longrightarrow (x^{'} * y^{'})R(x^{'} * y)$,
ce qui donne $(x * y)\underline{R}(x^{'} * y^{'})$
et donc $\overline{x * y} = \overline{x^{'} * y^{'}}$
soit $\overline{x} \dot{*} \overline{y} = \overline{x^{'}} \dot{*} \overline{y^{'}}$
La classe d'équivalence $\overline{x} \dot{*} \overline{y}$ ne dépend donc pas du représentant choisi dans les classes de x et y.

.

Proposition 57 *Si $(E, *)$ est un groupe et si R est une relation d'équivalence sur E compatible avec $*$; alors : $(E/R, \dot{*})$ est un groupe. De plus, si $*$ est commutative, alors $\dot{*}$ l'est aussi.*

Preuve : Comme on l'a vu précédement $\dot{*}$ est une loi de composition interne bien définie.
$(\overline{x} \dot{*} \overline{y}) \dot{*} \overline{z} = (\overline{x * y}) \dot{*} \overline{z} = \overline{(x * y) * z} = \overline{(x * (y * z)} = \overline{x} \dot{*} (\overline{y} \dot{*} \overline{z})$ Donc $\dot{*}$ est associative
Soit e l'élément neutre pour $*$, montrons que $\overline{e}$ est l'élément neutre pour $\dot{*}$ sur E/R.
Soit $\overline{x}$ une classe d'équivalence, dont un représentant est x. Alors $\overline{x} \dot{*} \overline{e} = \overline{x * e} = \overline{x}$, de même on a $\overline{e} \dot{*} \overline{x} = \overline{e * x} = \overline{x}$, donc $\overline{e}$ est l'élément neutre de $\dot{*}$.
Soit $\overline{x}$ une classe d'équivalence, dont un représentant est x. Considérons $x^{'}$, l'inverse de x pour $*$. Alors $\overline{x} \dot{*} \overline{x^{'}} = \overline{x * x^{'}} = \overline{e}$ et $\overline{x^{'}} \dot{*} \overline{x} = \overline{x^{'} * x} = \overline{e}$
Donc $\overline{x^{'}}$ est la classe d'équivalence inverse de $\overline{x}$ pour $\dot{*}$. Tout élément de E/R a donc un inverse. Conclusion : $(E/R, \dot{*})$ est un groupe.
De plus si $*$ est commutative on a : $\overline{x} \dot{*} \overline{y} = \overline{x * y} = \overline{y * x} = \overline{y} \dot{*} \overline{x}$ Donc $\dot{+}$ est commutative

Proposition 58 *Si $(A, *, \times)$ est un anneau unitaire et si R est une relation d'équivalence compatible avec $*$ et $\times$, alors $(A/R, \dot{*}, \dot{\times})$ est un anneau unitaire. De plus, si $\times$ est commutative, alors $\dot{\times}$ l'est également.*

Preuve :

D'après la proposition précédente $(A/R, \dot{*})$ es un groupe commutatif ;

D'autre part :

$(\overline{x} \dot{\times} \overline{y}) \dot{\times} \overline{z} = (\overline{x \times y}) \dot{\times} \overline{z} = \overline{(x \times y) \times z} = \overline{x \times (y \times z)} = \overline{x} \dot{\times} (\overline{y \times z}) = \overline{x} \dot{\times} (\overline{y} \dot{\times} \overline{z})$ Donc $\dot{\times}$ est associative ;

$\overline{x} \dot{\times} (\overline{y} \dot{*} \overline{z}) = \overline{x} \dot{\times} (\overline{y * z}) = \overline{x \times (y * z)} = \overline{(x \times y) * (x \times z)} = \overline{(x \times y)} \dot{*} \overline{(x \times z)} = (\overline{x} \dot{\times} \overline{y}) \dot{*} (\overline{x} \dot{\times} \overline{z})$ Donc $\dot{\times}$ est distributive par raport à $\dot{*}$

De plus si $\times$ est commutative on a : $\overline{x} \dot{\times} \overline{y} = \overline{x \times y} = \overline{y \times x} = \overline{y} \dot{\times} \overline{x}$ Donc $\dot{\times}$ est commutative

Si 1 est l'élement neutre de A pour la loi $\times$ on a : $\overline{x} \dot{\times} \overline{1} = \overline{x \times 1} = \overline{x}$ Donc $\overline{1}$ est l'élement neutre de A/R pour $\dot{\times}$

3.2.7 Etude de $\mathbb{Z}/n\mathbb{Z}$

frametitleEtude de Z/nZ

Soit n un entier > 1,considérons dans $\mathbb{Z}$ la relation d'équivalence $\equiv$ (congruence) définie par :

$$x \equiv y\,[n] \Leftrightarrow x - y \text{ est un multiple de } n.$$

On sait depuis le chapitre précédent que $\equiv$ est compatible avec l'addition et la multiplication dans $\mathbb{Z}$. c'est à dire:

1. si $a \equiv b\ [n]$ et $a' \equiv b'\ [n]$, alors $a + a' \equiv b + b'\ [n]$. et
2. si $a \equiv b\ [n]$ et $a' \equiv b'\ [n]$, alors $aa' \equiv bb'\ [n]$,

On a vu aussi que :

$\mathbb{Z}/n\mathbb{Z} = \left\{\dot{0}, \dot{1}, \dot{2}, ..., \dot{n-1}\right\} = \{n\mathbb{Z}, 1 + n\mathbb{Z}, ..., (n-1) + n\mathbb{Z}\}$

Donc on peut définir sur $\mathbb{Z}/n\mathbb{Z}$ une addition et une multiplication des classes de la façon suivante :

$\overline{x} \dot{+} \overline{y} = \overline{x + y}$ et $\overline{x} \dot{\times} \overline{y} = \overline{x \times y}$.

.

Proposition 59 $(\mathbb{Z}/n\mathbb{Z}, \dot{+}, \dot{\times})$ *est un anneau commutatif unitaire*

Preuve : C'est une conséquence de la proposition précédente car $(\mathbb{Z}, +, \times)$ est un anneau commutatif unitaire donc il l'est de même pour $(\mathbb{Z}/n\mathbb{Z}, \dot{+}, \dot{\times})$.

Exemple1 : On sait que $\mathbb{Z}/3\mathbb{Z} = \left\{\dot{0}, \dot{1}, \dot{2}\right\}$.On peut donc définir la loi $\dot{+}$ sur $\mathbb{Z}/3\mathbb{Z}$. de la façon suivante :

$\overline{0} \dot{+} \overline{1} = \overline{0+1} = \overline{1}$ $\qquad$ $\overline{1} \dot{+} \overline{1} = \overline{1+1} = \overline{2}$

$\overline{1} \dot{+} \overline{2} = \overline{1+2} = \overline{3} = \overline{0}$ $\qquad$ $\overline{2} \dot{+} \overline{2} = \overline{2+2} = \overline{4} = \overline{1}$

qu'on peut aussi représenter par le tableau suivant :

$a\backslash b$	$\overline{0}$	$\overline{1}$	$\overline{2}$
$\overline{0}$	$\overline{0}$	$\overline{1}$	$\overline{2}$
$\overline{1}$	$\overline{1}$	$\overline{2}$	$\overline{0}$
$\overline{2}$	$\overline{2}$	$\overline{0}$	$\overline{1}$

.

On peut aussi définir la loi $\dot{\times}$ sur $\mathbb{Z}/3\mathbb{Z}$. de la façon suivante :
$\overline{0} \dot{\times} \overline{1} = \overline{0 \times 1} = \overline{0}$
$\overline{1} \dot{\times} \overline{1} = \overline{1 \times 1} = \overline{1}$
$\overline{1} \dot{\times} \overline{2} = \overline{1 \times 2} = \overline{2}$
$\overline{2} \dot{\times} \overline{2} = \overline{2 \times 2} = \overline{4} = \overline{1}$
qu'on peut aussi représenter par le tableau suivant :

$a\backslash b$	$\overline{0}$	$\overline{1}$	$\overline{2}$
$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$
$\overline{1}$	$\overline{0}$	$\overline{1}$	$\overline{2}$
$\overline{2}$	$\overline{0}$	$\overline{2}$	$\overline{1}$

Exemple2 : Quelques calculs dans $\mathbb{Z}/10\mathbb{Z}$
$\dot{3} + \dot{8} = \dot{11} = \dot{1}$
$\dot{4} \times \dot{4} = \dot{16} = \dot{6}$
$\dot{2} + \dot{8} = \dot{10} = \dot{0}$ donc $\dot{8}$ est l'opposé de $\dot{2}$ et que $\dot{2}$ est l'opposé de $\dot{8}$.
$\dot{5} + \dot{5} = \dot{10} = \dot{0}$ donc $\dot{5}$ est égal à son opposé !
$\dot{2} \times \dot{5} = \dot{10} = \dot{0}$ donc 2 et $\dot{5}$ sont des diviseurs de zéros .
$\dot{3} \times \dot{7} = \dot{21} = \dot{1}$ donc $\dot{3}$ et $\dot{7}$ sont inversibles et $\dot{7}$ est l'inverse de $\dot{3}$ et que $\dot{3}$ est l'inverse de $\dot{7}$
$\dot{9} \times \dot{9} = \dot{81} = \dot{1}$ donc $\dot{9}$ est inversible et est égal à son inverse.
$(\dot{3})^{100} = ((\dot{3})^2)^{50} = (\dot{9})^{50} = ((\dot{9})^2)^{25} = (\dot{1})^{25} = \dot{1}$
.

Proposition 60 *Soit $\dot{x}$ un élément de $\mathbb{Z}/n\mathbb{Z}$ alors $\dot{x}$ ne peut pas être à la fois inversible et un diviseur de zéro.*

Preuve : Supposons qu'il existe $\dot{y}$ tel que $\dot{x} \times \dot{y} = \dot{1}$ et $\dot{z} \neq \dot{0}$ tel que $\dot{x} \times \dot{z} = \dot{0}$ alors

$$\dot{x} \times \dot{y} \times \dot{z} = \dot{z} = \dot{x} \times \dot{z} \times \dot{y} = \dot{0}$$

ce qui donne une contradiction.

Proposition 61 *Soit $\dot{x} \in \mathbb{Z}/n\mathbb{Z}$ on a :*

$$\dot{x} \text{ inversible} \Leftrightarrow x \wedge n = 1$$

Preuve : $\dot{x}$ est inversible ssi $\exists\ \dot{y}$ tel que $\dot{x} \times \dot{y} = \dot{1}$ ssi $\exists\ y \in \mathbb{Z}\,;\ k \in \mathbb{Z}$ tels que $xy = 1 + kn$ ssi $\exists\ y\,;\ k$ tels que $xy - kn = 1$ ssi $x \wedge n = 1$ (théorème de Bezout).

Corollaire1 : Dans $\mathbb{Z}/n\mathbb{Z}$ tout élément qui n'est pas inversible est un diviseur de zéro.

Preuve : Si $\dot{x}$ n'est pas inversible alors $x \wedge n = d$ avec $d \neq 1$, soit $y = \frac{n}{d} \in \mathbb{N}$, et $x' = \frac{x}{d}$. Or $xy = x'n$ est un multiple de n donc on a $\dot{x} \times \dot{y} = \dot{0}$.

Notation : On s'abstient de mettre les points au dessus des lettres désignant les éléments de $\mathbb{Z}/n\mathbb{Z}$, quand le contexte permet d'éviter toute confusion.

Corollaire2 : Si p est premier, Tous les éléments de $\mathbb{Z}/p\mathbb{Z}$ sont inversibles.

Lemme : Soit a et b dans $\mathbb{Z}/p\mathbb{Z}$ on a

$$(a+b)^p = a^p + b^p$$

Preuve : On a la la formule du binôme de Newton :

$(a+b)^p = \sum_{k=0}^{p} C_p^k a^{p-k} b^k = a^p + \sum_{k=1}^{p-1} C_p^k a^{p-k} b^k + b^p$

Or on a vu au chapitre précédent que C_p^k est un multiple de p pour $1 \leq k \leq p-1$ donc $\sum_{k=1}^{p-1} C_p^k a^{p-k} b^k \equiv 0\,[p]$, ce qui donne le résultat.

3.2.8 Équations et système d'équations dans $\mathbb{Z}/n\mathbb{Z}$

frametitleÉquations et système d'équations dans Z/nZ

a) Équation $ax = b$ dans $\mathbb{Z}/n\mathbb{Z}$.

La résolution de l'équation $ax = b$ est immédiate dans l'ensemble des nombres réels ou complexes.

Dans $\mathbb{Z}$, elle admet une solution si et seulement si b est un multiple de a.

Voyons ce qu'il en est dans $\mathbb{Z}/n\mathbb{Z}$.

Proposition 62 *On considère l'équation $ax = b$ dans $\mathbb{Z}/n\mathbb{Z}$, soit $d = a \wedge n$ on a :*

Si d ne divise pas b alors l'équation n'a pas de solution.

Si d divise b alors l'équation admet d solutions. En particulier si $d = 1$ alors la solution est $x = a^{-1}b$.

Preuve : Si d ne divise pas b supposons que x soit une solution de l'équation $ax = b$ dans $\mathbb{Z}/n\mathbb{Z}$. Il existerait alors un entier k tel que on ait

$ax = b + kn$ dans $\mathbb{Z}$, comme $d|a$ et $d|n$ cette équation implique que $d|b$ et on a une contradiction.

Si $d|b$, notons $a_1 = \frac{a}{d}$, $b_1 = \frac{b}{d}$, et $n_1 = \frac{n}{d}$ On cherche à résoudre l'équation à deux inconnues (x et k) dans $\mathbb{Z}$: $ax + kn = b$ qui est équivalente à $a_1 x + kn_1 = b_1$ qui donne $a_1 x = b_1$ dans $\mathbb{Z}/n_1\mathbb{Z}$ comme $a_1 \wedge n_1 = 1$, a_1 est inversible $\mathbb{Z}/n_1\mathbb{Z}$ et cette équation admet pour unique solution $x = a_1^{-1} b_1$. Par conséquent, les solutions de l'équation $ax = b$ dans $\mathbb{Z}/n\mathbb{Z}$ sont de la forme $x = a_1^{-1} b + jn_1$ et il n'y en a que d distinctes modulo n.

b)Théorème des restes chinois.

Ce théorème nous permet de résoudre explicitement un système d'équations à une seule inconnue !

Proposition 63 *Soit $n = n_1 \times n_2 ... \times n_k$ avec les nombres $(n_i)_{1\leq i\leq k}$ deux à deux premiers entre eux. Alors le système d'équation :*

$$\begin{cases} x \equiv a_1 \ [n_1] \\ x \equiv a_2 \ [n_2] \\ \quad ... \\ x \equiv a_k \ [n_k] \end{cases}$$

admet une unique solution dans $\mathbb{Z}/n\mathbb{Z}$ et celle ci se calcule par la formule :
$x \equiv a_1 q_1 q_1' + a_2 q_2 q_2' + ... + a_k q_k q_k' \ [n]$
où $q_i = \frac{n}{n_i}$ et q_i' est l'inverse de q_i dans $\mathbb{Z}/n_i\mathbb{Z}$.

Preuve : Tout d'abord notons que $q_i \wedge n_i = 1$ (car les nombres $(n_i)_{1\leq i\leq k}$ deux à deux premiers entre eux) et donc q_i est inversible dans $\mathbb{Z}/n_i\mathbb{Z}$.

On va montrer que x est une solution du système, donc que pour tout i on a $x \equiv a_i[n_i]$.

Si $i \neq j$ alors q_j est un multiple de n_i donc $q_j \equiv 0[n_i]$ donc $x \equiv a_i q_i q_i'[n_i]$

or par définition de q_i' on a $q_i q_i' \equiv 1[n_i]$ donc $x \equiv a_i[n_i]$.

Montrons maintenant l'unicité de la solution. Si x et y sont deux solutions du système alors pour tout i on a

$x - y \equiv 0[n_i]$ donc $x - y$ est multiple de tous les entiers n_i donc $x - y$ est multiple du produit des n_i car ceux-ci sont premiers entre eux donc

$x - y \equiv 0[n]$ c-à-d $x \equiv y[n]$.Ce qui conclut la preuve.

.

Proposition 64 *Soit $n = n_1 \times n_2 ... \times n_k$ avec les nombres $(n_i)_{1\leq i\leq k}$ deux à deux premiers entre eux. Alors l'application*

$\mathbb{Z}/n\mathbb{Z} \longrightarrow \mathbb{Z}/n_1\mathbb{Z} \times \mathbb{Z}/n_2\mathbb{Z} \times ... \times \mathbb{Z}/n_k\mathbb{Z}$

$x \longrightarrow (x_1, x_2, ..., x_k)$

où x_i est la classe de x modulo n_i, est un isomorphisme d'anneaux.

Preuve : Il découle immédiatement de la définition de $\mathbb{Z}/n\mathbb{Z}$ que cette application est un morphisme d'anneaux. Le théorème des restes chinois dit que pour tout élément il existe un antécédent et que celui-ci est unique et donc que l'application est bijective.

Corollaire : Si $n = n_1 \times n_2 ... \times n_k$ avec les nombres $(n_i)_{1\leq i\leq k}$ deux à deux premiers entre eux. Alors on a :

$$\varphi(n) = \varphi(n_1)\varphi(n_2)\varphi(n_k)$$

Preuve : Deux anneaux isomorphes ont le même nombre d'éléments inversibles il suffit alors de les compter dans $\mathbb{Z}/n\mathbb{Z}$ et dans $\mathbb{Z}/n_1\mathbb{Z} \times \mathbb{Z}/n_2\mathbb{Z} \times ... \times \mathbb{Z}/n_k\mathbb{Z}$.

Exemple : Si p et q sont deux nombres premiers

$\varphi(pq) = \varphi(p)\varphi(q) = (p-1)(q-1)$

En fait on peut maintenant donner une formule générale pour calculer $\varphi(n)$ à partir de sa décomposition en facteurs premiers.

Proposition 65 *Soit $n \in \mathbb{N}$ notons sa décomposition en facteurs irréductibles : $n = p_1^{n_1} p_2^{n_2} ... p_k^{n_k}$*

Alors on a :

$$\varphi(n) = n(\frac{p_1 - 1}{p_1})(\frac{p_2 - 1}{p_2})...(\frac{p_k - 1}{p_{k1}})$$

Preuve : D'après le résultat précédent on a : $\varphi(n) = \varphi(p_1^{n_1})\varphi(p_2^{n_2})...\varphi(p_k^{n_k})$
et on a vu que $\varphi(p^\alpha) = p^{\alpha-1}(p-1)$ la formule en découle immédiatement.

3.3 Corps

frametitleCorps

Définition 57 *On appelle corps tout anneau unifère tel que tout élément non nul soit inversible. C'est-à-dire,*
si $(A, +, \times)$ est un anneau unifére, on a : A corps $\Leftrightarrow$ $(A^*, \times)$ est un groupe.
Si de plus la loi $\times$ est commutative, on dit que le corps est commutatif .

Exemples
- $(Z, +, \times)$ et $(\mathbb{R}[X], +, \times)$ ne sont pas des corps.
- $(\mathbb{R}, +, \times)$ et $(\mathbb{R}(X), +, \times)$ sont des corps.
- $\mathbb{Z}/p\mathbb{Z}$ est un corps.ssi p est premier

.

Proposition 66 *Soit $(K, +, \times)$ un corps. Alors*

1. K possède au moins deux élements,
2. K est intègre.

Démonstration

– 1. Il s'agit de 0_K et 1_K puisque $0_K \neq 1_K$ (K est unifère c-àd distinct de l'anneau nul).
2. Supposons $ab = 0$ avec $a \neq 0$ et $b \neq 0$. Si $a \neq 0$, alors a est inversible $\Rightarrow a^{-1}ab = a^{-1}0 \Rightarrow b = 0$ absurde.
Donc $ab = 0 \Rightarrow a = 0$ ou $b = 0$

.
– Sous-corps
Définition On appelle sous-corps d'un corps, tout anneau de ce corps qui est un corps pour les lois induites.
De même que précédemment, on a les caractérisations pratiques suivantes :
Proposition Soit $(K, +, \times)$ un corps.
K' sous-corps de $K \Leftrightarrow K'$ est un sous-anneau de K et $\forall x \in K' \setminus \{0_K\}\,;\, x^{-1} \in K'$

$$\Leftrightarrow \begin{cases} K' \text{est un sous-groupe de } (K; +) \text{ et} \\ K' \setminus \{0_K\} \text{ est un sous-groupe de } (K' \setminus \{0_K\}\,; \times). \end{cases}$$

Si K' est un sous-corps de K, alors K est appelé sur-corps de K' ou encore extension de K'

. Idéaux d'un corps

Proposition 67 *Tout corps n'a que des idéaux triviaux.*

Preuve : D'abord, K et $\{0_K\}$ sont bien des idéaux (triviaux) de K. Il n'y en a pas d'autre.

Car si I est un idéal de K distinct de l'idéal nul $\{0_K\}$, montrons que $I = K$. Comme I n'est pas l'idéal nul, il existe un élément i de I distinct de 0_K. Soit i^{-1} son inverse dans K. Alors $i \times i^{-1} = 1_K \in I$ par définition d'un idéal. et donc On conclut par la proposition 2.3.14. que $I = K$.

.

– Morphisme de corps

Définition 58 *On appelle morphisme du corps* $(K, +, \times)$ *vers le corps* $(L, +, \times)$ *toute application* f *de* K *vers* L *telle que*

1. $\forall (x; y) \in K^2$, $f(x + y) = f(x) + f(y)$.
2. $\forall (x; y) \in K^2$, $f(x \times y) = f(x) \times f(y)$.
3. $f(1_K) = 1_L$.

Les conséquences immédiates sont que tout morphisme de corps f est un morphisme du groupe $(K; +)$ vers le groupe $(L; +)$. De plus, f est également un morphisme du groupe $(K \setminus \{0_K, \times\}$ vers le groupe $(L \setminus \{0_K, \times\}$. On remarquera qu'il s'agit bien d'une application ici car si x est inversible pour $\times$ dans K alors $f(x)$ est inversible pour $\times$ dans L (propriété d'anneau).