1 Groupes

Définition 1.1

On appelle groupe un couple composé d'un ensemble G et d'une loi de composition interne (lci) sur G vérifiant :

il existe un élément neutre e de G tel que $\forall x \in G, e.x = x.e = x$,

la lci est associative,

tout élément x admet un inverse.

Si de plus la lci est commutative, on dit que le groupe $(G, .)$ est commutatif ou encore abélien.

On note qu'un groupe est un couple ensemble-lci.
Dans le cas d'un groupe abélien, on aura tendance à noter la lci par $+$.
Inverse et élément neutre sont uniques.
On notera l'inverse de x dans le cas d'une loi . par x^{-1}.

Définition 1.2

Soit $(G, .)$ un groupe possédant un nombre fini d'éléments. Le cardinal de G est appelé ordre du groupe et noté $|G|$.

Proposition 1.1

Soit $(G, .)$ un groupe.

1. *Pour tout élément a de G, les applications $x \longmapsto a.x$ et $x \longmapsto x.a$ sont des bijections ;*
2. *L'application $x \longmapsto x^{-1}$ est une bijection ;*
3. *Si a et b sont deux éléments qui commutent, alors $(a.b)^n = a^n.b^n$ pour tout $n \in \mathbb{Z}$.*

Proposition 1.2

Soient $(G, .)$ et $(H, *)$ deux groupes. L'ensemble $G \times H)$ muni de la loi produit $(x, y).(x', y') := (x.x', y * y')$ est un groupe.

On notera le plus souvent de la même manière les lois de G et H, même si ce ne sont pas les mêmes.

Définition 1.3

Soit $(G,.)$ un groupe.
On dit que H une partie de G est stable pour la loi . si

$$\forall (x,y) \in H^2, x.y \in H.$$

Proposition 1.3

Soit $(G,.)$ un groupe et H une partie stable de G.
On appelle loi induite sur H l'application $\begin{array}{ccc} H \times H & \longrightarrow & H \\ (x,y) & \longmapsto & x.y \end{array}$.

Définition 1.4

Soit $(G,.)$ un groupe et H une partie stable de G. On dit que H est un sous-groupe de $(G,.)$ si $(H,.)$ est un groupe.
On notera $H < (G,.)$.

Proposition 1.4

Soit $(G,.)$ un groupe et H une partie de G.

H est un sous-groupe de $(G,.)$ si et seulement si $\left\{ \begin{array}{l} e \in H \\ H \text{ est stable} \\ \forall x \in H, x^{-1} \in H. \end{array} \right.$

Si $(G,.)$ est un groupe, H un sous-groupe de $(G,.)$ et K un sous-groupe de $(H,.)$, alors K est un sous-groupe de $(G,.)$.

Proposition 1.5

1. *Une intersection de sous-groupes est un sous-groupe*
2. *Si G' est un sous-groupe de $(G,.)$ et H' un sous-groupe de $(H,.)$ alors $G' \times H'$ est un sous-groupe de $(G \times H,.)$.*

1.1 Morphismes

Définition 1.5

Soient $(G,.)$ et $(G',.)$ deux groupes. Une application $f : G \longrightarrow G'$ est un morphisme de groupes de $(G,.)$ vers $(G',.)$ si $\forall (x,y) \in G \times G'$, $f(x.y) = f(x).f(y)$.

Attention au piège des notations multiplicatives. La fonction exponentielle est un morphisme de $(\mathbb{R},+)$ vers $(\mathbb{R}^{*+},.)$.
Un morphisme bijectif est appelé isomorphisme. Si $(G',.) = (G,.)$, on dira que c'est un endomorphisme. Si c'est à la fois un isomorphisme et un endomorphisme, on dira que c'est un automorphisme.

Proposition 1.6

Soit f un morphisme de $(G,.)$ vers $(G',.)$.

1. *L'image de l'élément neutre de G est celui de G' ; l'image de l'inverse est l'inverse de l'image.*
2. *La composée de deux morphismes est un morphisme (à condition de bien vérifier l'existence de la composée !)*
3. *L'image réciproque de l'élement neutre de G' est un sous-groupe de $(G,.)$. On l'appelle le noyau de f et on le note $Ker f$.*
4. *L'image d'un sous-groupe de $(G,.)$ est un sous-groupe de $(G',.)$. On appelle image de f, notée $Im f$ l'ensemble $f(G)$.*

Théorème 1.7

Soit f un morphisme de $(G,.)$ vers $(G',.)$.

1. *f est injectif si et seulement si $Kerf = \{e_G\}$;*
2. *Si f est injectif, alors $\begin{array}{ccc} G & \longrightarrow & f(G) \\ x & \longmapsto & f(x) \end{array}$ est un isomorphisme.*

Définition 1.6

Soit $(G,.)$ un groupe et A une partie de G. On appelle sous-groupe engendré par A le plus petit sous-groupe contenant A.

Proposition 1.8

Soit A une partie de $(G,.)$ un groupe. Le sous-groupe engendré par A est l'intersection de tous les sous-groupes contenant A.

Proposition 1.9

Soit $(G,.)$ un groupe et a un élément de G.
L'application $\begin{array}{ccc} \mathbb{Z} & \longrightarrow & G \\ n & \longmapsto & a^n \end{array}$ est un morphisme de groupes.
Le sous-groupe engendré par a est l'image de ce morphisme.

Théorème 1.10

Les sous-groupes de $(\mathbb{Z},+)$ sont de la forme $n\mathbb{Z}$, avec $n \in \mathbb{N}$.

Soit $(G,.)$ un groupe et a un élément de G. On considère $f_a : \begin{array}{ccc} \mathbb{Z} & \longrightarrow & G \\ n & \longmapsto & a^n \end{array}$.
Il s'agit d'un morphisme de groupes. Son noyau est donc soit réduit à $\{0_G\}$, soit un sous-groupe de $(\mathbb{Z},+)$ non réduit à un élément : il existe n un entier naturel non nultel que $Kerf_a = n\mathbb{Z}$.

Définition 1.7

Dans le premier cas, on dit que a est d'ordre infini, dans le second cas, il est fini d'ordre n.

Exercice 1 : Trouver tous les éléments d'ordre 1.

Proposition 1.11

Soit $(G,.)$ un groupe et a un élément de G d'ordre n.

1. *$\{k \in \mathbb{Z}/a^k = 1\} = n\mathbb{Z}$;*
2. *Soient k et l deux entiers. $\left(a^k = a^l\right) \Longleftrightarrow k \equiv \ mod\, n$.*
3. *L'ordre d'un élément est l'ordre du sous-groupe qu'il engendre. Dans ce cas, $< a >= \{e_G, a, a^2, \ldots, a^{n-1}\}$.*

Proposition 1.12

Soit f un morphisme de groupe de $(G,.)$ vers $(G',.)$.

1. *$f(a)$ est d'ordre fini et son ordre divise l'ordre de a ;*
2. *si f est un isomorphisme, a et $f(a)$ ont même ordre.*

Soit $(G,.)$ un groupe et $H < (G,.)$. On pose, pour $a \in G$, $aH := \{ax/x \in H\}$ et $Ha := \{xa/x \in H\}$.

Proposition 1.13

La relation binaire $\mathcal{R}_\}$ (respectivement $\mathcal{R}_\lceil$) définie par $x\mathcal{R}_\}y$ si $y \in xH$ (respectivement $y \in Hx$) est une relation d'équivalence.
Dans ce cas, la classe de x est xH et s'appelle la classe à gauche de x modulo H (respectivement la classe à droite).

Proposition 1.14

La multiplication par x définit des bijections $H \longmapsto Hx$ (multiplication à gauche) et $H \longmapsto xH$ (multiplication à droite).
L'application de G dans lui-même qui à un élément associe son inverse définit une bijection de xH vers Hx^{-1}.
L'application φ, de $G/\mathcal{R}_g$ vers $G/\mathcal{R}_d$ qui à xH associe Hx^{-1} est une bijection.

Définition 1.8

Soit $(G,.)$ un groupe et $H < (G,.)$. S'il y a un nombre fini de classes modulo H, le nombre de ces classes s'appellent l'indice de H dans $(G,.)$ et se note $[G:H]$.

Comme toutes les classes ont même ordre,

Théorème 1.15 (Lagrange)

Si $(G,.)$ est un groupe fini, et H est un sous-groupe de $(G,.)$, alors l'ordre de H divise l'ordre de G et

$$CardG = CardH.[G:H].$$

Corollaire 1.16

1. *L'ordre d'un élément divise donc l'ordre du groupe ;*
2. *Pour tout élément a de G, $a^{|G|} = e$;*
3. *Si a est un élement d'ordre p de G, si b un élement d'ordre q, qui commute avec a et si p et q sont premiers entre eux, ab est d'ordre pq.*

Définition 1.9

Un sous-groupe H de $(G,.)$ est distingué si pour tout $x \in G$, $XH = Hx$. On note $H \triangleleft (G,.)$.

Attention, cela ne veut pas dire que $xh = hx$! !

Proposition 1.17

$$\forall x \in G, \forall h \in H, xhx^{-1} \in H.$$

Dans un groupe abélien, tous les sous-groupes sont distingués.
Le noyau d'un morphisme est topujours un sous-groupe distingué du groupe de départ.
Il faut que le sous-groupe soit dsitingué pour qu'on puisse munir l'ensemble quotient (des classes d'équivalence) d'une structure naturelle de groupes. On le notera alors G/H

Théorème 1.18

Soit $H < (G, .)$.

1. *Dans G/H, l'opération $(xH)(yH) := xyH$ est bien définie et munit la structure G/H d'une structure de groupe. L'élément neutre est H*
2. *La projection canonique $x \longmapsto xH$ est un morphisme surjectif de noyau H*
3. *$|G| = |H|.|G/H|$.*

Exercice 2 : Écrire le théorèeme de décomposition canonique pour les groupes.

Exercice 3 :
Citer des exemples d'éléments générateurs pour des groupes issus de la géométrie.

2 Anneaux et corps

Définition 2.10

Un anneau est un ensemble A muni de deux lois de composition interne $+$(addition) et $\times$ (multiplication) pour lesquels $(A, +)$ est un groupe commutatif, la multiplication est associative, distributive par rapport à l'addition et qui admet un élément neutre.
Si de plus la multiplication est commutative, on dira que l'anneau est commutatif.

Un sous-anneau est un partie stable pour les deux lois qui est un anneau pour les lois induites.
Si $(A, +, \times)$ et $(B+, \times)$ sont des anneaux, alors le produit cartésien $A \times B$, munis des lois produit (addition terme à terme et multiplication terme à terme) est un anneau.
On considère une partie de $\mathbb{C}$ qui est $\mathbb{Z}[i] := \{a + bi, (a, b) \in \mathbb{Z}^2\}$. C'est un anneau, car un sous-anneau de $(\mathbb{C}, +, \times)$. On l'appelle l'anneau des entiers de Gauss.

Définition 2.11

Soit $(A, +, .)$ un anneau.

1. *Soient a et b deux éléments de A. On dit que a divise b ou que b est un multiple de a s'il existe q dans A tel que $b = qa$*
2. *Un élément a de A est inversible s'il existe a' dans A tel que*

$$aa' = a'a = 1.$$

Proposition 2.19

1. *L'inverse d'un élément est unique : on le note a^{-1} ;*
2. *0 n'est pas inversible ;*
3. *Si a est inversible, tout élément de A est un multiple de a ;*
4. *L'ensemble A^* des éléments inversibles de A est un groupe pour la multiplication (loi induite) ; l'élément neutre est 1 ;*
5. *Si $(B, +, .)$ est un anneau, $(A \times B)^* = A^* \times B^*$.*

Définition 2.12

Un anneau est dit intègre si, pour $(x, y) \in A^2$, $(xy = 0 \iff (x = 0 \ \ ou \ \ y = 0))$.

Définition 2.13

Un corps est un anneau $(K, +, .)$ dont tous les éléments non nuls sont inversibles.

Proposition 2.20

Un corps est un anneau intègre.

Définition 2.14

Une application d'un anneau dans un autre est un morphisme d'anneau si c'est un morphisme pour chacune des deux lois et si $f(1_A) = 1_B$.

Ainsi, l'application qui à un polynôme réel associe sa valeur en un point donné est un morphisme d'anneau.
La conjugaison dans $\mathbb{C}$ est un morphisme de corps et donc un morphisme d'anneau pour sa restriction sur l'"anneau des entiers de Gauss.

Proposition 2.21

L'image d'un élément inversible par un morphisme d'anneaux est inversible et l'inverse de l'image est l'image de l'inverse.
La restriction de f à A^* est un morphisme de groupes pour la multiplication.

Définition 2.15

Soit $(A, +, .)$ un anneau. Un idéal de A est un sous-groupe pour l'addition et

$$\forall a \in I,\ \forall x \in A, xa \in I \text{ et } ax \in I.$$

On parle d'idéal bilatère, mais il existe les idéaux à gauche et les idéaux à droite. Dans ce cours sur nombre et structures, les anneaux sont le plus souvent commutatifs.
Le singleton $\{0_A\}$ est donc un idéal. Mais certains autaurs l'excluent, du fait de son caractère particulier.

Proposition 2.22

1. *Pour tout élément a de A, l'ensemble $\{a.x, x \in A\}$ des multiples de a est un idéal de A noté $a.A$ ou (a). On dit que c'est l'idéal engendré par a.*
2. *Pour tous a et b éléments de A,*

$$aA \subset bA \iff b|a.$$

Définition 2.16

Si un idéal I d'une anneau $(A, +, .)$ est engendré par un élément, on dit que l'idéal est principal.
Un anneau pour lesquels tous les idéaux sont principaux est dit anneau pricipal

$\mathbb{Z}$ est un anneau principal.

Proposition 2.23

Le noyau d'une morhisme d'anneaux est un idéal de A.
L'image d'un morphisme d'anneau est un sous-anneau de l'anneau d'arrivée.

Proposition 2.24

Un anneau A est un corps si et seulement si les ses seuls idéaux sont $\{0_A\}$ et lui-même.
Soit K un corps et B un anneau. Tout morphisme de K dans B est injectif.

On a introduit la notion d'idéal pour des raisons de quotientage : c'est l'aspect absorbant des idéaux qui assure que l'on peut munir l'ensemble A/I (au sens de groupe car I est un groupe distingué de $(A, +)$ d'une deuxième loi interne (multiplication quotient).
Regardons de plus près : on va définir la multiplication quotient par, en notant p la projection canonique de A sur A/I.
On définit pour X et Y deux classes de A/I, $X.Y := x.y$, où x et y sont des représentants de X et Y ($X = p(x)$ et $Y = p(y)$). Pour que cette défintion existe, il faut montrer qu'en changeant de représentants pour les classes X et Y, le produit $x.y$ reste le même.
On a $X = p(x)$ et $Y = p(y)$. Soient x' et y' tels que $p(x) = p(x') = X$ et $p(y) = p(y') = Y$.
Alors on va montrer que $p(x.y) = p(x'.y')$.
Remarquons que $x - x' \in I$ et $y - y' \in I$.

$$xy - x'y' = (x - x').y + x'(y - y')$$

I est un idéal, donc $xy - x'y' \in I$ ce qui permet de conclure.

Théorème 2.25

Soit $(A, +, .)$ un anneau et I un idéal différent de A. Alors le groupe $(A/I, +)$ muni de la multiplication quotient définie ci-dessus est un anneau. La projection canonique est un morhisme d'anneau surjectif dont le noyau est I.
L'anneau $(A/I, +, .)$ est appelé l'anneau quotient de A par l'idéal I.

Exercice 4 Écrire le théorème de décomposition canocique pour les anneaux.

Corollaire 2.26

Soit f un morphisme d'anneaux de A vers B.
Il existe un unique morphisme d'anneaux de $A/Kerf$ vers B $\tilde{f}$ tel que $\tilde{f} \circ p = f$.
Le morphisme $\tilde{f}$ est injectif. Si f est surjectif, alors $\tilde{f}$ est un isomorphisme.

3 $\mathbb{Z}/n\mathbb{Z}$

Dans tous ce paragraphe, n est un entier naturel supérieur ou égal à 2.
On ne revient pas sur la définition de $\mathbb{Z}/n\mathbb{Z}$. De la section précédente on en déduit :

Théorème 3.27

$(\mathbb{Z}/n\mathbb{Z}), +, .)$ est un anneau commutatif.

Exercice 5 : Est-il intègre ?

Proposition 3.28

Pour tout entier k, l'élément $\dot{k} \in \mathbb{Z}/n\mathbb{Z}$ est inversible dans $\mathbb{Z}/n\mathbb{Z}$ si et seulement si k est premier avec n.

Exercice 6 : Quel est le lien entre un élément inversible pour la multiplication et un générateur du groupe additif $\mathbb{Z}/n\mathbb{Z}$?

On note p_n la projection canonique de Z sur $\mathbb{Z}/n\mathbb{Z}$.

Théorème 3.29 (chinois)

Soient p et q deux entiers au moins égaux à 2, premiers entre eux.
L'application $f : \begin{array}{ccc} \mathbb{Z} & \longrightarrow & \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/q\mathbb{Z} \\ k & \longmapsto & (p_p(k), p_q(k)) \end{array}$ *est un morphisme d'anneau.*
Alors $\tilde{f}$ est un isomorphisme d'anneaux de $\mathbb{Z}/pq\mathbb{Z}$ dans $\mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/q\mathbb{Z}$.

Exercice 7 : Détaillez l'application $\tilde{f}$.

Corollaire 3.30

Soit C_p un groupe cyclique à p éléments et D_q un groupe cyclique à q éléments.
Le groupe $C_p \times D_q$ est cyclique si et seulement si p et q sont premiers entre eux.

Théorème 3.31

Soient p et q deux entiers naturels premiers entre eux. L'isomorphisme des restes chinois définit un isomorphisme de groupe de $(\mathbb{Z}/pq\mathbb{Z})^*$ vers $(\mathbb{Z}/p\mathbb{Z})^* \times (\mathbb{Z}/q\mathbb{Z})^*$.

Définition 3.17

Soit n un entier au moins égal à 2.
On note $\varphi(n)$ le nombre d'entiers k permiers à n dans $[\![1, n]\!]$.
La fonction φ s'appelle la fonction d'Euler.

Théorème 3.32

1. *Le groupe$((\mathbb{Z}/n\mathbb{Z})^*, .)$ possède $\varphi(n)$ éléments ; Pour tout entier a premier avec n, on a $a^{\varphi(n)} \equiv 1 \ mod \ n$;*
2. *tout groupe cyclique à n éléments possède $\varphi(n)$ générateurs.*

Le calcul de la fonction d'Euler se trouve dans la feuille d'exercices sur les groupes.

Théorème 3.33

Soit n un entier supérieur ou égal à 2.
L'anneau $\mathbb{Z}/n\mathbb{Z}$ est un corps si et seulement si n est un nombre premier.
Dans ce cas, ce corps est noté $\mathbb{F}_n$.