Université de Bordeaux
Licence de Sciences, Technologies, Santé
Mathématiques, Informatique, Sciences de la Matière et Ingénierie

Algèbre 3 :
Résumé de cours

Table des matières

Chapitre 1

L'anneau $\mathbb{Z}$

1 La structure d'anneau de $\mathbb{Z}$

L'ensemble $\mathbb{Z}$ des entiers relatifs est muni d'une addition et d'une multiplication qui vérifient les propriétés suivantes :

1) L'addition est une *loi de composition interne* :

$$\forall (a,b) \in \mathbb{Z}^2 \ , \ a+b \in \mathbb{Z}$$

2) L'addition est *associative* :

$$\forall (a,b,c) \in \mathbb{Z}^3 \ , \ a+(b+c) = (a+b)+c$$

3) 0 est un *élément neutre* pour l'addition :

$$\forall a \in \mathbb{Z} \ , \ a+0 = 0+a = a$$

4) *Tout élément admet un opposé* pour l'addition :

$$\forall a \in \mathbb{Z} \ , \ a+(-a) = (-a)+a = 0$$

On résume les propriétés 1) à 4) en disant que $(\mathbb{Z},+)$ est un ***groupe***.

Qui plus est :

5) L'addition est *commutative* :

$$\forall (a,b) \in \mathbb{Z}^2 \ , \ a+b = b+a$$

En résumé, on dit que $(\mathbb{Z},+)$ est un groupe *commutatif* (ou *abélien*).

Pour ce qui est de la multiplication, elle possède les propriétés suivantes :

1) C'est une loi de composition interne : $\forall (a,b) \in \mathbb{Z}^2$, $a \cdot b = b \cdot a$

2) Elle possède un élément neutre (l'entier 1) : $\forall a \in \mathbb{Z}$, $a \cdot 1 = 1 \cdot a = a$

3) Elle est *distributive par rapport à l'addition*, ce qui signifie que

$$\forall (a,b,c) \in \mathbb{Z}^3 \text{ , } a \cdot (b+c) = a \cdot b + a \cdot c.$$

On dit que $(\mathbb{Z}, +\cdot)$ est un *anneau*.

2 Entiers relatifs et arithmétique

2.1 Division euclidienne

Théorème 1
Pour tout couple d'entiers naturels (a,b) avec $b \neq 0$, il existe un unique couple (q,r) d'entiers naturels tels que

$$\begin{cases} a = bq + r \\ 0 \leq r < b \end{cases} \tag{1.1}$$

Les entiers q et r sont respectivement le quotient et le reste de la division euclidienne de a par b.

Preuve. Pour l'existence, on considère l'ensemble $E = \{q \in \mathbb{N} \mid bq \leq a\}$; comme partie non vide et majorée de $\mathbb{N}$, il admet un plus grand élément q. On pose alors $r := a - bq$. Clairement, on a $0 \leq a - bq < b$, donc le couple (q,r) satisfait 1.1. Pour l'unicité, on suppose qu'il existe un autre couple (q',r') tel que

$$\begin{cases} a = bq' + r' \\ 0 \leq r' < b. \end{cases} \tag{1.2}$$

En particulier, $bq' = a - r' \leq a$, donc $q' \in E$, et par conséquent $q' \leq q = \max E$. Si q' était distinct de q, il serait au plus égal à $q-1$, et on aurait

$$r' = a - bq' \geq a - bq + b = r + b > b,$$

une contradiction. Donc $q' = q$ et par suite $r' = r$. □
La division euclidienne s'étend sans difficulté à l'ensemble $\mathbb{Z}$ des entiers relatifs :

Théorème 2
Pour tout couple d'entiers relatifs (a,b) avec $b \neq 0$, il existe un unique couple (q,r) d'entiers relatifs tels que

$$\begin{cases} a = bq + r \\ 0 \leq r < |b|. \end{cases} \tag{1.3}$$

2.2 Divisibilité

Définition 1
Soit a et b deux entiers relatifs. On dit que "a divise b" et on écrit " a | b " s' il existe $q \in \mathbb{Z}$ *tel que* $a = bq$.

Remarque : a divise b si et seulement si le reste de la division euclidienne de a par b est nul.

2.3 PGCD, PPCM

Définition 2

1) *Le PGCD de deux entiers relatifs a et b non tous les deux nuls est l'entier d défini par :*

$$d := \max \{k \in \mathbb{N}^* \mid k \text{ divise } a \text{ et } b\}$$

2) *Le PPCM de deux entiers relatifs a et b non nuls est l'entier m défini par :*

$$m := \min \{k \in \mathbb{N}^* \mid k \text{ est un multiple commun à } a \text{ et } b\}$$

2.4 Sous groupes de $\mathbb{Z}$ et théorème de Bézout

Définition 3
Un sous-groupe *de* $\mathbb{Z}$ *est une partie non vide et "stable par addition et soustraction". Plus précisément,* $F \subset \mathbb{Z}$ *est un sous-groupe si*

1) $F \neq \emptyset$,

2) *pour tout élément x de F et tout élément y de F, la différence* $x - y$ *appartient à F.*

Remarques : si F est un sous-groupe de $\mathbb{Z}$ alors

1) 0 appartient à F.

2) Si $x \in F$ alors $-x \in F$.

3) Plus généralement, si $x \in F$ alors $kx \in F$ pour tout $k \in \mathbb{Z}$.

Notation : si a est un entier (quelconque), on note $a\mathbb{Z}$ l'ensemble de ses multiples. Autrement dit

$$a\mathbb{Z} = \{am, m \in \mathbb{Z}\} = \{n \in \mathbb{Z} \mid \exists m \in \mathbb{Z}, n = am\}.$$

De même, si a et b sont deux entiers, on définit

$$a\mathbb{Z} + b\mathbb{Z} = \{ax + by, x, y \in \mathbb{Z}\} = \{n \in \mathbb{Z} \mid \exists x, y \in \mathbb{Z} \in \mathbb{Z}, n = ax + by\}.$$

Proposition 1

1) *Pour tout entier a, l'ensemble $a\mathbb{Z}$ est un sous-groupe de $\mathbb{Z}$.*

2) *Si a et b sont des entiers, on a l'équivalence : $a\mathbb{Z} \subset b\mathbb{Z} \Leftrightarrow b$ divise a.*

3) *Si a et b sont des entiers, l'ensemble $a\mathbb{Z} + b\mathbb{Z}$ est un sous-groupe de $\mathbb{Z}$.*

Théorème 3
Soit F un sous-groupe de $\mathbb{Z}$. Alors, il existe un unique entier naturel g tel que $F = g\mathbb{Z}$.

Preuve. Si $F = \{0\}$ alors $g = 0$ convient. Sinon, F contient un élément non nul x, ainsi que son opposé $-x$, donc il contient un élément strictement positif. Par conséquent, l'ensemble $F_+ = \{x \in F \mid x > 0\} \subset \mathbb{N}$ est non vide. Il admet donc, comme toute partie non vide de $\mathbb{N}$, un plus petit élément noté g. Clairement, g appartient à F, ainsi que tous ses multiples, donc $g\mathbb{Z} \subset F$. Inversement, si a est un élément (quelconque) de$F$, on peut effectuer la division euclidienne de a par g :

$$a = gq + r\ , \ \text{ avec } q, r \in \mathbb{Z} \text{ et } 0 \leq r < g.$$

On en déduit que $r = a - qg$ appartient à F, comme différence de deux éléments de F. S'il était > 0, cela contredirait la définition de g, donc $r = 0$, ce qui signifie que $a \in g\mathbb{Z}$. □

Corollaire 1
Soient a et b deux entiers non tous les deux nuls. On note d leur PGCD et m leur PPCM.

1) *$a\mathbb{Z} + b\mathbb{Z} = d\mathbb{Z}$ et $a\mathbb{Z} \cap b\mathbb{Z} = m\mathbb{Z}$.*

2) *(Théorème de Bézout) Si $\text{PGCD}(a, b) = d$ alors il existe deux entiers u et v tels que*

$$au + bv = d.$$

3) *Le PGCD de a et b est le "plus grand diviseur commun" à a et b au sens de la relation d'ordre usuelle sur $\mathbb{Z}$, mais également au sens de la relation de divisibilité.*

4) *Le PPCM de a et b est le "plus petit multiple commun" à a et b au sens de la relation d'ordre usuelle sur $\mathbb{Z}$ et au sens de la relation de divisibilité.*

Remarque : le corollaire précédent permet de lever la restriction "a et b non tous les deux nuls" dans la définition du PGCD et du PPCM, en posant $\text{PGCD}(0, 0) = \text{PPCM}(0, 0) = 0$.

2.5 Algorithme d'Euclide

Proposition 2
Soient a et b deux entiers, avec $b \neq 0$. Si r est le reste de la division euclidienne de a par b alors

$$\mathrm{PGCD}(a, b) = \mathrm{PGCD}(b, r).$$

Voici le principe de l'algorithme d'Euclide : soient a et b deux entiers positifs ; on pose $r_0 = a$ et $r_1 = b$, puis pour $k \geq 1$, **tant que** $r_k > 0$, on définit r_{k+1} comme le reste de la division euclidienne de r_{k-1} par r_k. En particulier, on a $r_{k+1} < r_k$ si r_k est non nul. La suite ainsi construite est donc strictement décroissante, ce qui garantit que l'algorithme s'arrête. On vérifie alors, en utilisant la Proposition 2, que le dernier terme non nul de la suite est le PGCD de a et b.

Entrées : a,b entiers naturels
Sorties : PGCD de a et b
tant que $b > 0$ **faire**
  $r \leftarrow a\%b$ `/* reste de la division euclidienne de a par b */`
  $a \leftarrow b$
  $b \leftarrow r$
fin
retourner a

Algorithme 1 : Algorithme d'Euclide

Voici maintenant une variante de l'algorithme d'Euclide qui permet de déterminer le PGCD de deux entiers a et b ainsi que deux entiers u et v tels que $au + bv = \mathrm{PGCD}(a, b)$. Cette variante est généralement appelée *algorithme d'Euclide étendu*.
On définit récursivement des entiers u_k et v_k de la façon suivante : on pose $u_0 = 1$, $v_0 = 0$, $u_1 = 0$, $v_1 = 1$ et pour $k \geq 1$

$$\begin{cases} u_{k+1} = u_{k-1} - u_k q_k \\ v_{k+1} = v_{k-1} - v_k q_k \end{cases}$$

On vérifie alors par récurrence sur k, que les entiers u_k et v_k ainsi définis vérifient la relation

$$r_k = au_k + bv_k$$

pour tout $k \geq 0$. En particulier, si n est l'indice du dernier reste non nul, on obtient

$$d = r_n = au_n + bv_n.$$

Entrées : a,b entiers naturels
Sorties : $d = \text{PGCD}(a,b)$ et $(u,v) \in \mathbb{Z}^2$ tel que $d = au + bv$
$u \leftarrow 1$
$v \leftarrow 0$
$s \leftarrow 0$
$t \leftarrow 1$
tant que $b > 0$ **faire**
  $q \leftarrow a/b$ `/* quotient de la division euclidienne de` a `par` b `*/`
  $r \leftarrow a\%b$ `/* reste de la division euclidienne de` a `par` b `*/`
  $a \leftarrow b$
  $b \leftarrow r$
  $X \leftarrow s$
  $s \leftarrow u - qs$
  $u \leftarrow X$
  $X \leftarrow t$
  $t \leftarrow v - qt$
  $v \leftarrow X$
fin
retourner a, u, v

Algorithme 2 : Algorithme d'Euclide étendu

Remarque : l'algorithme précédent fournit une preuve constructive du théorème de Bézout.

Corollaire 2
Soient a et b deux entiers non tous les deux nuls.

1) *Le PGCD de a et b est le "plus grand diviseur commun" à a et b au sens de la relation d'ordre usuelle sur $\mathbb{Z}$ et au sens de la relation de divisibilité.*

2) *Le PPCM de a et b est le "plus petit multiple commun" à a et b au sens de la relation d'ordre usuelle sur $\mathbb{Z}$ et au sens de la relation de divisibilité.*

2.6 Compléments

Dans ce paragraphe, on notera $a \wedge b$ le PGCD de deux entiers a et b, et $a \vee b$ leur PPCM. On dit que a et b sont *premiers entre eux* si $a \wedge b = 1$.

Théorème 4
Deux entiers a et b sont premiers entre eux si et seulement s'il existe deux entiers u et v tels que

$$au + bv = 1.$$

Proposition 3
Lemme de Gauss *Soient a, b et c trois entiers. Si a divise bc et $a \wedge b = 1$ alors a divise c.*

Proposition 4
Soient a, b et c trois entiers.
a) *Si a divise c et b divise c et si $a \wedge b = 1$ alors ab divise c.*
b) *Si $a \wedge b = 1$ et $a \wedge c = 1$ alors $a \wedge bc = 1$.*
c) *Si p est un nombre premier et si p divise ab alors p divise a ou p divise b.*

Théorème 5
Tout entier $a > 1$ s'écrit de manière unique

$$a = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_k^{\alpha_k}$$

où $\begin{cases} \text{les entiers } p_i \text{ sont premiers et vérifient } p_1 < p_2 < \dots < p_k \\ \text{les entiers } \alpha_i \text{ sont strictement positifs} \end{cases}$

La preuve de l'unicité de la décomposition en facteurs premiers repose sur le lemme de Gauss.

3 Congruences

Dans toute la suite, n désigne un entier naturel non nul fixé.

Définition 4
On dit que deux entiers relatifs a et b sont congrus modulo n ou encore que a est congru à b modulo n si n divise $a - b$. On notera $a \equiv b \bmod n$ ou $a \equiv b\ [n]$.

Proposition 5
La relation de congruence modulo n vérifie les propriétés suivantes

1) $\forall a \in \mathbb{Z} \quad a \equiv a \bmod n$ *("Réfléxivité"),*

2) $\forall (a,b) \in \mathbb{Z}^2 \quad a \equiv b \bmod n \iff b \equiv a \bmod n$ *("Symétrie"),*

3) $\forall (a,b,c) \in \mathbb{Z}^3 \quad (a \equiv b \bmod n \wedge b \equiv c \bmod n) \Rightarrow a \equiv c \bmod n$ *("Transitivité").*

On dit que la relation de congruence est une ***relation d'équivalence*** *sur l'ensemble des entiers.*

Proposition 6
Pour tout entier relatif a, il existe un unique entier naturel $r \in \{0, \dots, n-1\}$ tel que $n \equiv r \mod n$

Preuve. Il suffit de considérer le reste de la division euclidienne de a par n. □

Définition 5
Pour tout $a \in \mathbb{Z}$, on note $a + n\mathbb{Z}$ ou $\overline{a}$ la classe de congruence de a modulo n, c'est-à-dire

$$a + n\mathbb{Z} = \overline{a} := \{b \in \mathbb{Z} \mid b \equiv a \mod n\}.$$

On note $\mathbb{Z}/n\mathbb{Z}$ l'ensemble des classes de congruence modulo n.

La Proposition 6 admet le corollaire suivant :

Corollaire 3
$\mathbb{Z}/n\mathbb{Z} = \{\overline{0}, \overline{1}, \dots, \overline{n-1}\}$.

Proposition 7
Soit n un entier naturel non nul. On note a, b, a' et b' quatre entiers relatifs. On a les propriétés suivantes : si $a \equiv b \mod n$ et $a' \equiv b' \mod n$ alors

$$a + a' \equiv b + b' \mod n \qquad a - a' \equiv b - b' \mod n \qquad aa' \equiv bb' \mod n$$

Remarque : On dit que la relation de congruence est compatible avec l'addition, la soustraction et la multiplication définies sur $\mathbb{Z}$.
La Proposition7 permet en particulier de munir l'ensemble quotient $\mathbb{Z}/n\mathbb{Z}$ d'une addition et d'une multiplication définies comme suit.

Définition 6
Soient $\overline{x}$ et $\overline{y}$ deux éléments de $\mathbb{Z}/n\mathbb{Z}$. On pose :

1) *(Addition) $\overline{x} + \overline{y} := \overline{s}$, où s désigne le reste de la division euclidienne de $x + y$ par n,*

2) *(Multiplication) $\overline{x}\ \overline{y} := \overline{p}$, où p désigne le reste de la division euclidienne de xy par n.*

Muni de ces deux opérations, l'ensemble $\mathbb{Z}/n\mathbb{Z}$ a une structure d'anneau.
Pour illustrer cette construction, on donne ci-dessous les tables d'addition et de multiplication de $\mathbb{Z}/3\mathbb{Z}$:

$+$	$\overline{0}$	$\overline{1}$	$\overline{2}$
$\overline{0}$	$\overline{0}$	$\overline{1}$	$\overline{2}$
$\overline{1}$	$\overline{1}$	$\overline{2}$	$\overline{0}$
$\overline{2}$	$\overline{2}$	$\overline{0}$	$\overline{1}$

$\times$	$\overline{0}$	$\overline{1}$	$\overline{2}$
$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$
$\overline{1}$	$\overline{0}$	$\overline{1}$	$\overline{2}$
$\overline{2}$	$\overline{0}$	$\overline{2}$	$\overline{1}$

Chapitre 2

Le groupe des permutations

1 Définitions et premières propriétés

Définition 1
Soit n un entier naturel non nul. L'ensemble des bijections de $\{1, \ldots, n\}$ dans lui-même s'appelle le groupe symétrique sur n éléments. On le note S_n. Ses éléments s'appellent des permutations.

Plus généralement, l'ensemble des bijections d'un ensemble fini E dans lui-même s'appelle le groupe des permutations de E.
Il y a exactement $n!$ façons de permuter les entiers de 1 à n. On a donc

$$\text{Card } S_n = n!$$

Remarque : on ne définit pas "S_0", moyennant quoi, dans la suite, l'écriture S_n sous-entendra toujours que n est un entier naturel non nul.

Une façon commode de noter les éléments de S_n est d'utiliser un tableau à 2 lignes, la première contenant les entiers de 1 à n, et la seconde leurs images.
Exemple :

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

désigne la permutation de $\{1, \cdots, 5\}$ dans lui-même définie par

$$\sigma(1) = 5,\ \sigma(2) = 2,\ \sigma(3) = 4,\ \sigma(4) = 1 \text{ et } \sigma(5) = 3.$$

Sa bijection réciproque s'écrit

$$\sigma^{-1} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 4 & 2 & 5 & 3 & 1 \end{pmatrix}.$$

La composition des applications munit S_n d'une structure de groupe : la composée de deux permutations est une permutation, la composition est associative, S_n possède

un élément neutre (l'application "identité" qui applique chaque entier $i \in \{1, \dots, n\}$ sur lui-même), tout élément a un "inverse" (bijection réciproque).
Pour alléger les notations, on omettra le signe "$\circ$" de la composition, c'est-à-dire qu'on écrira $\sigma\gamma$ pour désigner la composée $\sigma \circ \gamma$.
Cependant, ce groupe *n'est pas commutatif* : par exemple, les deux éléments

$$\sigma_1 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} \text{ et } \sigma_2 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$$

de S_3 ne commutent pas (on a $\sigma_1\sigma_2 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}$ et $\sigma_2\sigma_1 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}$).

Définition 2 (support)
Le support *d'une permutation $\sigma \in S_n$ noté* $\operatorname{Supp}\sigma$ *est le complémentaire dans* $\{1, \cdots, n\}$ *de l'ensemble* $\operatorname{Fix}\sigma$ *de ses points fixes. Autrement dit*

$$\operatorname{Supp}\sigma = \{i \in \{1, \dots, n\} \mid \sigma(i) \neq i\} \text{ , } \operatorname{Fix}\sigma = \{i \in \{1, \dots, n\} \mid \sigma(i) = i\}.$$

Remarque : le support d'une permutation σ et son complémentaire sont stables par σ

$$\sigma(\operatorname{Supp}\sigma) = \operatorname{Supp}\sigma \text{ , } \sigma(\operatorname{Fix}\sigma) = \operatorname{Fix}\sigma.$$

La notion de support apparait dans la proposition (fondamentale) suivante.

Proposition 1
Soient σ et γ deux éléments de S_n de supports disjoints. Alors $\sigma\gamma = \gamma\sigma$. Autrement dit, "deux permutations de supports disjoints commutent".

⚠ La réciproque est fausse : il se peut que deux permutations de supports non disjoints commutent. Par exemple, toute permutation commute avec elle-même !
Preuve. Comparons les images par $\sigma\gamma$ et $\gamma\sigma$ d'un élément x de $\{1, \dots, n\}$

- Si x appartient au support de σ, alors il n'appartient pas au support de γ puisque ces deux supports sont disjoints, par hypothèse. Par conséquent, $\gamma(x) = x$ et

  $$\sigma\gamma(x) = \sigma(x). \tag{2.1}$$

  Par ailleurs $\sigma(x)$ appartient lui aussi au support de σ, puisque celui-ci est stable par σ (*cf.* remarque précédente), et n'appartient donc pas au support de γ. Par conséquent,

  $$\gamma(\sigma(x)) = \sigma(x). \tag{2.2}$$

  En comparant (2.1) et (2.2) on conclut que $\sigma\gamma(x) = \gamma(\sigma(x))$.

- Le raisonnement serait le même, en échangeant les rôles de σ et γ, si on supposait que x appartient au support de γ.

- Enfin, si x n'appartient à aucun des deux supports, alors $\sigma\gamma(x) = \gamma\sigma(x) = x$.

□

Définition 3 (orbite)
Soit $x \in \{1, \dots, n\}$ et $\sigma \in S_n$. On appelle orbite de x sous l'action de σ l'ensemble

$$\mathrm{Orb}_\sigma(x) := \left\{\sigma^k(x), k \in \mathbb{N}\right\}.$$

Proposition 2 (et définition)
Soit $\sigma \in S_n$.

1) *Pour tout $x \in \{1, \dots, n\}$, il existe un plus petit entier naturel non nul k tel que $\sigma^k(x) = x$. On a alors $\mathrm{Orb}_\sigma(x) = \left\{x, \sigma(x), \sigma^{k-1}(x)\right\}$, et les éléments $\sigma^\ell(i)$, $1 \leq \ell \leq k-1$ sont deux à deux distincts.*

2) *Il existe un* plus petit entier naturel non nul *k_0 tel que $\sigma^{k_0} = \mathrm{Id}$, que l'on appelle* l'ordre de *σ.*

Preuve.

1) L'ensemble $\left\{\sigma^k(x), k \in \mathbb{N}\right\}$ est contenu dans $\{1, \dots, n\}$ donc il est fini. Par conséquent, il existe deux exposants distincts i et j tels que $\sigma^i(x) = \sigma^j(x)$. Sans perte de généralité, on peut supposer $i > j$ auquel cas $\sigma^{i-j}(x) = x$. L'ensemble des entiers naturels non nuls k tels que $\sigma^k(x) = x$ est donc non vide (il contient $i - j$) et il admet par conséquent un plus petit élément.

2) De la même façon, l'ensemble des puissances σ^k de σ est fini (il est contenu dans S_n de cardinal $n!$). Il existe donc deux entiers i et $j$distincts tels que $\sigma^i = \sigma^j$, d'où l'on conclut comme précédemment à l'existence d'un plus petit entier naturel non nul k tel que $\sigma^k = Id$.

□

Corollaire 1
Soit σ un élément de S_n, et k_0 son ordre. Alors $\sigma^{-1} = \sigma^{k_0 - 1}$ et

$$\mathrm{Orb}_\sigma(x) = \left\{\sigma^k(x), k \in \mathbb{Z}\right\}.$$

Exercice :

1) Montrer que si $\sigma \in S_n$ est une permutation d'ordre d alors $\sigma^k = \mathrm{Id}$ si et seulement si d divise k. Plus généralement, montrer que $\sigma^i = \sigma^j$ si et seulement si $i \equiv j \mod d$.

2) Montrer que le cardinal de l'orbite d'un élément sous l'action d'une permutation σ divise l'ordre de σ.

2 Cycles

Définition 4
Soient n un entier naturel non nul, et k un entier compris entre 2 et n. Un élément σ de $S_n \setminus \{\mathrm{Id}\}$ s'appelle un cycle de longueur k (ou k-cycle) s'il existe une partie $\{a_1, a_2, \ldots, a_k\}$ de $\{1, \ldots n\}$ telle que

- $\sigma(a_1) = a_2$, $\sigma(a_2) = a_3, \ldots, \sigma(a_{k-1}) = a_k$, $\sigma(a_k) = a_1$
- $\sigma(x) = x$ *si* $x \notin \{a_1, a_2, \ldots, a_k\}$.

Un tel cycle se note : $\sigma = (a_1, a_2, \ldots, a_k)$.

Autrement dit, un k- cycle est un élément de S_n qui permute circulairement les éléments d'une partie à k éléments de $\{1, \ldots n\}$ et fixe les autres :

$$a_1 \to a_2 \to \cdots a_{k-1} \to a_k \to a_1.$$

Exemple: Dans S_4 le cycle $(1, 2, 4)$ désigne la permutation

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

Noter que le *support* du cycle $(a_1, a_2, \ldots, a_k)$ est égal à $\{a_1, a_2, \ldots, a_k\}$.

⚠ Un même k-cycle peut s'écrire de k façons distinctes. Plus précisement, les k écritures suivantes

$$(a_1, a_2, \ldots, a_k)\,,\ (a_2, a_3, \ldots, a_k, a_1)\,,\ \ldots,\ (a_k, a_1, a_2 \ldots, a_{k-1})$$

désignent toutes le même cycle.

À l'inverse, le support d'un cycle ne suffit pas à le définir : dans S_4, les cycles $(1, 2, 4)$ et $(1, 4, 2)$ ont même support mais sont distincts (exercice : combien y a-t-il de cycles distincts et de support donné ? Combien y a-t-il de cycles de longueur k dans S_n ?).

Un cas particulier important est celui des cycles de longueur 2, que l'on appelle *transpositions*.

Proposition 3
Toute permutation peut s'écrire comme produit de transpositions.

⚠ cette décomposition n'est pas unique !

Preuve. Récurrence sur le cardinal du support de σ : si $x \in \mathrm{Supp}\,\sigma$ et si τ désigne la transposition $(x, \sigma(x))$ alors le support de $\sigma' := \tau\sigma$ est contenu strictement dans celui de σ. □

Proposition 4
L'ordre d'un k-cycle est égal à k.

3 Décomposition en cycles disjoints

Proposition 5
Les orbites sous l'action d'une permutation σ de S_n fournissent une partition de l'ensemble $\{1, \ldots, n\}$. Plus précisément, il existe des éléments x_1, x_2, …, x_r dans $\{1, \ldots, n\}$ tels que $\{1, \ldots, n\}$ soit la réunion disjointe *des orbites* $\mathrm{Orb}_\sigma(x_1)$, …, $\mathrm{Orb}_\sigma(x_r)$ *:*

$$\{1, \ldots, n\} = \bigsqcup_{i=1}^{r} \mathrm{Orb}_\sigma(x_i).$$

Preuve. On remarque que la relation "appartenir à la même orbite" est une relation d'équivalence. □
Le théorème suivant est fondamental. Il fournit une décomposition "canonique" pour toute permutation.

Théorème 1
Toute permutation différente de l'identité se décompose de façon essentiellement unique comme produit commutatif *de cycles disjoints. Autrement dit, pour tout $\sigma \in S_n \setminus \{\mathrm{Id}\}$ il existe des cycles c_1, …, c_s à supports disjoints tels que*

$$\sigma = c_1 c_2 \ldots c_s$$

et cette décomposition est unique à l'ordre près des facteurs.

Preuve.

- **Existence :** soient $\Omega_1 = \mathrm{Orb}_\sigma(x_1), \Omega_2 = \mathrm{Orb}_\sigma(x_2), \ldots, \Omega_s = \mathrm{Orb}_\sigma(x_s)$ les orbites de σ *non réduites à un point*. Elles forment une partition du support de σ, dont on note les cardinaux k_1, k_2, …, k_s respectivement. On considère alors les cycles

$$\begin{aligned} c_1 &= \left(x_1, \sigma(x_1), \cdots, \sigma^{k_1-1}(x_1)\right), \\ c_2 &= \left(x_2, \sigma(x_2), \cdots, \sigma^{k_2-1}(x_2)\right), \\ &\vdots \\ c_s &= \left(x_s, \sigma(x_s), \cdots, \sigma^{k_s-1}(x_s)\right) \end{aligned}$$

  et on vérifie immédiatement que $\sigma = c_1 c_2 \cdots c_s$.

- **Unicité :** On suppose disposer pour une permutation $\sigma \in S_n$ de deux décompositions

$$\sigma = c_1 c_2 \cdots c_s = d_1 \cdots d_r$$

en produit commutatif de cycles disjoints. Clairement, les supports de $c_1, c_2, \ldots, c_r$ coïncident avec les orbites de σ. Comme celles-ci ne dépendent que de σ, et pas d'un décomposition particulière, on conclut que $s = r$ et que, quitte à réordonner les cycles, ce qui est possible puisqu'il s'agit de produits commutatifs, on a

$$\text{Supp}\, c_1 = \text{Supp}\, d_1,\ \text{Supp}\, c_2 = \text{Supp}\, d_2,\ \ldots, \text{Supp}\, c_r = \text{Supp}\, d_r.$$

Enfin, si x est un élément du support commun de c_i et d_i, on vérifie aisément que $c_i = (x, \sigma(x), \ldots, \sigma^{k_i - 1}(x)$, et pour les mêmes raisons, que $d_i = (x, \sigma(x), \ldots, \sigma^{k_i - 1}(x)$, moyennant quoi $d_i = c_i$, et ce pour tout i. □

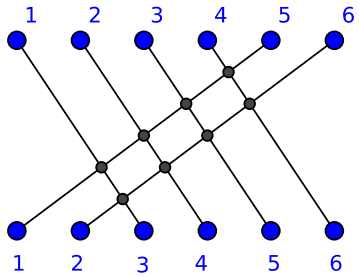
4 Signature

Définition 5
Soit $\sigma \in S_n$. On dit que σ réalise une inversion *sur le couple (i, j) si $i < j$ et $\sigma(i) > \sigma(j)$. On note $I(\sigma)$ le nombre d'inversion réalisées par σ. La signature de σ est le nombre*

$$\epsilon(\sigma) = (-1)^{I(\sigma)}.$$

Autrement dit, $\epsilon(\sigma)$ vaut $+1$ ou -1 selon que σ réalise un nombre pair ou impair d'inversions.

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



$$\varepsilon(\sigma) = (-1)^8 = +1$$

Proposition 6

1) *La signature d'une permutation $\sigma \in S_n$ est donnée par la formule*

$$\varepsilon(\sigma) = \prod_{\{i,j\} \in \mathcal{P}} \frac{\sigma(i) - \sigma(j)}{i - j}$$

où le produit est pris sur l'ensemble $\mathcal{P}$ des paires $\{i, j\}$ d'éléments de $\{1, \ldots, n\}$.

2) *La signature d'un produit est égale au produit des signatures :*

$$\forall \sigma \in S_n, \forall \gamma \in S_n, \ \varepsilon(\sigma\gamma) = \varepsilon(\sigma)\varepsilon(\gamma).$$

Preuve.

1) Clair.

2) Il suffit d'écrire

$$\begin{aligned}\varepsilon(\sigma\gamma) &= \prod_{\{i,j\}\in\mathcal{P}} \frac{\sigma\gamma(i)-\sigma\gamma(j)}{i-j} \\ &= \prod_{\{i,j\}\in\mathcal{P}} \frac{\sigma\gamma(i)-\sigma\gamma(j)}{\gamma(i)-\gamma(j)} \prod_{\{i,j\}\in\mathcal{P}} \frac{\gamma(i)-\gamma(j)}{i-j} \\ &= \prod_{\{i,j\}\in\mathcal{P}} \frac{\sigma(i)-\sigma(j)}{i-j} \prod_{\{i,j\}\in\mathcal{P}} \frac{\gamma(i)-\gamma(j)}{i-j}\end{aligned}$$

la dernière égalité étant justifiée par le fait que γ induit une bijection de $\mathcal{P}$ sur lui-même.

Proposition 7

1) *La signature d'un k-cycle est égale à* $(-1)^{k-1}$.

2) *Soit* $c_1c_2\ldots c_s$ *la décomposition en cycles à supports disjoints d'une permutation* $\sigma \in S_n$. *On note r le nombre de points fixes de* σ. *On a alors*

$$\varepsilon(\sigma) = (-1)^{n-(s+r)}.$$

Preuve.

1) On a vu en cours une démonstration basée sur la définition en termes de nombre d'inversions. On peut également remarquer que tout k-cycle peut se décomposer (de manière non canonique) comme produit de $k-1$ transpositions

$$(i_1, i_2, \ldots, i_k) = (i_1, i_k) \circ (i_1, i_{k-1}) \circ \cdots \circ (i_1, i_2)$$

et utiliser la multiplicativité de la signature, en remarquant qu'une transposition est clairement de signature -1.

2) C'est un corollaire immédiat du point précédent et de la multiplicativité de la signature : en notant k_i la longueur du ccyle c_i, on a

$$\varepsilon(\sigma) = (-1)^{(\sum_{i=1}^{s} k_i)-s} = (-1)^{n-r-s}.$$

□

Remarque : en combinant les propositions 3 et 6, on constate que la signature d'une permutation σ est égale à $+1$ (resp. -1) si σ se décompose en un produit d'un nombre *pair* (resp. *impair*) de transpositions. Ceci constitue un moyen de calcul efficace de la signature si l'on dispose d'une décomposition en produit de transpositions.

Chapitre 3

Théorie des groupes

1 Définition et premiers exemples

Définition 1
Un groupe est la donnée d'un ensemble G et d'une ***loi de composition interne*** $*$

$$\begin{array}{ccc} G \times G & \to & G \\ (x,y) & \mapsto & x*y \end{array}$$

qui vérifie les propriétés suivantes :

1) *la loi* $*$ *est associative :* $\forall (x,y,z) \in G^3$, $x*(y*z) = (x*y)*z$

2) *il existe un élément* $e \in G$*, qu'on appelle* ***élément neutre****, qui est tel que :* $forall x \in G$, $x*e = e*x = x$

3) *tout élément de G admet un* ***inverse*** *:* $\forall x \in G$, $\exists y \in G \mid x*y = y*x = e$.

Proposition 1
Dans un groupe $(G,*)$ *:*

1) *l'élément neutre est unique,*

2) *tout élément x admet un unique inverse, que l'on note* x^{-1}*,*

3) $e^{-1} = e$*,* $(x^{-1})^{-1} = x$ *pour tout élément x de G, et* $(x*y)^{-1} = y^{-1}*x^{-1}$ *pour tout couple* (x,y) *d'éléments de G.*

Exemples:

- $(\mathbb{Z},+)$
- $(\mathbb{R}^{\times},\times)$

- $(\mathbb{Z}/n\mathbb{Z}, +)$
- $(S_n, \circ)$
- $(\mathrm{GL}_n(\mathbb{R}), \times)$
- racines de l'unité.
- produit direct de deux groupes.

2 Ordre d'un élément

Définition 2
Soit G un groupe dont la loi est notée multiplicativement. On dit qu'un élément x de G est **d'ordre fini** *s'il existe un entier naturel non nul k tel que $x^k = e$. Si tel est le cas on appelle* **ordre de** *x le plus petit entier $k \in \mathbb{N}^\star$ tel que $x^k = e$.*

Proposition 2
Avec les mêmes hypothèses que précédemment, on définit, pour tout x de G, l'ensemble

$$E(x) = \left\{ k \in \mathbb{Z} \mid x^k = e \right\}.$$

Alors $E(x)$ est un sous-groupe de $\mathbb{Z}$, qui est différent de $\{0\}$ si et seulement si x est d'ordre fini, auquel cas l'ordre de x est le générateur positif de $E(x)$.

Corollaire 1
Soit x un élément d'ordre n de G. Alors on a, pour tout $m \in \mathbb{Z}$, l'équivalence

$$x^m = e \Leftrightarrow n \text{ divise } m.$$

3 Sous-groupes

3.1 Définitions

Définition 3
Soit G un groupe noté multiplicativement. Une partie non vide H de G est un sous-groupe si

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

2) $\forall x \in H$, $x^{-1} \in H$.

Remarquons en particulier qu'un sous-groupe d'un groupe G contient nécessairement l'élément neutre de G. Clairement, la loi de groupe de G, quand on la restreint à un sous-groupe H, induit une structure de groupe sur H. En pratique, on montrera souvent qu'un ensemble, muni d'une loi de composition interne est un groupe en l'identifiant à un sous-groupe d'un groupe connu.
La proposition suivante fournit une caractérisation très utile pour un sous-groupe :

Proposition 3
Soit H une partie non vide d'un groupe G noté multiplicativement. Alors H est un sous-groupe si et seulement si

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

3.2 Sous-groupe engendré par une partie

Proposition 4
L'intersection de deux sous-groupes, ou plus généralement d'une famille de sous-groupes, d'un groupe G est un sous-groupe de G.

⚠ La réunion de deux sous-groupes n'est en revanche pas un sous-groupe en général. Ce nest même essentiellement "jamais" le cas, comme le montre l'énoncé suivant (exercice)

> *"Si H et K deux sous-groupes d'un groupe G. Alors $H \cup K$ est un sous-groupe de G si et seulement si $H \subset K$ ou $K \subset H$."*

La proposition 4 permet de définir la notion de sous-groupe engendré par une partie :

Définition 4
Soit S une partie d'un groupe G. On appelle sous-groupe engendré par S, et on note $\langle S \rangle$ le plus petit sous-groupe contenant S. C'est l'intersection de tous les sous-groupes de G qui contiennent S.

La définition ci-dessus est peu exploitable en pratique. On dispose de la description plus explicite suivante :

Proposition 5
Soit G un groupe. Alors le sous-groupe engendré par une partie S de G est l'ensemble des éléments de la forme $x_1^{\varepsilon_1} x_2^{\varepsilon_2} \dots x_r^{\varepsilon_r}$ où :

- *r est un entier naturel non nul,*
- *les x_i sont des éléments de S,*
- *$\varepsilon_i = \pm 1$ pour tout i.*

3.3 Groupes monogènes

Pour alléger les notations, on note généralement $\langle x \rangle$ (au lieu de $\langle \{x\} \rangle$) le sous-groupe engendré par une partie $S = \{x\}$ réduite à un élément. Ce cas particulier important conduit à la notion de *groupe monogène*.

Définition 5
Un groupe G est dit monogène *s'il coïncide avec le sous-groupe engendré par un de ses éléments, autrement dit s'il existe $x \in G$ tel que $G = \langle x \rangle = \{x^k, k \in \mathbb{Z}\}$. Si de plus x est d'ordre fini n, on dit que G et* cyclique *d'ordre n, et on a alors $\langle x \rangle = \{e, x, x^2, \ldots, x^{n-1}\}$.*

Remarque : un groupe monogène (en particulier un groupe cyclique) est automatiquement abélien.
Remarque terminologique : le *cardinal* d'un groupe cyclique engendré par un élément x est donc égal à l'*ordre* de x. Par extension, on utilise le mot *ordre* pour désigner le *cardinal* d'un groupe quelconque, cyclique ou non. On adopte cet usage dans toute la suite.

Lemme 1
Soit $G = \{e, x, x^2, \ldots, x^{n-1}\}$ un groupe cyclique d'ordre n. Alors, pour tout $\ell \in \mathbb{Z}$, l'élément x^ℓ est d'ordre $\dfrac{n}{n \wedge \ell}$.

Preuve. Si D désigne le PGCD de ℓ et de n, on a

$$\begin{cases} n &= Dn' \\ \ell &= D\ell' \\ n' \wedge \ell' &= 1 \end{cases}.$$

On a alors les équivalences :

$$\left(x^\ell\right)^m = e \Leftrightarrow x^{\ell m} = e \Leftrightarrow n \mid \ell m \Leftrightarrow Dn' \mid D\ell' m \Leftrightarrow n' \mid \ell' m \Leftrightarrow n' \mid m \text{ (Gauss)}$$

ce qui signifie précisément que x^ℓ est d'ordre $n' = \dfrac{n}{n \wedge \ell}$. □

Théorème 1
1) *Les sous-groupes d'un groupe monogènes sont monogènes.*

2) *Si G est un groupe cyclique d'ordre n, alors tous ses sous-groupes sont cycliques et leur ordre divise n. Inversement, pour tout diviseur d de n il existe un unique sous-groupe G_d de G d'ordre d et on a*

$$G_d = \left\langle x^{\frac{n}{d}} \right\rangle = \left\{ g \in G \mid g^d = e \right\}.$$

Preuve.

1) C'est la même démonstration que pour les sous-groupes de $\mathbb{Z}$ au premier chapitre : si $G = \langle x \rangle$ est un groupe monogène engendré par un élément x et si H est un sous-groupe de G alors ses éléments sont des puissances de x. Si H est réduit à l'élément neutre e, alors il est monogène (engendré par e). Sinon, il existe un exposant k non nul tel que x^k appartienne à H, auquel cas $x^{-k} = (x^k)^{-1}$ appartient aussi à H. L'un des deux entiers k ou $-k$ est strictement positif, et il existe donc un plus petit entier naturel non nul k_0 tel que x^{k_0} appartienne à H. On vérifie alors que $H = \left\langle x^{k_0} \right\rangle$: l'inclusion $\left\langle x^{k_0} \right\rangle \subset H$ est évidente et en sens inverse, si x^k appartient à H, on effectue la division euclidienne de k par k_0 ($k = k_0 q + r$, $0 \leq r < k_0$) et on constate que $x^r = x^k \left(x^{k_0}\right)^{-q}$ appartient à H, comme produit d'éléments de H, ce qui n'est possible que si $r = 0$, en vertu de la minimalité de k_0 (r est strictement inférieur à k_0), c'est-à-dire si k_0 divise k.

2) Soit $G = \langle x \rangle$ un groupe cyclique d'ordre n, ce qui signifie en particulier que x est d'ordre n. Comme G est monogène, ses sous-groupes sont monogènes d'après la première partie du théorème, donc cycliques puisqu'ils sont finis.

Si d est un diviseur de n, c'est-à-dire si $n = qd$ pour un certain entier q, alors le sous-groupe engendré par x^q est cyclique d'ordre d. Considérons l'ensemble $G_d = \left\{ g \in G \mid g^d = e \right\}$. Clairement, cet ensemble contient tous les éléments d'ordre d de G (s'il en existe). Ainsi, un éventuel sous-groupe d'ordre d de G, qui sera nécessairement cyclique d'après la première partie du théorème, est automatiquement contenu dans G_d. De plus, pour qu'un élément $y = x^k$ de G appartienne à G_d, il faut et il suffit que $x^{kd} = e$, ce qui équivaut, par un calcul analogue au précédent, à la propriété que q divise k. Par conséquent, $G_d = \langle x^q \rangle$ qui est donc l'unique sous-groupe d'ordre d de G.

Il reste à montrer que l'ordre d'un sous-groupe de G est nécessairement un diviseur de n. Soit H un tel sous groupe. Il existe donc un entier ℓ tel que

$$H = \left\langle x^\ell \right\rangle = \left\{ x^{\ell k}, k \in \mathbb{Z} \right\}$$

et l'ordre de H est égal à l'ordre de l'élément $y = x^\ell$, qui vaut $\dfrac{n}{n \wedge \ell}$ d'après le lemme précédent. En particulier, c'est un diviseur de n.

□

4 Le Théorème de Lagrange

4.1 Rappel : relations d'équivalence

Définition 6
Une relation binaire $\mathcal{R}$ sur un ensemble E est une relation d'équivalence *si elle est*

- ***réflexive*** *:*
$$\forall x \in E \qquad x\mathcal{R}x \tag{3.1}$$
- ***symétrique*** *:*
$$\forall x, y \in E, \qquad (x\mathcal{R}y) \Rightarrow (y\mathcal{R}x) \tag{3.2}$$
- ***transitive***
$$\forall x, y, z \in E, \qquad (x\mathcal{R}y \text{ et } y\mathcal{R}z) \Rightarrow x\mathcal{R}z \tag{3.3}$$

La classe d'équivalence d'un élément x de E , notée $\mathrm{Cl}_{\mathcal{R}}(x)$, est l'ensemble des éléments de E qui sont en relation avec x.

$$\mathrm{Cl}_{\mathcal{R}}(x) = \{y \in E \mid x\mathcal{R}y\}. \tag{3.4}$$

L' ensemble quotient de E par la relation d'équivalence $\mathcal{R}$, noté $E/\mathcal{R}$, est l'ensemble des classes d'équivalence de E suivant $\mathcal{R}$:

$$E/\mathcal{R} = \{\mathrm{Cl}_{\mathcal{R}}(x) \mid x \in E\} \tag{3.5}$$

Proposition 6
L'ensemble des classes d'équivalence de E relativement à une relation d'équivalence $\mathcal{R}$ forme une partition de E, c'est-à-dire que les classes sont deux à deux disjointes *et que leur réunion est égale à E.*

4.2 Classes modulo un sous-groupe

Proposition 7 (et définition)
Soit H un sous-groupe d'un groupe G.

1) *La relation*
$$x \sim y \text{ si } x^{-1}y \in H$$
est une relation d'équivalence sur G. La classe d'équivalence d'un élément x est égale à xH ("classe ***à gauche*** *modulo H"). L'ensemble quotient est noté G/H.*

2) *De même, la relation*
$$x \sim y \text{ si } yx^{-1} \in H$$
est une relation d'équivalence sur G, qui définit des "classes ***à droite***" *Hx, dont l'ensemble est noté $H\backslash G$.*

3) *L'application $xH \mapsto Hx^{-1}$ définit une bijection de G/H sur $H\backslash G$, qui ont donc même cardinal. Quand celui-ci est fini on le note $(G : H)$ et on l'appelle* indice *de H dans G.*

Théorème 2 ("Théorème de Lagrange")
Soit G un groupe fini, et H un sous-groupe. Alors le cardinal de H divise celui de G et on a $(G : H) = \frac{|G|}{|H|}$.

Corollaire 2
Si G est un groupe fini, alors son ordre est un multiple de l'ordre de chacun de ses éléments.

Corollaire 3
Tout groupe G d'ordre p premier est cyclique.

5 Morphismes

5.1 Définitions

Définition 7
Une application φ d'un groupe G dans un groupe H est un morphisme de groupes si

$$\forall x \in G, \forall y \in G, \varphi(xy) = \varphi(x)\varphi(y).$$

Exemples:

1) morphismes de $\mathbb{Z}$ dans $\mathbb{Z}$.

2) Si G est un groupe ()quelconque) et x un élément fixé de G, l'application

$$\begin{array}{rccc} \varphi_x : & \mathbb{Z} & \longrightarrow & G \\ & k & \longmapsto & x^k. \end{array}$$

Proposition 8
Soit $\varphi : G \to H$ un morphismes de groupes. Alors

1) $\varphi(e_G) = e_H$.

2) $\forall x \in G, \varphi(x^{-1}) = \varphi(x)^{-1}$.

Proposition 9
1) *La composée de deux morphismes est un morphisme.*

2) *Si $\varphi : G \to H$ un morphismes de groupes* bijectif *alors φ^{-1} est un morphisme.*

5.2 Noyau, image

Proposition 10
Soit $\varphi : G \to H$ un morphismes de groupes. Alors

1) *l'image d'un sous-groupe est un sous-groupe.*

2) *l'image inverse d'un sous-groupe est un sous-groupe.*

Définition 8
Soit $\varphi : G \to H$ un morphisme de groupes.

- *On appelle* noyau de φ *et on note* $\ker \varphi$ *l'ensemble des antécédents par φ de l'élément neutre e_H de H*

$$\ker \varphi = \{g \in G \mid \varphi(g) = e_H\}.$$

- *On appelle* image de φ *et on, note* $\operatorname{Im} \varphi$ *l'ensemble des éléments de H admettant un antécédent par φ*

$$\operatorname{Im} \varphi = \{h \in H \mid \exists g \in G, \varphi(g) = h\}.$$

On obtient, comme corollaire immédiat de la proposition 10 :

Corollaire 4
Soit $\varphi : G \to H$ un morphisme de groupes. Le noyau de φ est un sous-groupe de G, et son image est un sous-groupe de H.

Proposition 11
Soit $\varphi : G \to H$ un morphisme de groupes. Alors φ est injectif si et seulement si $\ker \varphi = \{e_G\}$.

Proposition 12
Soit $\varphi : G \to H$ un morphismes de groupes. Alors

1) *L'ensemble* $\ker \varphi = \{x \in G \mid \varphi(x) = e_H\}$ *est un sous-groupe de G, appelé* noyau de φ.

2) *L'image* $\operatorname{Im} \varphi = \{\varphi(x), x \in G\}$ *est un sous-groupe de H.*

Proposition 13
Soit $\varphi : G \to H$ un morphismes de groupes. Alors φ est injectif si et seulement si $\ker \varphi = \{e_G\}$.

Remarque. Si x est un élément fixé dans un groupe G, le noyau du morphisme

$$\begin{array}{rccc} \varphi_x : & \mathbb{Z} & \longrightarrow & G \\ & k & \longmapsto & x^k \end{array}$$

est un sous-groupe de $\mathbb{Z}$, donc de la forme $a\mathbb{Z}$ pour un entier naturel a convenable. On a :

- $a = 0 \Leftrightarrow \varphi_x$ injectif $\Leftrightarrow x$ d'ordre infini.
- $a \neq 0 \Leftrightarrow x$ d'ordre fini égal à a.

Chapitre 4

Sous-groupes normaux, groupes quotients et théorème de factorisation

1 Sous-groupes normaux

On a vu comment définir l'ensemble des classes à gauche (resp. à droite) modulo un sous-groupe. Deux questions naturelles, et apparemment disjointes, se posent :

1) À quelle condition a-t-on coïncidence entre "classes à gauche" et "classes à droite" ?

2) À quelle condition peut-on munir l'ensemble quotient G/H (resp. $G\backslash H$) d'une structure de groupe ?

Les deux questions admettent la même réponse, qui repose sur la notion de sous-groupe normal (ou distingué).
Pour commencer, examinons la situation de $Z/n\mathbb{Z}$ que nous avons pu munir d'une addition (voir le premier chapitre). À cette occasion, il est apparu que si la définition choisie pour l'addition de $Z/n\mathbb{Z}$ avait bien un sens, c'était grâce à la propriété fondamentale suivante :

$$\left\{ \begin{array}{lcll} x' & \equiv & x & \mod n \\ y' & \equiv & y & \mod n \end{array} \right. \Rightarrow x' + y' \equiv x + y \mod n$$

Pour imiter cette démarche dans le cas général, on a envie, pour définir une loi de groupe sur G/H, de poser $xHyH := xyH$ (de sorte que $G \to G/H$ soit un morphisme). Mais a-t-on

$$\left\{ \begin{array}{lll} x' & \mathcal{R}_g & x \\ y' & \mathcal{R}_g & y \end{array} \right. \Rightarrow x'y'\mathcal{R}_g xy \, ?$$

c'est-à-dire

$$\left\{ \begin{array}{lll} x' & \in & xH \\ y' & \in & yH \end{array} \right. \Rightarrow x'y'H = xyH \, ?$$

Définition et proposition 1
On dit que H est normal *ou* distingué *dans G si l'une des 4 assertions équivalentes suivantes est satisfaite*

1) $\forall y \in G, \forall h \in H, y^{-1}hy \in H$

2) $\forall y \in G, y^{-1}Hy \subset H$

3) $\forall y \in G, y^{-1}Hy = H$

4) $\forall y \in G, Hy = yH$

Notation : $H \triangleleft G$.

Preuve. Voir le cours. □

Clairement, cette propriété apporte une réponse à la deuxième question posée en préambule de cette section : si $H \triangleleft G$, alors les classes à droite et à gauche de tout élément de G coïncident, c'est-à-dire que $\mathcal{R}_g$ et $\mathcal{R}_d$ sont égales, ainsi que les quotients G/H et $G\backslash H$.

Si l'on revient à notre question initiale, on voit que si H est distingué dans G on a bien :

- si $x' \in xH$, c'est-à-dire s'il existe $h \in H$ tel que $x' = xh$,
- si $y' \in yH$, c'est-à-dire s'il existe $k \in H$ tel que $y' = yk$,

alors :

$$x'y' = xhyk = xy(y^{-1}hy)k \in xyH.$$

On obtient donc une loi de composition interne bien définie sur G/H en posant

$$\forall x \in G,\ \forall y \in G,\ xHyH := xyH$$

Il reste à voir que la loi ainsi définie est bien une loi de groupe :

- elle possède un élément neutre, à savoir la classe de e, c'est-à-dire H, puisque $H\,(xH) = (xH)\,H = xH$ pour tout $x \in G$. En résumé, $e_{G/H} = H$
- tout élément de G/H admet un inverse : pour tout $x \in G$ on a $(xH)\left(x^{-1}H\right) = \left(x^{-1}H\right)(xH)$, autrement dit, $(xH)^{-1} = x^{-1}H$.

En résumé, la propriété pour H d'être distingué dans G est donc une condition *suffisante* pour que G/H admette un structure de groupe compatible avec la loi de groupe de G. On montre facilement que cette condition est également nécessaire. On résume tout cela dans l'énoncé suivant

Théorème 1
Si $H \triangleleft G$, il existe sur G/H une unique structure de groupe telle que la surjection π canonique soit un morphisme. Elle est définie par $xH \cdot yH = xyH$.

Exemples :

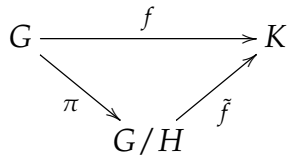
- Si G est abélien, tous ses sous-groupes sont distingués.
- Dans S_3, le sous-groupe engendré par (123) est distingué. En revanche, le sous-groupe engendré par (12) ne l'est pas.
- Tout sous-groupe d'indice 2 d'un groupe G est distingué dans G (voir TD).
- Dans le groupe diédral $D_{2n} = \langle \rho, \sigma \mid \rho^n = \sigma^2 = e\,,\ \sigma\rho\sigma = \rho^{-1} \rangle$, le sous-groupe engendré par ρ est distingué.

Proposition 1
Si $H \triangleleft G$, l'ensemble des sous-groupes de G/H est en bijection avec l'ensemble des sous-groupes de G qui contiennent H via l'application $K \mapsto \pi^{-1}(K)$.

2 Sous-groupes normaux et morphismes : le théorème de factorisation

Proposition 2
Le noyau d'un morphisme de groupe $\varphi : G \to H$ est un sous-groupe distingué dans G.

Théorème 2
Soit $f : G \longrightarrow K$ un morphisme de groupes et H un sous-groupe normal de G. On suppose $H \subset \ker f$. Alors il existe un unique morphisme de groupes $\tilde{f} : G/H \longrightarrow K$ tel que $f = \tilde{f} \circ \pi$, où π désigne la projection canonique de G sur G/H.



Remarques :

- $\operatorname{Im} \tilde{f} = \operatorname{Im} f$.
- Si $H = \ker f$, alors $\tilde{f}$ est injective.

- Les deux remarques précédentes montrent en particulier que, dans le cas où $H = \ker f$, $\tilde{f}$ est un *isomorphisme* de $G/\ker f$ sur $\operatorname{Im} f$.

$$\begin{array}{ccc} G & \xrightarrow{\quad f \quad} & K \\ {\scriptstyle\pi}\downarrow & & \uparrow{\scriptstyle i} \\ G/\ker f & \xrightarrow[\tilde{f}]{\sim} & \operatorname{Im} f \end{array}$$

Exemples :

- Le morphisme
$$\begin{array}{rccc} f: & \mathbb{R} & \longrightarrow & \mathbb{C}\setminus\{0\} \\ & x & \longmapsto & e^{2i\pi x} \end{array}$$
a pour noyau
$$\ker f = \mathbb{Z},$$
pour image
$$\operatorname{Im} f = U = \{z \in \mathbb{C} \mid |z| = 1\}$$
et induit donc un isomorphisme $\tilde{f} : \mathbb{R}/\mathbb{Z} \longrightarrow U$.

- Si x est un élément d'ordre n dans un groupe G, le morphisme
$$\begin{array}{rccc} \varphi_x: & \mathbb{Z} & \longrightarrow & G \\ & k & \longmapsto & x^k \end{array},$$
de noyau $\ker \varphi_x = n\mathbb{Z}$, induit un isomorphisme $\mathbb{Z}/n\mathbb{Z} \simeq \langle x \rangle$.

- S_n/A_n, GL_n/SL_n etc.

Application : théorème des restes chinois

Théorème 3
Soient a et b deux entiers naturels premiers entre eux. Alors le morphisme de groupes

$$\begin{array}{rccc} f & \mathbb{Z} & \longrightarrow & \mathbb{Z}/a\mathbb{Z} \times \mathbb{Z}/b\mathbb{Z} \\ & k & \longmapsto & (k \mod a, k \mod b) \end{array}$$

induit par passage au quotient un isomorphisme de $\mathbb{Z}/ab\mathbb{Z}$ sur $\mathbb{Z}/a\mathbb{Z} \times \mathbb{Z}/b\mathbb{Z}$.

Preuve. Le noyau de f est égal à $a\mathbb{Z} \cap b\mathbb{Z} = ab\mathbb{Z}$ puisque a et b sont premiers entre eux. Il induit donc, grâce au théorème de factorisation, un morphisme injectif de $\mathbb{Z}/ab\mathbb{Z}$ dans $\mathbb{Z}/a\mathbb{Z} \times \mathbb{Z}/b\mathbb{Z}$, qui est également surjectif puisque les deux groupes ont même cardinal. □

Chapitre 5

Anneaux

1 Définitions

Définition 1
Un anneau est la donnée d'un triplet $(A, +, \cdot)$ *où* A *est un ensemble et* $+$ *et* $\cdot$ *sont deux lois de composition internes telles que*

1) $(A, +)$ *est un* groupe abélien *d'élément neutre* 0.

2) *La multiplication est* associative *:* $\forall (a, b, c) \in A^3\ ,\ a \cdot (b \cdot c) = (a \cdot b) \cdot c$

3) *Elle est* distributive par rapport à l'addition*, ce qui signifie que*

$$\forall (a, b, c) \in A^3\ ,\ a \cdot (b + c) = a \cdot b + a \cdot c.$$

4) *Elle possède un* élément neutre *noté* 1 *caractérisé par la propriété*

$$\forall a \in A\ ,\ a \cdot 1 = 1 \cdot a = a.$$

De plus, l'anneau A *est dit* **commutatif** *si la multiplication est commutative.*

Proposition 1
$(A, +, \cdot)$ *un anneau.*

1) $\forall x \in A,\ 0 \cdot x = 0$.

2) *L'élément neutre pour* $\cdot$ *est unique.*

3) *Si* $A \neq \{0\}$ *alors* $0 \neq 1$.

4) $\forall x, y \in A, x \cdot (-y) = (-x) \cdot y - x \cdot y$.

Preuve.

1) $x = (1+0)x = 1x + 0x = x + 0x \Rightarrow 0x = 0$.

2) OK

3) Si $0 = 1$ alors $\forall x \in A$, $x = 1x = 0x = 0$.

4) $(-x)y + xy = (-x + x)y = 0$.

□

Une différence majeure entre $+$ et $\cdot$: tous les éléments ne sont pas inversibles pour la multiplication $\rightsquigarrow$ déf de $A^\times$.

Définition 2
Un élément a de A est dit inversible s'il existe $b \in A$ tel que $ab = ba = 1$. L'ensemble des éléments inversibles de A est noté $A^\times$ ou $U(A)$.

Remarque : certains auteurs parlent d'inverse à droite et à gauche (un élément peut avoir un inverse à droite mais pas à gauche...).
exercice : montrer que si $A \in A$ admet un inverse à droite et un inverse à gauche alors ils sont uniques et sont égaux (mieux : si $a \in A$ admet un unique inverse à droite, alors il admet un inverse à gauche...).

Proposition 2
$(A^\times)$ est un groupe de neutre 1.

Définition 3
1) *Un anneau* intègre *est un anneau commutatif dans lequel on a la propriété :*

$$\forall (a, b) \in A^2, ab = 0 \Rightarrow a = 0 \text{ ou } b = 0.$$

2) *Un anneau commutatif est un* corps *si tout élément non nul est inversible pour la multiplication.*

Remarque. Un corps est intègre, mais la réciproque n'est pas toujours vraie.

Proposition 3
$\mathbb{Z}/n\mathbb{Z}$ intègre $\Leftrightarrow$ $\mathbb{Z}/n\mathbb{Z}$ corps $\Leftrightarrow$ n premier.

Définition 4
1) *Un sous-anneau d'un anneau A est une partie B non vide de A telle que*

(a) *$(B, +)$ est un sous-groupe de $(A, +)$,*

(b) *B est stable pour la multiplication,*

(c) *1_A appartient à B.*

2) *Si A et B sont deux anneaux, leur produit cartésien $A \times B$ est canoniquement muni d'une structure d'anneau en posant :*

- $(x, y) + (x', y') = (x + x', y + y')$,
- $(x, y) \cdot (x', y') = (xx', yy')$

les éléments neutres pour l'addition et la multiplication étant définis respectivement par $0_{A\times B} = (0_A, 0_B)$ et $1_{A\times B} = (1_A, 1_B)$.

2 $\left(\mathbb{Z}/n\mathbb{Z}\right)^\times$

Proposition 4
Soit n un entier naturel non nul. Alors, pour tout entier relatif k, les propriétés suivantes sont équivalentes :

1) *la classe de k modulo n est inversible pour la multiplication.*

2) *la classe de k modulo n est un générateur du groupe additif $(\mathbb{Z}/n\mathbb{Z}, +)$.*

3) *k est premier à n.*

Preuve. Notons $\overline{k}$ la classe d'un entier k modulo n. Si ℓ est un entier relatif, on pose

$$\ell \cdot \overline{k} = \begin{cases} \underbrace{\overline{k} + \overline{k} + \cdots + \overline{k}}_{\ell \text{ fois}} \text{ si } \ell \in \mathbb{N} \\ \\ -\left((-\ell) \cdot \overline{k}\right) \text{ sinon} \end{cases}$$

Avec cette convention, il est clair que $\ell \cdot \overline{k} = \overline{\ell k} = \overline{\ell}\,\overline{k}$ pour tous ℓ et k dans $\mathbb{Z}$.

(1)) $\Leftrightarrow$ (2)) : $\overline{k}$ est inversible dans $\mathbb{Z}/n\mathbb{Z} \Leftrightarrow \exists \overline{\ell} \in \mathbb{Z}/n\mathbb{Z} \mid \overline{\ell}\,\overline{k} = \overline{1}$
$\Leftrightarrow \exists \ell \in \mathbb{Z} \mid \ell \cdot \overline{k} = \overline{1}$
$\Leftrightarrow \overline{1} \in \left\langle \overline{k} \right\rangle$
$\Leftrightarrow \overline{k}$ engendre $(\mathbb{Z}/n\mathbb{Z}, +)$

(1)) $\Leftrightarrow$ (3)) : $\overline{k}$ inversible dans $\mathbb{Z}/n\mathbb{Z} \Leftrightarrow \exists \overline{\ell} \in \mathbb{Z}/n\mathbb{Z} \mid \overline{\ell}\,\overline{k} = \overline{1}$
$\Leftrightarrow \exists \ell \in \mathbb{Z} \mid \ell k \equiv 1 \mod n$
$\Leftrightarrow \exists \ell \in \mathbb{Z}, \exists q \in \mathbb{Z} \mid \ell k + qn = 1$
$\underset{\text{(Bézout)}}{\Leftrightarrow} k \wedge n = 1$

Définition 5
La fonction indicatrice d'Euler φ est définie sur $n \in \mathbb{N} \setminus \{0\}$ par

$$\varphi(n) = \begin{cases} 1 \text{ si } n = 1 \\ |\,(\mathbb{Z}/n\mathbb{Z})^\times\,| \text{ sinon.} \end{cases}$$

Grâce à la caractérisation des inversibles de $\mathbb{Z}/n\mathbb{Z}$, jointe au fait que toute classe modulo n admet un unique représentant $k \in \{1, \ldots, n\}$, on voit que $\varphi(n)$ peut aussi être défini, pour $n > 1$, par

$$\varphi(n) = \text{Card } \{k \in \{1, \ldots, n\} \mid k \wedge n = 1\}\,. \tag{5.1}$$

Proposition 5
1) *Si p est un nombre premier et k un entier naturel non nul, on a*

$$\varphi(p^k) = p^{k-1}(p-1).$$

2) *Si a et b sont deux entiers premiers entre eux $\varphi(ab) = \varphi(a)\varphi(b)$.*

3) *Si n est un entier naturel non nul et si P_n désigne l'ensemble des nombres premiers qui le divisent, on a*

$$\varphi(n) = n \prod_{p \in P_n} (1 - \frac{1}{p}).$$

Preuve.

1) On va utiliser (5.1) pour calculer $\varphi(p^k)$ comme *nombre des entiers premiers à p^k compris entre 1 et p^k*. Un entier est premier à p^k si et seulement si il n'est pas divisible par p. Or, entre 1 et p^k, il y a exactement p^{k-1} multiples de p, à savoir $p, 2p, \ldots, p^{k-1}p = p^k$, donc $p^k - p^{k-1} = p^{k-1}(p-1)$ *non multiples* de p, d'où la conclusion.

2) Voir paragraphe suivant.

3) Application immédiate des deux points précédents.

□

Pour finir, on va établir une formule qui d'une part permet en principe de calculer $\varphi(n)$ récursivement, et jouera d'autre part un rôle important dans la démonstration de la cyclicité de $(\mathbb{Z}/p\mathbb{Z})^\times$ pour p premier (voir la dernière section du chapitre).

Proposition 6
Pour tout entier naturel non nul, on a

$$n = \sum_{d|n} \varphi(d).$$

Preuve. Pour tout entier naturel non nul, on définit

$$E_n = \left\{ \frac{1}{n}, \frac{2}{n}, \ldots, \frac{n}{n} \right\} \supset U_n = \{ \text{ fractions irréductibles dans } E_n \} .$$

On vérifie aisément que

- $E_n = \bigcup_{d|n} U_d$, réunion *disjointe*.
- $|U_n| = \varphi(n)$.

La formule annoncée s'en déduit immédiatement, sachant que $|E_n| = n$. □

3 Morphismes

Définition 6
Soient A et B deux anneaux. Une application f $A \to B$ est un morphisme d'anneaux si

1) *c'est un morphismes de groupes additifs de $(A, +)$ dans $(B, +)$*

2) $\forall (x, y) \in A^2$, $f(xy) = f(x)f(y)$

3) $f(1_A) = 1_B$.

Exemples.

1) $\mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$

2) conjugaison complexe

3) morphisme d'évaluation de $\mathbb{K}[X]$ dans $\mathbb{K}$

4) $A \mapsto P^{-1}AP$ de $M_n(\mathbb{K})$ dans lui-même

Comme pour les morphismes de groupes, un morphisme d'anneaux bijectif s'appelle un *isomorphisme d'anneaux*.
On montre facilement (exercice), que l'isomorphisme de groupes

$$\mathbb{Z}/ab\mathbb{Z} \simeq \mathbb{Z}/a\mathbb{Z} \times \mathbb{Z}/b\mathbb{Z}$$

établi au chapitre précédent (Théorème 3) **pour** a **et** b **premiers entre eux** est en fait un isomorphisme *d'anneaux*. Ceci permet d'établir très facilement la multiplicativité de la fonction indicatrice d'Euler annoncée au paragraphe précédent, modulo le lemme suivant :

Lemme 1
1) *Si $f : A :\longrightarrow B$ est un isomorphisme d'anneaux, alors $B^\times = f(A^\times)$.*

2) *Si A et B sont deux anneaux, alors $(A \times B)^\times = A^\times \times B^\times$.*

Preuve. Exercice □
Appliqué à l'isomorphisme $\mathbb{Z}/ab\mathbb{Z} \simeq \mathbb{Z}/a\mathbb{Z} \times \mathbb{Z}/b\mathbb{Z}$ **(pour a et b premiers entre eux)**, ce lemme entraîne que

$$(\mathbb{Z}/ab\mathbb{Z})^\times \simeq (\mathbb{Z}/a\mathbb{Z})^\times \times (\mathbb{Z}/b\mathbb{Z})^\times \text{ si } a \wedge b = 1.$$

On en déduit immédiatement, en comparant les cardinaux, la formule

$$\varphi(ab) = \varphi(a)\varphi(b) \text{ si } a \wedge b = 1.$$

4 Corps finis

Dans ce paragraphe, et conformément à la tradition anglo-saxonne, "corps" signifie "corps commutatif" (il existe néanmoins des corps "non commutatifs", par exemple le corps des quaternions, dont on ne parlera pas ici).
On a vu précédemment que, si p est premier, l'anneau $\mathbb{Z}/p\mathbb{Z}$ est un corps, que l'on note traditionnellement $\mathbb{F}_p$. L'étude systématique des corps finis dépasse le cadre de ce cours. Signalons simplement, sans aucune démonstration, que le cardinal d'un corps fini est nécessairement une puissance d'un nombre premier, et que réciproquement, pour tout entier $q = p^k$ (p premier, k entier ≥ 1), il existe, à isomorphisme près, un unique corps de cardinal q, noté $\mathbb{F}_q$.
On va démontrer pour finir un résultat très important, que l'on a déjà rencontré dans le cas du corps des nombres complexes (voir DS) :

Théorème 1
*Soit K un corps et G un sous-groupe **fini** du groupe multiplicatif $K^\times$. Alors G est cyclique. En particulier, pour tout nombre premier p, le groupe $(\mathbb{Z}/p\mathbb{Z})^\times$ est cyclique d'ordre $p-1$.*

Preuve. Voir cours □