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

Structures Algébriques 1 :
Résumé de cours

Table des matières

1 Théorie des groupes **5**
- 1 Définition et premiers exemples . . . 5
- 2 Sous-groupes . . . 6
  - 2.1 Définitions . . . 6
  - 2.2 Exemple : les sous groupes de $\mathbb{Z}$ . . . 6
- 3 Ordre d'un élément . . . 8
- 4 Sous-groupe engendré par une partie . . . 9
- 5 Le Théorème de Lagrange . . . 11
  - 5.1 Rappel : relations d'équivalence . . . 11
  - 5.2 Classes modulo un sous-groupe . . . 11

2 Le groupe des permutations **13**
- 1 Définitions et premières propriétés . . . 13
- 2 Cycles . . . 15
- 3 Décomposition en cycles disjoints . . . 16
- 4 Signature . . . 18

3 Morphismes, sous-groupes normaux, groupes quotients et théorème de factorisation **21**
- 1 Morphismes . . . 21
  - 1.1 Définitions . . . 21
  - 1.2 Noyau, image . . . 22
- 2 Sous-groupes normaux . . . 23
- 3 Sous-groupes normaux et morphismes : le théorème de factorisation . 25

4 Actions de groupes **27**
- 1 Définitions . . . 27
- 2 Exemples . . . 28
- 3 Équation des classes . . . 28
- 4 Une application : le théorème de Cauchy . . . 28

5 Anneaux **31**
- 1 Définitions . . . 31
- 2 L'anneau $(\mathbb{Z}/n\mathbb{Z})$ . . . 33

3 Morphismes 35
4 Corps finis (non traité en cours) 36

6 Idéaux **39**
1 Idéaux 39
2 Anneaux principaux 40
2.1 Définitions 40
2.2 Exemple : les anneaux euclidiens 40
3 Arithmétique 41
3.1 PGCD, PPCM, Bézout, Gauss 41
3.2 Décomposition en produit d'irréductibles 43

7 Polynômes et fractions rationnelles **45**
1 Définitions et premières propriétés 45
2 Division euclidienne 47
3 Racines et multiplicités 48
4 Polynômes irréductibles 50
5 Dérivées successives, formule de Taylor et applications (non traité en cours) 50
6 Fractions rationnelles 52
6.1 Corps des fractions d'un anneau intègre 52
6.2 Le corps des fractions rationnelles $K(X)$ 53

Chapitre 1

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 Sous-groupes

2.1 Définitions

Définition 2
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 2
Soit H une partie non vide d'un groupe G noté multiplicativement. Alors H est un sous-groupe si et seulement si

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

2.2 Exemple : les sous groupes de $\mathbb{Z}$

Théorème et définition 1.1 (division euclidienne)
Pour tout couple d'entiers relatifs (a, b) avec $b \neq 0$, il existe un unique couple (q, r) d'entiers relatifs tels que

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

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

Preuve.

- Existence : il y a deux cas à considérer, selon le signe de a.
  - si $a \geq 0$, on pose $q_0 = \max\{k \in \mathbb{N} \text{ tels que } k|b| \leq a\}$, $r = a - |b|q_0$ et $q = q_0$ ou $-q_0$ selon que b est positif ou négatif.
  - si $a < 0$, on pose $q_1 = \min\{k \in \mathbb{N} \text{ tels que } k|b| \geq -a\}$, $r = a + |b|q_1$ et $q = q_1$ ou $-q_1$ selon que b est négatif ou positif.
- Unicité : facile.

□

Définition 3

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 :*

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

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 3

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 1

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 : on peut donc définir le PGCD (resp. le PPCM) de deux entiers a et b comme le générateur positif du sous-groupe $a\mathbb{Z} + b\mathbb{Z}$ (resp. $a\mathbb{Z} \cap b\mathbb{Z}$). Si l'on adopte ce point de vue il n'y a plus lieu de conserver la restriction à *"a et b non tous les deux nuls"* dans la définition du PGCD et du PPCM, et on peut donc éventuellement poser $\text{PGCD}(0, 0) = \text{PPCM}(0, 0) = 0$.

3 Ordre d'un élément

Définition 4
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 4
Soit x un élément d'ordre n d'un groupe G dont la loi est notée multiplicativement. Alors on a, pour tout $m \in \mathbb{Z}$*, l'équivalence*

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

Preuve. On définit, pour tout x de G, l'ensemble

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

C' 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 $E(x)$. La proposition en découle. □

Remarque : si x est d'ordre n, les éléments $x^0 = e, x, x^2, \ldots, x^{n-1}$ sont deux à deux distincts. En particulier, l'ordre d'un élement d'un groupe G fini est majoré par le cardinal du groupe. On verra plus loin (théorème de Lagrange) qu'on a en fait une majoration beaucoup plus forte.

4 Sous-groupe engendré par une partie

Proposition 5
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 n'est 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 5 permet de définir la notion de sous-groupe engendré par une partie :

Définition 5
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 6
Soit G un groupe. Alors le sous-groupe engendré par une partie S de G est l'ensemble des éléments de la forme $x_1^{\varepsilon_1} x_2^{\varepsilon_2} \ldots x_r^{\varepsilon_r}$ où :

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

Si $S = \{x\}$ est une partie réduite à un élément d'un groupe G, on note $\langle x \rangle$ le sous-groupe engendré par S. Ce cas particulier important conduit à la notion de *groupe monogène*.

Définition 6
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.

Théorème 2
Les sous-groupes d'un groupe monogènes sont monogènes. En particulier, les sous-groupes d'un groupe cyclique sont cycliques.

Preuve. Si $G = \langle x \rangle$ est un groupe monogène engendré par un élément x et si H est un sous-groupe de G, alors l'ensemble $E = \{k \in \mathbb{Z}, x^k \in G\}$ est un sous-groupe de $\mathbb{Z}$, donc de la forme $a\mathbb{Z}$ pour un entier a convenable. Il s'ensuit que $H = \langle x^a \rangle$.
□

Exercice : 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 $\dfrac{n}{n \wedge \ell}$.

Dans le cas cyclique, le théorème de Lagrange (paragraphe suivant) montre en outre que les sous-groupes d'un groupe cyclique d'ordre n sont cycliques d'ordre un diviseur de n. Inversement, on a la proposition

Proposition 7
Si G est un groupe cyclique d'ordre n, alors 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. Voir TD □

5 Le Théorème de Lagrange

5.1 Rappel : relations d'équivalence

Définition 7
Une relation binaire $\mathcal{R}$ sur un ensemble E est une relation d'équivalence *si elle est*

- ***réflexive*** *:*
$$\forall x \in E \qquad x\mathcal{R}x \tag{1.2}$$
- ***symétrique*** *:*
$$\forall x, y \in E, \qquad (x\mathcal{R}y) \Rightarrow (y\mathcal{R}x) \tag{1.3}$$
- ***transitive***
$$\forall x, y, z \in E, \qquad (x\mathcal{R}y \text{ et } y\mathcal{R}z) \Rightarrow x\mathcal{R}z \tag{1.4}$$

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.*

$$\mathrm{Cl}_{\mathcal{R}}(x) = \{y \in E \mid x\mathcal{R}y\}. \tag{1.5}$$

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 $\mathcal{R}$:

$$E/\mathcal{R} = \{\mathrm{Cl}_{\mathcal{R}}(x) \mid x \in E\} \tag{1.6}$$

Proposition 8
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.*

5.2 Classes modulo un sous-groupe

Proposition 9 (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) *Toutes les classes (à droite ou à gauche) sont en bijection avec H.*

4) *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 3 ("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 $(G : H) = \dfrac{|G|}{|H|}$.

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.

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*

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

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

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

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 $\sigma\gamma(x) = \gamma\sigma(x) = x$.

□

2 Cycles

Définition 3
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 2
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 3
L'ordre d'un k-cycle est égal à k.

Proposition 4
Dans S_n, tous les cycles de même longueur sont conjugués. Plus précisément, pour un élément σ de S_n , les propriétés suivantes sont équivalentes :

(i) *σ est un cycle de longueur k.*

(ii) *Il existe $\gamma \in S_n$ tel que $\sigma = \gamma(1\ 2\ \ldots\ k)\gamma^{-1}$.*

3 Décomposition en cycles disjoints

Définition 4 (orbite)
Soit $x \in \{1, \ldots, n\}$ 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 5
Soit σ un élément de S_n. Alors, pour tout $x \in \{1, \ldots, n\}$, il existe un plus petit entier naturel non nul k tel que $\sigma^k(x) = x$. On a alors

$$k = |\,\mathrm{Orb}_\sigma(x)| \ \textit{ et } \ \mathrm{Orb}_\sigma(x) = \left\{x, \sigma(x), \ldots, \sigma^{k-1}(x)\right\}.$$

Qui plus est, l'entier k divise l'ordre de σ.

Remarque : dans la définition de l'orbite, on peut remplacer $\mathbb{N}$ par $\mathbb{Z}$. En effet, si σ est un élément de S_n d'ordre k_0, alors $\sigma^{-1} = \sigma^{k_0-1}$ et

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

Proposition 6
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 $x_1, x_2, \ldots, x_r$ dans $\{1, \ldots, n\}$ tels que $\{1, \ldots, n\}$ soit la réunion disjointe *des orbites $\mathrm{Orb}_\sigma(x_1), \ldots, \mathrm{Orb}_\sigma(x_r)$:*

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

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* $c_1, \ldots, c_s$ *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 $k_1, k_2, \ldots, k_s$ 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 *non ponctuelles* 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

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

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

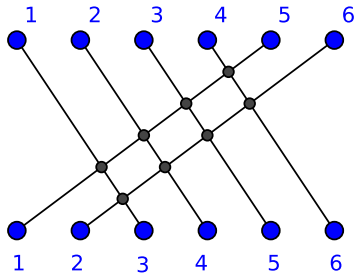
4 Signature

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 7
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 8

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) Grâce à la multiplicativité et à la proposition 4(ii), il suffit de le vérifier pour le cycle $(1\ 2\ \ldots\ k)$, pour lequel le résultat est immédiat.

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 2 et 7, on constate que la signature d'une permutation σ vaut $+1$ ou -1 selon que σ se décompose en un produit d'un nombre *pair* ou *impair* de transpositions. En particulier, bien qu'une telle décomposition en produit de transpositions ne soit pas unique, la parité du nombre de facteurs ne varie pas d'une décomposition à l'autre.

Chapitre 3

Morphismes, sous-groupes normaux, groupes quotients et théorème de factorisation

1 Morphismes

1.1 Définitions

Définition 1
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

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

3) Le logarithme définit un morphisme de $(]0, +\infty[, \times)$ dans $(\mathbb{R}, +)$.

Proposition 1
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 2
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.*

1.2 Noyau, image

Proposition 3
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 2
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* $\mathrm{Im}\, \varphi$ *l'ensemble des éléments de H admettant un antécédent par φ*

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

On obtient, comme corollaire immédiat de la proposition 3 :

Corollaire 1
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 4
Soit $\varphi : G \to H$ un morphisme de groupes. Alors φ est injectif si et seulement si $\ker \varphi = \{e_G\}$.

Exemple. Le noyau du morphisme

$$\begin{array}{rccc} \varphi : & \mathbb{Z}/6\mathbb{Z} & \longrightarrow & \mathbb{Z}/6\mathbb{Z} \\ & \overline{k} & \longmapsto & \overline{3k} \end{array}$$

est le sous-groupe $< \overline{2} >= \{\overline{0}, \overline{2}, \overline{4}\}$.

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.

2 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 :

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

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

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

c'est-à-dire

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

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.

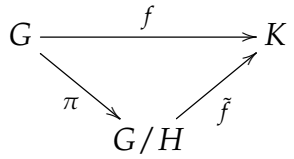
- Dans S_3, le sous-groupe engendré par (123) est distingué. En revanche, le sous-groupe engendré par (12) ne l'est pas.
- Tout sous-groupe d'indice 2 d'un groupe G est distingué dans G (voir TD).
- Dans le groupe diédral $D_{2n} = \langle \rho, \sigma \mid \rho^n = \sigma^2 = e\,,\ \sigma\rho\sigma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

Proposition 5
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 $K \mapsto \pi^{-1}(K)$.

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

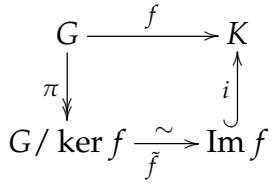
Proposition 6
Le noyau d'un morphisme de groupe $\varphi : G \to H$ est un sous-groupe distingué dans G.

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 $\operatorname{Im} f$.



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
$$\mathrm{Im}\, f = U = \{z \in \mathbb{C} \mid |z| = 1\}$$
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 $\mathbb{Z}/n\mathbb{Z} \simeq \langle x \rangle$.

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 4

Actions de groupes

1 Définitions

Définition 1
On dit qu'un groupe G agit (à gauche) sur un ensemble X si on s'est donné une application

$$\begin{array}{ccc} G \times X & \to & X \\ (g, x) & \mapsto & g \cdot x \end{array}$$

qui vérifie :

1) $e \cdot x = x$ *pour tout* $x \in X$

2) $g \cdot (h \cdot x) = (gh) \cdot x$ *pour tout* $x \in X$ *et tout couple* $(g, h) \in G \times G$.

Proposition 1
Étant donné une action d'un groupe G sur un ensemble X, la relation

$$x \sim y \text{ si il existe } g \in G \text{ tel que } y = g \cdot x$$

est une relation d'équivalence.

La classe d'équivalence d'un élément x de X modulo cette relation est notée $G \cdot x$ et s'appelle l'*orbite* de x

$$G \cdot x = \{g \cdot x, g \in G\}.$$

Le *stabilisateur* de x, noté G_x est l'ensemble

$$G_x = \{g \in G \mid g \cdot x = x\}.$$

c'est un sous-groupe de G.

Proposition 2
Pour tout $x \in X$, l'application

$$\begin{array}{ccc} G & \to & G.x \\ g & \mapsto & g \cdot x \end{array}$$

induit une bijection de G/G_x sur $G \cdot x$.

2 Exemples

1) Opération de S_n sur $\{1, 2, \ldots, n\}$.

2) L'action de $\mathrm{GL}_2(\mathbb{R})$ sur $\mathbb{R}^2$.

3) Action de $\mathbb{Z}/3\mathbb{Z}$ sur les sommets d'un triangle.

3 Équation des classes

Dans cette section, on s'intéresse aux opérations d'un groupe G sur un ensemble fini X.

Proposition 3
Soit G un groupe agissant sur un ensemble fini X et $\{x_1, x_2, \ldots, x_k\}$ un ensemble (fini) de représentants des orbites pour cette action. Alors

1) *Pour tout $x \in X$, le stabilisateur G_x de x est d'indice fini dans G.*

2) $X = \bigsqcup_{i=1}^{k} G \cdot x_i$ *(réunion disjointe).*

3) $|X| = \sum_{i=1}^{k} |G \cdot x_i| = \sum_{i=1}^{k} (G : G_{x_i})$.

4 Une application : le théorème de Cauchy

Théorème 1
Soit G un groupe fini, et p un diviseur premier de son cardinal. Alors G contient un élément d'ordre p.

Preuve. Posons $n = |G|$. Soit $E = \left\{(x_1, x_2, \ldots, x_p) \in G^p \mid x_1 x_2 \cdots x_p = e\right\}$. c'est un ensemble fini, de cardinal n^{p-1}. Considérons, dans S_p, le sous-groupe H engendré par le p-cycle $\gamma = (1\ 2\ \cdots\ p)$. Le groupe H opère sur E par la formule

$$\sigma \cdot (x_1, x_2, \ldots, x_p) = (x_{\sigma(1)}, x_{\sigma(2)}, \ldots, x_{\sigma(p)}).$$

Clairement, l'ensemble des points fixes est constitué des p-uplets $(x, x, \cdots, x)$ où x est un élément de G tel que $x^p = e$, ce qui se produit exactement si $x = e$ ou si x est un élément d'ordre p. Supposons, par l'absurde, que G ne contienne pas d'élément d'ordre p. Il y a alors un seul point fixe, à savoir le p-uplet $(e, e, \cdots, e)$. En notant E^H l'ensemble des points fixes et $H \cdot u_1$, $H \cdot u_2$, …, $H \cdot u_t$ les orbites non ponctuelles, on a, en appliquant l'équation des classes

$$|E| = |E^H| + \sum_{i=1}^{t} |H \cdot u_i. \tag{4.1}$$

On remarque alors que le cardinal de chacune des orbites non ponctuelles est égal à p. En effet, $H \cdot u_i$ est en bijection avec H/H_{u_i}, et H_{u_i} est un sous-groupe de H, il est donc d'ordre 1 ou p (théorème de Lagrange, sachant que $|h| = p$ premier). Si l'orbite n'est pas réduite à un point, c'est donc que $|H_{u_i}| = 1$ et que $|H \cdot u_i| = p$. La formule (4.1) entraîne que

$$n^{p-1} = |E| \equiv |E^H| \mod p. \tag{4.2}$$

Par conséquent, puisque p divise n, donc n^{p-1}, le cardinal de E^H doit lui aussi être divisible par p. En particulier, il ne peut pas être égal à 1. □

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.*

Exemples : $\mathbb{Z}$, $\mathbb{Z}/n\mathbb{Z}$, $\mathcal{M}_n(K)$, $K[X]$.

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 L'anneau $(\mathbb{Z}/n\mathbb{Z})$

Proposition 4 (Caractérisation des inversibles)
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. On note $\overline{k}$ la classe modulo n d'un entier k. On a, pour tout $\ell \in \mathbb{Z}$:

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

Il est clair que, pour tous ℓ et k dans $\mathbb{Z}$ on a : $\ell.\overline{k} = \overline{\ell k} = \overline{\ell}\overline{k}$.

1) $\Leftrightarrow$ 2)

$$\begin{aligned} \overline{k} \text{ inversible dans } \mathbb{Z}/n\mathbb{Z} &\Leftrightarrow \exists \overline{\ell} \in \mathbb{Z}/n\mathbb{Z} \mid \ell\,\overline{k} = \overline{1} \\ &\Leftrightarrow \overline{1} \in \left\langle \overline{k} \right\rangle \\ &\Leftrightarrow \overline{k} \text{ engendre } (\mathbb{Z}/n\mathbb{Z}, +) \end{aligned}$$

1) $\Leftrightarrow$ 3)

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

□

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 3, 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 `(non traité en cours)`

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 $\mathbb{F}_q$.

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. Posons $n = |G|$. Pour tout diviseur d de n, on considère l'ensemble G_d des éléments d'ordre d de G et l'ensemble K_d des racines du polynôme $X^d - 1$ dans K. Clairement, $G_d \subset K_d$, et $|K_d| \leq d$, *puisque K est un corps commutatif*. Par ailleurs, si G_d est non vide, et si a est un élément de G_d, le sous-groupe $\langle a \rangle$ qu'il engendre est contenu dans K_d, donc il lui est égal puisque $|\langle a \rangle| = d$ et $|K_d| \leq d$. En particulier, G_d est l'ensemble des éléments d'ordre d dans $\langle a \rangle$ est possède donc $\varphi(d)$ éléments. En résumé, $|G_d| = 0$ ou $\varphi(d)$, selon que G_d est vide ou non, et on a donc

$$n = |G| = \sum_{d|n} |G_d| \leq \sum_{d|n} \varphi(d) = n,$$

d'où l'on déduit qu'aucun des G_d n'est vide. En particulier, G possède un élément d'ordre n et est donc cyclique. □

Chapitre 6

Idéaux

1 Idéaux

Définition 1
Une partie I d'un anneau A est un idéal à gauche (resp. à droite) si

1) *$(I, +)$ est un sous-groupe de $(A, +)$.*

2) *Pour tout $a \in A$, pour tout $x \in I$, on a $ax \in I$ (resp. $xa \in I$.)*

On dit que I est un idéal bilatère s'il est à la fois un idéal à gauche et à droite.

exemples :

- A, $\{0\}$.
- idéal engendré par un élément : Aa (idéal à gauche), aA (idéal à droite).
- idéaux de Z.
- exemples d'idéaux de $\mathcal{M}_n(K)$.

Proposition 1

1) *La somme $I + J := \{x+, x \in I, y \in J\}$ et l'intersection $I \cap J$ de deux idéaux à gauche (resp. à droite), I et J est un idéal à gauche (resp. à droite).*

2) *La réunion $I \cup J$ de deux idéaux à gauche (resp. à droite) I et J est un idéal à gauche (resp. à droite)* ***si et seulement si*** *$I \subset J$ ou $J \subset I$.*

Preuve. Exercice (voir énoncé analogue pour les sous-groupes). □

2 Anneaux principaux

2.1 Définitions

Définition 2
Soit A un anneau intègre (donc commutatif).

1) *un idéal I de A est dit* principal *s'il existe $a \in A$ tel que $I = aA$.*

2) *On dit que A est un anneau principal si tous ses idéaux sont principaux.*

Exemple : $\mathbb{Z}$

Remarque (notation) : dans un anneau commutatif l'idéal *à gauche* Aa engendré par un élément a coïncide avec l'idéal *à droite* aA engendré par ce même élément. Dans ce cas, il est courant de noter (a) cet idéal :

$$(a) = aA = Aa.$$

2.2 Exemple : les anneaux euclidiens

Définition 3
Un anneau intègre (donc commutatif) A est dit euclidien s'il existe une application $\nu : A \setminus \{0\} \to \mathbb{N}$ telle que pour tout couple (a, b) d'éléments de A avec $b \neq 0$, il existe un couple (q, r) d'éléments de A tels que $a = bq + r$ avec

$$\begin{cases} r = 0 \\ \text{ou} \\ \nu(r) < \nu(b). \end{cases}$$

L'application ν s'appelle un stathme euclidien.

Remarque : ni la commutativité, ni l'intégrité ne sont réellement essentielles, et on peut sans problème définir une notion d'euclidianité à gauche, resp. à droite.

Théorème 1
Un anneau euclidien est principal.

Preuve. La démonstration est, formellement, identique à celle que l'on a donnée pour la description des sous-groupes de $\mathbb{Z}$ dans un chapitre précédent. Soit I un idéal de A. Si $I = \{0\}$ alors il est principal, engendré par 0. Sinon, il existe au moins un élément non nul dans I. Considérons alors l'ensemble (non vide)

$$E = \{\nu(x)\ ,\ x \in I \setminus \{0\}\} \subset \mathbb{N}$$

et posons

$$n_0 = \min E,$$

ce qui a bien un sens car E, comme toute partie non vide de $\mathbb{N}$, admet un minimum. Soit alors x_0 un élément de $I \setminus \{0\}$ tel que $\nu(x_0) = n_0$. Clairement, l'idéal (x_0) qu'il engendre est contenu dans I (stabilité de I par multiplication par A). Il reste donc à montrer, à l'inverse, que $I \subset (x_0)$. Pour cela, considérons un élément x quelconque de I, et effectuons sa "division euclidienne" par x_0, au sens de la définition 3 : il existe un couple (q, r) d'éléments de A tels que $x = x_0 q + r$ avec

$$r = 0 \text{ ou } \nu(r) < \nu(x_0).$$

Si $r = 0$, on a alors $x = x_0 q \in (x_0)$ et l'on peut conclure. Sinon, on a

$$0 \neq r = x - x_0 q \in I$$

et

$$\nu(r) < \nu(x_0) = n_0,$$

ce qui signifie que $\nu(r)$ est un élément de E strictement plus petit que $n_0 = \min E$, une contradiction. □

3 Arithmétique

3.1 PGCD, PPCM, Bézout, Gauss

Dans toute cette section A désigne un anneau intègre (donc commutatif). Si a et b sont deux éléments de A, on dit que a divise b, et on écrit $a|b$ s'il existe $c \in A$ tel que $b = ac$. La proposition suivante est immédiate, mais d'usage constant :

Proposition 2
Pour a et b deux éléments de A on a :

1) $a|b \Leftrightarrow (a) \supset (b)$.

2) $(a) = (b) \Leftrightarrow$ *il existe* $u \in A^\times$ *tel que* $b = au$.

Deux éléments vérifiant les conditions équivalentes de 2) sont dits *associés*.

Définition 4
Soient a et b deux éléments d'un anneau A principal (donc intègre, donc commutatif...)

1) *On appelle PGCD de a et b tout élément d de A tel que* $(d) = (a) + (b)$.

2) *On appelle PPCM de a et b tout élément m de A tel que* $(m) = (a) \cap (b)$.

On dit que a et b sont premiers entre eux *s'ils admettent* 1 *pour PGCD.*

Remarques.

1) Deux PGCDs (resp. PPCMs) d'un même couple d'éléments sont associés (c'est-à-dire se déduisent l'un de l'autre par multiplication par un inversible de A).

2) On peut définir plus généralement un PGCD (resp. un PPCM) d'une famille d'éléments $(a_1, \ldots, a_n)$ comme étant un générateur de l'idéal $(a_1) + \cdots + (a_n)$ (resp. $(a_1) \cap \cdots \cap (a_n)$)

3) La relation "être associés" est une relation d'équivalence sur $A^* := A \setminus \{0\}$, qu'on note $\sim$ dans la suite :

$$x \sim y \Leftrightarrow \exists u \in A^\times, y = xu.$$

Sur le quotient $\overline{A} := A^*/\sim$, la relation de divisibilité est alors une relation d'ordre (ce ne serait pas le cas sur $A \setminus \{0\}$, où l'on n'a pas, en général, l'antisymétrie).

Proposition 3
(Bézout, Gauss) Soient a, b et c des éléments d'un anneau principal A.

1) *(Bézout) a et b de A sont premiers entre eux si et seulement s'il existe u et v éléments de A tels que* $au + bv = 1$.

2) *(Gauss 1) Si a et b sont premiers entre eux et si a divise bc, alors a divise c.*

3) *(Gauss 2) Si a et b sont premiers entre eux et divisent tous les deux c, alors ab divise c*

Preuve. Exercice. □

Proposition 4
Si a et b sont deux éléments d'un anneau principal A, et si d et m désignent respectivement un PGCD et un PPCM de a et b, alors :

1) *Pour tout* $x \in A$, *on a : x divise a et b* $\Leftrightarrow$ *x divise d.*

2) *Pour tout* $y \in A$, *on a : a et b divisent y* $\Leftrightarrow$ *m divise y.*

3) $(ab) = (dm)$.

Preuve. 3) On écrit $a = da'$ e$b = db'$ et $(a') + (b') = A$. On a alors $da'b' = ab' = a'b$, donc $da'b'$ est un multiple commun de a et de b donc de m, ou autrement dit

$$(m) \supset (da'b').$$

Inversement, en écrivant

$$\begin{aligned} m &= xa = xda' \\ &= yb = ydb' \end{aligned}$$

on obtient que $xa' = yb'$, d'où l'on conclut (Gauss) que a' divise y et b' divise x. Il suit que $da'b'$ divise m, c'est-à-dire $(m) \subset (da'b')$. □

3.2 Décomposition en produit d'irréductibles

Définition 5
Un élément x d'un anneau A commutatif et intègre est dit irréductible *s'il n'est ni inversible, ni produit de deux éléments non inversibles. Autrement dit, x est irréductible s'il n'est pas inversible et si*

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

Exemple : dans $\mathbb{Z}$, "irréductible" $\Leftrightarrow$ "premier".

Lemme 1
Dans un anneau principal, toute suite croissante d'idéaux est stationnaire. Autrement dit, il n'existe pas de suite infinie d'idéaux strictement *croissante.*

Preuve. Soit $I_0 \subset I_1 \subset I_2 \subset \cdots$ une suite croissante d'idéaux. Alors $I := \bigcup_{n\in\mathbb{N}} I_n$ est un idéal de A (attention : ce serait en général FAUX si la suite n'était pas croissante). Il existe donc $x \in I$ tel que $I = (x)$. Mais alors, il existe $k \in \mathbb{N}$ tel que $x \in I_k$, auquel cas $I_k \subset I = Ax \subset I_k$, donc $I_k = I$ et $I_\ell = I_k$ pour tout $\ell \geq k$. □

Remarque. On peut reformuler ce lemme en disant que toute suite décroissante (au sens de la divisibilité) d'éléments de $\overline{A}$ est stationnaire (voir remarque 3)).

Proposition 5
Soit a un élément non nul d'un anneau principal A. Alors

1) *Si a est et non inversible, alors il admet un diviseur irréductible.*

2) *Pour tout élément irréductible p, l'ensemble $\left\{k \in \mathbb{N} \mid p^k \text{ divise } a\right\}$ est majoré.*

3) *L'ensemble des éléments irréductibles deux à deux non associés qui divisent a est fini.*

Preuve.

1) Si a est irréductible, c'est clair. Sinon, $a = a_1 b_1$ avec a_1 et b_1 non inversibles. Si a_1 est irréductible, on obtient bien un diviseur irréductible de a. Sinon, $a_1 = a_2 b_2$ avec a_2 et b_2 non inversibles, etc. Si le processus ne s'arrêtait jamais, on construirait ainsi une suite d'éléments $a_0 = a$, a_1, a_2, ... tels que a_i divise strictement a_{i-1} pour tout $i \geq 1$. La suite des idéaux (a_i) serait donc strictement croissante, ce qui est impossible en vertu du lemme 1. Donc le processus s'arrête, et le dernier terme a_k construit est irréductible.

2) Supposons, par l'absurde, que a soit divisible par p^k pour tout $k \in \mathbb{N}$. Il existe alors, pour tout $k \in \mathbb{N}$, un élément a_k de A tel que $a = p^k a_k$ et la suite (a_k) est strictement croissante, ce qui est impossible.

3) Si l'ensemble des diviseurs irréductibles de a deux à deux non associés est infini, on construit par récurrence une suite infinie $(p_n)_{n\in\mathbb{N}}$ d'irréductibles deux à deux non associés et une suite strictement croissante d'idéaux de la façon suivante :

$$a = p_1 a_1 = p_1 p_2 a_2 = p_1 p_2 p_3 a_3 = \cdots$$

(attention : on utilise Gauss à chaque étape !) et on a alors $(a_1) \subsetneq (a_2) \subsetneq \cdots$.

□

Définition 6
À tout élément irréductible p d'un anneau principal A est associée une application $v_p : A \setminus \{0\} \to \mathbb{N}$ définie par

$$v_p(a) = \max\left\{k \in \mathbb{N} \mid p^k \text{ divise } a\right\}.$$

Théorème 2
Soit a un élément non nul et non inversible d'un anneau principal A. On note $\mathbb{P}(a)$ l'ensemble de ses diviseurs irréductibles deux à deux non associés. Alors il existe $u \in A^\times$ tel que

$$a = u \prod_{p\in\mathbb{P}(a)} p^{v_p(a)}.$$

Chapitre 7

Polynômes et fractions rationnelles

Dans tout la suite, A désigne un anneau commutatif et K désigne un corps.

1 Définitions et premières propriétés

Définition 1
Un polynôme à coefficients dans A est une suite $(a_n)_{n\in\mathbb{N}}$ nulle à partir d'un certain rang, c'est-à-dire telle qu'il existe $N \in \mathbb{N}$ avec la propriété que a_n est nul pour tout $n > N$.

Informellement, un polynôme est donc une suite

$$(a_0, a_1, a_2, a_3, \ldots, a_N, 0, 0, 0 \ldots).$$

Avec cette définition il est immédiat de définir la somme de deux polynômes :

Définition 2
si $P = (a_n)_{n\in\mathbb{N}}$ et $Q = (b_n)_{n\in\mathbb{N}}$ sont deux polynômes, leur somme est le polynôme $P + Q = (a_n + b_n)_{n\in\mathbb{N}}$.


Il faut vérifier que la somme $P + Q$ que l'on vient de définir est bien un *polynôme*, c'est-à-dire qu'elle est nulle à partir d'un certain rang. Or il existe $N_1 \in \mathbb{N}$ tel que a_n est nul pour tout $n > N_1$ et $N_2 \in \mathbb{N}$ tel que b_n est nul pour tout $n > N_2$, donc $a_n + b_n$ est nul pour tout $n > N := \max(N_1, N_2)$.

On peut également, de façon un peu moins immédiate, définir le produit de deux polynômes :

Définition 3
Le produit de deux polynômes $P = (a_n)_{n\in\mathbb{N}}$ et $Q = (b_n)_{n\in\mathbb{N}}$ est le polynôme $PQ = (c_n)_{n\in\mathbb{N}}$ où c_n est défini par la formule

$$c_n = a_0 b_n + a_1 b_{n-1} + a_2 b_{n-2} + \ldots + a_{n-1} b_1 + a_n b_0 = \sum_{k=0}^{n} a_k b_{n-k}.$$

Remarque. Là encore, il faut s'assurer que c_n est nul pour n "assez grand", ce qui est clair : $a_n = 0$ pour tout $n > N_1$ et $b_n = 0$ pour tout $n > N_2$, alors $c_n = \sum_{k=0}^{n} a_k b_{n-k}$ est nul dès que $n > N_1 + N_2$.

Proposition 1
Muni des deux lois précédentes, l'ensemble $A[X]$ est un anneau, d'élément neutre additif le polynôme nul $(0, 0, \ldots)$ et d'élément neutre multiplicatif le polynôme $(1, 0, 0, \ldots)$.

Preuve. C'est immédiat. □

Après ce préambule un peu formel, on peut revenir à une notation plus familière en posant

$$X := (0, 1, 0, 0, 0, \ldots).$$

On vérifie alors sans difficulté (récurrence) que

$$\begin{aligned} X^2 &= (0, 0, 1, 0, \ldots), \\ X^3 &= (0, 0, 0, 1, 0, \ldots), \\ &\vdots \\ X^n &= (0, 0, \ldots, 0, 1, 0, 0, \ldots), \\ \text{et également } X^0 &= (1, 0, 0, 0, \ldots). \end{aligned}$$

Avec ces notations, on voit qu'un polynôme $P = (a_0, a_1, \ldots, a_N, 0, 0, \ldots)$ peut s'écrire

$$P = a_0 + a_1 X + \ldots + a_n X^n.$$

On convient de noter $A[X]$ l'ensemble des polynômes à coefficients dans A.

Définition 4
Le degré d'un polynôme P non nul, noté $\deg P$, est le plus grand entier n tel que le coefficient a_n de X^n dans P soit non nul.
Par convention, le degré du polynôme nul, est égal à $-\infty$. On convient également que :

- *$n + -\infty = -\infty$ pour tout $n \in \mathbb{N}$,*
- *$n > -\infty$ pour tout $n \in \mathbb{N}$.*

Proposition 2
Soient P et Q deux polynômes à coefficients dans un anneau A **intègre**.

1) $\deg(P + Q) \leq \max(\deg P, \deg Q)$ *et on a égalité si* $\deg P \neq \deg Q$.

2) *Si A est* **intègre**, $\deg(PQ) = \deg P + \deg Q$.

Une conséquence immédiate de la formule $\deg(PQ) = \deg P + \deg Q$ est le

Corollaire 1
Soient P et Q deux polynômes non nuls à coefficients dans un anneau A **intègre**. *Si P divise Q, alors* $\deg P \leq \deg Q$.

2 Division euclidienne

Théorème 1
Soient F et G deux polynômes à coefficients dans un anneau intègre A. ***Si le coefficient dominant de G est inversible dans*** *A, alors il existe un unique couple (Q, R) de polynômes qui vérifie*

$$\begin{cases} F = GQ + R \\ \deg R < \deg G \end{cases}$$

Preuve.

- Existence. Posons

  $$G = g_0 + g_1 X + \ldots + g_d X^d, \text{ avec } g_d \in A^\times \text{ (en particulier, } \deg G = d)$$

  et

  $$F = f_0 + f_1 X + \ldots + f_n X^n.$$

  - Si $n < d$, alors le couple $(Q, R) = (0, F)$ convient.
  - Sinon, le polynôme $F_1 := F - f_n g_d^{-1} X^{n-d} G$ est de degré strictement inférieur à n. On reprend alors le processus avec le couple (F_1, G).

- Unicité. Si $F = GQ_1 + R_1 = GQ_2 + R_2$ avec $\deg R_1 < \deg G$ et $\deg R_2 < \deg G$, alors

  $$G(Q_1 - Q_2) = R_2 - R_1$$

  d'où

  $$\deg(G(Q_1 - Q_2)) = \deg G + \deg(Q_1 - Q_2) = \deg(R_2 - R_1) < \deg G$$

  ce qui n'est possible que si $Q_1 - Q_2 = 0$, auquel cas on a également $R_2 - R_1 = 0$.

□

Corollaire 2
Si K est un corps, l'anneau $K[X]$ est euclidien donc principal.

3 Racines et multiplicités

À un polynôme $P = a_0 + a_1X + \cdots + a_nX^n \in A[X]$, on associe une *fonction polynomiale*

$$\begin{array}{rccc} \widetilde{P}: & A & \longrightarrow & A \\ & \alpha & \longmapsto & \widetilde{P}(\alpha) = a_0 + a_1\alpha + \cdots + a_n\alpha^n. \end{array}$$


Il faut prendre garde de ne pas identifier un polynôme à la fonction polynomiale qui lui est associée, à cause du gag suivant : le polynôme $P(X) = X^2 + X \in \mathbb{Z}/2\mathbb{Z}[X]$ est non nul, mais sa fonction polynomiale associée $\widetilde{P}$ l'est, puisque $\widetilde{P}(0) = \widetilde{P}(1) = 0$. Cependant, ce problème ne se pose si l'on considère des polynômes à cooefficients dans un corps K infini, car alors l'application $P \mapsto \widetilde{P}$ est injective (exercice).

Ceci étant, on comment le plus souvent l'abus de notation consistant à noter "$P(\alpha)$" l'image de α par la fonction $\widetilde{P}$ (plutôt que "$\widetilde{P}(\alpha)$").

Proposition 3
Les propriétés suivantes sont équivalentes :

1) *α est racine de P.*

2) *$(X - \alpha)$ divise P.*

Preuve. On effectue la division euclidienne de P par $X - \alpha$:

$$P = (X - \alpha)Q + R \text{ avec } \deg R < 1. \tag{7.1}$$

Autrement dit, R est un polynôme constant, éventuellement nul (auquel cas $\deg R = -\infty$). Supposons que α soit racine de P. Alors, en évaluant le polynôme P en α et en utilisant l'équation (7.1) on obtient que

$$0 = P(\alpha) = R(\alpha),$$

ce qui signifie que $R = 0$ puisque R est un polynôme constant. Donc $X - \alpha$ divise P. Inversement, si $X - \alpha$ divise P, alors il existe $Q \in A[X]$ tel que $P = (X - \alpha)Q$ auquel cas $P(\alpha) = 0$. □

Théorème 2
*Soient $\alpha_1, \alpha_2, \ldots, \alpha_k$ des racines deux à deux distinctes d'un polynôme $P \in A[X]$, où A **est un anneau intègre**. Alors le produit $(X - \alpha_1)(X - \alpha_2) \cdots (X - \alpha_k)$ divise P. En particulier, le nombre de racines deux à deux distinctes d'un polynôme à coefficients dans un anneau intègre est au plus égal à n.*

Preuve. La proposition précédente montre que $X - \alpha_1$ divise P ; il existe donc $Q_1 \in A[X]$ tel que

$$P = (X - \alpha_1)Q_1.$$

Comme α_2 est racine, on a

$$0 = P(\alpha_2) = (\alpha_2 - \alpha_1)Q_1(\alpha_2)$$

et donc $Q_1(\alpha_2) = 0$ puisque $\alpha_2 - \alpha_1 \neq 0$ **et que** A **est intègre**. En vertu de la proposition 3, on peut donc affirmer que $X - \alpha_2$ divise Q_1, c'est-à-dire qu'il existe $Q_2 \in A[X]$ tel que

$$Q_1 = (X - \alpha_2)Q_2$$

et par conséquent

$$P = (X - \alpha_1)(X - \alpha_2)Q_2.$$

En poursuivant ce raisonnement, on montre que $(X - \alpha_1)(X - \alpha_2) \cdots (X - \alpha_k)$ divise P. □


Le résultat est faux si l'anneau A n'est pas intègre. Par exemple, si $A = \mathbb{Z}/6\mathbb{Z}$ le polynôme $X^2 - X \in A[X]$ a quatre racines dans A !

Définition 5
Soit P un polynôme à coefficients dans A et $\alpha \in A$ une racine de P. On appelle multiplicité de la racine α le plus grand entier naturel n tel que $(X - \alpha)^n$ divise P.

Remarque : la multiplicité d'une racine est majorée par le degré du polynôme.

On obtient alors le raffinement suivant du théorème 2 :

Théorème 3
Soient P un polynôme à coefficients dans un anneau intègre A et $\alpha_1, \alpha_2, \ldots, \alpha_k$ ses racines deux à deux distinctes dans A, de multiplicités respectives $n_1, n_2, \ldots, n_k$. Alors il existe un polynôme $Q \in A[X]$, sans racine dans A, tel que

$$P = (X - \alpha_1)^{n_1}(X - \alpha_2)^{n_2} \cdots (X - \alpha_k)^{n_k}Q.$$

En particulier, le nombre de racines de P dans A, comptées avec multiplicité, est majoré par le degré de P.

Preuve. Exercice (copier la preuve du théorème 2). □

4 Polynômes irréductibles

On a vu (Corollaire 2) que l'anneau $K[X]$ était euclidien. En particulier, tout polynôme P de $K[X]$ s'écrit de façon essentiellement unique comme produit de polynômes irréductibles (*cf.* Théorème 2).

Exemples.

1) Pour tout $a \in K$, le polynôme $X - a$ est irréductible dans $K[X]$.

2) Le polynôme $X^2 + 2$ est irréductible dans $\mathbb{R}[X]$ mais pas dans $\mathbb{C}[X]$.

3) Le polynôme $X^2 - 2$ est irréductible dans $\mathbb{Q}[X]$ mais pas dans $\mathbb{R}[X]$.

4)

$$\begin{aligned} X^4 + 1 &= (X - e^{i\pi/4})(X - e^{-i\pi/4})(X - e^{3i\pi/4})(X - e^{-3i\pi/4}) \text{ dans } \mathbb{C}[X] \\ &= (X^2 - \sqrt{2}X + 1)(X^2 + \sqrt{2}X + 1) \text{ dans } \mathbb{R}[X] \\ &\text{et il est irréductible dans } \mathbb{Q}[X]. \end{aligned}$$

5 Dérivées successives, formule de Taylor et applications

`(non traité en cours)`

Dans cette section, on considère des polynômes à coefficients dans un corps K.

Définition 6
Soit $P = a_0 + a_1 X + \ldots + a_n X^n \in K[X]$. On appelle polynôme dérivé de P et on note P', le polynôme

$$P' = a_1 + 2a_2 X + \ldots + n a_n X^{n-1}.$$

En particulier, si $P = a_0$, on a $P' = 0$. On définit de manière analogue les polynômes dérivés successifs de P, que l'on note $P^{(1)} = P'$, $P^{(2)}$, $P^{(3)}$, ...

Remarque : il est commode également de noter par convention $P^{(0)} = P$.

Théorème 4
Soit P un polynôme de degré n à coefficient dans un corps K **de caractéristique nulle**. *On a alors, pour tout $\alpha \in K$, l'identité :*

$$\begin{aligned} P &= P(\alpha) + P'(\alpha)(X - \alpha) + \frac{P''(\alpha)}{2}(X - \alpha)^2 + \ldots + \frac{P^{(n)}(\alpha)}{n!}(X - \alpha)^n \\ &= \sum_{k=0}^{n} \frac{P^{(k)}(\alpha)}{k!}(X - \alpha)^k. \end{aligned}$$

Preuve. Dans un premier temps, on donne la preuve dans le cas où $\alpha = 0$. Il existe des coefficients $a_0, a1, \ldots, a_n$ tels que

$$P = a_0 + a_1 X + \ldots + a_n X^n. \tag{7.2}$$

En évaluant P en 0 on trouve :

$$P(0) = a_0. \tag{7.3}$$

Si l'on dérive (7.2), et que l'on évalue l'identité trouvée en 0, on obtient de même :

$$P'(0) = a_1 \tag{7.4}$$

En poursuivant ce procédé de dérivations successives et évaluation en 0 on montre facilement que $P(0) = a_0, P'(0) = a_1, P''(0) = 2a_2, \ldots, P^{(n)}(0) = n!a_n$, ou autrement dit que

$$P = \sum_{k=0}^{n} \frac{P^{(k)}(0)}{k!} X^k.$$

Le cas général s'obtient en appliquant le cas particulier précédent au polynôme

$$Q(X) := P(X + a),$$

après avoir établi (récurrence immédiate) la propriété : $Q^{(k)}(0) = P^{(k)}(a)$. □

Corollaire 3
Les assertions suivantes, pour un polynôme $P \in K[X]$ et un élément α de K, sont équivalentes :

1) *$(X - \alpha)^k$ divise P.*

2) *$P(\alpha) = P'(\alpha) = \ldots = P^{(k-1)}(\alpha) = 0$.*

En particulier, α est racine de P avec multiplicité exactement k si et seulement si

$$P(\alpha) = P'(\alpha) = \ldots = P^{(k-1)}(\alpha) = 0 \text{ et } P^{(k)}(\alpha) \neq 0.$$

6 Fractions rationnelles

6.1 Corps des fractions d'un anneau intègre

Définition 7
Soit A un anneau intègre et $\mathcal{C} = A \times (A \setminus \{0\})$.
Sur $\mathcal{C}$ on introduit deux opérations $+$ et $\times$ définies comme suit : pour tous (a,b) et (c,d) de $\mathcal{C}$, on pose

$$(a,b) \times (c,d) = (ac, bd)$$

et

$$(a,b) + (c,d) = (ad + cb, bd).$$

Définition 8
Sur $\mathcal{C}$ on définit la relation $\mathcal{R}$ suivante

$$(a,b)\mathcal{R}(c,d) \;\; si \;\; ad = cb.$$

Théorème 5
La relation $\mathcal{R}$ est une relation d'équivalence compatible avec les opérations $+$ et $\times$ définies précédemment. Celles-ci induisent une structure d'anneau sur le quotient $\mathcal{C}/\mathcal{R}$, et cet anneau est un corps.

Preuve. On vérifie facilement que $\mathcal{R}$ est une relation d'équivalence (l'intégrité de A est cruciale pour établir la transitivité).
La compatibilité des opérations avec $\mathcal{R}$ est un calcul facile. Par exemple, si $(a,b)\mathcal{R}(a',b')$ et $(c,d)\mathcal{R}('c,d')$, alors

$$\begin{aligned}(ad+bc)b'd' - (a'd'+b'c')bd &= (ab')dd' + (cd')bb' - (a'b)dd' - (c'd)bb' \\ &= (a'b)dd' + (c'd)bb' - (a'b)dd' - (c'd)bb' \\ &= 0\end{aligned}$$

donc $(a,b) + (c,d)\mathcal{R}(a',b') + (c',d')$.
Si on note (provisoirement) $[a,b]$ la classe modulo $\mathcal{R}$ d'un élément (a,b) de $\mathcal{C}$, on peut donc munir le quotient $\mathcal{C}/\mathcal{R}$ de deux lois $+$ et $\times$

$$[a,b] + [c,d] = [ad+cb, bd] \text{ et } [a,b] \times [c,d] = [ac, bd]$$

dont on vérifie facilement qu'elles définissent sur $\mathcal{C}/\mathcal{R}$ une structure d'anneau. En particulier, le neutre additif est égal à $[0,1]$ et le neutre multiplicatif à $[1,1]$.
Si $[a,b]$ est un élément de $\mathcal{C}/\mathcal{R}$ son opposé est $[-a,b]$, car $[-a,b] + [a,b] = [a,b] + [-a,b] = [0,b^2] = [0,1]$.
Vérifions enfin que $\mathcal{C}/\mathcal{R}$ est un corps : si $[a,b] \neq [0,1]$, c'est-à-dire si $b \neq 0$, alors $(b,a) in \mathcal{C}$ et $[a,b] \times [b,a] = [ab, ab] = [1,1]$. □

Définition 9
L'anneau $\mathcal{C}/\mathcal{R}$ s'appelle le corps des fractions de A. On le note Fr A.

On convient de noter désormais $\frac{a}{b}$ la classe d'un élément (a, b) dans Fr A.

Proposition 4
Si A est un anneau principal, tout élément de Fr A *admet un réprésentant* irréductible, *c'est-à-dire de la forme $\frac{a}{b}$ avec a et b premiers entre eux.*

Proposition 5
L'application

$$\begin{array}{rccc} i: & A & \longrightarrow & \text{Fr } A \\ & a & \longmapsto & \dfrac{a}{1} \end{array}$$

est un morphisme d'anneaux injectif.

Par conséquent, on peut identifier A à un sous anneau de son corps des fractions Fr A, en identifiant l'élément $a \in A$ avec son image $\frac{a}{1}$ dans Fr A.

6.2 Le corps des fractions rationnelles $K(X)$

Théorème 6
Soit $F \in K(X)$ une fraction rationnelle non nulle. Soit $F = \frac{N}{D}$ un représentant irréductible de F, c'est-à-dire avec N et D premiers entre eux, et soit

$$D = {P_1}^{\alpha_1} \dots {P_r}^{\alpha_r}$$

la décomposition de D en facteurs irréductibles de $K[X]$. Alors on peut écrire de manière unique sous la forme

$$F = E + \sum_{i=1}^{r} \left(\sum_{j=1}^{\alpha_i} \frac{A_{i,j}}{P_i^j} \right)$$

où E et les $A_{i,j}$ sont des polynômes et $\deg(A_{i,j}) < deg(P_i)$ *pour tout i et tout j. Le polynôme E s'appelle la* partie entière *de F.*

Preuve.

- **Existence.** La démonstration se déroule en trois temps :

  1) Si $F = \frac{N}{D}$, il existe un unique couple (E, R) de polynômes tels que

  $$F = E + \frac{R}{D} \qquad \text{et} \qquad \deg R < \deg D$$

  obtenu en faisant la division euclidienne de N par D

2) On suppose désormais que $F = \dfrac{N}{D}$, avec N et D premiers entre eux et $\deg N < \deg D$.

(a) Si $D = PQ$ avec $P \wedge Q = 1$, il existe un unique couple (A, B) de polynômes tels que

$$F = \frac{A}{P} + \frac{B}{Q} \quad , \quad \deg A < \deg P \quad \text{et} \quad \deg B < \deg Q.$$

(b) Si $F = \dfrac{A}{P^k}$ avec $\deg A < k \deg P$, il existe un unique k-uplet $(A_1, \ldots, A_k)$ de polynômes tels que

$$F = \frac{A_1}{P^k} + \frac{A_2}{P^{k-1}} + \cdots \frac{A_k}{P} \quad \text{et} \quad \deg A_j < \deg P \text{ pour tout } j.$$

- **Unicité :** un peu fastidieux, mais pas difficile (exercice !).

□

Quelques exemples de calcul :

1) Soit K un corps commutatif et Q un polynôme à coefficients dans K, scindé sur K, et n'ayant que des racines simples, c'est-à-dire $Q(X) = \prod_{i=1}^{n}(X - x_i)$, avec $x_i \neq x_j$ si $i \neq j$. Alors, pour tout $P \in K[X]$

$$\frac{P}{Q} = \sum_{i=1}^{n} \frac{P(x_i)}{P'(x_i)(X - x_i)}.$$

Application : déterminer la décomposition en éléments simples de la fraction rationnelle $\dfrac{1}{X^n - 1}$ dans $\mathbb{R}(X)$, où n désigne un entier naturel non nul.

2) (*Exercice*) Déterminer la décomposition en éléments simples de

$$F(X) = \frac{X^2 + 1}{(1 + X)^2(1 + X + X^2)^2}$$

dans $\mathbb{R}(X)$.