

# Chapitre 10. Algèbre générale

## 1 Conjugaison dans un groupe. Théorème de Lagrange

### 1.1 Morphisme de conjugaison

**Définition 1.1.** Soit  $H$  un groupe,  $h \in G$

Alors

$$\varphi_h : \begin{cases} G \rightarrow G \\ g \mapsto hgh^{-1} \end{cases}$$

est un morphisme de conjugaison (ou encore un automorphisme intérieur).

**Proposition 1.2.**  $\varphi_h$  est bien un automorphisme et

$$\Phi : \begin{cases} G \rightarrow \text{Aut } G = \{f : G \rightarrow G \mid f \text{ automorphisme}\} \\ h \mapsto \varphi_h \end{cases}$$

est un morphisme de groupes.

**Définition 1.3.** Soit  $G$  un groupe,  $g, g' \in G$

On dit que  $g$  et  $g'$  sont conjugués s'il existe  $h \in G$  tel que  $g' = hgh^{-1}$

**Proposition 1.4.** Sur un groupe, la relation "être conjugué" est une relation d'équivalence. On appelle classe de conjugaison les classes pour cette relation.

### 1.2 Classe à gauche, classe à droite selon un sous-groupe

**Définition 1.5.** Soit  $G$  un groupe,  $H$  un sous-groupe.

On définit la congruence à gauche modulo  $H$  par

$$x \sim y \iff y \in xH \iff \exists h \in H, y = xh$$

**Proposition 1.6.** La congruence à gauche modulo  $H$  est une relation d'équivalence et la classe de  $x$  est  $\bar{x} = xH$

**Théorème 1.7** (Théorème de Lagrange).

Soit  $G$  un groupe fini. Le cardinal d'un sous-groupe de  $G$  divise celui de  $G$

### 1.3 Relations compatibles avec une loi. Groupe quotient

**Définition 1.8.** Soit  $(M, *)$  un monoïde,  $\equiv$  une relation d'équivalence sur  $M$

On dit que  $*$  et  $\equiv$  sont compatibles si  $\forall a, x, y \in M, x \equiv y \implies \begin{cases} a * x \equiv a * y \\ x * a \equiv y * a \end{cases}$

**Théorème 1.9.** Soit  $(G, +)$  un groupe abélien. On note  $G|_H$  le quotient de  $G$  par la congruence modulo  $H$  sur lequel on définit une loi quotient  $+$  :  $\bar{x} + \bar{y} = \overline{x+y}$

Alors  $(G|_H, +)$  est un groupe (abélien) appelé groupe quotient de  $G$  par  $H$

**Définition 1.10.** Un sous-groupe  $H$  de  $G$  tel que  $\forall x \in G, xHx^{-1} \subset H$  est dit distingué.

**Proposition 1.11.** Si  $H$  est distingué de  $G$  alors  $\equiv$  (congruence modulo  $H$ ) et  $\times$  sont compatibles.

**Théorème 1.12.**  $G|_H$  peut être muni d'une loi quotient qui en fait un groupe.

**Théorème 1.13** (Théorème d'isomorphisme). Soit  $f : G \rightarrow G'$  un morphisme de groupes. On pose

$$\bar{f} : \begin{cases} G/\ker f \rightarrow \operatorname{im} f \\ \bar{x} \mapsto \bar{f}(\bar{x}) = f(x) \end{cases}$$

$\bar{f}$  est bien définie et c'est un isomorphisme (canoniquement associé à  $f$ )

$$G/\ker f \simeq \operatorname{im} f$$

## 1.4 Ordre d'un élément dans un groupe

**Définition 1.14.** Soit  $G$  un groupe,  $a \in G$

L'ordre de  $a$  dans  $G$  est le "cardinal" du sous-groupe engendré par  $a$

**Proposition 1.15.** Si  $a$  est d'ordre fini  $n$  dans un groupe  $G$  alors  $n$  est le plus petit entier  $k \geq 1$  avec  $a^k = 1$

**Théorème 1.16** (Théorème de Lagrange). Soit  $G$  un groupe fini de cardinal  $n$ ,  $a \in G$

- \* L'ordre de  $a$  divise  $n$
- \*  $a^n = 1$

## 1.5 Le groupe symétrique

**Définition 1.17.** Soit  $a_1, \dots, a_p \in E$  2 à 2 distincts,  $p \geq 2$

On note

$$(a_1, a_2, \dots, a_p) : x \mapsto \begin{cases} a_{i+1} \text{ si } x = a_i \text{ avec } i \in \llbracket 1, p-1 \rrbracket \\ a_1 \text{ si } x = a_p \\ x \text{ si } x \notin \{a_1, \dots, a_p\} \end{cases}$$

$(a_1, \dots, a_p)$  est appelé  $p$ -cycle, de support  $\{a_1, \dots, a_p\}$  de longueur  $p$

Si  $p = 2$  on parle de transpositions.

**Proposition 1.18.**

- \* Un  $p$ -cycle  $\sigma$  et  $S_E$  est un élément d'ordre  $p$  de  $(S_E, \circ)$
- \* Si  $\sigma \in S_E$ ,  $c = (a_1, \dots, a_p)$  alors

$$\sigma \circ c \circ \sigma^{-1} = \sigma \circ (a_1, \dots, a_p) \circ \sigma^{-1} = (\sigma(a_1), \dots, \sigma(a_p))$$

- \*  $(a_1 a_2 \dots a_p) = (a_1 a_2) \circ (a_2 a_3) \circ \dots \circ (a_{p-1} a_p)$
- \* Si  $\sigma$  et  $\sigma'$  sont des cycles à support disjoints, alors  $\sigma \circ \sigma' = \sigma' \circ \sigma$

**Théorème 1.19** (Théorème de décomposition en produit de cycles à support disjoint).

Soit  $\sigma \in S_E$  et soit  $\Omega_1, \dots, \Omega_n$  les orbites de  $E$  sous l'action de  $\sigma$

Alors il existe  $c_1, \dots, c_n$  cycles à supports disjoints tels que

$$\sigma = c_1 \circ c_2 \circ \dots \circ c_n$$

**Corollaire 1.20.**

- \* Les cycles engendrent  $S_E$
- \* Les transpositions engendrent  $S_E$  : tout  $\sigma \in S_E$  est un produit de transpositions.

## 1.6 Signature d'une permutation

**Lemme 1.21.** Soit  $\sigma, \sigma' \in S_n$

On note  $N(\sigma) = \text{Card} \{(i, j) \in \llbracket 1, n \rrbracket \mid i < j \text{ et } \sigma(j) < \sigma(i)\}$  et  $\varepsilon(\sigma) = (-1)^{N(\sigma)}$

Alors  $\varepsilon(\sigma' \circ \sigma) = \varepsilon(\sigma')\varepsilon(\sigma)$

**Théorème 1.22.** Il existe un unique morphisme de groupes non trivial

$$\varepsilon : \begin{cases} S_n \rightarrow \{-1, 1\} \\ \sigma \mapsto \varepsilon(\sigma) \end{cases}$$

appelée signature. Si  $\sigma = \tau_1 \circ \dots \circ \tau_r$  avec  $\tau_i$  transpositions alors  $\varepsilon(\sigma) = (-1)^r$

**Définition 1.23.**  $\sigma$  est dite paire si  $\varepsilon(\sigma) = 1$

$\ker \varepsilon$  est un sous-groupe de  $S_n$  appelé groupe alternée d'ordre  $n$  noté  $\mathfrak{A}_n$

On a  $|\mathfrak{A}_n| = \frac{n!}{2}$

## 2 Congruence modulo un idéal

### 2.1 Anneaux quotients

Ici les anneaux sont commutatifs.

**Théorème 2.1.** Soit  $A$  un anneau et  $I$  un idéal différent de  $A$

$(A/I, +, \times)$  est un anneau commutatif appelé anneau quotient de  $A$  par  $I$

**Théorème 2.2** (Corps de rupture d'un polynôme irréductible).

Soit  $A = K[X]$  et  $\Pi$  un polynôme irréductible de  $K[X]$

$$L = \frac{K[X]}{\Pi K[X]}$$

est appelé corps de rupture du polynôme  $\Pi$  et

$$\dim_K \frac{K[X]}{\Pi K[X]} = \deg \Pi$$

**Théorème 2.3** (Théorème d'isomorphisme). Soit  $f : A \rightarrow B$  un morphisme d'anneaux.

Alors

$$\bar{f} : \begin{cases} A_{|\ker f} \rightarrow \text{im } f \\ \bar{x} \mapsto \bar{f}(\bar{x}) = f(x) \end{cases}$$

est un isomorphisme.

$$A_{|\ker f} \simeq \text{im } f$$

On dit que  $\bar{f}$  est l'isomorphisme canoniquement associé à  $f$

### 2.2 Congruences modulo $a$

**Définition 2.4.** Soit  $A$  un anneau et  $a \in A$

La congruence modulo  $a$  est la congruence modulo  $aA$ . On la note pour  $x, y \in A$

$$x \equiv y \pmod{a} \iff y - x \in aA \iff a \mid y - x$$

## 2.3 Le petit théorème de Fermat

### Théorème 2.5.

- \* Si  $a \in \mathbb{Z}$  et  $p \nmid a$  ( $p \in \mathbb{P}$ ) alors  
 $a^{p-1} \equiv 1[p]$
- \* Si  $a \in \mathbb{Z}$  et  $p \in \mathbb{P}$  alors  
 $a^p \equiv a[p]$   
 $\bar{a}^p = \bar{a}$  dans  $\mathbb{F}_p = \mathbb{Z}_{|p}\mathbb{Z}$

**Proposition 2.6.** Dans  $\mathbb{F}_p[X] = \mathbb{Z}_{|p}\mathbb{Z}[X]$

$$X^p - X = X(X - \bar{1}) \dots (X - \overline{p-1})$$

$$X^{p-1} - 1 = (X - \bar{1}) \dots (X - \overline{p-1})$$

$$\overline{(p-1)!} = -1 \text{ (Théorème de Wilson)}$$

## 2.4 La caractérisation d'un anneau, d'un corps

Soit  $A$  un anneau commutatif et

$$f : \begin{cases} \mathbb{Z} \rightarrow A \\ k \mapsto k1_A = (1_A + \dots + 1_A) \end{cases}$$

$$A_0 = \text{im } f = \{k1_A\}_{k \in \mathbb{Z}}$$

$\ker f = n\mathbb{Z}$  avec  $n \in \mathbb{N}^*$  unique car  $\ker f$  est un idéal de  $\mathbb{Z}$

Si  $f$  est injective, alors  $n = 1$  et  $A_0 \simeq \mathbb{Z}$ , on dit que  $A$  est de caractéristique nulle

Sinon,  $n \geq 2$  et  $A_0 \simeq \mathbb{Z}_{|n}\mathbb{Z}$ , on dit que  $A$  est de caractéristique  $n$

## 2.5 Complément sur les corps

**Proposition 2.7.** La caractéristique d'un corps est nulle ou finie égale à un nombre premier.

### 2.5.1 Complément 1

**Théorème 2.8.** Soit  $P \in K[X]$ ,  $P \neq 0$

Alors il existe un surcorps de  $K$  sur lequel  $P$  est scindé.

### 2.5.2 Complément 2 : construction de corps fini

En utilisant les corps de rupture on peut construire les corps de taille donné.

Par exemple :  $\Pi = X^3 + X + 1$  est irréductible dans  $\mathbb{F}_2[X]$ , ainsi

$$L = \mathbb{F}_8 = \frac{\mathbb{F}_2[X]}{\Pi} = \text{Vect}(1, \alpha, \alpha^2)$$

avec  $\alpha^3 + \alpha + 1 = 0$

### 3 L'indicatrice d'Euler

#### 3.1 Le théorème chinois

**Théorème 3.1** (Théorème chinois). Soit  $m, n \geq 1$  premiers entre eux.

Alors

$$\bar{f} : \begin{cases} \mathbb{Z}_{mn\mathbb{Z}} \rightarrow \mathbb{Z}_{m\mathbb{Z}} \rightarrow \mathbb{Z}_{n\mathbb{Z}} \\ \bar{k} \mapsto (\bar{k}, \bar{k}) \end{cases}$$

est un isomorphisme d'anneaux :

$$\mathbb{Z}_{m\mathbb{Z}} \times \mathbb{Z}_{n\mathbb{Z}} \simeq \mathbb{Z}_{mn\mathbb{Z}}$$

en tant qu'anneaux.

Extension : Si  $n_1, \dots, n_r$  sont premiers 2 à 2 alors

$$\mathbb{Z}_{n_1\mathbb{Z}} \times \dots \times \mathbb{Z}_{n_r\mathbb{Z}} \simeq \mathbb{Z}_{n_1 \dots n_r \mathbb{Z}}$$

#### 3.2 Expression de l'indicatrice d'Euler

**Définition 3.2.** On note  $\varphi(1) = 1$  et pour  $n \geq 2$

$\varphi$  est le nombre d'entiers  $k \in \llbracket 1, n \rrbracket$  tels que  $k \wedge n = 1$

$\varphi : \mathbb{N}^* \rightarrow \mathbb{N}$  est appelée indicatrice d'Euler.

**Proposition 3.3.** Soit  $n \geq 2$ . On a :

- \*  $\varphi(n) = \text{Card}\{k \in \llbracket 0, n-1 \rrbracket \mid k \wedge n = 1\}$
- \*  $\varphi(n) = \text{Card}(\mathbb{Z}_{n\mathbb{Z}})^\times$
- \*  $\varphi(n) = \text{Card}\{x \in \mathbb{Z}_{n\mathbb{Z}} \mid x \text{ engendre } (\mathbb{Z}_{n\mathbb{Z}}, +)\}$
- \*  $\varphi(n) = \text{nombre de racines } n\text{-ièmes primitives de l'unité.}$
- \*  $\varphi(n) = \text{nombre de générateurs de } (\mathbb{U}_n, \times)$

**Théorème 3.4** (Théorème d'Euler-Fermat). Soit  $n \geq 2$

Si  $a$  est premier avec  $n$  alors

$$a^{\varphi(n)} \equiv [n]$$

**Théorème 3.5.** Si  $m, n \in \mathbb{N}^*$

$$m \wedge n = 1 \implies \varphi(mn) = \varphi(m)\varphi(n)$$

**Lemme 3.6.** Si  $A$  et  $B$  anneaux, alors  $(A \times B)^\times = A^\times \times B^\times$

**Théorème 3.7.** Soit  $n = p_1^{\alpha_1} \dots p_r^{\alpha_r}$  sa décomposition en facteurs premiers.

$$\varphi(n) = (p_1^{\alpha_1} - p_1^{\alpha_1-1}) \dots (p_r^{\alpha_r} - p_r^{\alpha_r-1})$$

$$\varphi(n) = n \left(1 - \frac{1}{p_1}\right) \dots \left(1 - \frac{1}{p_r}\right)$$

#### 3.3 Complément La formule sommatoire d'Euler

**Théorème 3.8** (formule sommatoire d'Euler). Pour  $n \geq 1$  on a

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

## 4 Exercices classiques

### 4.1 Théorème de Wilson

1. Montrer que si  $p$  est premier alors  $(p-1)! \equiv -1[p]$
2. Si  $n \geq 2$  et  $(n-1)! \equiv -1[n]$  montrer que  $n$  est premier.

### 4.2 Groupes tels que $x^2 = 1$

Soit  $(G, \times)$  un groupe tel que  $\forall x \in G, x^2 = 1_G$

1. Montrer que  $G$  est abélien.
2. Si  $G$  est fini, montrer que  $G \simeq ((\mathbb{Z}/2\mathbb{Z})^n, +)$

### 4.3 Carrés de $\mathbb{F}_p$

Soit  $p$  un nombre premier impair.

1. Dénombrer les carrés de  $(\mathbb{Z}/p\mathbb{Z})^*$
2. Montrer que si  $x \in (\mathbb{Z}/p\mathbb{Z})^*$  alors  $x$  carré  $\iff x^{\frac{p-1}{2}} = 1$
3. Montrer que  $-1$  carré dans  $\mathbb{Z}/p\mathbb{Z} \iff p \equiv 1[4]$
4. En déduire qu'il existe une infinité de nombres premiers  $\equiv 1[4]$

### 4.4 Groupe diagonal $\mathbb{D}_{2n}$

On note  $\mathbb{D}_n$  le groupe des isométries affines du plan complexe qui laissent  $\mathbb{U}_n$  globalement invariant.

1. Préciser les éléments de  $\mathbb{D}_{2n}$  et son cardinal.  
 $\mathbb{D}_{2n}$  est appelé le groupe diédral d'ordre  $2n$
2. Montrer que  $\mathbb{D}_{2n}$  est engendré par deux éléments :  
 $R$  d'ordre  $n$ ,  $S$  d'ordre 2 tels que  $SR = R^{-1}S$
3. Réciproquement, si un groupe  $G, G = \langle R, S \rangle$  avec  $R$  d'ordre  $n$  et  $S$  d'ordre 2 et  $SR = R^{-1}S$  montrer que  $G \simeq \mathbb{D}_{2n}$
4. Montrer que tout sous-groupe fini du groupe des isométries du plan complexe est isomorphe à  $(\mathbb{Z}/n\mathbb{Z})$  (cyclique) ou à  $\mathbb{D}_{2n}$  (avec  $n \geq 3$ )