

Algèbre 2
Julien Hébert-Doutreloux
December 7, 2020



Table des matières

1 Relation binaire et d'équivalence	3
2 Groupes et propriétés	4
3 Groupes symétriques	6
4 Corps et groupes de matrices	8
5 Groupe des quaternions	9
6 Homomorphismes et isomorphismes	10
7 Sous-groupes	12
8 Groupes et sous-groupes cycliques	13
9 Centralisateur et normalisateur	14
10 Sous-groupe engendré par un sous-ensemble	15
11 Treillis des sous-groupes	16
12 Groupe quotient	17
13 Le théorème de Lagrange	18
14 Les théorèmes d'isomorphisme	19
15 Théorème de Jordan-Hölder	20
16 Action d'un groupe sur un ensemble	21
17 L'équation de classes	23
18 Le théorème de Cayley	24
19 Action d'un groupe sur soi-même par conjugaison	25
20 Les théorèmes de Sylow	26

1 Relation binaire et d'équivalence

Définition 1 (Relation binaire). Une relation binaire sur un ensemble X est un sous-ensemble $R \subseteq X \times X$. On écrit $x \sim y \iff (x, y) \in R$

Définition 2 (Relation d'équivalence). Une relation binaire est une relation d'équivalence si elle satisfait aux trois propriétés suivantes :

1. Réflexive si $x \sim x, \forall x \in X$
2. Symétrique si $x \sim y \implies y \sim x, \quad \forall x, y \in X$
3. Transitive si $x \sim y$ et $y \sim z \implies x \sim z, \quad \forall x, y, z \in X$

Définition 3 (Classe d'équivalence). SI un \sim est une relation d'équivalence sur X , la classe d'équivalence de $x \in X$ est donnée par

$$Cl(x) = \bar{x} = \{y \in X | y \sim x\}$$

Proposition 4. Soit \sim une relation d'équivalence sur X . On a

1. $Cl(x) = Cl(y) \iff x \sim y$
2. Si $Cl(x) \neq Cl(y) \implies Cl(x) \cap Cl(y) = \emptyset$
3. $X = \bigcup_{x \in X} Cl(x)$ Disjoint.

2 Groupes et propriétés

Définition 5 (Élément neutre). Un élément neutre pour une opération $*$ sur S est un élément $x \in S$ tel que $x * y = y * x = y \quad \forall y \in S$.

Définition 6 (Opération binaire). Une opération binaire sur un ensemble S est une application des éléments du produit cartésien $S \times S$ à S :

$$f : S \times S \longrightarrow S$$

Propriété(s) 7 (Commutativité). Une opération binaire $*$ sur un ensemble S est appelée *commutative* si :

$$x * y = y * x, \quad \forall x, y \in S$$

Propriété(s) 8 (Associativité). Une opération binaire $*$ sur un ensemble S est appelée *associative* si :

$$(x * y) * z = x * (y * z), \quad \forall x, y, z \in S$$

Propriété(s) 9 (Distributivité). Étant donné un ensemble S et deux opérations binaires $+$ et $*$ sur S , l'opération $*$:
est distributive à gauche sur $+$ si, pour tout $x, y, z \in S$,

$$x * (y + z) = (x * y) + (x * z)$$

est distributive à droite sur $+$ si, pour tout $x, y, z \in S$,

$$(y + z) * x = (y * x) + (z * x)$$

et est distributive sur $+$ si elle est distributive à gauche et à droite.

Remarque 10. Lorsque $*$ est commutatif, les trois conditions ci-dessus sont logiquement équivalentes.

Définition 11 (Groupe). Un groupe est un ensemble, G , muni d'une opération \cdot qui combine deux éléments quelconques a et b pour former un autre élément, noté, $a \cdot b$ ou ab . Pour se qualifier en tant que groupe, l'ensemble et l'opération, (G, \cdot) , doivent satisfaire quatre propriétés connues sous le nom d'axiomes de groupe :

- **Loi de composition interne**
Pour tous a et b éléments de G , le résultat $a \cdot b$ est aussi dans G .
- **Associativité**
- **Élément neutre**
- **Élement inverse (unique)**

Définition 12 (Demi-groupe). Un demi-groupe est une paire $(S, *)$ avec S un ensemble et $*$ une opération binaire associative.

Définition 13 (Monoïde). Un monoïde est un demi-groupe $(S, *)$ où l'opération interne possède qu'un seul élément neutre.

Définition 14 (Ordre). Soit $x \in G$. L'ordre de x est le plus petit $n \in \mathbb{Z}_{>0}$ tel que $x^n = 1$. Si aucun n n'existe, l'ordre de x est infini. On écrit $|x| = |x^{-1}| = \text{ord}(x)$.

Propriété(s) 15.

1. $|x| = |x^{-1}|$
2. $\text{ord}\{(g, h)\} = \text{lcm}[\text{ord}(g), \text{ord}(h)]$
3. Dans $(\mathbb{Z}/n\mathbb{Z}, +)$, $n \in \mathbb{Z}_{>0}$. Pour $a \in \{1, \dots, n-1\}$, on a

$$|\bar{a}| = \frac{\text{lcm}[a, n]}{a} = \frac{n}{\text{gcd}(a, n)}$$

Définition 16 (Cardinalité). Soit G un groupe. La cardinalité de G , noté $\text{card}(G)$, est le nombre d'éléments de G si G est fini. Sinon, $\text{card}(G) = \infty$.

Définition 17 (Groupe Diédral). Le groupe Diédral D_{2n} est le groupe de symétries du polygone régulier à n côtés $|D_{2n}| = 2n$.

Propriété(s) 18.

- | | |
|---------------------------------------|--|
| 1. $ r = n$ | 4. $sr^i \neq sr^j$, $0 \leq i \neq j \leq n-1$ |
| 2. $ s = 2$ | 5. $rs = sr^{-1}$ |
| 3. $s \neq r^i$, $0 \leq i \leq n-1$ | 6. $r^i s = sr^{-i}$ |

3 Groupes symétriques

Définition 19. Soit E un ensemble $\neq \emptyset$. Considérons

$$\mathbb{S}_E = \{\sigma : E \longrightarrow E \mid \sigma \text{ bijective}\}$$

Un tel σ est aussi appelé une permutation.

Définition 20. On dit que (\mathbb{S}_E, \circ) est le groupe symétrique sur E . On écrit $\mathbb{S}_n := \mathbb{S}_{\{1,2,3,\dots,n\}}$. On a $\text{card}(\mathbb{S}_n) = n!$.

Définition 21 (Conjugaison). La conjugaison de $\sigma = (x_1 x_2 \dots)$ par τ est donnée par

$$\tau\sigma\tau^{-1} = (\tau(x_1) \tau(x_2) \dots)$$

Deserve a title

Définition 22 (Algorithme d'Euclide).

$$\gcd(a, b) = r_n = r_{n-2} - q_n r_{n-1} = r_{n-2} - q_n(r_{n-3} - q_{n-1}r_{n-2}) = \cdots$$

Définition 23 (Élément de \mathbb{S} qui ont des inverses multiplicatifs).

$$(\mathbb{Z}/n\mathbb{Z})^* = \{\bar{a} \in \mathbb{Z}/n\mathbb{Z} : \exists \bar{x} \in \mathbb{Z}/n\mathbb{Z}, \bar{a}\bar{x} = \bar{1}\}$$

$((\mathbb{Z}/n\mathbb{Z})^*, \cdot)$ est un groupe Abélien

Théorème 24 (Théorème fondamental de l'arithmétique). Soit $n \in \mathbb{Z}_{>1}$, alors n est produit de nombres premiers p_n dont la décomposition est unique

$$n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_s^{\alpha_s}, \quad \alpha_n \in \mathbb{N}$$

Définition 25 (Fonction indicatrice d'Euler).

$$|(\mathbb{Z}/n\mathbb{Z})^*| = \varphi(n) = \#\{r \in \mathbb{N} : r \leq n \wedge \gcd(r, n) = 1\}$$

$$\varphi(p_1^{\alpha_1} \cdots p_k^{\alpha_k}) = \varphi(p_1^{\alpha_1}) \cdots \varphi(p_k^{\alpha_k}), \text{ où } \varphi(p^\alpha) = p^\alpha - p^{\alpha-1} = p^{\alpha-1}(p-1)$$

Remarque 26. Le nombre de générateurs de $(\mathbb{Z}/n\mathbb{Z}, +)$ est donné par $\varphi(n)$.

4 Corps et groupes de matrices

Définition 27 (Corps). Un corps est un ensemble \mathbb{F} avec deux opérations $+$ et \bullet telles que $(\mathbb{F}, +)$ et $(\mathbb{F} \setminus \{0\}, \bullet)$ sont des groupes abéliens et tels qu'on à la propriété distributive

$$a \bullet (b + c) = a \bullet b + a \bullet c$$

On écrit $\mathbb{F}^* = \mathbb{F} \setminus \{0\}$.

Remarque 28. En général, il y a des corps finis \mathbb{F}_q pour n'importe q puissance de p premiers.

Définition 29 (Goupes (général) linéaire).

$$GL(n, \mathbb{F}) = \{A | A \in \mathbb{M}_{n \times n} \wedge \forall i, j, \quad A_{ij} \in \mathbb{F} \wedge \det(A) \neq 0\}$$

Définition 30 (Groupe spécial linéaire).

$$SL(n, \mathbb{F}) = \{A | A \in \mathbb{M}_{n \times n} \wedge \forall i, j, \quad A_{ij} \in \mathbb{F} \wedge \det(A) = 1\}$$

Définition 31 (Groupe orthogonal).

$$O(n, \mathbb{F}) = \{A | A \in GL(n, \mathbb{F}) \wedge AA^T = A^T A = I\}$$

Définition 32 (Groupe spécial orthogonal).

$$SO(n, \mathbb{F}) = \{A | A \in O(n, \mathbb{F}) \wedge \det(A) = 1\}$$

5 Groupe des quaternions

Définition 33 (Quaternions). En termes de générateurs et de relations on a

$$\mathbb{Q}_8 = \langle i, j | i^4 = 1, i^2 = j^2, ij = -ji \rangle$$

6 Homomorphismes et isomorphismes

Définition 34 (Homomorphisme). Soit $(G, *)$ et $(H, \tilde{*})$ deux groupes. Un homomorphisme ou un morphisme (de groupe) est une application $\varphi : G \rightarrow H$ telle que

$$\varphi(g_1 * g_2) = \varphi(g_1) \tilde{*} \varphi(g_2) \quad \forall g_1, g_2 \in G$$

Définition 35 (Monomorphisme). Un monomorphisme est un homomorphisme injectif,

$$g_1 \neq g_2 \in G \implies \varphi(g_1) \neq \varphi(g_2) \in H$$

Définition 36 (Épimorphisme). Un épimorphisme est un homomorphisme surjectif,

$$\forall h \in H, \exists g \in G : \varphi(g) = h$$

Définition 37 (Isomorphisme). Un isomorphisme est un homomorphisme bijectif,

$$\forall h \in H, \exists! g \in G : \varphi(g) = h$$

Définition 38 (Endomorphisme). Un endomorphisme est un homomorphisme d'un groupe dans lui-même, $(G, *) = (H, \tilde{*})$

Définition 39 (Automorphisme). Un automorphisme est un endomorphisme bijectif. L'ensemble d'automorphisme est noté $\text{Aut}(G)$.

Proposition 40. Soit $\varphi : G \rightarrow H$ homomorphisme :

1. $\varphi(1_G) = 1_H$
2. $\varphi(g^{-1}) = \varphi(g)^{-1}, \quad \forall g \in G$
3. $\varphi(g^n) = \varphi(g)^n, \quad \forall n \in \mathbb{Z}$

Définition 41 (Noyau). Soit $\varphi : G \rightarrow H$ un homomorphisme. Le noyau de φ est

$$\text{Ker } \varphi = \{g \in G | \varphi(g) = 1_H\} \subset G$$

Définition 42 (Image). Soit $\varphi : G \rightarrow H$ un homomorphisme. L'image de φ est

$$\text{Im } \varphi = \{h \in H | \exists g \in G : \varphi(g) = h\} \subseteq H$$

Remarque 43 (Lemme). Soit $\varphi : G \rightarrow H$ un homomorphisme, alors φ monomorphisme si et seulement si $\text{Ker } \varphi = \{1_G\}$

Proposition 44. Soit $\varphi : G \xrightarrow{\sim} H$ un isomorphisme. Alors $G \simeq H$

1. $|G| = |H|$
2. G abélien $\iff H$ abélien
3. $\forall g \in G, \quad |g| = |\varphi(g)|$

Définition 45 (Matrice de permutation). Soit $L_\sigma \in \mathbb{M}_{n \times n}$ à coefficient réel défini comme

$$\begin{cases} 1, & \sigma(i) = j \\ 0, & \sigma(i) \neq j \end{cases}$$

L_σ est dite la matrice de permutation associée à σ . Si

$$e_1 = \begin{pmatrix} 1 \\ 0 \\ \vdots \\ 0 \end{pmatrix}, e_2 = \begin{pmatrix} 0 \\ 1 \\ \vdots \\ 0 \end{pmatrix}, \dots \implies L_\sigma e_i = e_{\sigma(i)}$$

Soit $P_n = \{L_\sigma | \sigma \in \mathbb{S}_n\}$, l'ensemble des matrices $n \times n$ ayant seul coefficient 1 dans chacune de ses lignes et ses colonnes (le reste des éléments étant des 0)

Remarque 46 (Lemme). Si $L \in P_n \implies \det(L) = \pm 1$

Définition 47 (Signe). Si $\sigma \in \mathbb{S}$, le signe de σ est $\text{sg}(\sigma) = \det(L_\sigma)$. On a $\text{sg}(\sigma) \text{sg}(\tau) = \text{sg}(\sigma \circ \tau)$ pour $\sigma, \tau \in \mathbb{S}$, car $L_{\sigma \circ \tau} = L_\sigma L_\tau$

Remarque 48 (Parité du signe). Le signe est un homomorphisme de groupes. Les permutations

$$\text{sg} : \mathbb{S}_n \longrightarrow (\{-1, 1\}, \bullet)$$

Si $\text{sg} = 1$ les permutations sont appelées paires sinon avec $\text{sg} = -1$ elles sont appelées impairs.

Définition 49 (Groupe alterné). Les permutations paires $\mathbb{A}_n = \{\sigma \in \mathbb{S}_n | \text{sg}(\sigma) = 1\}$ forment, avec la composition, le groupe alterné d'ordre n .

Remarque 50. C'est le noyau de l'homomorphisme $\text{sg} : \mathbb{S}_n \longrightarrow \mathbb{C}^*$. Tous les éléments de \mathbb{S}_n peuvent être écrit comme produit de 2-cycles (ou transpositions). Les éléments de \mathbb{A}_n sont exactement ceux qui ont un nombre pair de transpositions.

7 Sous-groupes

Définition 51 (Sous-groupes). Soit (G, \bullet) un groupe. On dit que $H \subset G$ est un sous-groupe de G si $H \neq \emptyset$ et si

1. $\forall h_1, h_2 \in H, \quad h_1 \bullet h_2 \in H$
2. $\forall h \in H, \quad h^{-1} \in H$

On écrit $H \leq G$ ou $H < G$ (sous-groupe propre où $H \neq G$)

Proposition 52. Soit H un sous-ensemble du groupe (G, \bullet) . Alors H est un sous-groupe si et seulement si :

1. $H \neq \emptyset$
2. $\forall h_1, h_2 \in H, \quad h_1 h_2^{-1} \in H$

Si $|H| < \infty$ il suffit de vérifier que $\forall h_1, h_2 \in H, \quad h_1 h_2 \in H \neq \emptyset$

Proposition 53.

- a) L'image $\text{Im } \varphi$ d'un homomorphisme de groupe $\varphi : K \longrightarrow G$ est un sous-groupe de G et le noyau $\text{Ker } \varphi$ est un sous-groupe de K
- b) Un sous-ensemble de $H \subset G$ d'un groupe G est un sous-groupe de G si et seulement si il existe un homomorphisme de groupes $\varphi : K \longrightarrow G$ tel que $H = \text{Im } \varphi$.

8 Groupes et sous-groupes cycliques

Définition 54 (Groupe cyclique). Un groupe H est dit cyclique si H est engendré par un seul élément, c.-à-d., $H = \{h^\ell | \ell \in \mathbb{Z}\}$

Propriété(s) 55. Si $H = \{h^\ell | \ell \in \mathbb{Z}\}$, alors $|H| = |h|$
Si $|h| = \ell$, alors $1 \neq h \neq h^2 \neq \dots \neq h^\ell$, sinon

$$\begin{aligned} 0 &\leq a < b < \ell \\ h^a &= h^b \\ \implies 1 &= h^{b-a} \\ \ell &\leq b - a \Rightarrow \Leftarrow \end{aligned}$$

Si $|h| = \infty$, alors $h^a \neq h^b$ si $a \neq b$

Proposition 56. Soit G un groupe, $g \in G$, $m, n \in \mathbb{Z} : g^n = 1g^m \implies g^{\gcd(m,n)} = 1$. Alors, si $g^m = 1 \implies |g|$ divise m .

Théorème 57. Deux groupes cycliques du même ordre sont isomorphes.

On dénote C_n ou Z_n le groupe cyclique d'ordre n avec la multiplication (engendré par g).

Proposition 58. Soit G un groupe $g \in G$, $a \in \mathbb{Z} \setminus \{0\}$

1. $|g| = \infty \implies |g^a| = \infty$
2. $|g| = n < \infty \implies |g^a| = \frac{n}{\gcd(n,a)}$
3. $|g| = n < \infty \wedge a|n \wedge a > 0 \implies |g^a| = \frac{n}{a}$

Proposition 59. Soit $G = \langle g \rangle = \{g^k | k \in \mathbb{Z}\}$ cyclique, on a

1. Si $|g| = \infty$, alors $G = \langle g^a \rangle \iff a = \pm 1$
2. Si $|g| = \ell < \infty$, alors $G = \langle g^a \rangle \iff \gcd(a, \ell) = 1$

Théorème 60. Soit $G = \langle g \rangle$ cyclique, on a

1. Si $H \leq G$, alors $H = \{1\}$ ou $H = \langle g^d \rangle$
2. Si $|G| = \infty$, $a, b \in \mathbb{Z}_{>0} : a \neq b$, alors $\langle g^a \rangle \neq \langle g^b \rangle$
3. Si $|G| = n$, $\forall a > 0 : a|n$, alors il y a un seul $H \leq G$ avec $|H| = a$. En plus, $H = \langle g^d \rangle$ où $d = \frac{n}{a}$

9 Centralisateur et normalisateur

Définition 61 (Centre d'un groupe). Soit G un groupe. Le centre de G est donné par

$$Z(G) = \{g \in G \mid \forall x \in G, gx = xg\}$$

Définition 62 (Centralisateur). Soit G un groupe et $A \subseteq G$ un sous-ensemble. Le centralisateur de A en G est donné par

$$C_G(A) = \{g \in G \mid \forall a \in A, ga = ag\}$$

Remarque 63. $Z(G) = C_G(G)$

Proposition 64. $C_G(A) \leq G$

Si $A = \{a\}$, on écrit $C_G(a)$. On a que $\forall n \in \mathbb{Z}, a^n \in C_G(a)$.

Définition 65. Soit $gAg^{-1} = \{gag^{-1} \mid a \in A\}$

Proposition 66. Si $gAg^{-1} \subseteq A$, alors $gAg^{-1} = A$.

Définition 67 (Normalisateur). Soit G un groupe et $A \subseteq G$ un sous-ensemble. Le normalisateur de A en G est donné par

$$N_G(A) = \{g \in G \mid gAg^{-1} = A\}$$

Proposition 68. $N_G \leq G$

10 Sous-groupe engendré par un sous-ensemble

Lemme 69. Soit G un groupe. L'intersection d'une famille quelconque de sous-groupe de G est aussi un sous-groupe de G .

Définition 70. Soit G un groupe et soit $S \subseteq G$ un sous-ensemble. Le sous-groupe engendré par S est le plus petit sous-groupe de G qui contient S . Il est l'intersection de tous les sous-groupes $H \leq G$ contenant S . On écrit $\langle S \rangle$, les éléments de S sont des générateurs de H .

Proposition 71.

$$\forall x \in \langle S \rangle, x = \prod_{i=1}^n s_i, \text{ où } s_i, s_i^{-1} \in S$$

Théorème 72.

$$\mathbb{A}_n = \langle \{3\text{-cycles}\} \rangle, \quad n \geq 3$$

Théorème 73.

$$\mathbb{S}_n = \langle (i, i+1) \rangle, \quad i = 1, \dots, n-1$$

Théorème 74.

$$\mathbb{S}_n = \langle (1, 2), (1, 2, 3, \dots, n) \rangle$$

11 Treillis des sous-groupes

Définition 75 (Commutateur). Soit G un groupe et $x, y \in G$. Le commutateur de la paire (x, y) est l'élément $[x, y] = xyx^{-1}y^{-1} \in G$

Définition 76 (Sous-groupe dérivé). Le sous-groupe dérivé de G est $[G, G] := \langle S \rangle$ (aussi noté G').

Remarque 77. On dit que G est résoluble si $G^{(n)} = \{1\}$ pour un certain $n \in \mathbb{Z}$. On peut écrire

$$1 = G^{(n)} \subseteq \cdots \subseteq G'' \subseteq G' \subseteq G$$

Lemme 78. Pour chaque homomorphisme $\varphi : G \longrightarrow A$ où A est abélien, on a $G' \subseteq \text{Ker } \varphi$

Proposition 79.

1. $[\mathbb{S}_n, \mathbb{S}_n] = \mathbb{A}_n$
2. $[\mathbb{A}_n, \mathbb{A}_n] = \{1\}$ si $1 \leq n \leq 3$

Remarque 80.

$$[\mathbb{A}_4, \mathbb{A}_4] = V_4$$

$$[\mathbb{A}_n, \mathbb{A}_n] = \mathbb{A}_n \text{ si } n \geq 5$$

Corollaire 81. \mathbb{S}_n est résoluble si, et seulement si $n \leq 4$.

Remarque 82. Le fait que \mathbb{S}_n ne soit pas résoluble pour $n \geq 5$ est relié au fait qu'il n'y a pas de formule pour les racines du polynôme général de degré $n \geq 5$.

12 Groupe quotient

Définition 83 (Translaté gauche/droite). Soit G un groupe, $H \leq G$ et $g \in G$. Les ensembles $gH = \{gh \mid h \in H\}$ et $Hg = \{hg \mid h \in H\}$ s'appellent les translatés à gauche et à droite de H .

Définition 84 (Groupe normal). Soit G un groupe. Si $a, b \in G$, aba^{-1} s'appelle conjugué de b . Si $H \leq G$, on dit que H est normal si $gHg^{-1} = H$, $\forall g \in G$ si, et seulement si $N_G(H) = G$ si, et seulement si $gH = Hg$, $\forall g \in G$. On note alors, $H \trianglelefteq G$.

Définition 85. Soit $H \leq G$ et soit $G/H = \{gH \mid g \in G\}$. Alors, gH est un sous-ensemble de G et aussi un élément de G/H .

Théorème 86. Soit (G, \circ) un groupe et $H \leq G$. Les propositions suivantes sont équivalentes :

- i) $\forall g, k \in G$, $g \circ H \circ k \circ H = (g \circ k) \circ H$
- ii) Il existe une opération interne $*$ sur l'ensemble G/H , pour laquelle $(G/H, *)$ est un groupe et pour laquelle l'application $\nu_H : G \longrightarrow G/H$ tel que $\nu_H(g) = gH$ est un épimorphisme.
- iii) Il existe un groupe K et un homomorphisme $\phi : G \longrightarrow K$ tel que $H = \text{Ker } \phi$
- iv) On a $\forall g \in G \wedge \forall h \in H$, $g \circ h \circ g^{-1} \in H$ (normal)
- v) $\forall g \in G$, $g \circ H = H \circ g$ comme sous-ensembles

Définition 87 (Groupe simple). Un groupe G est simple si les seules sous-groupes normaux sont G et $\{1_G\}$.

13 Le théorème de Lagrange

Lemme 88. Soit $H \leq G$ un sous-groupe d'un groupe (G, \cdot) . Alors, chaque élément de G est contenu dans un seul translaté à gauche de H et dans un seul translaté à droite de H . Si deux translatés à gauche sont différents, l'intersection est vide. Il y a une bijection entre H et gH .

Théorème 89 (Théorème de Lagrange). Soit G un groupe fini et soit $H \leq G$. Alors, $|H|$ divise $|G|$. En plus, le nombre de translatés à gauche de H est $\frac{|G|}{|H|}$.

Définition 90 (Indice). Soit G un groupe, $H \leq G$. Le nombre de translatés à gauche s'appelle l'indice de H dans G , noté $[G : H]$. Alors, $[G : H] = \frac{|G|}{|H|}$ si $|G| < \infty$.

Corollaire 91. Si $x \in G$ et $|G| < \infty$, alors $|x|$ divise $|G|$. En particulier $x^{|G|} = 1$.

Corollaire 92. Si G est un groupe et $|G| = p$ avec p premier, alors G est cyclique et $G \simeq \mathbb{Z}/p\mathbb{Z}$.

Résultat

- $G/Z(G)$ cyclique $\implies G$ abélien
- G/G' abéliens, (G abélien si, et seulement si, $G' = \{1\}$)
- $H \leq G, [G : H] = 2 \implies H \trianglelefteq G$

Proposition 93. Soit A un groupe abélien fini. Soit m le plus grand ordre d'un élément de A :

$$\forall a \in A, |a| \mid m$$

Proposition 94. Soit $P(x) = a_0 + a_1x^2 + \cdots + a_nx^n$ un polynôme de degré n avec $a_i \in \mathbb{F}$ corps, et supposons $a_n \neq 0$. Alors P a au plus n racines, c'est-à-dire, il existe au plus n éléments différents $\alpha_1, \dots, \alpha_n \in \mathbb{F}$ tel que $P(\alpha_i) = 0$

Proposition 95. Chaque sous-groupe fini H du groupe multiplicatif \mathbb{F}^\times d'un corps est cyclique.

Définition 96. Soit $H, K \leq G$ avec G un groupe. On écrit $HK = \{hk \mid h \in H, k \in K\}$.

Proposition 97. Soit G un groupe, $H, K \leq G$. Si $|H|, |K| \leq \infty$, alors

$$|HK| = \frac{|H||K|}{|H \cap K|}$$

Proposition 98. $H, K \leq G$, alors $HK \leq G \iff HK = KH$

14 Les théorèmes d'isomorphisme

Théorème 99 (Premier théorème d'isomorphisme). Si $\varphi : G \rightarrow H$ est un homomorphisme de groupes, alors, $\text{Ker } \varphi \trianglelefteq G$ et $G / \text{Ker } \varphi \simeq \varphi(G)$.

Corollaire 100. $[G : \text{Ker } \varphi] = |\varphi(G)|$

Théorème 101 (Deuxième théorème d'isomorphisme). Soit G un groupe, $A, B \leq G$ tel que $A \leq N_G(B)$. Alors $AB \leq G$, $B \trianglelefteq AB$, $A \cap B \trianglelefteq A$ et $A / _{A \cap B} \simeq AB / B$.

$$\frac{|AB|}{|B|} = \frac{|A|}{|A \cap B|}$$

Théorème 102 (Troisième théorème d'isomorphisme). Soit G un groupe, $A, B \trianglelefteq G$ avec $A \leq B$. Alors, $A \trianglelefteq B$, $B/A \trianglelefteq G/A$ et $G/A / B/A \simeq G/B$

Théorème 103 (Théorème de correspondance). Soit $N \trianglelefteq G$ il y a une correspondance entre les sous-groupes A de G qui contiennent N et les sous-groupes A/N de G/N . En particulier, si $A, B \leq G$ avec $N \leq A, N \leq B$

1. $A \leq B \iff A/N \leq B/N$
2. $A \leq B \implies [B : A] = [B/N : A/N]$
3. $\langle A, B \rangle / N = \langle A/N, B/N \rangle$
4. $(A \cap B) / N = A/N \cap B/N$
5. $A \trianglelefteq G \iff A/N \trianglelefteq G/N$

Théorème 104 (Théorème fondamental des homomorphismes). Soit $\varphi : G \rightarrow H$ un homomorphisme et soit $\psi : G \rightarrow K$ un épimorphisme, alors

- i) Il existe $\rho : K \rightarrow H$ homomorphisme tel que $\rho \circ \psi = \varphi \iff \text{Ker } \psi \subseteq \text{Ker } \varphi$
- ii) Si ρ existe, il est unique
- iii) $\text{Im}(\rho) = \text{Im}(\varphi)$ alors, ρ épimorphisme $\iff \varphi$ épimorphisme
- iv) $\psi(\text{Ker}(\varphi)) = \text{Ker}(\rho)$ alors, ρ monomorphisme $\iff \text{Ker } \psi = \text{Ker } \varphi$

$$\begin{array}{ccc} G & \xrightarrow{\varphi} & H \\ \psi \downarrow & \nearrow \dashv \rho & \\ K & & \end{array}$$

15 Théorème de Jordan-Hölder

Définition 105 (Groupe maximal). Un groupe G est simple si les sous-groupes normaux sont $\{1\}$ et G . Un sous-groupe $H \trianglelefteq G$ est dit maximal si $H \neq G$ et s'il n'y a pas de sous-groupe normal $K \trianglelefteq G$ tel que $H \not\leq K \neq G$. Donc $H \trianglelefteq G$ maximal $\iff H \neq G$, et G/H simple

Définition 106 (Suite de décomposition). Si G un groupe fini, alors il contient un sous-groupe normal maximal G_1 . Si $G_1 \neq \{1\}$, alors il contient un sous-groupe normal maximal G_2 , etc. Une suite de décomposition (ou suite de Jordan-Hölder) de G est

$$\{1\} = G_s \trianglelefteq G_{s-1} \trianglelefteq \cdots \trianglelefteq G_2 \trianglelefteq G_1 \trianglelefteq G_0 = G, \quad \text{avec } G_{i-1}/G_i \text{ simple}$$

Théorème 107 (Théorème de Jordan-Hölder). Soit G un groupe fini et soient

$$\begin{aligned} \{1\} &= G_s \trianglelefteq G_{s-1} \trianglelefteq \cdots \trianglelefteq G_2 \trianglelefteq G_1 \trianglelefteq G_0 = G \\ \{1\} &= K_t \trianglelefteq K_{t-1} \trianglelefteq \cdots \trianglelefteq K_2 \trianglelefteq K_1 \trianglelefteq K_0 = K \end{aligned}$$

deux suites de décomposition (G_{i-1}/G_i et K_{i-1}/K_i simples $\forall i$). Alors $s = t$ et il existe une permutation $\pi \in \mathbb{S}$ telle que

$$G_{i-1}/G_i \simeq K_{\pi(i)-1}/G_{\pi(i)} \quad 1 \leq i \leq s$$

Lemme 108. Soit G un groupe, $H, K \trianglelefteq G$. Supposons que $K \not\leq H$ et que H est maximal. Alors $(K \cap H) \trianglelefteq K$ est maximal et

$$K/(K \cap H) \simeq G/H$$

16 Action d'un groupe sur un ensemble

Définition 109 (*G-action*). Soit $(G, *)$ un groupe et X un ensemble. Une *G-action* (ou action de G ou une *G-opération*) sur X est une application

$$\begin{aligned}\circ : G \times X &\longrightarrow X \\ (g, x) &\longmapsto g \circ x\end{aligned}$$

qui satisfait les deux conditions suivantes :

1. $1_G \circ x = x$
2. $(g_1 * g_2) \circ x = g_1 \circ (g_2 \circ x)$

On dit aussi que (X, \circ) est un *G-ensemble*. (Action de groupe par G sur X)

Définition 110 (*Sous-G-ensemble*). Un *sous-G-ensemble* de X est un $Y \subseteq X$ tel que $\forall y, \forall g \in G, g \circ y \in Y$.

Définition 111 (Orbite). Un *sous-G-ensemble* non-vide de X qui ne contient pas de *sous-G-ensemble* propre non-vide s'appelle une orbite. L'orbite de $x \in X$ est $\text{Orb}(x) = O_x = G \circ x = \{g \circ x | g \in G\} \subseteq X$. On dit qu'une action est transitive si elle a une seule orbite, $O_x = X$.

Notation

$$\boxed{\text{Orb}(x) \longleftrightarrow O_x \longleftrightarrow G \circ x}$$

Définition 112 (Stabilisateur). Le stabilisateur de $x \in X$ est

$$\text{Stab}(x) = G_x = \{g \in G | g \circ x = x\} \leq G (\subseteq G).$$

Notation

$$\boxed{\text{Stab}_G(x) \longleftrightarrow \text{Stab}(x) \longleftrightarrow G_x}$$

Définition 113 (Noyau*). Le noyau de l'opération est

$$G_X = \{g \in G | g \circ x = x, \forall x \in X\} \trianglelefteq G (\subseteq G).$$

Définition 114 (Action fidèle). On dit qu'une action est fidèle si $G_X = \{1\}$.

Définition 115 (Point fixe). Un élément $x \in X$ est appelé un point fixe pour l'action de G sur X si $\forall g \in G, g \circ x = x$. On écrit

$$X^G = \{x \in X | \forall g \in G, g \circ x = x\} \subseteq X$$

Remarque 116. On voit que $|O_x| = 1 \iff x \in X^G$. Une orbite contient seulement un élément x si et seulement si x est un point fixe.

Définition 117 (L'ensemble de *G-orbite*). L'ensemble des *G-orbites* de X est dénoté par X/G (les orbites sont disjointes)

Théorème 118 (Théorème fondamental des actions). Soit $(G, *)$ un groupe et (X, \circ) un G -ensemble.

1. X est la réunion (union) disjointe de ses G -orbites
2. Chaque $x \in X$ est contenu dans une unique G -orbite
3. Il existe une bijection $O_x \longrightarrow G/G_x$ (quotient de G par $\text{Stab}(x)$)

17 L'équation de classes

Théorème 119 (Équation de classes). Soit X un G -ensemble fini. Alors,

$$|X| = \sum_{O \in X/G} |O| = |X^G| + \sum_{\substack{O \in X/G \\ |O| > 1}} |O|$$

où X^G est l'ensemble de points fixes. Soit $O \in X/G$ et $x \in O$ ($O_x = O$). Alors $|O| = [G : \text{Stab}(x)]$. En particulier, la cardinalité de chaque orbite est un diviseur de l'ordre du groupe.

Lemme 120. Soit G un groupe fini et p le plus petit diviseur premier de $|G| \neq 1$. Soit X un G -ensemble. Si x n'est pas un point fixe, alors $|O_x| \geq p$. En particulier, si $X \setminus X^G$ (i.e. $X - X^G$) à moins que p éléments, alors G agit trivialement, $X = X^G$.

Lemme 121. Soit p un nombre premier et P un groupe d'ordre p^r . Soit X un P -ensemble fini. Alors $|X| - |X^P|$ est divisible par p . En particulier, si $p \nmid |X|$, alors il existe un point fixe $x \in X^P$.

18 Le théorème de Cayley

Soit G un groupe qui agit sur lui-même par multiplication à gauche. Cela donne une action transitive, fidèle, avec stabilisateur trivial.

Soit $H \leq G$. Alors G agit sur G/H par

$$g \circ (aH) \quad g \in G, aH \in G/H$$

Théorème 122. Soit G un groupe $H \leq G$ avec l'action ci-dessus.

1. L'action est transitive
2. $\text{Stab}(1H) = H$
3. Le noyau de l'action est $\bigcap_{x \in G} xHx^{-1}$, le plus grand sous-groupe normal de G contenu dans H

Corollaire 123 (Théorème de Cayley). Tout groupe est isomorphe à un sous-groupe du groupe symétrique. Si G est un groupe fini d'ordre n , alors G est isomorphe à un sous-groupe de \mathbb{S}_n .

Corollaire 124. Soit G un groupe fini $|G| = n$ et soit p le plus petit premier qui divise n . Si $H \leq G$, $[G : H] = p$, alors $H \trianglelefteq G$.

19 Action d'un groupe sur soi-même par conjugaison

Définition 125 (Classes de conjugaison). Les orbites de l'action par conjugaison s'appellent classes de conjugaison.

Théorème 126 (Équation de classes avec conjugaison).

$$|G| = |Z(G)| + \sum_{i=1}^r [G : C_G(g_i)]$$

où g_1, \dots, g_r sont les représentants des classes de conjugaison différentes.

Théorème 127. Soit p premier et G un groupe tel que $|G| = p^r, r \in \mathbb{Z}_{>0}$. Alors, $Z(G) \neq 1$.

Corollaire 128. Si $|G| = p^2$ avec p premier, alors G est abélien et $G \simeq C_{p^2}$ ou $G \simeq C_p \times C_p$

Définition 129 (Type de décomposition et partition).

1. Si $\sigma \in \mathbb{S}, \sigma = c_1 c_2 \cdots c_k$ cycles disjoints avec c_i des n_i -cycle (incluant les 1-cycles) et $n_1 \leq n_2 \leq \cdots \leq n_k$. On dit que σ a un type de décomposition n_1, n_2, \dots, n_k .
2. Si $n \in \mathbb{N}$, une partition de n est une suite $n_1 \leq n_2 \leq \cdots \leq n_k$ telle que $n = n_1 + n_2 + \cdots + n_k$.

Proposition 130. Soient $\sigma, \tau \in \mathbb{S}_n$ sont conjugués si, et seulement si, ils ont le même type de décomposition. On a donc que le nombre de classes de conjugaison est égal au nombre de partitions de n .

Théorème 131 (Théorème de Cauchy). Soit G un groupe fini et soit p premier tel que $p \mid \text{ord}(G)$. Alors, G contiens un élément d'ordre p .

Définition 132 (Produits semi-directs). Soit G, N deux groupes et soit $\phi : G \longrightarrow \text{Aut}(N)$ un homomorphisme. ($\text{Aut}(N)$ est le groupe d'automorphismes de N). Le produit semi-direct $N \rtimes_\phi G$ est donné par $N \times G$ comme ensemble, avec opération $(n_1, g_1) * (n_2, g_2) = (n_1 \cdot \phi(g_1)(n_2), g_1 g_2)$.

Lemme 133. $N \rtimes_\phi G$ est un groupe.

Proposition 134. Soit G un groupe avec $H \trianglelefteq G, K \leq G, H \cap K = \{1\}$ et $HK = G$. Soit $\phi : K \longrightarrow \text{Aut}(H), \phi(k)(h) = khk^{-1}$. Alors $G \simeq H \rtimes_\phi K$.

Proposition 135. Soit G un groupe d'ordre pq , où $p < q$ sont deux nombres premiers. Alors, il existe un homomorphisme $\phi : C_p \longrightarrow \text{Aut } C_q$ tel que $g \simeq C_q \rtimes_\phi C_p$. Si G est abélien, alors G est cyclique. Si $p \nmid q - 1$ alors G est abélien.

20 Les théorèmes de Sylow

Vocabulaire

Si G est un groupe d'ordre fini, un *p-sous-groupe* est un sous-groupe d'ordre p^ℓ et un *p-Sylow* est un sous-groupe d'ordre p^n : $p^n \mid \text{card}(G) \implies p^{n+1} \nmid \text{card}(G)$. Les *3-sous-groupes* sont sous-groupe de *3-Sylow*, mais les *3-sous-groupes* ne sont pas forcément sous-groupe de *5-Sylow*.

Définition 136 (*p-Sylow*). Soit G un groupe d'ordre p^sm , $p \nmid m$ avec p premiers. Un sous-groupe d'ordre p^s est appelé un *p-sous-groupe-de-Sylow* ou *p-Sylow*. Si $s > 1$, alors les sous-groupes d'ordre p^ℓ avec $\ell \leq s$ sont appelés les *p-sous-groupes*.

Théorème 137. Soit $|G| = p^sm$ avec $p \nmid m$,

1. Il existe un *p-Sylow* sous-groupe.
2. Si P est un *p-Sylow* sous-groupe et Q est un *p-sous-groupe*, alors $\exists g : Q \leq gPg^{-1}$. Tous les *p-Sylow* de G sont conjugués entre eux, c'est-à-dire que si H et K sont deux *p-Sylow* de G , alors il existe un élément g dans G vérifiant $gHg^{-1} = K$.
3. Le nombre de *p-Sylow* sous-groupes n_p satisfait $n_p \equiv 1 \pmod{p}$. Si P est un *p-Sylow* sous-groupe, $n_p = [G : N_G(P)]$, donc $n_p \mid m$.

Lemme 138. Soit G un *p-sous-groupe* et X un *G-ensemble*. Alors $|X| \equiv |X^G| \pmod{p}$.

Corollaire 139. Soit G un groupe, P un *p-Sylow* sous-groupe. Les énoncés suivants sont équivalents

1. $n_p = 1$
2. $P \trianglelefteq G$

Si G est un groupe d'ordre fini ayant un sous-groupe normal, alors n'est pas un groupe simple.