Algèbre 1

Gaëtan Chenevier

4 novembre 2023

Table des matières

1 Ensembles Quotients

1.1 Partitions et Relations d'Equivalence

Définition 1.1.1. *Une* partition *d'un ensemble X est un ensemble de parties non vides de X de réunion disjointe X.*

Définition 1.1.2. *On appelle* fibre *d'une application $f : X \to Y$ en $y \in Y$ l'ensemble $f^{-1}(y) = \{x \in X \mid f(x) = y\}$. Il s'agit d'une partition de X indexée par Y. Toute partition de X s'obtient ainsi.*

Définition 1.1.3. *Une* relation d'arité n *sur un ensemble X est la donnée d'un ensemble $R \subseteq X^n$. Une relation binaire R i.e. une partie de $X \times X$ est dite d'*équivalence *si elle est réflexive, transitive et symétrique. On appelle* classe de R-équivalence *de x l'ensemble $[x]_R = \{y \in X \mid \{x, y\} \in R\}$*

Proposition 1.1.1. *Les classes d'équivalences d'une relation R sur X forment une partition de X.*

Définition 1.1.4. *Si R est une relation d'équivalence sur X, le sous-ensemble de $P(X)$ constitué des classes de R-équivalence est appelé* ensemble quotient *de X par R, noté X/R. L'application $\pi_R : X \to X/R, x \mapsto [x]_R$ est appelée* projection canonique *associée à R. C'est une surjection dont les fibres sont par définition les classes d'équivalences de R.*

Exemple 1.1. *On définit $\mathbb{Z}/n\mathbb{Z}$ l'ensemble quotient de $\mathbb{Z}$ pour la relation $n \mid b - a$. On note $\overline{k}$ la classe de k.*

1.2 Passage au Quotient

Théorème 1.2.1 (Propriété Universelle du Quotient)**.** *Soient $f : X \to Y$ une application et R une relation d'équivalence sur X. On suppose que f est constante sur chaque classe d'équivalence sur X. Alors, il existe une unique application $g : X/R \to Y$ telle que $g([x]_R) = f(x)$ pour tout $x \in X$, i.e. vérifiant $g \circ \pi_R = f$.*

Démonstration. Par surjectivité de π_R, g est unique. De plus, si C est une classe de R-équivalence, il y a un sens à poser $g(C) = f(x)$ car C est une classe d'équivalence sur laquelle f est constante. ■

1.3 Sections et systèmes de représentants

Définition 1.3.1. *Une* section *de $f : X \to Y$ est une application $s : Y \to X$ telle que $f \circ s = id_Y$*

Proposition 1.3.1. *f possède une section $\Rightarrow$ f est surjective*

Définition 1.3.2 (Axiome du Choix)**.** *Pour tout ensemble X il existe une application $\tau : P(X) \setminus \{\varnothing\} \to X$ telle que $\tau(E) \in E$ pour toute partie non vide E de X. On appelle τ fonction de choix sur X.*

Proposition 1.3.2. *Les propositions suivantes sont équivalentes à l'axiome du choix (donc fausses) :*

1. *Toute surjection admet une section.*
2. *Pour toute famille d'ensembles non vides $\{X_i\}_{i \in I}$, $\pi_{i \in I} X_i$ est non vide.*

Définition 1.3.3. *Un* représentant *d'une classe de R-équivalence d'un ensemble X est un élément de cette classe. Un* système de réprésentants *de (X, R) est la donnée d'une partie de X contenant un et un seul représentant de chaque classe de R-équivalence. C'est l'image d'une section de π_R.*

Remarque 1.3.0.1. *Ceci est également équivalent à 1.3.2*

1.4 Lemme de Zorn

Définition 1.4.1. — *Un* relation d'ordre *sur un ensemble X est une relation binaire $\leq$ réfléxive, transitive et antisymétrique. On dit alors que X est ordonné.*

— *L'ordre $\leq$ est total quand tous deux éléments de X sont comparables.*

— *On appelle majorant d'une partie Y de X, tout élément $x \in X$ tel que $y \leq x$ pour tout $y \in Y$. On parle de plus grand élément dans le cas $Y = X$.*

— *$x \in X$ est un élément maximal si le seul $y \in X$ tel que $y \leq x$ est x. Un plus grand élément est nécessairement maximal, et unique s'il existe.*

— *On appelle X inductif si tout sous-ensemble totalement ordonné admet et majorant.*

— *On appelle bon ordre un ordre pour lequel toute partie non vide admet un plus petit élément.*

Théorème 1.4.1 (Lemme de Zorn)**.** *Un ensemble ordonné inductif possède au moins un élément maximal. Ceci est équivalent à l'axiome du choix 1.3.2.*

Corollaire 1.4.1.1. *Tout espace vectoriel possède une base.*

Corollaire 1.4.1.2 (Théorème de Zermelo)**.** *Tout ensemble peut être muni d'un bon ordre.*

Démonstration. C'est équivalent à l'axiome du choix donc faux et les preuves prennent trois plombes. ■

2 Généralités sur les Groupes

2.1 Exemples de Groupes

Définition 2.1.1. *Une* loi de composition interne *est une application* $\star : X \times X \to X$.

Définition 2.1.2 (Groupe)**.** *Un groupe est un ensemble* G *muni d'une loi de composition associative, unifère et inversible, i.e. :*

1. $\forall\ (x, y, z) \in G,\ x \star (y \star z) = (x \star y) \star z$
2. $\exists\ e \in G,\ \forall x \in G,\ e \star x = x \star e = x.$
3. $\forall x \in G,\ \exists y \in G,\ x \star y = y \star x = e$

Remarque 2.1.0.1. *Le neutre est unique.*

Exemple 2.1 (Groupe Symétrique)**.** *On note :* $\mathfrak{S}_X = X^X$ *le groupe muni de la loi* $\circ$ *de composition des applications, appelé* groupe symétrique *de* X*, de neutre* id_X*. L'inverse d'une bijection* σ *est sa bijection réciproque* σ^{-1}*. On note* $\mathfrak{S}_n = |1, n|^{|1,n|}$ *et alors* $|\mathfrak{S}_n| = n!$.

Définition 2.1.3. *Un groupe est dit* abélien *lorsque tous deux élements commutent.*

Définition 2.1.4. *Une partie* H *d'un groupe* G *est un* sous-groupe *de* G *lorsque la loi induite par le produit dans* G *fait de* H *un groupe. On le notera ici* $H \leq G$.

Exemple 2.2 (Groupes d'ordre n)**.** *Pour* $n \geq 1$*, on note* μ_n *le sous-groupe de* $\mathbb{C}^\times$ *composé des racines* n*-ièmes de l'unité. C'est un sous-groupe d'ordre* n*. L'application* $\mathbb{Z}/n\mathbb{Z} \to \mu_n, \overline{k} \mapsto e^{2ik\pi/n}$ *est un isomorphisme de groupe.*

Définition 2.1.5. *Un* anneau *est un groupe abélien* $(A, +)$ *muni d'une loi associative unifère et distributive sur* $+$*, notée* $\times$*. Il est dit commutatif lorsque la loi produit est commutative.*

Définition 2.1.6. *On note* $A^\times$ *le groupe des inversibles du monoïde* $(A, \cdot)$.

Proposition 2.1.1. *La loi d'un groupe vérifie les propriété de la loi produit usuelle sur* $\mathbb{R}$.

Définition 2.1.7. *On appelle groupe engendrée par une partie* X *de* G *le plus petit sous groupe de* G *contenant* X*. C'est l'ensemble des produits de puissances d'éléments de* X.

2.2 Morphismes

Définition 2.2.1. *On appelle* morphisme *une application entre deux groupes qui préserve le produit. On note* $Hom(G, G')$ *l'ensemble des morphismes de* G *dans* G'*. Ce n'est à priori pas naturellement un groupe si* G' *n'est pas abélien.*
On dit que G *et* G' *sont isomorphes lorsqu'il existe un morphisme bijectif de l'un vers l'autre. La réciproque d'un isomorphisme est un isomorphisme. On note alors* $G \simeq G'$.

Proposition 2.2.1 (Transport de Structure)**.** *Si* G *est un groupe,* $\varphi : X \to G$ *une bijection, il existe une unique loi de groupe sur* X *telle que* φ *soit un isomorphisme, à savoir* $x \star y = \varphi^{-1}(\varphi(x)\varphi(y))$*. On dit que la loi est* déduite *de celle de* G *par transport de structure via* φ.

Définition 2.2.2. *On appelle* automorphisme *de* G *un isomorphisme de* G *dans* G*. L'ensemble des automorphismes* $Aut(G)$ *est un sous groupe de* S_G*. On appelle automorphisme intérieur associé à* $g \in G$ *l'application :* $h \in G \mapsto ghh^{-1}$.

Définition 2.2.3. *On appelle* noyau *d'un morphisme* $\ker(f) = f^{-1}(1) = \{g \in G \mid f(g) = 1\}$*. C'est un sous-groupe de* G.

Proposition 2.2.2. *Si* $f \in Hom(G, G')$ *:*

1. $H \leq G \Rightarrow f(H) \leq G'$
2. $H \leq G' \Rightarrow f^{-1}(H) \leq G$ *Avec* $\mathcal{A}$ *l'ensemble des sous-groupes de* G *contenant* $\ker f$ *et* $\mathcal{B}$ *celui des sous-groupes de* G' *inclus dans* Imf*, alors :*

3. $\mathcal{A} \to \mathcal{B}, H \mapsto f(H)$ *est une bijection croissante.*

Proposition 2.2.3. *Les fibres non vides de* f *sont en bijection avec* $\ker f$*. En particulier :*

— f *injective* $\Leftrightarrow \ker f = \{1\}$.

— *Si* G *est fini,* $|G| = |Im\ f|\,|\ker f|$.

Théorème 2.2.1 (Cayley)**.** *Tout groupe d'ordre fini* n *est isomorphe à un sous-groupe de* S_n.

Lemme 2.2.2. *Si* $\varphi : X \to Y$ *est bijective, l'application :* $\varphi_{X,Y} : S_X \to S_Y, \sigma \mapsto \varphi \circ \sigma \circ \varphi^{-1}$ *est un isomorphisme de groupes.*

Définition 2.2.4. *Un morphisme d'anneau est un morphisme des groupes additifs et des monoïdes multiplicatifs (en particulier, il envoie* 1 *sur* 1*).*

2.3 Groupes Cycliques et Monogènes

Proposition 2.3.1. *Les sous-groupes de* $\mathbb{Z}$ *sont les* $n\mathbb{Z}$.

Proposition 2.3.2. *Si* $g \in G$ *est d'ordre fini* n*, alors* $\langle g \rangle$ *a exactement* n *éléments et est isomorphe à* $\mathbb{Z}/n\mathbb{Z}$.

Définition 2.3.1. *Un groupe* G *est* monogène *s'il est engendré par un seul élément, appelé* générateur*. Il est* cyclique *s'il est fini.*

Corollaire 2.3.0.1. *Un groupe* G *est monogène infini si et seulement si il est isomorphe à* $\mathbb{Z}$*. Il est cyclique d'ordre* $n \geq 1$ *si et seulement si isomorphe à* $\mathbb{Z}/n\mathbb{Z}$.

Proposition 2.3.3 (Générateurs d'un Groupe Cyclique)**.**

— *Les générateurs de* $\mathbb{Z}, +$ *sont les* $k \in \mathbb{Z}$ *tels que* $\mathbb{Z} = k\mathbb{Z}$*, i.e.* $k = \pm 1$.

— *Pour* $k \in \mathbb{Z}$*,* $G = \langle g \rangle$ *un groupe cyclique d'ordre* n*, on a équivalence entre :*

1. $\langle g^k \rangle = G$
2. $g \in \langle g^k \rangle$
3. $\exists k' \in \mathbb{Z},\ kk' = 1\ mod\ n$
4. $\overline{k} \in (\mathbb{Z}/n\mathbb{Z})^\times$
5. $k \wedge n = 1$

Corollaire 2.3.0.2. *Un groupe cyclique d'ordre* n *a exactement* $\varphi(n)$ *générateurs.*

Corollaire 2.3.0.3. *Si* G *est cyclique d'ordre* n *:* $Aut(G) = \left\{g \mapsto g^k \mid k \in (\mathbb{Z}/n\mathbb{Z})^\times\right\}$*. On a alors un isomorphisme de* $(\mathbb{Z}/n\mathbb{Z})^\times$ *dans* $Aut(G)$.

Remarque 2.3.0.1. *Si* $g \in G$ *est d'ordre fini* n*, si* $d \geq 1$*,* g^d *est d'ordre fini* $\frac{n}{n \wedge d}$.

Proposition 2.3.4. *Si* G *est cyclique d'ordre* n*,* $d \mapsto G_d = \left\{g^d \mid g \in G\right\}$ *est une bijection de l'ensemble des diviseurs de* n *sur l'ensemble des sous-groupes de* G.

Théorème 2.3.1 (Chinois)**.** *Soient* $m, n \in \mathbb{Z}$ *premiers entre eux. L'application* $\mathbb{Z} \to (\mathbb{Z}/n\mathbb{Z}) \times (\mathbb{Z}/m\mathbb{Z}),\ k \mapsto (k \mod n, k \mod m)$ *définit un isomorphismepar par passage au quotient de par la propriété universelle 1.2.1.*

2.4 Théorème de Lagrange

Définition 2.4.1. *Si* A, B *sont deux parties d'un groupe,* $AB = \{ab \mid a \in A, b \in B\}$*. Si* $A = \{g\}$*, on le note* gB.

Lemme 2.4.1. $H \leq G \Leftrightarrow \left(H \neq \varnothing, HH = H, H^{-1} = H\right)$.

Définition 2.4.2. *On pose* $g \sim_H g'$ *si* $g' \in gH$*. C'est une relation d'équivalence. On note* G/H *son ensemble quotient, et on appelle indice de* H *dans* G *son cardinal noté* $[G : H]$.

Théorème 2.4.2 (Lagrange)**. ??** *Si H est un sous-groupe de G, $G \sim H \times (G/H)$. En particulier, si deux des trois ensembles $G, H, G/H$ sont finis, $|G| = |H|\,[G : H]$.*

Corollaire 2.4.2.1. — *Si H est un sous-groupe du groupe fini G, $|H| \mid |G|$.*
— *Si G est fini, $g \in G$, $g^{|G|} = 1$.*
— *$n^{p-1} \cong 1$ mod p pour $n \in \mathbb{Z}, p \in \P$.*
— *Tout groupe d'ordre premier p est isomorphe à $\mathbb{Z}/p\mathbb{Z}$.*

Théorème 2.4.3 (Cauchy)**.** *Soit G un groupe fini, p un nombre premier divisant $|G|$. G possède un élément d'ordre p. Si G est abélien, on peut généraliser immédiatement à tout $p \in \mathbb{Z}$.*

2.5 Sous-groupes finis de $k^\times$ et $(\mathbb{Z}/n\mathbb{Z})^\times$

Théorème 2.5.1. *Si k est un corps, tout sous-groupe fini de $k^\times$ est cyclique.*

Lemme 2.5.2 (Cauchy)**.** *Soit G un groupe, x, y deux éléments qui commutent d'ordres a et b premiers entre eux. Alors, xy est d'ordre ab.*

Théorème 2.5.3 (Gauss)**.** *Pour p premier, le groupe $(\mathbb{Z}/p\mathbb{Z})^\times$ est cyclique.*

Définition 2.5.1. *Un isomorphisme de groupes $(\mathbb{Z}/p\mathbb{Z})^{times} \simeq \mathbb{Z}/(p-1)\mathbb{Z}$ est appelé un logarithme discret.*

Définition 2.5.2. *Pour un groupe, on note $G^{(n)}$ le groupe des puissances n-ièmes.*

Proposition 2.5.1. *Soient $p \in \P$, $n \geq 1$ et $m = (p-1) \wedge n$.*

1. *$(\mathbb{Z}/p\mathbb{Z})^{\times,(n)}$ est cyclique d'ordre $\frac{p-1}{m}$ et égal à $(\mathbb{Z}/p\mathbb{Z})^{\times,(m)}$*
2. *Pour $x \in ((\mathbb{Z}/p\mathbb{Z}))^\times$, on a $x \in ((\mathbb{Z}/p\mathbb{Z}))^{\times,(n)}$ si et seulement si $x^{\frac{p-1}{m}} = 1$, i.e. $X^{\frac{p-1}{m}}$ a au plus $\frac{p-1}{m}$ racines dans $(\mathbb{Z}/p\mathbb{Z})$ et donc ses racines sont exactement les puissances n-èmes.*

Proposition 2.5.2. *Si p est premier impair, $m \geq 1$, alors $((\mathbb{Z}/p^m\mathbb{Z}))^\times$ est cyclique. Si $m \geq 2$, $((\mathbb{Z}/2^m\mathbb{Z}))^\times \simeq (\mathbb{Z}/2\mathbb{Z}) \times \left(\mathbb{Z}/2^{n-2}\mathbb{Z}\right)$*

2.6 Groupes Quotients

Définition 2.6.1. *Un sous-groupe H de G est dit* distingué*, noté $H \lhd G$ si l'une des conditions équivalentes suivantes est vérifiée :*

1. *$gHg^{-1} \subset H,\ \forall g \in G$*
2. *$gHg^{-1} = H,\ \forall g \in G$*
3. *$gH = Hg,\ \forall g \in G$.*

Remarque 2.6.0.1. *Tous les sous-groupes d'un groupe abélien sont distingués. Un groupe d'indice 2 dans G est distingué.*

Définition 2.6.2. *Le normalisateur de H dans G est le sous-groupe de G défini par $N_G(H) = \left\{g \in G \mid gHg^{-1} = H\right\}$.*

Théorème 2.6.1. *Soit H un sous groupe d'un groupe G.*

1. *Il existe au plus une loi de groupe sur G/H telle que la projection canonique $G \to G/H$ soit une loi de groupe.*
2. *Une telle loi existe si, et seulement si, on a $H \lhd G$, auquelle cas c'est la loi induite par le produit sur $P(G)$.*

Définition 2.6.3. *Si $H \lhd G$, le groupe quotient G/H est la donnée de l'ensemble G/H muni de son unique loi de groupe telle que la projection canonique est un morphisme de groupes.*

Définition 2.6.4. *On pose $\left(\frac{x}{p}\right) = 1$ si x est un carré non nul, 0 si x est nul et -1 sinon. $x \mapsto \left(\frac{x}{p}\right)$ est un morphisme multiplicatif.*

On va étudier les groupes en chercher à étudier des groupes plus simples : étant donné un groupe G, on cherche $H \subsetneq G$ un groupe distingué non trivial pour étudier H et G/H, d'ordres plus petits.

Définition 2.6.5. *Un groupe G est dit* simple *si ses seuls groupes distingués sont $\{1\}$ et G.*

Théorème 2.6.2 (Propriété Universelle des Groupes Quotients)**.** *Si $H \lhd G$, et si $f : G \to G'$ est un morphisme, $g = f \circ \pi$ est un morphisme de G/H dans G' tel que $g(H) = 1$.*

Théorème 2.6.3 (Premier Théorème d'Isomorphisme)**.** *Si f est un morphisme de G dans G', alors f induit par passage au quotient un isomorphisme de groupes de $G/\ker f$ dans $\mathrm{Im} f$*

Proposition 2.6.1 (Troisième Théorème d'Isomorphisme)**.** *Soit $H \lhd G$:*

1. *$H \mapsto K/H$ induit une bijection croissante entre sous groupes de G contenant H et sous-groupes de G/H.*
2. *Dans cette bijection, $K/H \lhd G/H \Leftrightarrow K \lhd G$ auquel cas le morphisme naturel $G/H \to G/K$ induit un isomorphisme $(G/H)/(K/H) \to G/K$.*

3 Groupes Abéliens de Type Fini

3.1 Caractères

Définition 3.1.1. *Un* caractère *d'un groupe G est un morphisme de G dans $\mathbb{C}^\times$.*

Proposition 3.1.1. *Soit $G = \langle g \rangle$ un groupe cyclique d'ordre n. Pour $\zeta \in \mu_n$, il existe un unique caractère χ_ζ de G tel que $\chi_\zeta(g) = \zeta$. De plus, $\zeta \mapsto \chi_\zeta$ est un isomorphisme de groupes.*

3.2 Décomposition de Fourier finie

Définition 3.2.1. *Si G est un groupe fini, on note $L^2(G)$ le $\mathbb{C}$-espace vectoreil des fonctions $G \to \mathbb{C}$ muni du produit hermitien. C'est un espace de dimension finie $|G|$. On note $\hat{G}$ l'ensemble des caractères de G. On rappelle que $\mathbb{C}^\times$ étant abélien, $\hat{G} = Hom(G, \mathbb{C}^\times)$*

Théorème 3.2.1. *Soit G un groupe fini.*

1. *L'ensemble $\hat{G}$ est une famille livre et orthonormée de $L^2(G)$ (Orthogonalité des Caractères)*
2. *Si G est abélien, $\hat{G}$ est une base de $L^2(G)$.*

Corollaire 3.2.1.1. *Soit G abélien fini*

1. *On a $\left|\hat{G}\right| = |G|$*
2. *Pour toute fonction $f : G \to \mathbb{C}$ on a $f = \sum_{\chi \in \hat{G}} \langle f, \chi \rangle \chi$*

Proposition 3.2.1. *Soit G abélien fini, $H \subset G$ un sous-groupe. Pour tout caractère χ de H, il existe $\tilde{\chi}$ de G tel que $\tilde{\chi_{|H}} = \chi$*

Définition 3.2.2. *Un groupe abélien D est* divisible *si le morphisme de groupes $x \mapsto x^n$ est surjectif pour tout $n \geq 1$.*

Proposition 3.2.2 (Prolongement des Morphismes)**.** *Soient G, H, D des groupes abéliens avec D divisible, $H \subset G$ et $f : H \to D$ un morphisme de groupes. Alors il existe un morphisme de groupes $\tilde{f} : G \to D$ tel que $\tilde{f}_{|H} = f$.*

3.3 Structure des groupes abéliens finis

Théorème 3.3.1. *Soit G abélien fini, il existe un unique entier $n \geq 0$ et des uniques entiers $a_i > 1$ vérifiant $a_1 \mid a_2 \mid \ldots \mid a_n$ et $G \simeq \prod_{i=1}^n (\mathbb{Z}/a_i\mathbb{Z})$.*

Définition 3.3.1. *L'*exposant *d'un groupe fini G est le plus petit entier $e \geq 1$ vérifiant $g^e = 1$ pour tout $g \in G$. C'est le ppcm des ordres des éléments de G.*

3.4 Existence

Lemme 3.4.1. *Si G est abélien fini, il existe un élément d'ordre l'exposant.*

Proposition 3.4.1. *Soit G un groupe, $H \leq G, K \leq G$. On suppose $H \cap K = 1$, $G = HK$ et enfin $hk = kh$ pour tout $h \in H$, $k \in K$. L'application produit sur $H \times K$ définit un isomorphisme de groupes.*

De ces deux propositions, on peut prouver la partie existence du théorème.

3.5 Exemple

Définition 3.5.1. *Soit p un nombre premier. Un groupe abélien fini est p-élémentaire si on a $g^p = 1$ pour tout $g \in G$.*

Définition 3.5.2. *On définit $G^\sharp$ le $(\mathbb{Z}/p\mathbb{Z})$-espace vectoriel dont G est le groupe additif.*

Proposition 3.5.1. *Soit p premier, G abélien fini. G est p-élémentaire si et seulement si $G \simeq ((\mathbb{Z}/p\mathbb{Z}))^n$ pour un certain $n \geq 1$. Le nombre minimal de générateurs de G est $\dim_{(\mathbb{Z}/p\mathbb{Z})} G^\sharp$.*

3.6 Unicité

Définition 3.6.1. *On note* $\min(G)$ *le nombre minimal de générateurs de* G*. Il est fini si et seulement si* G *est de type fini.*

Proposition 3.6.1. *Supposons qu'on écrit une décomposition de* G *comme dans le théorème 3.3.1. On a* $n = \min(G)$

Définition 3.6.2. *Soit* G *abélien. Le sous-ensemble* $G[n] = \{g^n = 1\}$ *est un sous groupe de* G *appelé* n*-torsion de* G*.*

Lemme 3.6.1. *Soit* G *et* H *abéliens et* $n \geq 1$*.*

1. *On a* $(G \times H)[n] = G[n] \times H[n]$
2. *Tout (iso-)morphisme* $G \to H$ *induit un (iso-)morphisme* $G[n] \to H[n]$*.*
3. *Supposons* G *cyclique d'ordre* m *et* p *premier. Alors* $G[p] = \{1\}$ *sauf si* $p \mid m$ *auquel cas* $G[p] \simeq (\mathbb{Z}/p\mathbb{Z})$ *et* $G/G[p] \simeq (\mathbb{Z}/m/p\mathbb{Z})$*.*

3.7 Groupes Abéliens de Type Fini

On note ici G un groupe abélien additif

Définition 3.7.1. *Soit* $\mathcal{F} = \{g_1, \ldots, g_n\}$ *une famille d'éléments de* G *et*

$$f : \mathbb{Z}^n \to G, (m_i) \mapsto \sum_{i=1}^{n} m_i g_i$$

On dit que $\mathcal{F}$ *est libre (ou* $\mathbb{Z}$*-libre) si* f *est injectif. On dit que* $\mathcal{F}$ *est génératrice si* f *est surjectif, et est une base si* f *est bijectif.*

Définition 3.7.2. *Un groupe abélien est dit* libre de rang n *s'il possède une* $\mathbb{Z}$ *base à* n *éléments, i.e. s'il est isomorphe à* $\mathbb{Z}^n$*. Par conventions,* $\{0\}$ *est libre de rang* 0*.*

Lemme 3.7.1. *Pour tout entier* $n \geq 0$*,* $\min(\mathbb{Z}^n) = n$*. En particulier,* $\mathbb{Z}^n \simeq Z^m \Leftrightarrow n = m$*.*

Définition 3.7.3. *On appelle* sous-groupe de torsion *de* G*, le sous-groupe de* G *noté* $G_{tor} = \{g \in G \mid \exists n \geq 1,\ ng = 0\}$

Théorème 3.7.2 (Dirichlet)**.** *Si* G *est abélien de type fini,* G_{tor} *est fini et il existe un unique* $n \in \mathbb{N}$ *tel que* $G \simeq G_{tor} \times \mathbb{Z}^n$*.*

Corollaire 3.7.2.1. *Un groupe abélien de type fini sans torsion est libre*

Lemme 3.7.3. *Si* $f : G \to \mathbb{Z}$ *est surjectif,* $G \simeq \mathbb{Z} \times \ker f$*.*

Lemme 3.7.4. *Si* A, B *sont deux groupes abéliens avec* A *fini et* B *libre de rang fini, alors, avec* $G = A \times B$ *:* $G_{tor} = A \times \{0\}$ *et* $G/G_{tor} \simeq B$*.*

4 Groupe Symétrique et Dévissage

4.1 Actions de Groupes

Définition 4.1.1. *Une action de G sur X est une application $: \cdot : G \times X \to X$ vérifiant : $1 \cdot x = x$ et $g \cdot (h \cdot x) = (gh) \cdot x$.*

Définition 4.1.2. *Soit G agissant sur X, et $x \in X$.*

- *$O_x = \{gx \mid g \in G\} \subset X$ est l'*orbite *de x sous G, aussi notée Gx.*
- *Le sous-groupe $G_x = \{g \in G \mid gx = x\}$ est appelé* stabilisateur *de x ou* groupe d'isotropie de *x, noté $Stab_G(x)$.*

Lemme 4.1.1. *On a : $G_{gx} = gG_xg^{-1}$.*

Proposition 4.1.1.
- *Les orbites sous G forment une partition de X.*
- *Pour tout $x \in X$, on a une bijection $G/G_x \xrightarrow{\sim} O_x$ envoyant gG_x sur gx. En particulier, si G est fini, on a $|G| = |G_x|\,|O_x|$*

Corollaire 4.1.1.1. *On note x_i des représentants des orbites de G dans X. On a :*

$$|X| = \sum_{i \in I} |O_{x_i}| = \sum_{i \in I} |G| \,/\, |G_{x_i}|$$

Théorème 4.1.2 (Premier Théorème de Sylow)**.** *Soit G fini d'ordre $p^n m$ avec p premier et $m \wedge p = 1$. Alors G possède un sous-groupe d'ordre p^n, appelé un p-Sylow de G.*

Définition 4.1.3. *Une action de G sur X est* transitive *si on a $X \neq \varnothing$ et si $\forall\ x, y \in X,\ \exists\ g \in G,\ y = gx$, i.e. que X a une et une seule orbite sous l'action de G.*

Définition 4.1.4. *Le noyau d'une action est le noyau du morphisme $G \to S_X$ associé à l'action. C'est un sous-groupe distingué de G. Une action est dite* fidèle *si son noyau est $\{1\}$.*

Définition 4.1.5. *Une action est* libre *si on a toujours $G_x = \{1\}$.*

Définition 4.1.6. *Deux actions d'un même groupe sur deux ensembles X et Y sont* isomorphes *s'il existe une bijection f vérifiant $f(g \cdot x) = g \star f(x)$.*

Proposition 4.1.2. *Une action transitive $(X, \cdot)$ est isomorphe à l'action par translations de G sur G/G_x*

Proposition 4.1.3. *Deux actions transitives sont isomorphes si et seulement si elles ont les mêmes stabilisateurs.*

4.2 Groupes Symétriques et Alternés

Proposition 4.2.1. *Toute permutation σ de S_n s'écrit comme un produit de cycles à supports disjoints. L'ordre de σ est alors le ppcm des longueurs des cycles.*

Proposition 4.2.2. *Les transpositions engendrent S_n*

Lemme 4.2.1. *Si $\sigma \in S_n$, $c = (i_1, \ldots, i_k)$ est un k-cycle : $\sigma c \sigma^{-1} = (\sigma(i_1), \ldots, \sigma(i_k))$.*

Proposition 4.2.3.
- *Les $(i, i+1)$ engendrent S_n. Ils sont appelés générateurs de Coxeter.*
- *La transposition $(1, 2)$ et le cycle $(12 \ldots n)$ engendrent S_n.*

En particulier, $\min S_n = 2$.

Définition 4.2.1.
- *Une partition de l'entier n est une suite décroissante $n_1 \geq \ldots \geq n_r$ d'entiers strictement positifs de somme n.*
- *Le type de $\sigma \in S_n$ est la partition de l'entier n définie par les cardinaux des orbites de σ.*

Proposition 4.2.4. *Deux éléments de S_n sont conjugués si et seulement si ils ont même type.*

Définition 4.2.2. *Pour $k \geq 1$ entier, G agissant sur X avec $|X| \geq k$, G agit k-transitivement sur X si pour deux k-uplets d'éléments distincts de X il existe $g \in G$ tel que $gx_i = y_i$ pour tout i.*

Définition 4.2.3. *La* signature *de $\sigma \in S_n$ est :*

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

C'est un morphisme de groupes $S_n \to \{\pm 1\}$ valant -1 sur les transpositions. On note A_n son noyau. C'est un sous-groupe distingué.

Proposition 4.2.5. *Pour $n \geq 3$, A_n agit $(n-2)$-transitivement sur $|1, n|$. Les k-cycles sont conjugués sous l'action de A_n pour $k \in |2, n-2|$.*

4.3 Les suites exactes

Définition 4.3.1. *Une suite de $n \geq 2$ morphismes de groupes $(f_1, \ldots, f_n)$ est* exacte *si $\mathrm{Im}\, f_i = \ker f_{i+1}$ pour tout i.*

Définition 4.3.2. *Une suite exacte de la forme $1 \to H \xrightarrow{i} G \xrightarrow{\pi} K \to 1$ est une suite exacte* courte.

Proposition 4.3.1. *Il est équivalent de se donner :*

- *Une suite exacte $1 \to H \xrightarrow{i} G \xrightarrow{\pi} K \to 1$*
- *Un sous-groupe distingué $H' \subset G$ et des isomorphismes $i' : H \xrightarrow{\sim} H'$ et $\pi' : G/H' \xrightarrow{\sim} K$.*

Définition 4.3.3 (Groupe diédral)**.** *Pour $n \geq 3$, on définit le groupe diédral D_{2n} comme le sous groupe de S_n engendré par $(12 \ldots n)$ et l'élément τ défini par $\tau(i) = n + 1 - i$.*

Définition 4.3.4. *Si G, H, K sont des groupes donnés, G est extension de K par H s'il existe une suite exacte courte $1 \to H \to G \to K \to 1$.*

4.4 Dévissage de S_n

Théorème 4.4.1. *Les seuls sous-groupes distingués de S_n sont $\{1\}, A_n, S_n$ et K_4 dans le cas $n = 4$.*

Théorème 4.4.2. *Pour $n \geq 5$, A_n est simple non abélien.*

Corollaire 4.4.2.1.
- *Pour $n \neq 4$, toute action de A_n est fidèle ou triviale.*
- *Une action transitive de S_n sur un ensemble à $m > 2$ éléments est fidèle, sauf peut-être si $n = 4$ et $m = 3$ ou 6.*

4.5 Commutateur et Groupes Dérivés

Définition 4.5.1. *Le groupe dérivé d'un groupe G est le sous-groupe $D(G) = [G, G]$ engendré par les $[x, y] = xyx^{-1}y^{-1}$. On a $D(G) = \{1\}$ si et seulement si G est abélien.*

Corollaire 4.5.0.1. *$D(G)$ est un sous-groupe caractéristique de G.*

Corollaire 4.5.0.2. *Soit G un groupe.*

- *Tout morphisme $f : G \to G'$ avec G' abélien vérifie $D(G) \subset \ker f$.*
- *Pour $H \lhd G$ alors G/H est abélien si et seulement si, $D(G) \subset H$.*

Proposition 4.5.1. *On a :*

- $D(S_n) = A_n$
- $D(A_n) = A_n$ *pour* $n \geq 5$.
- $D(A_4) = K_4$ *et* $D(A_n) = \{1\}$ *pour* $n \leq 3$

Définition 4.5.2. *Un groupe G est résoluble s'il existe n tel que $D^n(G) = \{1\}$. Le plus petit n est appelé classe de résolubilité de G.*

Proposition 4.5.2. *Si G est un groupe et $H \lhd G$, G est résoluble si et seulement si H et G/H le sont. Alors, la classe de G est inférieure à la somme des classes de H et de G/H.*

Proposition 4.5.3. *Le groupe $T_n(k)$ est résoluble de classe $\leq 1 + \lceil \log_2(n) \rceil$.*

4.6 Dévissage en Produit Semi-Direct

Définition 4.6.1. *Si $H \leq G$, un* complément *de H dans G est $K \leq G$ tel que $G = HK$ et $H \cap K = \{1\}$*

Remarque 4.6.0.1. *Soit $N \lhd G$, et K un complément de N dans G. Pour tout $n, n' \in N$, $k, k' \in K$, on a :*

$$(nk)(n'k') = n(kn'k^{-1})kk' \text{ avec } kn'k^{-1} \in N$$

Autrement dit :

$$(nk)(n'k') = nint_k(n')kk'$$

La structure de groupe de G se déduit de celle de N, K et de la connaissance de l'application : $\alpha : k \in K \mapsto int_{k|N}$

On se fixe dans la suite deux tels groupes N et K, et un morphisme de groupe α de K dans $\mathrm{Aut}(N)$.

Définition 4.6.2. *La loi $\star_\alpha : (N \times K) \times (N \times K) \to N \times K, (n,k),(n',k') \mapsto (n\alpha_k(n'), kk')$ est une loi de groupe, qui munit $N \times K$ d'une structure de groupe noté $N \rtimes_\alpha K$ et appelé produit semi-direct (externe) de K par N associé à α.*

Proposition 4.6.1. *Soit G un groupe, $N \lhd G$ et K un complément de N dans G. Soit $\alpha : K \to Aut(N),\ k \mapsto \alpha_k$. La bijection $N \times K \to G, (n,k) \mapsto nk$ est un isomorphisme de groupes : $N \rtimes_\alpha K \xrightarrow{\sim} G$. On dit aussi que G est* produit semi-direct interne *de K par N*

Proposition 4.6.2 (Suivi des Isomorphismes)**.** *Soit $G = N \rtimes_\alpha K$, $a : N' \xrightarrow{\sim} N$ et $b : K' \xrightarrow{\sim} K$ des isomorphismes. La bijection $N' \times K' \to G, (n',k') \mapsto a(n')b(k')$ est un isomorphisme de groupes de $N' \rtimes_{\alpha'} K'$ dans G, où $\alpha' : k' \mapsto \alpha_{k'} = a^{-1} \circ \alpha_{b(k')} \circ a$.*

Proposition 4.6.3. *Un groupe d'ordre $2p$ avec p premier impair est soit isomorphe à $(\mathbb{Z}/p\mathbb{Z})$ soit à D_{2p}.*

Proposition 4.6.4. *Les groupes non abéliens d'ordre ≤ 8 sont S_3, D_8 et H_8.*