Algèbre 1

Gaëtan Chenevier

27 octobre 2023

Table des matières

Première partie
Ensembles Quotients

1 Partitions et Relations d'Equivalence

Définition 1.0.1. *Une* partition *d'un ensemble X est un ensemble de parties non vides de X de réunion disjointe X.*

Définition 1.0.2. *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 1.0.3. *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 1.0.1. *Les classes d'équivalences d'une relation R sur X forment une partition de X.*

Définition 1.0.4. *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.*

2 Passage au Quotient

Théorème 2.0.1 (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. ■

3 Sections et systèmes de représentants

Définition 3.0.1. *Une* section *de $f : X \to Y$ est une application $s : Y \to X$ telle que $f \circ s = id_Y$*

Proposition 3.0.1. *f possède une section $\Rightarrow$ f est surjective*

Définition 3.0.2 (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 3.0.2. *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 3.0.3. *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 3.0.0.1. *Ceci est également équivalent à 3.0.2*

4 Lemme de Zorn

Définition 4.0.1. — *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 4.0.1 (Lemme de Zorn)**.** *Un ensemble ordonné inductif possède au moins un élément maximal. Ceci est équivalent à l'axiome du choix 3.0.2.*

Corollaire 4.0.1.1. *Tout espace vectoriel possède une base.*

Corollaire 4.0.1.2 (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. ■

Deuxième partie

Généralités sur les Groupes

5 Exemples de Groupes

Définition 5.0.1. *Une* loi de composition interne *est une application* $\star : X \times X \to X$.

Définition 5.0.2 (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 5.0.0.1. *Le neutre est unique.*

Exemple 5.1 (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 5.0.3. *Un groupe est dit* abélien *lorsque tous deux élements commutent.*

Définition 5.0.4. *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 5.2 (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 5.0.5. *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 5.0.6. *On note* $A^\times$ *le groupe des inversibles du monoïde* $(A, \cdot)$.

Proposition 5.0.1. *La loi d'un groupe vérifie les propriété de la loi produit usuelle sur* $\mathbb{R}$.

Définition 5.0.7. *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.

6 Morphismes

Définition 6.0.1. *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 6.0.1 (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 6.0.2. *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 6.0.3. *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 6.0.2. *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 6.0.3. *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 6.0.1 (Cayley)**.** *Tout groupe d'ordre fini* n *est isomorphe à un sous-groupe de* S_n*.*

Lemme 6.0.2. *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 6.0.4. *Un morphisme d'anneau est un morphisme des groupes additifs et des monoïdes multiplicatifs (en particulier, il envoie* 1 *sur* 1*).*

7 Groupes Cycliques et Monogènes

Proposition 7.0.1. *Les sous-groupes de* $\mathbb{Z}$ *sont les* $n\mathbb{Z}$*.*

Proposition 7.0.2. *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 7.0.1. *Un groupe* G *est* monogène *s'il est engendré par un seul élément, appelé* générateur*. Il est* cyclique *s'il est fini.*

Corollaire 7.0.0.1. *Un groupe* G *est monogène infini si et seulement s'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 7.0.3 (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 7.0.0.2. *Un groupe cyclique d'ordre* n *a exactement* $\varphi(n)$ *générateurs.*

Corollaire 7.0.0.3. *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 7.0.0.1. *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 7.0.4. *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 7.0.1 (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 2.0.1.*

8 Théorème de Lagrange

Définition 8.0.1. *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 8.0.1. $H \leq G \Leftrightarrow \big(H \neq \varnothing, HH = H, H^{-1} = H\big)$.

Définition 8.0.2. *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 8.0.2 (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 8.0.2.1.

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

Théorème 8.0.3 (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 $p \in \mathbb{Z}$.*

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

Théorème 9.0.1. *Si k est un corps, tout sous-groupe fini de $k^\times$ est cyclique.*

Lemme 9.0.2 (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 9.0.3 (Gauss)**.** *Pour p premier, le groupe $(\mathbb{Z}/p\mathbb{Z})^\times$ est cyclique.*

Définition 9.0.1. *Un isomorphisme de groupes $(\mathbb{Z}/p\mathbb{Z})^{times} \simeq \mathbb{Z}/(p-1)\mathbb{Z}$ est appelé un logarithme discret.*

Définition 9.0.2. *Pour un groupe, on note $G^{(n)}$ le groupe des puissances n-ièmes.*

Proposition 9.0.1. *Soient $p \in ¶$, $n \geq 1$ 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 9.0.2. *Si p est premier impair, $m \geq 1$, alors $((\mathbb{Z}/p^m\mathbb{Z}))^\times$ est cyclique.*

10 Groupes Quotients