B2. Groupe fondamental

B2.0 Éléments de la théorie des groupes

Définition 2.2.1. Un *groupe* est la donnée d'un ensemble G et d'une fonction $*\colon G\times G \to G$, appelée *loi de composition interne*, qui vérifie les propriétés suivantes : pour tout $g, h, k \in G$, on a

1. (Associativité) $(g * h) * k = g * (h * k)$;
2. (Élément neutre) il existe $e \in G$ tel que $e * g = g$ et $g * e = g$;
3. (Inversion) il existe $g^{-1} \in G$ tel que $g * g^{-1} = e$ et $g^{-1}g = e$.

****

Exemple 2.2.1. 1. $(\mathbb{Z}, +)$ est un groupe, où 0 est l'élément neutre et pour tout $n \in \mathbb{Z}$, $-n$ est l'inverse de n.

2. $(\mathbb{N}, +)$ n'est pas un groupe, car pour 1, quelque soit $n \in \mathbb{N}$, on n'a pas $1 + n = 0$, donc il n'y a pas d'inverse.
3. $\big((0, \infty), \cdot\big)$ est un groupe, où $\cdot$ est le produit usuel, 1 est l'élément neutre et $\frac{1}{x}$ est l'inverse de x.
4. Soit $\mathrm{Mat}(n \times n, \mathbb{R})$, l'ensemble des matrices carrées $n \times n$. On pose $\mathrm{GL}(n, \mathbb{R}) := \{A \in \mathrm{Mat}(n \times n, \mathbb{R}) \mid \det(A) \neq 0\}$. Alors $(\mathrm{GL}(n, \mathbb{R}), \cdot)$ est un groupe, où $\cdot$ est la multiplication matricielles.
   Remarque. $\big(\mathrm{Mat}(n \times n, \mathbb{R}), \cdot\big)$ n'est pas un groupe, puisqu'il y a des éléments qui n'ont pas d'inverse. Cependant, $\big(\mathrm{Mat}(n \times n, \mathbb{R}), +\big)$ est un groupe.
5. Montrons que si $e_1, e_2 \in G$ sont des éléments neutres, alors $e_1 = e_2$.
   On a $e_1 * e_2 = e_1$ et $e_1 * e_2 = e_2$, donc $e_1 = e_2$.
6. Montrer que l'inverse de x est unique.
   Soit x^{-1} et y des inverses de x. On a $(x^{-1} * x) * y = e * y = y$ et $x^{-1} * (x * y) = x^{-1} * e = x^{-1}$. Puisque la loi de composition interne est assiciative, il suit que $y = x^{-1}$.

Définition 2.2.2. Un *homomorphisme* est une application entre deux groupes qui respecte les structures de groupes. Autrement dit, si $(G_1, *)$ et $(G_2, \bullet)$ sont deux groupes, alors $h\colon G_1 \to G_2$ est un homorphisme si pour tout $a, b \in G_1$, on a

$$h(a * b) = h(a) \bullet h(b).$$

****

Exemple 2.2.2. 1. Soit $h\colon (G_1, *) \to (G_2, \bullet)$. Vérifions que $h(x^{-1}) = h(x)^{-1}$.
   On a $h(x * x^{-1}) = h(e_1) = e_2$, où e_i est l'élément neutre de G_i. D'autre part, on a $h(x * x^{-1}) = h(x) \bullet h(x^{-1})$. En combinant, on trouve donc

$$h(x) \bullet h(x^{-1}) = e_2.$$

De la même manière, on peut obtenir l'équation $h(x^{-1}) \bullet h(x) = e_2$. Ceci montre que $h(x^{-1})$ est l'inverse de $h(x)$. Comme l'inverse dans un groupe est unique, on a $h(x^{-1}) = h(x)^{-1}$.

2. log est un homomorphisme entre $\big((0,\infty),\cdot\big)$ et $(\mathbb{R},+)$.
En effet, on a $\log(xy) = \log(x) + \log(y)$, ce qui vérifie la propriété d'un homomorphisme. (Remarquons d'ailleurs que $\log\big(\frac{1}{x}\big) = -\log(x)$, comme on a montré à l'exemple 1.)

Définition 2.2.3. Un groupe $(G,*)$ est dit *commutatif* (ou *abélien*) si pour tout $g,h \in G$, on a $g * h = h * g$.

****

Exemple 2.2.3. $\to$ $(\mathbb{Z},+)$, $(\mathbb{R},+)$ et $\big((0,\infty),\cdot\big)$ sont commutatifs.
$\to$ $(\mathrm{GL}(n,\mathbb{R}),\cdot)$ n'est pas commutatif pour $n \geq 2$.

Définition 2.2.4. Soit $(G,*)$ un groupe, dont l'élément neutre est noté e.

1. On dit que $H \subseteq G$ est un *sous-groupe* de G si
   i) pour tout $h,k \in H$, on a que $h * k \in H$;
   ii) $e \in H$;
   iii) pour tout $h \in H$, on a que $h^{-1} \in H$.
2. On dit que H est un *sous-groupe normal* de G si H est un sous-groupe et si pour tout $g \in G$ et tout $h \in H$, on a $ghg^{-1} \in H$. Dans ce cas, on écrit $H \trianglelefteq G$.

****

Proposition 2.2.5. *Soit $(G,*)$ un groupe, dont l'élément neutre est e.*
i) $H \subseteq G$ est un sous-groupe si et seulement si $e \in H$ et pour tout $h,k \in H$, $hk^{-1}H$.
ii) Si G est abélien, alors tout sous-groupe est normal.

Exemple 2.2.4. 1. $(\mathbb{Z},+)$ est un sous-groupe de $(\mathbb{R},+)$. Comme $\mathbb{R}$ est abélien, c'est un sous-groupe normal.

2. Soit $n \in \mathbb{Z}^*$ fixé. Alors $n\mathbb{Z} = \{nx \mid x \in \mathbb{Z}\}$ est un sous-groupe normal de $\mathbb{Z}$.
3. $D_{2\times 2} := \{A \in \mathrm{GL}(2,\mathbb{R}) \mid A \text{ est diagonale}\}$ est un sous-groupe de $\mathrm{GL}(2,\mathbb{R})$, mais il n'est pas un sous-groupe normal. En effet, avec $g := \left(\begin{smallmatrix} 1 & 1 \\ 1 & 0 \end{smallmatrix}\right) \in \mathrm{GL}(2,\mathbb{R})$ et $h := \left(\begin{smallmatrix} 2 & 0 \\ 0 & 3 \end{smallmatrix}\right) \in D_{2\times 2}$, on a
$$\begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} 2 & 0 \\ 0 & 3 \end{pmatrix}\begin{pmatrix} 0 & 1 \\ 1 & -1 \end{pmatrix} = \begin{pmatrix} 3 & -1 \\ 0 & 2 \end{pmatrix} \notin D_2.$$
(C'est-à-dire que $ghg^{-1} \notin D_2$.)

Étant donné un sous-groupe H de $(G,*)$ et un élément $g \in G$, on définit
$$gH := \{g * h \mid h \in H\} \qquad \text{et} \qquad Hg := \{h * g \mid h \in H\}.$$
On peut vérifier que $gH = Hg$ pour tout $g \in G$ si et seulement si H est normal dans G.

Proposition 2.2.6. *(Groupe quotient) Soit $(G,*)$ un groupe et $H \trianglelefteq G$. On définit la relation $\sim$ sur G par $g_1 \sim g_2$ ssi il existe $h_1,h_2 \in H$ tels que $g_1 * h_1 = g_2 * h_2$. Alors*
1. $\sim$ est une relation d'équivalence; on note l'ensemble des classes d'équivalence par G/H;

2. *les classes d'équivalence de G/H sont $[g] = gH = Hg$;*
3. *Puisque H est normal dans G, on a $[g_1] * [g_2] = [g_1 * g_2]$; la loi de G induit une loi sur G/H de sorte que $\big(G/H, *\big)$ forme un groupe, où $[e] = eH = H$ est l'élément neutre et $[g^{-1}]$ est l'inverse de $[g]$.*

On appelle $G/\sim$ le groupe quotient de G par H et on le note G/H. On dit parfois que l'on quotiente G par H.

Exemple 2.2.5. 1. On a vu que $2\mathbb{Z}$ est un sous-groupe normal de $\mathbb{Z}$. Le groupe quotient est $\mathbb{Z}/2\mathbb{Z} = \{[0], [1]\}$, *le* groupe à deux éléments. Dans ce groupe, on a $[0] + [0] = [0]$, $[0] + [1] = [1]$ et $[1] + [1] = [0]$.

2. De manière similaire, quelque soit $n \in \mathbb{N}$, $\mathbb{Z}/n\mathbb{Z}$ est un groupe à n éléments, dont $[0]$ est l'élément neutre et $[n - k]$ est l'inverse de $[k]$, car
$$[k] + [n - k] = [k + n - k] = [n] = [0].$$

3. La *fonction quotient* $\pi\colon G \to G/H; g \mapsto [g] = gH = Hg$ est un homomorphisme de groupe.

   [Soit $g_1, g_2 \in G$. On a $\pi(g_1 * g_2) = [g_1 * g_2] = [g_1] * [g_2]$, par la proposition précédente.]

Définition 2.2.7. 1. Soit $h\colon (G_1, *) \to (G_2, \bullet)$ un homomorphisme de groupes. Le *noyau* de h est
$$\ker h = \{x \in G_1 \mid h(x) = e_2\},$$
où e_2 est l'élément neutre de G_2.

2. Un isomorphisme $h\colon (G_1, *) \to (G_2, \bullet)$ est application bijective telle que h et h^{-1} sont des homomorphismes.

****

La notation *ker* vient de *kernel* (en anglais) ou de *kern* (en allemand), qui signifient tout deux « noyau ».

Remarque. Une application linéaire est un homomorphisme d'espace vectoriel, car un $\mathbb{R}$-espace vectoriel $(V, +)$ forme un groupe abélien. Ainsi, le noyau d'une application linéaire correspond à son noyau d'homomorphisme.

****

Exemple 2.2.6. 1. Un homomorphisme $h\colon (G_1, *) \to (G_2, \bullet)$ est injectif si et seulement si $\ker h = \{e_1\}$.

   $\Rightarrow$) h est injective, donc $h(x) = e_2$ si et seulement si $x = e_1$, car on sait que $h(e_1) = e_2$.

   $\leftrightarrow$) Supposons que $h(x) = h(y)$. On a alors
$$\begin{aligned} h(x) = h(y) \quad &\Leftrightarrow \quad h(x) \bullet h(y)^{-1} = e_2 \\ &\Leftrightarrow \quad h(x) \bullet h(y^{-1}) = e_2 \\ &\Leftrightarrow \quad h(x * y^{-1}) = e_2. \end{aligned}$$

Il suit que $x * y^{-1} \in \ker h = \{e_1\}$, donc $x * y^{-1} = e_1$, donc $x = y$. Ceci montre que h est injective.

2. Un homomorphisme bijectif est nécessairement un isomorphisme.

   [Soit $h\colon (G_1, *) \to (G_2, \bullet)$ un homomorphisme de groupes. Soit $a, b \in G_2$. D'une part, on a

   $$h\big(h^{-1}(a \bullet b)\big) = a \bullet b$$

   et d'autre part, on a

   $$h\big(h^{-1}(a) * h^{-1}(b)\big) = h\big(h^{-1}(a)\big) \bullet h\big(h^{-1}(b)\big) = a \bullet b.$$

   Comme h est injective, on doit avoir $h^{-1}(a) \bullet h^{-1}(b) = h^{-1}(a * b)$, d'où h^{-1} est un homomorphisme.

Proposition 2.2.8. *Le noyau d'un homomorphisme est un sous-groupe normal.*

Théorème Premier théorème d'isomorphisme 2.2.9. *Soit $h\colon (G_1, *) \to (G_2, \bullet)$ un homomorphisme de groupe. Si h est surjective, alors h induit un isomorphisme*

$$\hat{h}\colon G_1/\ker h \to G_2.$$

Remarques. 1. On suppose que h est surjective. On pourrait également dire que $\hat{h}$ est un isomorphisme de G_1/H sur $h(G_2)$ (car $h\colon G_1 \to h(G_2)$ est toujours surjective).

2. Comme h est surjective, la seule chose qui lui prévient d'être un isomorphisme est l'injectivité. Or, on a vu dans l'exemple que l'injectivité est caractérisée par le noyau.

****

Nous aurons besoin d'un type de groupes particulier, appelé *groupe libre*. Commençons par un exemple.

Exemple 2.2.7. Soit $S = \{a, b\}$, où $a \neq b$ sont deux éléments quelconques. On introduit les symboles a^{-1}, b^{-1} et 1. On appelles $\{a, b, a^{-1}, b^{-1}, 1\}$ des *lettres*. On construit des *mots* à partir des lettres par concaténation, c'est-à-dire en collant les symboles ensembles. La lettre 1 joue le rôle d'élément neutre, donc $aa^{-1} = 1$, $a1b = ab$, etc.

Par exemple, avec a, a, b, on peut construire les mots aab, aba et baa. Lorsque des lettres se répètent, on peut les combiner : $aab = a^2b$, $baa = ba^2$.

Lorsque a et a^{-1} ou b et b^{-1} se suivent, on peut les simplifier. Par exemple, $abb^{-1}a = aa$. On dit qu'un mot est *réduit* si l'on a effectué toutes les simplications possibles.

Le *groupe libre* de rang 2 est alors l'ensemble de tous les mots réduits de toutes les longueurs muni de la concaténation. Après avoir concaténé deux mots, il faut ensuite le réduire.

L'élément neutre est le *mot vide* 1. (C'est un mot de longueur 0.)

L'inverse d'un mot est obtenu en reversant l'ordre des lettres et en changeant ℓ par ℓ^{-1} et *vice versa*, où $\ell \in \{a, b, a^{-1}, b^{-1}\}$.

Par exemple, $(abba^{-1}b)^{-1} = b^{-1}ab^{-1}b^{-1}a^{-1}$. On a bien

$$\begin{aligned}(abba^{-1}b)(b^{-1}ab^{-1}b^{-1}a^{-1}) &= abba^{-1}1ab^{-1}b^{-1}a^{-1}\\ &= abb(a^{-1}a)b^{-1}b^{-1}a^{-1}\\ &= abb1b^{-1}b^{-1}a^{-1}\\ &= ab(bb^{-1})b^{-1}a^{-1}\\ &= ab1b^{-1}a^{-1}\\ &= a(bb^{-1})a^{-1}\\ &= a1a^{-1}\\ &= aa^{-1}\\ &= 1.\end{aligned}$$

Pour définir formellement le groupe libre à partir d'un ensemble fini S, on considère $S^{-1} = \{s^{-1} \mid s \in S\}$ et 1, des symboles différents de ceux de S, et un mot est alors une suite $f\colon \mathbb{N} \to S \cup S^{-1} \cup \{1\}$ qui se stabilise à 1, c'est-à-dire qu'il existe $N \in \mathbb{N}$ tel que pour tout $n \geq N$, $f(n) = 1$. On peut aussi l'écrire comme suit

$$(s_1, s_2, \ldots, s_{N_1}, 1, 1, 1, \ldots)$$

Un mot $s = (s_1, s_2, s_3, \ldots)$ est *réduit* si
1. $s_{i+1} \neq s_i^{-1}$ pour tout i avec $s_i \neq 1$;
2. si $s_k = 1$ pour un certain k, alors $s_i = 1$ pour tout $i \geq k$.

On définit $F(S) = \{\text{mots réduits}\}$.

On peut identifier un mot $(s_1, s_2, \ldots, s_N, 1, 1, 1, \ldots)$ à $s_1 s_2 \ldots s_N$. La loi de composition interne se fait en deux étapes : 1) concaténer deux mots et 2) réduire. La réduction se produit lorsque s et s^{-1} se suivent, on peut alors les simplifier, et lorsque 1 se trouve dans un mot, auquel cas on peut le retirer.

On accepte le théorème suivant.

Théorème 2.2.10. *$F(S)$ muni de l'opération de concaténation-réduction est un groupe. Il est unique à isomorphisme près.*

Le *rang* de $F(S)$ est le nombre d'élément de S.

Remarque. $F(S)$ est abélien s'il est de rang 1. Il n'est pas abélien s'il est de rang $n \geq 2$.

****

Exemple 2.2.8. Si $S = \{a\}$, alors $F(S)$ est isomorphe à $(\mathbb{Z}, +)$.

[Un mot de $F(S)$ est de la forme a^n. Ainsi, on a l'isomorphisme $f(a^n) = n$.]