Remarques sur le partiel de théorie des groupes

1 Rappels sur les définitions

Un groupe G est **simple** si ses seuls sous-groupes **distingués** sont $\{e_G\}$ et G.

Un groupe simple G peut donc avoir des sous-groupes autre que $\{e_G\}$ et G. Ces sous-groupes ne sont juste pas distingués (voir Exemple 3).

Exemple 1 ($\mathbb{Z}/5\mathbb{Z}$ est simple). Si $G = \mathbb{Z}/5\mathbb{Z}$. On a vu (Lagrange) que si $H \leqslant G$ alors $|H|$ divise $|G| = 5$. Donc $|H| \in \{1, 5\}$. Donc
- ou bien $|H| = 1$ et ainsi $H = \{0_{\mathbb{Z}/5\mathbb{Z}}\}$
- ou bien $|H| = 5$ et alors $H = \mathbb{Z}/5\mathbb{Z}$.

Donc $\mathbb{Z}/5\mathbb{Z}$ est simple. *Remarque : Ceci est aussi vrai pour $G = \mathbb{Z}/p\mathbb{Z}$ avec p un nombre premier quelconque.*

Exemple 2 ($\mathfrak{A}_4$ n'est pas simple). Soit $\mathfrak{A}_4$ le groupe alterné. On rappelle que $\mathfrak{A}_4$ contient : l'identité, les 3-cycles à support dans $\{1, 2, 3, 4\}$ et les doubles-transpositions à support dans $\{1, 2, 3, 4\}$, c'est-à-dire :

$$\mathfrak{A}_4 := \left\{\mathrm{id}, (123), (132), (143), (134), (124), (142), (234), (243), (12)(34), (13)(24), (14)(23)\right\}$$

Soit $V_4 := \left\{\mathrm{id}, (12)(34), (13)(24), (14)(23)\right\}$ le groupe des doubles transpositions [1]. Montrons que V_4 est distingué dans $\mathfrak{A}_4$.
Soit $g \in \mathfrak{A}_4$ et x une double transposition de V_4. Alors le type de x est $(2, 2)$. Or, la conjugaison préserve le type de la permutation. Donc le type de gxg^{-1} est $(2, 2)$, c'est-à-dire que gxg^{-1} est une double transposition et donc est contenue dans V_4. Ainsi $gV_4g^{-1} = V_4$.
Donc $\mathfrak{A}_4$ contient un sous-groupe distingué V_4 qui n'est ni $\mathfrak{A}_4$ ni $\{\mathrm{id}\}$ et ainsi $\mathfrak{A}_4$ n'est pas simple.

Exemple 3 ($\mathfrak{A}_5$ est simple). Soit $G = \mathfrak{A}_5$ le groupe alterné de $\mathfrak{S}_5$. Ainsi $\mathfrak{A}_5$ contient :
- l'identité,
- les 3-cycles à support dans $\{1, 2, 3, 4, 5\}$,
- les doubles-transpositions à support dans $\{1, 2, 3, 4, 5\}$
- les 5-cycles à support dans $\{1, 2, 3, 4, 5\}$.

Vous avez vu dans le cours que $\mathfrak{A}_5$ est un groupe simple : ses seuls sous-groupes **distingués** sont $\{\mathrm{id}\}$ et $\mathfrak{A}_5$. Cependant, $\mathfrak{A}_5$ **admet d'autres sous-groupes. Ils ne sont juste pas distingués.** Par exemple :
- Soit $(345) \in \mathfrak{A}_5$. Alors $\langle(345)\rangle = \{\mathrm{id}, (345), (354)\}$ est un sous-groupe (non-distingué) de $\mathfrak{A}_5$.
- Soit $(32415) \in \mathfrak{A}_5$ un 5-cycle. Alors $\langle(32415)\rangle = \{\mathrm{id}, (32415), (34521), (31254), (35142)\}$ est un sous-groupe (non-distingué) de $\mathfrak{A}_5$.

Remarque 1 (Le cas de $\mathfrak{A}_3$). On a $\mathfrak{A}_3 := \{\mathrm{id}, (123), (132)\} = \langle(123)\rangle$.
Donc $(\mathfrak{A}_3, \circ) \simeq (\mathbb{Z}/3\mathbb{Z}, +)$. En particulier $\mathfrak{A}_3$ est simple.

Soit $n \in \mathbb{N}\backslash\{0, 1\}$ et $\sigma \in \mathfrak{S}_n$.
- On appelle **ordre** de σ le plus petit entier $k > 0$ tel que $\sigma^k = \mathrm{id}$, ie.

$$\mathrm{ord}(\sigma) := \min\left\{k \in \mathbb{N}^* \ : \ \sigma^k = \mathrm{id}\right\}.$$

1. *On appelle V_4 le **groupe de Klein**.*

Notons $\sigma = \sigma_1\sigma_2 \cdots \sigma_m$ la décomposition de σ en produit de cycles à supports disjoints. Pour tout $i \in \{1, \dots, k\}$, on note ℓ_i la longueur du cycle σ_i, *ie.* $\ell_i := |\text{supp}(\sigma_i)|$.
— On appelle **type** de σ le m-uplet $(l_1, l_2, \dots, l_m)$.
— La **signature** de σ est notée $\varepsilon(\sigma)$ et elle vérifie :

$$\varepsilon(\sigma) = \varepsilon(\sigma_1) \cdot \varepsilon(\sigma_2) \cdots \varepsilon(\sigma_n) = (-1)^{l_1-1}(-1)^{l_2-1} \dots (-1)^{l_m-1}.$$

En particulier $\varepsilon(\sigma) \in \{1, -1\}$.

Exemple 4. Si $\sigma = (123) \in \mathfrak{S}_3$. Alors $\text{ord}(\sigma) = 3$, $\text{type}(\sigma) = (3)$, $\varepsilon(\sigma) = 1$
Si $\sigma = (123)(57)(46) \in \mathfrak{S}_7$ alors : $\text{ord}(\sigma) = \text{ppcm}\{\text{ord}(123), \text{ord}(57), \text{ord}(46)\} = \text{ppcm}\{3, 2\} = 6$
$\text{type}(\sigma) = (3, 2, 2)$
$\varepsilon(\sigma) = (-1)^{3-2}(-1)^{2-1}(-1)^{2-1} = 1$

2 Groupes quotient

Si $(G, \times)$ est un groupe et $H \leqslant G$, alors

$$G/H = \{gH \ : \ g \in G\}$$

Et en notation additive : Si $(G, +)$ *est un groupe et* $H \leqslant G$, *alors* $G/H = \{g + H \ : \ g \in G\}$.

Exemple 5. Si $G = \mathbb{Z}$ et $H = n\mathbb{Z}$, alors $G/H = \mathbb{Z}/n\mathbb{Z} = \{x + n\mathbb{Z} \ : \ x \in \mathbb{Z}\}$.

Exemple 6. Dans le cas où $G = \mathbb{C}$ et $H = \mathbb{R}$ on a

$$G/H = \mathbb{C}/\mathbb{R} = \{z + \mathbb{R} \ : \ z \in \mathbb{C}\}$$

Remarque : Ici on ne précise pas la loi sur $\mathbb{C}$ mais il s'agit de la loi « + ». En effet, ni $\mathbb{C}$ ni $\mathbb{R}$ ne sont des groupes pour la multiplication.

Soit $(G/H, \times)$ un groupe quotient.

1. Soit gH une classe à gauche, il peut y avoir $g' \neq g$ dans G tel que $gH = g'H$.
2. Donc, quand on définit une application f sur G/H en utilisant un choix de représentant **il faut vérifier que la définition de f ne dépend pas du représentant choisi**, ie. que si $g_1, g_2 \in G$ vérifient $g_1H = g_2H$, alors on a bien $f(g_1H) = f(g_2H)$.

Exemple 7. Soit $G/H = \mathbb{Z}/6\mathbb{Z}$. On a $G/H = \{x + 6\mathbb{Z} \ : \ x \in \mathbb{Z}\}$.

1. Étant donnée une classe $x + 6\mathbb{Z}$, on a plusieurs choix de représentant x possibles. Par exemple : soit $x_1 = 3$ et $x_2 = 21$, alors $x_2 = 21 \equiv 3[6]$. Ainsi $3 + 6\mathbb{Z} = 21 + 6\mathbb{Z}$.
2. Soit maintenant

$$f : \begin{cases} \mathbb{Z}/6\mathbb{Z} & \to \mathbb{Z}/6\mathbb{Z}, \\ x + 6\mathbb{Z} & \mapsto 2x + 6\mathbb{Z}. \end{cases}$$

Pour montrer que f est bien définie, on doit vérifier que si $x_1 + 6\mathbb{Z} = x_2 + 6\mathbb{Z}$, alors $f(x_1 + 6\mathbb{Z}) = f(x_2 + 6\mathbb{Z})$. C'est-à-dire montrer que $2x_2 + 6\mathbb{Z} = 2x_2 + 6\mathbb{Z}$.

Soient donc $x_1, x_2 \in \mathbb{Z}$ tels que $x_1 + 6\mathbb{Z} = x_2 + 6\mathbb{Z}$. Alors il existe $k \in \mathbb{N}$ tel que $x_1 = x_2 + 6k$. Ainsi

$$2x_1 = 2(x_2 + 6k) = 2x_2 + 6(2k) \equiv 2x_2[6].$$

Donc $2x_1 + 6\mathbb{Z} = 2x_2 + 6\mathbb{Z}$. Et ainsi $f(x_1 + 6\mathbb{Z}) = f(x_2 + 6\mathbb{Z})$.

Exemple 8. On considère le groupe quotient $(\mathbb{C}/\mathbb{R}, +)$

1. Soient $z_1 = 1 + 4i$ et $z_2 = 42 + 4i$. Alors ces deux nombres complexes vérifient $z_1 + \mathbb{R} = z_2 + \mathbb{R}$. En effet : soit $w \in z_1 + \mathbb{R}$, alors il existe $x \in \mathbb{R}$ tel que $w = z_1 + x$. Et alors :

$$w = z_1 + x = 1 + 4i + x = 42 + 1 + 4i + x - 42 = (42 + 4i) + (x - 41).$$

Comme $x \in \mathbb{R}$, on a $(x-41) \in \mathbb{R}$ et donc $w \in (42+4i)+\mathbb{R} = z_2+\mathbb{R}$. Ce qui montre $z_1+\mathbb{R} \subseteq z_2+\mathbb{R}$. De la même manière on montre que $z_2 + \mathbb{R} \subseteq z_1 + \mathbb{R}$. Et donc on a $z_1 + \mathbb{R} = z_2 + \mathbb{R}$

2. Donc si on définit

$$f : \begin{cases} \mathbb{C}/\mathbb{R} = \{z + \mathbb{R} \ : \ z \in \mathbb{C}\} & \to \mathbb{R}, \\ z + \mathbb{R} & \mapsto \mathrm{Im}(z). \end{cases}$$

Il faut vérifier que si on a z_1, z_2 deux nombres complexes qui vérifient $z_1 + \mathbb{R} = z_2 + \mathbb{R}$ alors $f(z_1) = f(z_2)$, c'est-à-dire $\mathrm{Im}(z_1) = \mathrm{Im}(z_2)$.
Si $z_1 + \mathbb{R} = z_2 + \mathbb{R}$ alors il exsite $x \in \mathbb{R}$ tel que $z_2 = z_1 + x$. Alors

$$\mathrm{Im}(z_2) = \mathrm{Im}(z_1 + x) = \mathrm{Im}(z_1) + \mathrm{Im}(x) = \mathrm{Im}(z_1).$$

Donc f est bien définie.

3 Groupes engendrés

Soit $S \subseteq G$ une partie finie d'un groupe G. Le **sous-groupe engendré par** S est :

$$\langle S \rangle := \left\{ x_1^{\varepsilon_1} \cdots x_n^{\varepsilon_n} \ : \ n \in \mathbb{N}, \ x_i \in S, \ \varepsilon_i \in \{\pm 1\} \right\}.$$

Exemple 9 (Groupes cycliques). Si $G = \mathbb{Z}/6\mathbb{Z}$ on a :
- $\langle \bar{2} \rangle = \{\bar{0}, \bar{2}, \bar{4}\} \simeq \mathbb{Z}/3\mathbb{Z}$;
- $\langle \bar{3} \rangle = \{\bar{0}, \bar{3}\} \simeq \mathbb{Z}/2\mathbb{Z}$;
- $\langle \bar{1} \rangle = \{\bar{0}, \bar{1}, \bar{2}, \bar{3}, \bar{4}, \bar{5}\} = G$.

Exemple 10 (Groupes Diédraux). Soit $n \geqslant 3$ et D_{2n} le groupe des isométries du n-gone régulier. Alors $D_{2n} = \langle r, s \rangle$ où r est la rotation d'angle $2\pi/n$ et s une symétrie par rapport à un des axes du n-gone.

Exemple 11 (Groupes symétriques/alternés).
- $\mathfrak{S}_n$ est engendré par les transpositions. Ainsi $\mathfrak{S}_n = \left\langle \tau \mid \tau \in \mathfrak{S}_n, \ |\mathrm{supp}(\tau)| = 2 \right\rangle$.
- $\mathfrak{A}_n$ est engendré par les 3-cycles. Par exemple si $n = 4$ on a

$$\mathfrak{A}_4 := \big\langle (123), (132), (143), (134), (124), (142), (234), (243) \big\rangle.$$

Soit G est un groupe. On note $D(G) := \langle [g, h] \ : g \in G, h \in H \rangle$ le **groupe dérivé** de G. Autrement dit $D(G)$ est le sous-groupe de G engendré par $S_{D(G)}$ où

$$S_{D(G)} := \{ghg^{-1}h^{-1} \ : g \in G, h \in G\}.$$

Si G n'est pas commutatif, il peut y avoir plein de valeurs possibles pour les commutateurs de G. Donc $\{ghg^{-1}h^{-1} \ : g \in G, h \in G\}$ peut contenir de nombreux éléments. En particulier $D(G)$ **n'a aucune raison d'être systématiquement un groupe cyclique**.

Exemple 12 (Groupes abéliens). Si G est abélien, alors pour tous $g, h \in G$ on a

$$ghg^{-1}h^{-1} = gg^{-1}hh^{-1} = e_G e_G = e_G.$$

Donc dans ce cas $S_{D(G)} = \{ghg^{-1}h^{-1} \ : g \in G, h \in G\} = \{e_G\}$ et donc $\boxed{D(G) = \{e_G\}}$.

Exemple 13 (Groupe dérivé du groupe symétrique).

1. Montrons d'abord que $D(\mathfrak{S}_n) \leqslant \mathfrak{A}_n$.
   On a $\varepsilon_n : \mathfrak{S}_n \to \{1, -1\}$ qui vérifie :
   — $\{1, -1\}$ est abélien ;
   — $\ker(\varepsilon_n) = \mathfrak{A}_n$.
   Donc [2] $D(G) \subseteq \mathfrak{A}_n$.
2. Montrons maintenant que $\mathfrak{A}_n \subseteq D(\mathfrak{S}_n)$.
   On sait que $\mathfrak{A}_n$ est engendré par les 3-cycles. Or, si (abc) est un trois cycle, il vérifie

   $$(abc) = (ab)(ac)(ab)^{-1}(ac)^{-1}.$$

   Ainsi $(abc) = \big[(ab), (ac)\big]$ est un commutateur.
   Donc la partie génératrice de $\mathfrak{A}_n$ est contenue dans la partie génératrice de $D(\mathfrak{S}_n)$.
   Donc $\mathfrak{A}_n \leqslant D(G)$.

Conclusion : $\boxed{D(\mathfrak{S}_n) = \mathfrak{A}_n}$.

4 Groupes symétriques : cas particuliers

Soit $n \geqslant 2$. On rappelle que $|\mathfrak{S}_n| = n! = 1 \times 2 \times 3 \times \cdots \times n$.

Exemple 14 (Groupes symétriques).

— Si $n = 2$ on a $|\mathfrak{S}_2| = 2$.
  En fait $\mathfrak{S}_2 := \{\mathrm{id}, (12)\}$. Donc $(\mathfrak{S}_2, \circ) \simeq (\mathbb{Z}/2\mathbb{Z}, +)$.
— Si $n = 3$ on a $|\mathfrak{S}_3| = 2 \times 3 = 6$.
  On a $\mathfrak{S}_3 := \{\mathrm{id}, (12), (13), (23), (123), (132)\}$.

Un théorème du cours dit « $\forall n \geqslant 5$, $\mathfrak{A}_n$ est simple ». **Mais ce théorème ne dit rien si $n \leqslant 4$.** Pour $n \leqslant 4$, il faut en fait faire du cas par cas.

Exemple 15 (Groupes alternés).

— $\mathfrak{A}_2 = \{\mathrm{id}\}$. Il s'agit donc du groupe trivial (qui n'est pas simple, par convention).
— $\mathfrak{A}_3 := \{\mathrm{id}, (123), (132)\} = \langle (123) \rangle$.
  Donc $(\mathfrak{A}_3, \circ) \simeq (\mathbb{Z}/3\mathbb{Z}, +)$.
  Remarque. *En particulier $\mathfrak{A}_3$ est abélien et simple.*
— On a vu (Exemple 2) que $\mathfrak{A}_4$ n'est pas simple.

2. **(Propriété universelle du groupe dérivé)** Si A est abélien et $f : G \to A$ est un morphisme, alors $D(G) \subseteq \ker(f)$.