PLAN DU COURS DE THÉORIE DES GROUPES

LICENCE 3, 1er SEMESTRE 2017

par

Benoît Claudon

Table des matières

1. Notions de base

1.1. Groupes. —

Définition 1.1. — Une loi de composition interne sur un ensemble E est la donnée d'une application

$$\star : \begin{cases} E \times E & \longrightarrow & E \\ (x, y) & \mapsto & x \star y \end{cases}$$

La loi $\star$ sera dite *associative* si

$$(x \star y) \star z = x \star (y \star z)$$

pour tout $(x, y, z) \in E^3$.

Remarque 1.2. — Si la loi $\star$ est associative, on peut donc se passer de parenthèses et l'expression

$$x^n = \underbrace{x \star \cdots \star x}_{n \text{ fois}}$$

est définie sans ambiguïté.

Définition 1.3. — Un groupe est un couple $(G, \star)$ où G est un ensemble muni d'une loi de composition interne $\star$ et qui vérifie :

(i) $\star$ est associative ;

(ii) il existe un élément $e \in G$ tel que $e \star x = x \star e = x$ pour tout $x \in G$;

(iii) pour tout $x \in G$, il existe un élément $y \in G$ tel que $x \star y = y \star x = e$.

Un élément $e \in G$ comme ci-dessus est dit *neutre* pour $\star$; l'élément y est appelé un inverse de x.

Remarque 1.4. — Si $(G, \star)$ est un groupe, alors e est unique ; de même, l'élément y ci-dessus est unique : tout élément x de G a un unique inverse qui sera noté x^{-1}. Nous noterons souvent la loi comme un produit $xy := x \star y$ et le neutre $1 := e$ (ou 1_G si la situation le nécessite).

Définition 1.5. — Le groupe G est dit *abélien* (ou *commutatif*) si l'égalité

$$xy = yx$$

est vérifiée pour tout $(x, y) \in G^2$.

Remarque 1.6. — Si G est abélien, on notera 0 le neutre de G et la loi sera notée additivement $x + y$, l'inverse de x étant alors $-x$.

1.2. Morphismes. —

Définition 1.7. — Une application $\varphi : G \to H$ entre les groupes $(G, \cdot)$ et $(H, \star)$ est un morphisme de groupes si on a

$$\varphi(x \cdot y) = \varphi(x) \star \varphi(y)$$

pur tout $(x, y) \in G^2$.

Proposition 1.8. — *Soit $\varphi : G \to H$ un morphisme de groupes.*

1. *On a nécessairement* $\varphi(1_G) = 1_H$.
2. *Si* φ *est bijectif, alors* $\varphi^{-1} : H \to G$ *est un morphisme.*

Définition 1.9. — Un morphisme de groupes bijectif $\varphi : G \to H$ sera appelé un *isomorphisme*. Si $G = H$, φ sera appelé un *automorphisme* de G ; on notera $\mathrm{Aut}(G)$ l'ensemble des automorphismes de G.

Proposition 1.10. — *Muni de la composition des applications, l'ensemble* $\mathrm{Aut}(G)$ *est un groupe d'élément neutre* Id_G.

1.3. Sous-groupes. —

Définition 1.11. — Un sous-groupe d'un groupe G est une partie non vide $H \subset G$ telle que la restriction de la loi de G à H confère à H une structure de groupe. Si H est un sous-groupe de G, nous noterons $H < G$. Un sous-groupe $H < G$ sera dit *propre* si $H \neq G$.

Proposition 1.12. — *Une partie* $H \subset G$ *est un sous-groupe de* G *si et seulement si elle vérifie :*

1. *l'élément neutre* 1 *est dans* H *;*
2. *pour tout* $(x, y) \in H^2$, $xy \in H$ *;*
3. *pour tout* $x \in H$, $x^{-1} \in H$.

Remarque 1.13. — Il revient au même de demander que H soit non vide et que $xy^{-1} \in H$ pour tout $(x, y) \in H^2$.

Proposition 1.14. — *Soit* $\varphi : G_1 \to G_2$ *un morphisme de groupes et* $H_1 < G_1$ *et* $H_2 < G_2$ *des sous-groupes de* G_1 *et* G_2.

*(*i*) L'image directe de* H_1 *est un sous-groupe de* G_2 *:* $\varphi(H_1) < G_2$

*(*ii*) L'image réciproque de* H_2 *est un sous-groupe de* G_1 *:* $\varphi^{-1}(H_2) < G_1$.

*(*iii*) En particulier,* $\varphi(G_1) < G_2$ *et* $\varphi^{-1}(\{1_{G_2}\}) < G_1$.

Définition 1.15. — Si $\varphi : G \to H$ est un morphisme de groupes, on note

$$\mathrm{Im}(\varphi) := \varphi(G) \quad \text{et} \quad \ker(\varphi) := \varphi^{-1}(\{1\})$$

l'*image* et le *noyau* de φ (qui sont donc respectivement des sous-groupes de H et G).

Proposition 1.16. — *Un morphisme de groupes* $\varphi : G \to H$ *est injectif si et seulement si* $\ker(\varphi) = 1$.

1.4. Sous-groupe engendré par une partie. —

Proposition 1.17. — *Si* G *un groupe et* $(H_i)_{i\in I}$ *une famille de sous-groupes de* G*, l'intersection*

$$H := \bigcap_{i\in I} H_i$$

est alors un sous-groupe de G*.*

Définition 1.18. — Si $A \subset G$ est une partie d'un groupe G, on notera

$$\langle A\rangle := \bigcap_{A\subset H} H,$$

où l'intersection porte sur les sous-groupes de G qui contiennent A. Le sous-groupe $\langle A\rangle$ (*cf* la proposition 1.17 ci-dessus) est alors le plus petit sous-groupe de G contenant A ; on l'appelle le *sous-groupe engendré par* A.

Définition 1.19. — Si $\langle A\rangle = G$ on dit que A est une *partie génératrice* de G ou encore que les éléments de A sont des *générateurs* de G.

Si un groupe G admet une partie génératrice finie, on dira que G est *de type fini.*

Proposition 1.20. — *Si* A *est une partie du groupe* G*, on a alors l'égalité suivante :*

$$\langle A\rangle = \bigcup_{m\geq 1} \left\{a_1\cdots a_m \mid \forall i = 1\dots m,\ a_i \in A\cup A^{-1}\right\}.$$

Remarque 1.21. — En posant

$$AB := \{ab \mid a\in A \text{ et } b\in B\},$$

l'égalité ci-dessus se réécrit

$$\langle A\rangle = \bigcup_{m\geq 1} \left(A\cup A^{-1}\right)^m.$$

Définition 1.22. — Si G est engendré par un unique élément $x\in G$, on dit que G est *cyclique* (ou *monogène*). Dans ce cas,

$$G = \{x^m \mid m\in\mathbb{Z}\}$$

et G est abélien.

1.5. Ordre d'un groupe. —

Définition 1.23. — Si G est un groupe, son cardinal est également appelé son *ordre* noté $|G|$ (on autorise donc $|G| = \infty$). Si $x\in G$, l'*ordre* de x (noté $o(x)$) est l'ordre du sous-groupe de G qu'il engendre :

$$o(x) := |\langle x\rangle|.$$

Définition 1.24. — Si $H < G$, la relation

$$x \sim y \Leftrightarrow y^{-1}x \in H$$

est une relation d'équivalence, dite engendrée par H. On note

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

l'ensemble des classes d'équivalence et la quantité

$$[G : H] := |G/H|$$

s'appelle l'indice de H dans G.

***Théorème 1.25* (Lagrange, 1771)**. — *Si G est un groupe fini et $H < G$ un sous-groupe, on a alors :*

$$|G| = [G : H]|H|.$$

En particulier, l'ordre de H divise celui de G.

Corollaire 1.26. — *Si G est un groupe fini et $x \in G$, $o(x)$ divise $n := |G|$ et on a donc $x^n = 1$. En particulier, si n est premier, alors G est cyclique.*

2. Groupes cycliques

2.1. Le groupe $\mathbb{Z}$. — On se contente ici de quelques observations et rappels :

1. Si G est un groupe cyclique d'ordre infini, alors G est isomorphe à $\mathbb{Z}$.
2. Les sous-groupes de $\mathbb{Z}$ sont de la forme $n\mathbb{Z}$ avec $n \in \mathbb{Z}$.
3. Les seuls éléments qui engendrent $\mathbb{Z}$ sont 1 et -1.
4. Le groupe $\mathrm{Aut}(\mathbb{Z})$ est d'ordre 2, engendré par

$$\varphi : \left\{ \begin{array}{ccc} \mathbb{Z} & \longrightarrow & \mathbb{Z} \\ n & \mapsto & \varphi(n) := -n \end{array} \right.$$

2.2. Groupes finis cycliques. — Si $n \geq 2$ est un entier, on considère $\mathbb{Z}/n\mathbb{Z}$ l'ensemble des classes d'équivalence de la relation « modulo n ». Si $k \in \mathbb{Z}$, on note $\bar{k}$ sa classe dans $\mathbb{Z}/n\mathbb{Z}$. On constate que l'addition et la multiplication sont bien définies dans $\mathbb{Z}/n\mathbb{Z}$ (de neutre respectif $\bar{0}$ et $\bar{1}$), ce qui fait de ce dernier un anneau (commutatif).

Proposition 2.1. — *L'application naturelle $\mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$ qui envoie un entier sur sa classe modulo n est un morphisme de groupes.*

On notera (comme dans tout anneau)

$$(\mathbb{Z}/n\mathbb{Z})^* := \{x \in \mathbb{Z}/n\mathbb{Z} \mid \exists y \in \mathbb{Z}/n\mathbb{Z},\ xy = 1\}$$

l'ensemble des éléments inversibles de $\mathbb{Z}/n\mathbb{Z}$. On observe enfin que si G est un groupe cyclique d'ordre n alors G est isomorphe à $(\mathbb{Z}/n\mathbb{Z}, +)$.

Proposition 2.2. — *L'ensemble des générateurs de $\mathbb{Z}/n\mathbb{Z}$ s'identifie à $(\mathbb{Z}/n\mathbb{Z})^*$. On en déduit que l'application*

$$\Phi : \left\{ \begin{array}{ccc} \mathrm{Aut}(\mathbb{Z}/n\mathbb{Z}) & \longrightarrow & (\mathbb{Z}/n\mathbb{Z})^* \\ f & \mapsto & f(1) \end{array} \right.$$

est bien définie et que c'est un isomorphisme de groupes.

Définition 2.3. — Pour $n \geq 2$, on pose

$$\varphi(n) := |\,(\mathbb{Z}/n\mathbb{Z})^*\,|.$$

La fonction φ s'appelle l'indicatrice d'Euler.

***Théorème 2.4* (des restes chinois).** — *Si m et n sont deux entiers premiers entre eux, l'application*

$$\Psi : \left\{ \begin{array}{ccc} \mathbb{Z}/nm\mathbb{Z} & \longrightarrow & \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z} \\ \bar{x} & \mapsto & (x \bmod n, x \bmod m) \end{array} \right.$$

est un isomorphisme d'anneaux et envoie donc inversibles sur inversibles. En particulier, on en déduit :

$$m \wedge n = 1 \Rightarrow \varphi(mn) = \varphi(m)\varphi(n).$$

Comme $\varphi(p^\alpha) = p^\alpha - p^{\alpha-1}$ pour p premier et $\alpha \geq 1$ entier, on obtient :

Corollaire 2.5. —

$$\varphi(n) = \prod_{i=1}^{r} (p_i^{\alpha_i} - p_i^{\alpha_i - 1}) = n \prod_{i=1}^{r} (1 - \frac{1}{p_i})$$

si $n = p_1^{\alpha_1} \cdots p_r^{\alpha_r}$ est la décomposition en facteurs premiers de n.

Théorème 2.6. — *Le groupe $(\mathbb{Z}/p^\alpha\mathbb{Z})^*$ (avec p premier et $\alpha \geq 1$) est :*
- *cyclique si $p \geq 3$ (et donc isomorphe à $\mathbb{Z}/p^{\alpha-1}(p-1)\mathbb{Z}$) ;*
- *trivial si $p = 2$ et $\alpha = 1$;*
- *isomorphe à $\mathbb{Z}/2^{\alpha-2}\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ si $p = 2$ et $\alpha \geq 2$.*

3. Groupes abéliens de type fini

Dans tout ce chapitre, on considère G un groupe abélien de type fini, c'est-à-dire possédant une famille génératrice finie (*cf* définition 1.19). Comme les groupes sont supposés abéliens, nous noterons la loi de façon additive $x+y$ (le neutre est donc noté 0 et mx avec $m \in \mathbb{Z}$ désigne le « produit » de x avec lui-même).

Définition 3.1. — Une famille génératrice finie $(x_1, \ldots, x_k)$ de G sera appelée une *pseudo-base* si

$$\forall\, (m_1, \ldots, m_k) \in \mathbb{Z}^k,\ \sum_{i=1}^{k} m_i x_i = 0 \Rightarrow m_i x_i = 0,\ \forall\, i = 1 \ldots k.$$

On dira que $(x_1, \dots, x_k)$ est une *base* de G si

$$\forall (m_1, \dots, m_k) \in \mathbb{Z}^k, \sum_{i=1}^{k} m_i x_i = 0 \Rightarrow m_i = 0, \forall i = 1 \dots k.$$

Remarque 3.2. — Si G admet un pseudo-base $(x_1, \dots, x_k)$, alors

$$G \simeq \langle x_1 \rangle \times \cdots \times \langle x_k \rangle$$

et G est produit de groupes cycliques (certains facteurs pouvant être finis). Si G admet une base, alors $G \simeq \mathbb{Z}^k$.

Définition 3.3. — La torsion d'un groupe abélien G est l'ensemble des éléments d'ordre fini :

$$\mathrm{Tor}(G) := \{g \in G \mid \exists m \neq 0,\ mg = 0\}.$$

Remarque 3.4. — La torsion d'un groupe abélien est un sous-groupe de G : $\mathrm{Tor}(G) < G$. Si G admet une base, G est alors sans torsion : $\mathrm{Tor}(G) = \{0\}$.

Théorème 3.5. — *Tout groupe abélien de type fini admet une pseudo-base (et s'écrit donc comme un produit de groupes cycliques).*

La démonstration s'appuie sur le résultat suivant.

Lemme 3.6. — *Soient* $(x_1, \dots, x_k)$ *une famille génératrice d'un groupe abélien* G *et* $(c_1, \dots, c_k) \in \mathbb{Z}^k$ *avec* $\mathrm{pgcd}(c_1, \dots, x_k) = 1$. *Il existe alors une famille génératrice* $(y_1, \dots, y_k)$ *de* G *avec* $y_1 := \sum_{i=1}^{k} c_i x_i$.

Corollaire 3.7. — *Tout groupe abélien de type fini se décompose donc de la façon suivante :*

$$G \simeq \mathrm{Tor}(G) \times \mathbb{Z}^r$$

avec $r \geq 0$ *un entier ne dépendant que de* G. *On note* $\mathrm{rg}(G) := r$ *cet entier, c'est le* rang *de* G.

Théorème 3.8. — *Si* G *est un groupe abélien de type fini et* $H < G$ *un sous-groupe de* G *alors* H *est également de type fini et* $\mathrm{rg}(H) \leq \mathrm{rg}(G)$.

On s'intéresse enfin à la partie de torsion qui s'écrit donc comme un produit de groupes de la forme $\mathbb{Z}/n_j\mathbb{Z}$. Le théorème Chinois 2.4 montre qu'il n'y a pas unicité de la décomposition en général ; il faut fixer des conditions arithmétiques sur les entiers n_j.

Théorème 3.9 **(Structures des groupes abéliens finis)**
Un groupe abélien fini se décompose d'un unique façon en produit de groupes cycliques

$$G \simeq \mathbb{Z}/n_1\mathbb{Z} \times \cdots \times \mathbb{Z}/n_r\mathbb{Z}$$

sous l'une *des deux conditions suivantes :*

(a) pour tout $i = 1 \dots r-1$, n_i *divise* n_{i+1} *;*

(b) les entiers n_j *sont de la forme* $n_j = p_j^{\alpha_j}$ *avec* p_j *premier.*

On utilise au cours de la démonstration le résultat suivant.

Lemme 3.10. — *Dans le groupe* $\mathbb{Z}/n_1\mathbb{Z} \times \cdots \times \mathbb{Z}/n_r\mathbb{Z}$*, le nombre de solutions de l'équation* $mx = 0$ *(c'est-à-dire le nombre d'éléments dont l'ordre divise* m*) est :*

$$\operatorname{pgcd}(m, n_1) \operatorname{pgcd}(m, n_2) \dots \operatorname{pgcd}(m, n_r).$$

4. Sous-groupes normaux

4.1. Premiers pas. — On commence par remarquer que si $f : G \to H$ est un morphisme de groupes, alors le sous-groupe $\ker(f)$ vérifie la propriété suivante :

$$\forall\, g \in G, \forall\, x \in \ker(f),\ gxg^{-1} \in \ker(f).$$

Définition 4.1. — Si $g \in G$, alors l'application

$$\operatorname{int}_g : \left\{ \begin{array}{ccc} G & \longrightarrow & G \\ x & \mapsto & gxg^{-1} \end{array} \right.$$

est un automorphisme de G, appelé automorphisme intérieur. On notera $\operatorname{Int}(G) \subset \operatorname{Aut}(G)$ l'ensemble des automorphismes intérieurs.

Définition 4.2. — Un sous-groupe $H < G$ est dit ***normal dans*** G si H est stable par tout automorphisme intérieur :

$$\forall\, g \in G,\ gHg^{-1} = H.$$

On notera $H \lhd G$ lorsque H est normal dans G (on dit aussi *distingué dans* G).

Remarque 4.3. — Si G est un groupe abélien, tout sous-groupe $H < G$ est normal dans G.

Proposition 4.4. — *Soit* $\varphi : G_1 \longrightarrow G_2$ *un morphisme de groupes et* $H_1 < G_1$ *et* $H_2 < G_2$ *des sous-groupes.*

1. $H_2 \lhd G_2 \Rightarrow \varphi^{-1}(H_2) \lhd G_1$ *;*
2. *Si* H_1 *est normal dans* G_1*, alors* $\varphi(H_1)$ *est* ***normal dans*** $\varphi(G_1)$ *;*
3. *En particulier, si* φ *est surjective,* $\varphi(H_1)$ *est normal dans* G_2 *mais ce n'est pas le cas en général.*

Définition 4.5. — Un groupe G est dit *simple* si les seuls sous-groupes normaux de G sont $\{1\}$ et G lui-même.

4.2. Groupe quotient. —

Théorème 4.6. — *Si* $H \lhd G$*, alors il existe sur l'ensemble quotient* G/H *une unique loi de groupe faisant de la projection canonique* $\pi : G \longrightarrow G/H$ *un morphisme de groupes.*

Remarque 4.7. — Si $H \lhd G$, alors H est le noyau de l'application $\pi : G \longrightarrow G/H$.

***Théorème 4.8* (Propriété universelle du quotient).** — *Soit* $f : G \longrightarrow H$ *un morphisme de groupes et* $N := \ker(f)$ *son noyau. Il existe alors un unique morphisme de groupes injectif* $\varphi : G/N \longrightarrow H$ *tel que* $f = \varphi \circ \pi$. *En particulier,* G/N *est isomorphe à* $\mathrm{Im}(f)$.

***Théorème 4.9*.** — *Soit* $N \lhd G$. *Il existe une correspondance bijective :*

$$\{H < G \mid N \subset H\} \longleftrightarrow \left\{\bar{H} < G/N\right\}$$

qui envoie un sous-groupe H *de* G *(contenant* N*) sur* $\bar{H} := \pi(H)$ *et un sous-groupe* $\bar{H}$ *de* G/N *sur* $H := \pi^{-1}(\bar{H})$.

Dans cette correspondance, H *est normal dans* G *si et seulement si* $\bar{H}$ *est normal dans* G/N.

***Théorème 4.10* (Théorème d'isomorphisme).** — *Soient* $H, N < G$ *avec* N *normal dans* G. *Le produit* HN *(comme dans la remarque 1.21) est alors un sous-groupe de* G *dans lequel* N *est distingué et on a un isomorphisme canonique*

$$\begin{cases} H/(H \cap N) & \xrightarrow{\sim} & HN/N \\ h(H \cap N) & \mapsto & hN. \end{cases}$$

4.3. Exemples fondamentaux. — Si x et y sont deux éléments d'un groupe G, on note $[x, y] := xyx^{-1}y^{-1}$ le commutateur de x et y.

***Définition 4.11*.** — Si G est un groupe, on note

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

C'est un sous-groupe normal (et abélien) de G appelé le *centre de* G.

Le sous-groupe

$$D(G) := [G, G] := \langle [x, y] \mid (x, y) \in G^2 \rangle$$

engendré par les commutateurs s'appelle le *groupe dérivé de* G : c'est également un sous-groupe normal et le quotient $G/D(G)$ est abélien.

***Proposition 4.12*.** — *Si* G *est un groupe et* $N \lhd G$, *alors* G/N *est abélien si et seulement si* $D(G) \subset N$. *Le groupe* $G/D(G)$ *est donc le plus gros quotient abélien de* G *(appelé* abélianisé *de* G*).*

***Proposition 4.13*.** — *Pour tout groupe* G, *l'application*

$$\mathrm{int} : \begin{cases} G & \longrightarrow & \mathrm{Aut}(G) \\ g & \mapsto & \mathrm{int}_g \end{cases}$$

est un morphisme de groupes, d'image $\mathrm{Int}(G)$ *et de noyau* $Z(G)$. *On a donc :*

$$G/Z(G) \simeq \mathrm{Int}(G).$$

De plus, $\mathrm{Int}(G)$ *est un sous-groupe normal de* $\mathrm{Aut}(G)$.

5. Notion d'action de groupe

5.1. Vocabulaire des actions. —

Définition 5.1. — Soient G un groupe et X un ensemble (non vide). Une *action* de G sur X (ont dit aussi que G *opère* sur X ou que X est un G-ensemble) est la donnée d'une application $\alpha : G \times X \longrightarrow X$ vérifiant

1. pour tout $x \in X$, $\alpha(1, x) = x$;
2. pour tout $(g, h) \in G^2$ et tout $x \in X$, $\alpha(g, \alpha(h, x)) = \alpha(gh, x)$.

On notera aussi l'action sous la forme $\alpha(g, x) = g \cdot x$.

Proposition 5.2. — *La donnée d'une action de* G *sur* X *est équivalente à celle d'un morphisme de groupes*

$$G \longrightarrow S_X.$$

Définition 5.3. — Soient G un groupe et X un G-ensemble. Pour un élément $x \in X$, on note

– $G \cdot x := \{g \cdot x \mid g \in G\}$ l'orbite de x (sous G) ;
– $G_x := \{g \in G \mid g \cdot x = x\}$ le stabilisateur de x dans G. C'est un sous-groupe de G.

L'action est dite *fidèle* lorsque le morphisme $G \longrightarrow S_X$ est injectif. L'action est dite *libre* si $G_x = 1$ pour tout $x \in X$.

Proposition 5.4. — *Si* G *agit sur* X *et* $x \in X$*, l'application*

$$\begin{cases} G/G_x & \longrightarrow & G \cdot x \\ gG_x & \mapsto & g \cdot x \end{cases}$$

est bien définie et est une bijection. En particulier, si G *ou* X*sont finis, on a* $|G/G_x| = |G \cdot x|$.

5.2. Les exemples à avoir en tête. —

Exemple 5.5. — Si G est un groupe, $\alpha(g, x) = gx$ définit une action de G sur lui-même appelée action par *translations à gauche*. Cette action est libre et fidèle.

***Théorème 5.6* (Cayley, 1854)**. — *Si* G *est fini d'ordre* $|G| = n$*, alors il existe un morphisme injectif*

$$G \hookrightarrow S_n.$$

Exemple 5.7. — Le morphisme $\mathrm{int} : G \longrightarrow \mathrm{Aut}(G)$ définit une action de G sur lui-même dite action par *conjugaison*. Si $x \in G$, son orbite s'appelle sa *classe de conjugaison* et son stabilisateur et aussi appelé le *centralisateur* de x dans G :

– classe de conjugaison de x dans G : $\left\{gxg^{-1} \mid g \in G\right\}$.
– centralisateur : $C_G(x) := \{g \in G \mid gx = xg\}$.

Exemple 5.8. — Si G agit sur X et $H < G$, alors la restriction de $\alpha : G \longrightarrow S_X$ à H définit une action de H sur X.

Exemple 5.9. — Si $H < G$ alors on peut faire agir G sur les classes à gauche G/H par

$$(g, xH) \mapsto gxH.$$

Orbites ? Stabilisateur de xH ?

Exemple 5.10. — Un groupe G agit *par conjugaison* sur l'ensemble $X := \{H < G\}$ de ses sous-groupes :

$$(g, H) \mapsto gHg^{-1}.$$

Les éléments de l'orbite de H sont appelés les conjugués de H et son stabilisateur est

$$N_G(H) := \{g \in G \mid gH = Hg\}$$

que l'on appelle le *normalisateur* de H dans G. On a évidemment $H \lhd N_G(H)$ et $N_G(H)$ est le plus grand sous-groupe de G dans lequel H est distingué.

Exemple 5.11. — Le groupe $GL_n(\mathbb{R})$ agit sur $\mathbb{R}^n$ (orbites ? stabilisateurs ?). De même, le groupe $O_n(\mathbb{R})$ agit sur la sphère $\mathbb{S}^{n-1} = \{x \in \mathbb{R}^n \mid \|x\| = 1\}$ (orbites ? stabilisateurs ?). Le groupe dihédral D_n agit sur le polygone régulier à n côtés.

5.3. Équations aux classes et conséquences. — Dans ce paragraphe, X et G sont supposés finis. Si G agit sur X, on constate que les orbites forment une partition de X : elles recouvrent X et sont deux à deux disjointes. Si on choisit un représentant x_i de chaque orbite ($i = 1 \dots r$ avec r le nombre d'orbites), on a alors :

$$|X| = \sum_{i=1}^{r} |G \cdot x_i| = \sum_{i=1}^{r} |G|/|G_{x_i}|.$$

Proposition 5.12 **(Équation aux classes)**. — *Si G est un groupe fini, on considère l'action par conjugaison de G sur lui-même et on note $(g_j)_{1 \leq j \leq k}$ des représentants des orbites qui ne sont pas réduites à un point. On a alors :*

$$|G| = |Z(G)| + \sum_{j=1}^{k} [G : C_G(g_j)].$$

Définition 5.13. — Un p-groupe (avec p premier) est un groupe G d'ordre $|G| = p^n$.

Proposition 5.14. — *Si G est un p-groupe agissant sur X, on a alors*

$$|X| \equiv |X^G| \bmod p$$

avec $X^G := \{x \in X \mid \forall\, g \in G,\ g \cdot x = x\}$.

Corollaire 5.15. — *Le centre d'un p-groupe n'est pas réduit à l'identité.*

Théorème 5.16 **(Cauchy, 1845)**. — *Si l'entier premier p divise l'ordre du groupe fini G, alors G contient un élément d'ordre p.*

6. Étude du groupe symétrique

On rappelle que S_n est le groupe symétrique sur $\{1 \dots n\}$, d'ordre $n!$.

6.1. Signature d'une permutation. —

Définition 6.1. — La signature d'une permutation $\sigma \in \mathsf{S}_n$ est le nombre

$$\epsilon(\sigma) := \prod_{1 \leq i < j \leq n} \frac{\sigma(j) - \sigma(i)}{j - i}$$

qui vaut ± 1.

Proposition 6.2. — *L'application* $\epsilon : \mathsf{S}_n \longrightarrow \{\pm 1\} \simeq \mathbb{Z}/2\mathbb{Z}$ *est un morphisme de groupes.*

6.2. Décomposition en produit de cycles et conséquences. —

Définition 6.3. — – Le support d'une permutation $\sigma \in \mathsf{S}_n$ est

$$\mathrm{Supp}(\sigma) := \{1 \leq i \leq n \mid \sigma(i) \neq i\}.$$

- Un k-cycle (ou cycle de longueur k) est une permutation dont on peut écrire le support $\mathrm{Supp}(\sigma) = \{a_1, a_2, \ldots, a_k\}$ et qui vérifie : $\sigma(a_i) = a_{i+1}$ pour $1 \leq i \leq k-1$ et $\sigma(a_k) = a_1$.
- Un 2-cycle est aussi appelé une transposition.

Le k-cycle de support $\{a_1, a_2, \ldots, a_k\}$ sera noté $(a_1\ a_2\ \ldots\ a_k)$.

Proposition 6.4. — *Deux permutations à supports disjoints commutent :*

$$\mathrm{Supp}(\sigma) \cap \mathrm{Supp}(\tau) = \emptyset \Rightarrow \sigma\tau = \tau\sigma.$$

Théorème 6.5. — *Toute permutation s'écrit comme un produit de cycles à supports disjoints. L'écriture est de plus unique à l'ordre près. L'ordre d'une permutation est le plus petit commun multiple des longueurs des cycles qui apparaissent dans sa décomposition en produit de cycles.*

Remarque 6.6. — On vérifié aisément :

$$\sigma(a_1\ a_2\ \ldots\ a_k)\sigma^{-1} = (\sigma(a_1)\ \sigma(a_2)\ \ldots\ \sigma(a_k)).$$

Théorème 6.7. — *Deux permutations* σ *et* τ *sont conjuguées dans* S_n *si et seulement si* σ *et* τ *ont le même nombre de* k*-cycles dans leurs décompositions pour tout* $k = 1 \ldots n$.

Proposition 6.8. — *Les transpositions engendrent* S_n.

Proposition 6.9. — *(i) Une transposition a signature* -1 *;*

(ii) si σ *est un* k*-cycle,* $\epsilon(\sigma) = (-1)^{k-1}$ *;*

(iii) en général, $\epsilon(\sigma) = (-1)^{n - m_\sigma}$ *avec* m_σ *le nombre d'orbites de* σ.

6.3. Groupe alterné et simplicité. —

Définition 6.10. — Le groupe *alterné* est le noyau de la signature :

$$\mathsf{A}_n := \ker(\epsilon) \lhd \mathsf{S}_n.$$

C'est un sous-groupe normal d'indice 2 de S_n et d'ordre $|\mathsf{A}_n| = \dfrac{n!}{2}$.

Proposition 6.11. — *Le groupe alterné (pour $n \geq 3$) est engendré par les 3-cycles. Si $n \geq 5$, les 3-cycles sont de plus conjugués* dans A_n.

Proposition 6.12. — *Les centres et groupes dérivés de S_n et A_n sont donnés par :*
- $\mathsf{Z}(\mathsf{S}_n) = \{1\}$ *si* $n \geq 3$ *et* $\mathsf{Z}(\mathsf{A}_n) = \{1\}$ *si* $n \geq 4$ *;*
- $\mathsf{D}(\mathsf{S}_n) = \mathsf{A}_n$ *pour tout* $n \geq 2$ *et* $\mathsf{D}(\mathsf{A}_n) = \mathsf{A}_n$ *si* $n \geq 5$.

Théorème 6.13 **(Galois, 1830)**. — *Si $n \geq 5$, le groupe alterné A_n est simple.*

Corollaire 6.14. — *Si $n \geq 5$, les seuls sous-groupes normaux de S_n sont $\{1\}$, A_n et S_n.*

7. Produits semi-directs

7.1. produit direct. —

Définition 7.1. — Si G_1 et G_2 sont deux groupes, la loi :

$$\begin{cases} (\mathsf{G}_1 \times \mathsf{G}_2) \times (\mathsf{G}_1 \times \mathsf{G}_2) & \longrightarrow & \mathsf{G}_1 \times \mathsf{G}_2 \\ ((g_1, g_2), (h_1, h_2)) & \mapsto & (g_1 g_2, h_1 h_2) \end{cases}$$

munit l'ensemble $\mathsf{G} := \mathsf{G}_1 \times \mathsf{G}_2$ d'une structure de groupe, appelé le *produit direct de* G_1 et G_2.

Proposition 7.2. — *Un groupe G s'écrit comme un produit direct de deux groupes si (et seulement si) il existe $\mathsf{N}, \mathsf{Q} < \mathsf{G}$ deux sous-groupes de G tels que :*

*(*i*)* $\mathsf{N} \lhd \mathsf{G}$ *ainsi que* $\mathsf{Q} \lhd \mathsf{G}$ *;*

*(*ii*)* $\mathsf{N} \cap \mathsf{Q} = \{1\}$ *;*

*(*iii*)* $\mathsf{NQ} = \mathsf{G}$.

7.2. produit semi-direct. —

La situation d'un produit semi-direct correspond au cas où l'un des deux sous-groupes n'est plus distingué.

Définition 7.3. — Soient N et Q deux groupes, ainsi que $\alpha : \mathsf{Q} \longrightarrow \mathrm{Aut}(\mathsf{N})$ un morphisme. Le produit semi-direct de N par Q (sous l'action α) est le groupe dont l'ensemble sous-jacent est le produit $\mathsf{G} := \mathsf{N} \times \mathsf{Q}$ muni de la loi :

$$\begin{cases} \mathsf{G} \times \mathsf{G} & \longrightarrow & \mathsf{G} \\ ((n, q), (n', q')) & \mapsto & (n\alpha(q)(n'), qq') \end{cases}$$

Ce groupe est noté $\mathsf{G} = \mathsf{N} \rtimes_\alpha \mathsf{Q}$ ou simplement $\mathsf{N} \rtimes \mathsf{Q}$.

Remarque 7.4. — Dans $G := N \rtimes Q$, l'inverse est donné par $(n, q)^{-1} = (\alpha(q)^{-1}(n^{-1}), q^{-1})$. On vérifie facilement que $N \simeq N \times \{1\}$ est normal dans G.

Proposition 7.5. — *Un groupe G peut s'écrire comme le produit semi-direct de deux groupes si et seulement si $G = NQ$ avec N et Q deux sous-groupes de G vérifiant*

$$N \cap Q = \{1\} \quad \text{et} \quad N \lhd G.$$

7.3. Lien avec les extensions. —

Définition 7.6. — Une extension (ou suite exacte courte) est la donnée de deux morphismes :

$$f : N \longrightarrow G \quad \text{et} \quad \pi : G \longrightarrow Q$$

tels que :

1. f est injectif et π surjectif ;
2. $\ker(\pi) = \mathrm{Im}(f)$.

On résume cette situation en une *suite exacte courte* :

$$1 \longrightarrow N \xrightarrow{f} G \xrightarrow{\pi} Q \longrightarrow 1.$$

Remarque 7.7. — Une suite exacte consiste donc en la donnée d'un sous groupe normal $N \lhd G$ ou d'un morphisme surjectif $G \twoheadrightarrow Q$ car

$$Q \simeq G/\ker(\pi) = G/\mathrm{Im}(f) = G/N.$$

Définition 7.8. — On dira que la suite

$$1 \longrightarrow N \xrightarrow{f} G \xrightarrow{\pi} Q \longrightarrow 1$$

est *scindée* s'il existe un morphisme $s : Q \longrightarrow G$ tel que $\pi \circ s = \mathrm{Id}_Q$. Un tel morphisme est appelé une *section* de π.

Proposition 7.9. — *La suite*

$$1 \longrightarrow N \xrightarrow{f} G \xrightarrow{\pi} Q \longrightarrow 1$$

est scindée si et seulement s'il existe $\bar{Q} < G$ un sous-groupe tel que la restriction de π à $\bar{Q}$ soit un isomorphisme $\pi_{|\bar{Q}} : \bar{Q} \xrightarrow{\sim} Q$.

Dans ce cas, le groupe G est alors le produit semi-direct de N par Q (pour une action de Q sur N).

7.4. Étude du groupe dihédral. —

8. Théorèmes de Sylow

8.1. Rappels sur les p-groupes. — On rappelle qu'un p-groupe est un groupe dont l'ordre est de la forme p^n (définition 5.13) et que le centre d'un p-groupe n'est pas trivial (corollaire 5.15).

Proposition 8.1. — *Si* G *est un* p*-groupe avec* $|G| = p^n$*, alors* G *a des sous-groupes (*resp. *sous-groupes normaux) d'ordre* p^r *pour tout* $1 \leq r \leq n$*. Les sous-groupes d'indice* p *sont normaux dans* G *et tout sous-groupe de* G *est contenu dans un sous-groupe d'indice* p*.*

8.2. Énoncés des théorèmes. —

Définition 8.2. — Soit G un groupe d'ordre $n = p^r m$ avec $m \wedge p = 1$. Un sous-groupe P de G d'ordre $|P| = p^r$ est appelé un p-Sylow de G. L'ensemble des p-Sylow de G est noté

$$\mathrm{Syl}_p(G) = \{P < G \mid |P| = p^r\}.$$

***Théorème 8.3* (Sylow I, 1872)**. — *Si* G *est comme ci-dessus, alors* $\mathrm{Syl}_p(G) \neq \emptyset$*. En particulier,* G *a des sous-groupes d'ordre* p^s *pour tout* $s \leq r$*.*

Dans la suite, on va noter $s_p(G) := |\mathrm{Syl}_p(G)|$ le nombre de p-Sylow de G.

Lemme 8.4. — *Soient* $P < G$ *un* p*-Sylow d'un groupe* G *et* $H < G$ *un* p*-sous-groupe de* G*. Si* H *normalise* P *(c'est-à-dire si* $H \subset N_G(P)$*, alors* $H \subset P$*. En particulier, si* H *est un* p*-Sylow, alors* $H = P$*.*

***Théorème 8.5* (Sylow II)**. — *Soit* G *un groupe comme ci-dessus. On a alors :*

1. *deux éléments de* $\mathrm{Syl}_p(G)$ *sont conjugués : si* P *et* Q *sont deux* p*-Sylow de* G*, il existe alors* $g \in G$ *tel que* $P = gQg^{-1}$ *;*
2. $s_p(G) \equiv 1\,(p)$ *et* $s_p(G)$ *divise* m *;*
3. *tout* p*-sous-groupe de* G *est contenu dans un* p*-Sylow de* G*.*

Corollaire 8.6. — *Un* p*-Sylow d'un groupe* G *est normal dans* G *si et seulement si c'est l'unique* p*-Sylow de* G *(*$s_p(G) = 1$*).*

8.3. Conséquences pour les groupes de petit ordre. —

9. Groupes résolubles

9.1. Suite de composition et suite de Jordan-Hölder. —

Définition 9.1. — Une *suite de composition* (ou *suite sous-normale*) d'un groupe G est une suite décroissante de sous-groupes

$$\{1\} = G_n < G_{n-1} < \cdots < G_1 < G_0 = G$$

tels que $G_{i+1} \lhd G_i$ pour tout $i = 0 \ldots n-1$. Les quotients successifs G_i/G_{i+1} sont appelés les facteurs de la suite.

Définition 9.2. — Une suite de composition dont tous les facteurs sont simples est appelée une suite de Jordan-Hölder.

Théorème 9.3. — *Si* G *est un groupe fini, alors* G *admet au moins une suite de Jordan-Hölder.*

Remarque 9.4. — Le véritable contenu du théorème de Jordan-Hölder est de d'affirmer que si l'on prend deux suites de Jordan-Hölder, alors elles ont même longueur et les facteurs de ces deux suites sont les mêmes à permutation près des indices.

Parmi les groupes simples, les plus faciles à appréhender sont les groupes cycliques d'ordre premier. Nous allons voir que les groupes dont les facteurs de Jordan-Hölder sont cycliques forment une classe de groupes très intéressante.

9.2. suite dérivée d'un groupe. —

Définition 9.5. — Si G est un groupe, on définit par récurrence la suite décroissante de sous-groupes suivante :

$$D^0(G) := G \quad \text{et} \quad D^{i+1}(G) := [D^i(G), D^i(G)] \, \forall \, i \geq 0.$$

Cette suite s'appelle la *suite dérivée* de G.

Proposition 9.6. — *La suite dérivée d'un groupe est constituée de sous-groupes normaux de* G *:*

$$\forall \, i \geq 0, \ D^i(G) \lhd G.$$

De plus, les quotients successifs $D^i(G)/D^{i+1}(G)$ *sont abéliens.*

***Proposition 9.7* (fonctorialité de la suite dérivée)**. — *Si* $f : G \longrightarrow H$ *est un morphisme de groupes, on a alors :*

$$\forall \, i \geq 0, \ f\left(D^i(G)\right) = D^i\left(f(G)\right).$$

En particulier, $f\left(D^i(G)\right) \subset D^i(H)$ *pour tout* $i \geq 0$.

9.3. Notion de résolubilité. —

Définition 9.8. — Un groupe G est dit *résoluble* s'il existe un entier $n \geq 1$ tel que $D^n(G) = \{1\}$. On dit que G est résoluble *de classe* n si n est le plus entier i vérifiant $D^i(G) = \{1\}$.

Remarque 9.9. — Par convention, $\{1\}$ est le seul groupe de classe 0. Les groupes résolubles de classe 1 sont les groupes abéliens.

Proposition 9.10. — *Si* G *est résoluble, alors tout sous-groupe et tout quotient de* G *est encore résoluble.*

Réciproquement, si un groupe G *possède un sous-groupe normal* $N \lhd G$ *tel que* N *et* G/N *sont résolubles, alors* G *est lui-même résoluble.*

Théorème 9.11. — *Un groupe* G *est résoluble si et seulement s'il admet une suite de composition*

$$\{1\} = G_n < G_{n-1} < \cdots < G_1 < G_0 = G$$

dont les facteurs G_i/G_{i+1} *sont abéliens (pour* $1 \leq i \leq n-1$*).*

Corollaire 9.12. — *Un groupe fini est résoluble si et seulement si les facteurs de Jordan-Hölder sont des groupes cycliques d'ordres premiers.*

9.4. Classification des groupes finis simples (panorama). — À la fin du XIX$^{\text{ème}}$ siècle, il a semblé intéressant à quelques mathématiciens (par exemple Otto Hölder) de savoir si la classification des groupes finis simples était possible. Cet horizon est resté très lointain mais à partir des années 1950, les travaux autour de cette question se sont intensifiés (avec notamment Brauer) et le début des années 1960 a vu la démonstration d'une vieille conjecture sur les groupes simples.

Théorème 9.13 **(Feit-Thompson, 1963)**. — *Tout groupe d'ordre impair est résoluble. De façon équivalente, un groupe simple non abélien est d'ordre pair.*

La démonstration de ce résultat occupe un volume entier du *Pacific Journal of Mathematics* (plus de deux cents pages).

Le théorème précédent montre qu'un groupe simple admet des éléments d'ordre 2 et en examinant le centralisateur de ces involutions, il a été possible de dégager une liste complète des groupes finis simples à isomorphismes près. Ces groupes se répartissent en 4 classes :

1. les groupes cycliques d'ordres premiers ;
2. les groupes alternés A_n pour $n \geq 5$;
3. les groupes de type Lie (comme par exemple $\mathrm{PSL}_n(\mathbb{F}_q)$ pour $n \geq 3$ ou $n = 2$ et $q > 3$) ;
4. la classe des groupes *sporadiques*.

La dernière classe est finie contrairement aux 3 premières : il existe 26 groupes sporadiques qui échappent à toute classification. Le plus petit est un des groupes dits *de Mathieu* $M_{11} < S_{11}$:

$$|M_{11}| = 7920 = 2^4 \cdot 3^2 \cdot 5 \cdot 11.$$

Il y a 5 groupes de Mathieu découverts par Émile Mathieu entre 1861 et 1873.

Le plus gros des ces 26 groupes sporadiques a été baptisé le *Monstre* (découvert par Griess et Fischer en 1981) car son cardinal vaut :

$$\begin{aligned} |\text{Monstre}| &= 2^{46} \cdot 3^{20} \cdot 5^9 \cdot 7^6 \cdot 11^2 \cdot 13^3 \cdot 17 \cdot 19 \cdot 23 \cdot 29 \cdot 31 \cdot 41 \cdot 47 \cdot 59 \cdot 71 \\ &\approx 8{,}5 \cdot 10^{53} \end{aligned}$$

En guise de comparaison, on estime que le nombre d'atomes de l'univers est de l'ordre de 10^{80} ...

Pour aboutir à cette liste, il a fallu mettre ensemble des centaines d'articles ce qui représente des dizaine de milliers de pages. Pendant 20 ans (entre 1980 et le début des

années 2000), un important travail de synthèse (et parfois de réécriture) a été effectué et la communauté mathématique considère maintenant la liste ci-dessus comme étant complète.

Benoît Claudon