Université Aix-Marseille 2019–2020

Master 1 – Mathématiques & Applications
Algèbre & Géométrie

Notes de cours

Groupes (géométrie)

1 Généralités

1.1 Groupes et sous-groupes

Définition 1.1.1. On appelle *groupe* tout ensemble G muni d'une opération $.: G \times G \longrightarrow G$ associative ($\forall g_1, g_2, g_3 \in G, (g_1.g_2).g_3 = g_1.(g_2.g_3)$), admettant un élément neutre ($\exists e \in G, \forall g \in G, e.g = g.e = g$) et tel que tout élément possède un inverse ($\forall g \in G, \exists g' \in G, g.g' = g'.g$ élément neutre). On dit de plus que G est *abélien* si l'opération . est commutative ($\forall g_1, g_2 \in G, g_1.g_2 = g_2.g_1$).

Proposition 1.1.2.

- L'élément neutre de G est unique, et il est caractérisé comme l'unique solution dans G à l'équation $x * x = x$.
- Pour tout $g \in G$, l'inverse à droite et l'inverse à gauche de g sont uniques et égaux.

Notation 1.1.3. Dans tout ce qui suit, et sauf mention contraire, G et toute variation de la notation G sera un groupe. Si G est nommément abélien, on notera par $+$ son opération, par 0_G, ou 0 s'il n'y a pas d'ambiguité, son élément neutre, par $-g$ l'inverse de $g \in G$, par ng la somme itérée $n \in \mathbb{N}$ fois de $g \in G$ et par $-ng$ la somme itérée n fois de son inverse. Autrement, on notera par . son opération, par e_G, ou e s'il n'y a pas d'ambiguité, son élément neutre, par g^{-1} l'inverse de $g \in G$, par g^n le produit itéré $n \in \mathbb{N}$ fois de $g \in G$ et par g^{-n} le produit itéré n fois de son inverse.

Proposition 1.1.4.

- Pour tout $g \in G$ et tout $n_1, n_2 \in \mathbb{Z}$, on a $g^{n_1+n_2} = g^{n_1}.g^{n_2}$ et $g^{n_1 n_2} = (g^{n_1})^{n_2}$.
- Pour tous $g_1, g_2 \in G$, $(g_1.g_2)^{-1} = g_2^{-1}.g_1^{-1}$.

Définition 1.1.5. On appelle *ordre de* G, noté $|G|$, son cardinal (éventuellement infini) en tant qu'ensemble. Pour tout $g \in G$, on appelle *ordre de* g, noté $|g|$, le cardinal de l'ensemble $\{g^n \mid n \in \mathbb{Z}\}$.

Proposition 1.1.6. Pour tout élément $g \in G$, on a $|g| := \min\{n \in \mathbb{N} \mid g^n = e\}$, avec la convention que $\min \emptyset = \infty$.

Définition 1.1.7. Pour tout $g \in G$, on appelle *conjugué* de g tout élément de la forme $h^{-1}.g.h$ avec $h \in G$.

Proposition 1.1.8. La relation de conjugaison entre éléments d'un groupe est une relation d'équivalence. On peut notamment parler des *classes de conjugaison* d'un groupe.

Définition 1.1.9. Un sous-ensemble non vide $H \subset G$ est un *sous-groupe* s'il est stable par . et par inverse. On dit de plus que H est distingué s'il est stable par conjugaison, on note alors $H \lhd G$.

Proposition 1.1.10.

- Un sous-ensemble non vide $H \subset G$ est un sous-groupe ssi, pour tout $g_1, g_2 \in H$, $g_1.g_2^{-1} \in H$.
- Tout sous-groupe $H \subset G$ est un groupe dont l'élément neutre et les inverses sont identiques à ceux de G.

Exemple 1.1.11. Pour tout $g \in G$, le *centralisateur de* g, $Z_G(g) := \{g' \in G \mid g.g' = g'.g\}$, est un sous-groupe de G. Le *centre de* G, $Z(G) := \{g \in G \mid \forall g' \in G, g.g' = g'.g\}$, est un sous-groupe distingué de G.

Définition 1.1.12. On dit que G est *simple* si ses seuls sous-groupes distingués sont G et $\{e\}$.

1.2 Morphismes de groupes

Définition 1.2.1. Une application $f\colon G_1 \longrightarrow G_2$ entre deux groupes est un *morphisme de groupes* si elle respecte les opérations ($\forall g_1, g_2 \in G_1, f(g_1.g_2) = f(g_1).f(g_2)$). On parle même plus précisement de *monomorphisme*, d'*épimorphisme* et d'*isomorphisme de groupes* si f est respectivement injective, surjective ou bijective ; et on parle d'*endomorphisme de groupe* si $G_1 = G_2$, et d'*automorphisme* si f est simultanément un isomorphisme et un endomorphisme de groupes.

Exemple 1.2.2. Pour tout $g \in G$, l'application $\mathrm{conj}_g\colon G \longrightarrow G$ définie, pour tout $h \in G$, par $\mathrm{conj}_g(h) = g^{-1}.h.g$ est un automorphisme de groupe.

Proposition 1.2.3.

- Si $f\colon G_1 \longrightarrow G_2$ est un morphisme de groupes, alors $f(e_{G_1}) = e_{G_2}$ et, pour tout $g \in G$, $f(g^{-1}) = f(g)^{-1}$.
- La composé de deux morphismes de groupes est un morphisme de groupes et la réciproque d'un isomorphisme de groupes est un isomorphisme de groupes.

Proposition 1.2.4. L'ensemble des automorphismes de G, noté $\mathrm{Aut}(G)$, muni de la composition est un groupe dont Id_G est l'élément neutre.

Exemple 1.2.5. L'application $\mathrm{conj}\colon \begin{array}{ccc} G & \longrightarrow & \mathrm{Aut}(G) \\ g & \longmapsto & \mathrm{conj}_g \end{array}$ est un morphisme de groupes.

Définition 1.2.6. Soit $f\colon G_1 \longrightarrow G_2$ un morphisme de groupes. On appelle *image* de f, notée $\mathrm{Im}(f)$, son image ensembliste, et *noyau* de f, noté $\mathrm{Ker}(f)$, l'image réciproque de e_{G_2}.

Proposition 1.2.7. Soit $f\colon G_1 \longrightarrow G_2$ un morphisme de groupes. Alors :

- pour tout sous-groupe $H \subset G_1$, $f(H) \subset G_2$ est un sous-groupe ; notamment $\mathrm{Im}(f)$ est un sous-groupe de G_2 ;
- pour tout sous-groupe (distingué) $H \subset G_2$, $f^{-1}(H) \subset G_1$ est un sous-groupe (distingué) ; notamment $\mathrm{Ker}(f)$ est un sous-groupe distingué de G_2 ;
- f est un monomorphisme de groupes si et seulement si $\mathrm{Ker}(f) = \{e_{G_1}\}$.

Définition 1.2.8. On dit que G_1 et G_2 sont *isomorphes* s'il existe un isomorphisme de groupes $f\colon G_1 \longrightarrow G_2$.

Essentiellement, deux groupes isomorphes ne sont l'un pour l'autre qu'un renommage des éléments, cela ne change aucune de leurs propriétés algébriques. On n'étudie donc en général les groupes qu'*à isomorphisme près*. Mais attention toutefois, car l'isomorphisme entre deux groupes isomorphes n'est en général pas canonique !

1.3 Opérations sur les groupes

1.3.1 Opérations ensemblistes

Proposition 1.3.1. Soit $\left(H_i\right)_{i\in I}$ une famille de sous-groupes (resp. sous-groupes distingués) de G, alors $\bigcap\limits_{i\in I} H_i$ est un sous-groupe (resp. sous-groupe distingué) de G.

Exemple 1.3.2. On a $\bigcap\limits_{g\in G} Z_G(g) = Z(G)$.

Par contre, la réunion de sous-groupes n'est en général pas un sous-groupe car la stabilité par produit n'est pas assurée. Cela conduit à la notion suivante.

Définition 1.3.3. Soit $X \subset G$ un sous-ensemble non vide, on appelle *sous-groupe engendré* par X, noté $\langle X \rangle$, l'intersection de tous les sous-groupes de G contenant X. Il s'agit du plus petit sous-groupe de G contenant X.

Proposition 1.3.4. Soit $X =: \{g_i \mid i \in I\} \subset G$ un sous-ensemble non vide, alors

$$\langle X \rangle = \left\{ g_{i_1}^{\varepsilon_1} g_{i_2}^{\varepsilon_2} \cdots g_{i_k}^{\varepsilon_k} \mid k \in \mathbb{N}, i_1, \ldots, i_k \in I, \varepsilon_1, \ldots, \varepsilon_k \in \{\pm 1\} \right\},$$

avec la convention qu'un produit vide vaut e_G.

Définition 1.3.5. On dit qu'une famille $\left(g_i\right)_{i \in I}$ d'éléments de G *engendre* G si $\langle g_i \mid i \in I \rangle = G$.

1.3.2 Produits

Définition 1.3.6. Soit $\varphi \colon G_2 \longrightarrow \mathrm{Aut}(G_1)$ un morphisme de groupes. Alors l'opération

$$(g_1, g_2).(g_1', g_2') := \left(g_1 . {g_1'}^{\varphi(g_2)} \ , \ g_2 . g_2'\right),$$

avec ${g_1'}^{\varphi(g_2)} := \big(\varphi(g_2)\big)(g_1')$, muni $G_1 \times G_2$ d'une structure de groupe que l'on note $G_1 \rtimes_\varphi G_2$.

Exemples 1.3.7.

- En considérant le morphisme de groupes constant $\mathrm{Id}_{G_1} \colon G_2 \longrightarrow \mathrm{Aut}(G_1)$ qui envoie tout élément de G_2 sur Id_{G_1}, on définit le *produit direct* de G_1 et G_2, noté tout simplement $G_1 \times G_2$.
- Soit $\mathcal{E}$ un espace affine d'espace directeur E. Pour tout $x_0 \in \mathcal{E}$, chaque bijection affine f de $\mathcal{E}$ dans lui-même se décompose de manière unique en $f = f_{x_0} \circ t_{u_f}$, où $f_{x_0} \in \left\{h : \mathcal{E} \to \mathcal{E} \text{ affine} \mid h(x_0) = x_0\right\} \simeq \mathrm{GL}(E)$ et $t_{u_f} \in \left\{t \text{ translations de } \mathcal{E}\right\} \simeq E$. Cela définit une bijection entre le groupe des bijections affines de $\mathcal{E}$ dans lui-même et le produit cartésien $E \times \mathrm{GL}(E)$. En utilisant cette bijection pour transporter la structure de groupe des bijections affines sur $E \times \mathrm{GL}(E)$, on obtient $E \rtimes_{\mathrm{Id}_{\mathrm{GL}(E)}} \mathrm{GL}(E)$.
- Soit $H_1, H_2 \subset G$ deux sous-groupes tels que $H_1 \cap H_2 = \{e\}$ et $H_1 \lhd G$. Sous ces conditions, on peut montrer que $\langle H_1 \cup H_2 \rangle$ est en bijection avec $H_1 \times H_2$. En utilisant cette bijection pour transporter la structure de groupe de $\langle H_1 \cup H_2 \rangle$ sur $H_1 \times H_2$, on obtient $H_1 \rtimes_{\mathrm{conj}^{|H_1}_{|H_2}} H_2$ avec

$$\mathrm{conj}^{|H_1}_{|H_2} \colon \begin{array}{ccc} H_2 & \longrightarrow & \mathrm{Aut}(H_1) \\ g & \longmapsto & h \mapsto \mathrm{conj}_g(h) \end{array}.$$

1.3.3 Quotients

Proposition 1.3.8. Soit G un groupe. Pour tout sous-groupe $H \subset G$, les relations

$$g_1 \, {}_H\!\sim g_2 \Leftrightarrow g_1^{-1}.g_2 \in H \qquad\qquad g_1 \sim_H g_2 \Leftrightarrow g_1.g_2^{-1} \in H$$

définies sur G sont des relations d'équivalence dont les classes d'équivalences correspondent, respectivement, à $\left\{g.H := \{g.h | h \in H\} \mid g \in G\right\}$ et $\left\{H.g := \{h.g | h \in H\} \mid g \in G\right\}$.

Définition 1.3.9. On définit les *classes à gauche* (resp. *classes à droite*) d'un sous-groupe $H \subset G$ comme les classes d'équivalence de ${}_H\!\sim$ (resp. $\sim_H$).

Proposition 1.3.10. Soit $H \subset G$ un sous-groupe.

- Les classes à gauche (resp. à droite) de H forment une partition de G.
- Toute classe à gauche ou à droite de H est en bijection avec H.

Définition 1.3.11. On appelle *indice* d'un sous-groupe $H \subset G$ le cardinal, noté $[G : H]$, de ses classes à gauche.

Proposition 1.3.12. Pour tout sous-groupe $H \subset G$, on a $|G| = [G : H].|H|$.

Corollaire 1.3.13 (théorème de Lagrange)**.** Si G est fini et si $H \subset G$ est un sous-groupe, alors $|H|$ divise $|G|$.

Corollaire 1.3.14. Si G est fini, alors l'ordre de tout élément divise $|G|$.

Proposition 1.3.15. Soit G un groupe et $H \subset G$ un sous-groupe. Alors les propositions suivantes sont équivalentes :

i. $H \lhd G$;
ii. les relations d'équivalence ${}_H\!\sim$ et $\sim_H$ sont égales ;
iii. pour tout $g \in G$, $g.H = H.g$.

Proposition 1.3.16. Pour tout $H \lhd G$, l'opération de groupe de G induit une structure de groupe sur l'espace quotient $G/_{H\sim}$.

Notation 1.3.17. Pour tout $H \lhd G$, on note G/H le groupe quotient associé, et $\pi_H : G \longrightarrow G/H$ la surjection canonique qui envoie tout $g \in G$ sur $g.H$.

Proposition 1.3.18 (propriété universelle du groupe quotient)**.** Soit $H \lhd G$. Pour tout groupe K, on note $\mathcal{P}_H$ la propriété suivante :
Il existe un morphisme de groupe $\pi : G \longrightarrow H$ avec $H \subset \mathrm{Ker}(\pi)$ vérifiant que, pour tout morphisme de groupes $f : G \longrightarrow G'$ avec $H \subset \mathrm{Ker}(f)$, il existe un unique morphisme de groupes $\overline{f} : G/H \longrightarrow G'$ tel que

$$\begin{array}{ccc} G & \xrightarrow{f} & G' \\ {\scriptstyle\pi}\downarrow & \circlearrowleft & \nearrow{\scriptstyle\overline{f}} \\ K & & \end{array} .$$

Alors K satisfait $\mathcal{P}_H$ ssi il est isomorphe à G/H.

Remarque 1.3.19. Cette propriété énonce non seulement que G/H satisfait $\mathcal{P}_H$, mais aussi que $\mathcal{P}_H$ caractérise G/H à isomorphisme près.

Corollaire 1.3.20. Soit $H_1 \lhd G_1$, $H_2 \lhd G_2$ et un morphisme de groupes $f : G_1 \longrightarrow G_2$ tel que $f(H_1) \subset H_2$. Il existe un unique morphisme de groupes $\overline{f} : G_1/H_1 \longrightarrow G_2/H_2$ tel que

$$\begin{array}{ccc} G_1 & \xrightarrow{f} & G_2 \\ {\scriptstyle\pi_{H_1}}\downarrow & \circlearrowleft & \downarrow{\scriptstyle\pi_{H_2}} \\ G_1/H_1 & \xrightarrow[\overline{f}]{} & G_2/H_2 \end{array} .$$

La notion de groupe quotient permet d'établir trois résultats important d'isomorphismes.

Proposition 1.3.21 (premier théorème d'isomorphisme)**.** Soit $f : G_1 \longrightarrow G_2$ un morphisme de groupes. Alors $\mathrm{Im}(f) \cong G_1/\mathrm{Ker}(f)$.

Lemme 1.3.22. Soit $H \lhd G$ et $H' \subset G$ un sous-groupe. Alors $H.H' := \{h.h' \mid h \in H, h' \in H'\} \subset G$ est un sous-groupe de G, $H \cap H' \lhd H'$ et $H \lhd H.H'$.

Proposition 1.3.23 (second théorème d'isomorphisme)**.** Soit $H \lhd G$ et $H' \subset G$ un sous-groupe. Alors $H'/H \cap H' \cong H.H'/H$.

Lemme 1.3.24. Soit $H \lhd G$. L'application

$$\psi : \begin{array}{ccc} \{K \lhd G/H\} & \longrightarrow & \{K \lhd G \mid H \subset K\} \\ K & \longmapsto & \pi_H^{-1}(K) \end{array}$$

est une bijection. En particulier, si $H \subset K \lhd G$, alors $H'/H \lhd G/H$.

Proposition 1.3.25 (troisième théorème d'isomorphisme)**.** Soit $H \lhd G$. Alors pour tout $H \subset K \lhd G$ $\big(G/H\big)/\big(H'/H\big) \cong G/H'$.

1.4 Actions de groupe

Définition 1.4.1. On dit que G *agit* (à gauche) sur un ensemble X s'il existe une application $._a : G \times X \longrightarrow X$ telle que, pour tout $x \in X$, $e._a x = x$ et, pour tous $g_1, g_2 \in G$, $g_1._a(g_2._a x) = (g_1.g_2)._a x$. On parle alors d'*action de G sur X*.

Notation 1.4.2. Lorsqu'il n'y a pas d'ambiguité, on notera $.$ pour $._a$, cela permet d'interpréter la seconde condition comme un phénomène d'associativité. Il faudra toutefois rester vigilant aux arguments et ne pas confondre l'opération de groupe et l'action.

Exemples 1.4.3.

- Tout groupe G agit trivialement sur tout ensemble X par $g.x := x$.
- Tout groupe G agit sur lui-même par [1]
  - translation à gauche $g.h := g.h$;
  - translation à droite $g.h := h.g^{-1}$;
  - conjugaison $g.h := g.h.g^{-1}$.
- Le groupe $\mathbb{R}^2$ agit par translation sur les points du plan.
- Le groupe des isométries du plan agit sur les points du plan, sur les droites du plan, sur les cercles du plan.
- Le groupe des bijections affines du plan agit sur les ellipses du plan.

Proposition 1.4.4. Soit G un groupe et X un ensemble. Alors l'application

$$\xi : \begin{array}{ccc} \{a \text{ action de } G \text{ sur } X\} & \to & \big\{\rho : G \to \mathrm{Bij}(X) \text{ morphisme de groupes}\big\} \\ a & \mapsto & g \mapsto (x \mapsto g.x) \end{array}$$

est une bijection d'inverse $\xi^{-1}(\rho) = \Big((g,x) \mapsto \big(\rho(g)\big)(x)\Big)$.

Définition 1.4.5. Soit une action de G sur un ensemble X.

- Pour tout $x \in X$, on appelle *orbite* de x l'ensemble $\mathcal{O}(x) := \big\{g.x \mid g \in G\big\}$ et *stabilisateur* de x l'ensemble $\mathrm{Stab}(x) := \big\{g \in G \mid g.x = x\big\}$.
- On appelle *ensemble des points fixe de l'action* l'ensemble $\mathrm{Fix}(G) := \bigcap\limits_{g \in G} \mathrm{Fix}(g)$ avec, pour tout $g \in G$, $\mathrm{Fix}(g) := \big\{x \in X \mid g.x = x\big\}$.

Proposition 1.4.6. Soit une action de G sur un ensemble X et x un point de X :

- $\mathrm{Stab}(x)$ est un sous-groupe de G ;
- pour tout $y \in \mathcal{O}(x)$, $\mathrm{Stab}(y) = g.\mathrm{Stab}(x).g^{-1}$ avec $g \in G$ tel que $g.x = y$;
- les orbites forment une partition de X.

Proposition 1.4.7 (formule aux classes)**.** Soit une action de G sur un ensemble X. Alors pour tout $x \in X$, on a $|\mathcal{O}(x)| = [G : \mathrm{Stab}(x)]$.

Proposition 1.4.8. Soit une action de G sur un ensemble X. On note $\mathfrak{O}$ l'ensemble des orbites. Alors

- (équation aux classes) $|X| = \sum\limits_{\mathcal{O} \in \mathfrak{O}} [G : \mathrm{Stab}(x_{\mathcal{O}})]$, où $x_{\mathcal{O}} \in \mathcal{O}$. [2]
- (formule de Burnside) $|\mathfrak{O}|.|G| = \sum\limits_{g \in G} |\mathrm{Fix}(g)|$.

Définition 1.4.9. On dit qu'une action est :

- *transitive* si elle ne posède qu'une seule orbite ;
- *libre* si tous les stabilisateurs sont réduit à l'élément neutre ;
- *fidèle* si l'intersection de tous les stabilisateurs est réduit à l'élément neutre ;
- *simplement transitive* si elle est transitive et libre.

1. attention, le signe . à gauche du := dénote l'action tandis que ceux à droite dénotent le produit dans G
2. $[G : \mathrm{Stab}(x_{\mathcal{O}})]$ ne dépend pas du choix de $x_{\mathcal{O}} \in \mathcal{O}$

2 Exemples

2.1 Groupes symétriques

2.1.1 Définitions

Définition 2.1.1. Soit X un ensemble, on appelle *groupe des permutations de* X l'ensemble $\mathfrak{S}_X$ des bijections de X dans lui-même muni de la composition.

Notation 2.1.2. Pour tout $n \in \mathbb{N}$, on note $\mathfrak{S}_n := \mathfrak{S}_{[\![1,n]\!]}$ avec la convention que $[\![1,0]\!] = \emptyset$.

Proposition 2.1.3.

- Pour tout ensemble X, $\mathfrak{S}_X$ agit naturellement sur X.
- Si X_1 et X_2 sont deux ensembles équipotents, alors les groupes $\mathfrak{S}_{X_1}$ et $\mathfrak{S}_{X_2}$ sont isomorphes. En particulier, si X est fini, on a $\mathfrak{S}_X \cong \mathfrak{S}_{|X|}$.
- Si $X_1 \subset X_2$, il existe un monomorphisme de groupes envoyant $\mathfrak{S}_{X_1}$ dans $\mathfrak{S}_{X_2}$. En particulier, $\mathfrak{S}_n$ peut être vu comme un sous-groupe de $\mathfrak{S}_{n+1}$.
- Pour tout ensemble X, $\mathfrak{S}_X$ est abélien ssi $|X| \leq 2$.
- Pour tout $n \in \mathbb{N}$, on a $|\mathfrak{S}_n| = n!$.

Remarque 2.1.4. Le fait que $\mathfrak{S}_X$ agissent sur X permet d'introduire tout le vocabulaire associée : orbites, stabilisateurs, éléments fixes, etc.

Notation 2.1.5. Pour tout ensemble fini non vide $X = \{x_1, \ldots, x_n\}$, on peut noter tout élément $\sigma \in \mathfrak{S}_X$ par

$$\begin{pmatrix} x_1 & x_2 & \cdots & x_n \\ \sigma(x_1) & \sigma(x_2) & \cdots & \sigma(x_n) \end{pmatrix}.$$

Le cas échéant, on pourra omettre les colonnes correspondant aux éléments de $\mathrm{Fix}(\sigma)$.

Théorème 2.1.6 (de Cayley)**.** Tout groupe G est isomorphe à un sous-groupe de $\mathfrak{S}_G$

2.1.2 Décompositions

Définition 2.1.7. On définit le *support* d'une permutation comme l'ensemble des éléments non fixes pour cette permutation. On appelle *cycle* ou *permutation circulaire* toute permutation dont le support est formée d'une unique orbite. Pour tout entier $k \geq 2$, on appelle *k–cycle* tout cycle dont le support est de cardinal k ; si $k = 2$, on parle aussi de *transposition*.

Proposition 2.1.8.

- Deux cycles à supports disjoints commutent.
- Pour toute permutation et à l'ordre des facteurs près, il existe une unique décomposition en produit de cycles disjoints.

Proposition 2.1.9.

- L'ordre d'un cycle est égal au cardinal de son support.
- Si X est fini, l'ordre de $\sigma \in \mathfrak{S}_X$ est égal au ppcm des ordres des cycles apparaissant dans sa décomposition en cycles disjoints.

Notation 2.1.10. Pour tout $n \in \mathbb{N}^*$,

- on peut noter tout cycle $\sigma \in \mathfrak{S}_n$ comme $\big(i, \sigma(i), \sigma^2(i), \ldots, \sigma^{|\sigma|-1}(i)\big)$ où i est le plus petit élément du support de σ ;

- on peut utiliser l'unique décomposition en cycles disjoints pour noter toute permutation $\sigma \in \mathfrak{S}_n$ comme $\big(i_1, \sigma(i_1), \dots\big)\big(i_2, \sigma(i_2), \dots\big) \cdots \big(i_k, \sigma(i_k), \dots\big)$ où, pour tout $j \in [\![1, k]\!]$, $\big(i_j, \sigma(i_j), \dots\big)$ correspond au cycle de la décomposition tel i_j soit le plus petit élément du support de σ privé de toutes les orbites contenant les valeurs $i_1, \dots, i_{j-1}$.

Remarque 2.1.11. La concaténation des cycles dans la notation précédente correspond au produit . des cycles ; l'ordre de lecture n'importe pas puisque tous les cycles commutent. On peut, bien entendu, considérer des produits $\big(i_1, \sigma(i_1), \dots\big).\big(i_2, \sigma(i_2), \dots\big)$ de cycles même s'ils sont non disjoints, mais l'ordre de lecture est alors important. Pour les permutations, le lecture se fait classiquement de droite à gauche.

Proposition 2.1.12.
- Pour tout ensemble fini X, $\mathfrak{S}_X$ est engendré par les transpositions.
- Pour tout $n \in \mathbb{N}$, $\mathfrak{S}_n$ est engendré par les transpositions de la forme $\big(i(i+1)\big)$ avec $i \in [\![1, n-1]\!]$.
- Pour tout $n \in \mathbb{N}$, $\mathfrak{S}_n$ est engendré par (12) et $(123 \cdots n)$.

Proposition 2.1.13. Pour tout $n \in \mathbb{N}$, les transpositions de $\mathfrak{S}_n$ sont deux à deux conjuguées.

2.1.3 Signature

Dans cette partie, on fixe un entier $n \geq 2$.

Lemme 2.1.14. Pour toute permutation $\sigma \in \mathfrak{S}_n$, la parité des quantités suivantes sont égales :
- le nombre de facteurs dans une décomposition de σ en produit de transpositions ;
- le nombre de k–cycles avec k pair dans la décomposition de σ en produits de cycles disjoints ;
- le nombre d'*inversions* de σ, c'est-à-dire le nombre de couples (i, j), avec $1 \leq i < j \leq n$, tels que $\sigma(i) > \sigma(j)$;
- $n - k$, où k est le nombre d'orbites de σ.

Proposition 2.1.15. Il existe un unique épimorphisme de groupes sign : $\mathfrak{S}_n \longrightarrow \big\{\pm 1\big\}$, appelé *signature*.

Définition 2.1.16. On définit $\mathcal{A}_n$, le $n^{ième}$ *groupe alterné* comme le noyau de sign : $\mathfrak{S}_n \longrightarrow \big\{\pm 1\big\}$.

Proposition 2.1.17. On a
- $\mathcal{A}_n \lhd \mathfrak{S}_n$;
- $|\mathcal{A}_n| = \frac{n!}{2}$, notamment $\mathcal{A}_2$ est réduit à l'élément neutre ;
- $\mathcal{A}_n$ est engendré par les 3–cycles ;
- Si $n \geq 5$, $\mathcal{A}_n$ est simple.

2.2 Groupes linéaires et orthogonaux

Dans toute cette partie, et sauf mention contraire, on fixe E un espace vectoriel de dimension finie $n \in \mathbb{N}^*$ sur un corps k.

2.2.1 Groupe linéaire

2.2.1.1 Définitions et générations

Définition 2.2.1. On définit
- le *groupe linéaire* $\mathrm{GL}(E)$ comme le groupe des endomorphismes bijectifs de E pour la composition ;
- le *groupe spécial linéaire* $\mathrm{SL}(E)$ comme le noyau du morphisme $\det \mathrm{GL}(E) \to k^*$.

Remarque 2.2.2. Le groupe linéaire $\mathrm{GL}(E)$ est isomorphe au groupe $\mathrm{GL}_n(k)$ des matrices inversibles de taille n à coefficients dans k, muni du produit matriciel.

A l'instar du groupe symétrique, engendré par les transposition qui sont les permutations non triviales laissant le plus de points fixes, montrons que $\mathrm{GL}(E)$ est engendré par les applications linéaires non triviales fixant le plus de points.

Proposition 2.2.3. Soit $u \in \mathrm{GL}(E)$ laissant fixe un hyperplan $H \subset E$. Les propositions suivantes sont équivalentes :

- $det(u) =: \lambda \neq 1$;
- u est diagonalisable et admet une valeur propre $\lambda \neq 1$;
- $E = H \oplus \mathrm{Im}(u - \mathrm{Id})$;
- il existe une base dans laquelle la matrice de u est diagonale avec des coefficienst qui valent tous 1 sauf le dernier qui vaut $\lambda \neq 1$.

Définition 2.2.4. Si l'une des assertions de la proposition est vérifiée, on dit que u est une dilation de rapport λ et de droite $\mathrm{Im}(u - \mathrm{Id})$.

Proposition 2.2.5. Soit $u \in \mathrm{GL}(E) \setminus \{\mathrm{Id}\}$ laissant fixe un hyperplan $H \subset E$. Les propositions suivantes sont équivalentes :

- $det(u) = 1$;
- u n'est pas diagonalisable ;
- $\mathrm{Im}(u - \mathrm{Id}) \subset H$;
- il existe une base dans laquelle la matrice de u est de la forme :

$$\left(\begin{array}{ccc|cc} & & & 0 & 0 \\ & I_{n-1} & & \vdots & \vdots \\ & & & 0 & 0 \\ \hline 0 & \cdots & 0 & 1 & 1 \\ 0 & \cdots & 0 & 0 & 1 \end{array}\right).$$

Définition 2.2.6. Si l'une des assertions de la proposition est vérifiée, on dit que u est une transvection d'hyperplan H et de droite $\mathrm{Im}(u - \mathrm{Id})$.

Remarque 2.2.7. Attention, par définition, l'identité n'est pas une transvection. De plus, une transvection n'est pas déterminée de manière unique par son hyperplan et sa droite.

Proposition 2.2.8.

- L'ensemble des dilatations et l'ensemble des transvections sont chacun stable par conjugaison et prise d'inverse.
- Deux dilatations sont conjugués dans $\mathrm{GL}(E)$ ssi elles ont le même rapport ; elles le sont alors également dans $\mathrm{SL}(E)$.
- Deux transvections sont toujours conjugués dans $\mathrm{GL}(E)$, et elles le sont également dans $\mathrm{SL}(E)$ si $n \geq 3$.

Proposition 2.2.9.

- SL_n est engendré par transvections.
- GL_n est engendré par les transvections et les dilatations.

Démonstration. On travaille par récurrence sur n en choisissant un vecteur x_0 et en imposant qu'il soit fixé en utilisant le lemme suivant :

Lemme 2.2.10. Si $n \geq 2$ alors, pour tout $x_1, x_2 \in E$ non nuls il existe une transvection ou un produit de deux transvections envoyant x_1 sur x_2.

Il se démontre en traitant d'abord le cas où x_1 et x_2 ne sont pas colinéaires. On considère $\big(x \mapsto x + f(x).(x_2 - x_1)\big)$ avec f une forme linéaire telle que $x_2 - x_1 \in \mathrm{Ker}(f)$ et $f(x_1) = 1$. S'ils sont colinéaires, on utilise un troisième point x_3 qui ne l'est pas. □

2.2.1.2 Géométrie projective

Eléments de géométrie projective

Définition 2.2.11. On appelle *espace projectif associé à* E, noté $\mathbb{P}(E)$ ou $\mathbb{P}^{n-1}(\mathbb{K})$ si $E = \mathbb{K}^n$, l'espace des droites vectoriels de E.
On dit que $\mathbb{P}(E)$ est de dimension finie $n-1$. Si $n = 2$, on parle de *droite projective*, et si $n = 3$, on parle de *plan projectif*.

Exemples 2.2.12.

- Si $E = \{0\}$, alors $\mathbb{P}(E)$ est vide.
- Si $n = 1$, alors $\mathbb{P}(E)$ contient un unique point.
- L'espace $P^{n-1}(\mathbb{R})$ est homéomorphe à $S^{n-1}/\!/x \sim -x$. Si $n = 2$, cela donne S^1. Si $n = 3$, cela donne une surface non orientable obtenue en recollant un disque sur le bord d'un ruban de Möbius.
- L'espace $P^1(\mathbb{C})$ est homéomorphe à S^2.
- L'espace $P^1(\mathbb{F}_2)$ contient 3 points et $P^2(\mathbb{F}_2)$, appelé *plan de Fano*, en contient 7.

Définition 2.2.13. On dit qu'une partie X de $\mathbb{P}(E)$ est un *sous-espace projectif* si elle est elle-même l'espace projectif associé à un sous-espace-vectoriel de E, c'est-à-dire si il existe $F \subset E$ sous-espace vectoriel tel que $X = \mathbb{P}(F)$.
Si $\dim(F) = 2$, on parle de *droite projective de* $\mathbb{P}(E)$ et si $\dim(F) = \dim(E) - 1$, on parle d'*hyperplan projectif de* $\mathbb{P}(E)$.

Exemples 2.2.14.

- L'ensemble vide est un sous-espace projectif.
- Chaque point d'un espace projectif est un sous-espace projectif.

Proposition 2.2.15. Si P_1 et P_2 sont deux sous-espaces projectifs de $\mathbb{P}(E)$ tels que $\dim(P_1)+\dim(P_2) \geq n-1$, alors $P_1 \cap P_2 \neq \emptyset$. En particulier, deux droites distinctes d'un plan projectif s'intersectent toujours en un point.

Plus généralement, les trois propositions suivantes sont vraies pour tout espace projectif et ceci permet de définir une notion d'*espace projectif abstrait*.

Proposition 2.2.16. Soit $\mathbb{P}(E)$ un espace projectif.

- Par deux points distincts $a \neq b \in \mathbb{P}(E)$ il passe une unique droite projective que l'on note (ab).
- Toute droite projective contient au moins 3 points.
- Si $a, b, c, d \in \mathbb{P}(E)$ sont quatre points distincts tels que les droites (ab) et (cd) se coupent, alors les droites (ac) et (bd) se coupent aussi.

Exemple 2.2.17. Dessin du plan de Fano avec ses 7 droites.

Proposition 2.2.18.

- Le complémentaire d'un hyperplan projectif $\mathbb{H} \subset \mathbb{P}(E)$ est homéomorphe à un espace affine de dimension $n-1$.
- Tout espace affine peut être prolongé en un espace projectif.
- Tout espace projectif de dimension d peut être décomposé en la réunion $\sqcup_{i=0}^{d} A_i$ de $d+1$ espaces affines tels que $\dim(A_i) = i$ pour tout $i \in \{0, 1, \ldots, d\}$.

Exemples 2.2.19.

- $P^1(\mathbb{R}) \simeq S^1$ peut se décomposer en une droite (ou un segment) plus un point collé simultanément aux deux extrémités.
- $P^2(\mathbb{R})$ peut se décomposer en un plan (ou un disque) plus une copie de $P^1(\mathbb{R})$ collé sur son bord, ou encore comme la réunion d'un point, d'un segment et d'un disque.

- $P^1(\mathbb{C}) \simeq S^2$ peut se décomposer comme une droite complexe (c'est-à-dire un plan réel) et un point.

Théorème 2.2.20.

- (Desargues) Soit $a_1, b_1, c_1, a_2, b_2, c_2$ six points en position générale d'un espace projectif. On note $a_0 = (b_1c_1) \cap (b_2c_2)$,$b_0 = (c_1a_1) \cap (c_2a_2)$ et $c_0 = (a_1b_1) \cap (a_2b_2)$. Alors a_0, b_0, c_0 alignés ssi $(a_1a_2), (b_1b_2), (c_1c_2)$ concourantes.
- (Pappus) Si k est commutatif, alors pour toutes droites D_1, D_2 d'un plan projectif sur k, tous points $a_1, b_1, c_1 \in D_1 \setminus D_2$, et tous points $a_2, b_2, c_2 \in D_2 \setminus D_1$, on a $(a_1b_2) \cap (a_2b_1)$, $(b_1c_2) \cap (b_2c_1)$ et $(c_1a_2) \cap (c_2a_1)$ alignés.

Groupes projectifs Dans ce qui suit, on note $\pi_E : E \setminus \{0\} \to \mathbb{P}(E)$ la surjection canonique définie par $\pi_E(x) = k.x$ et π_E^{-1} n'importe quel inverse à droite de π_E.

Lemme 2.2.21. Pour $f \in \mathrm{GL}(E)$, $\pi_E \circ f \circ \pi_E^{-1} : \mathbb{P}(E) \to \mathbb{P}(E)$, appelé *projectivisé* de f, est bien défini.

Définition 2.2.22. On appelle *homographie* de $\mathbb{P}(E)$ toute application de la forme $P(f)$ avec $f \in \mathrm{GL}(E)$, et on note $\mathrm{PGL}(E)$ l'ensemble des homographies de $\mathbb{P}(E)$. On note $\mathrm{PSL}(E) \subset \mathrm{PGL}(E)$ le sous-groupe des éléments de la forme $P(f)$ avec $f \in \mathrm{SL}(E)$.

Remarque 2.2.23. On peut, bien entendu, définir des applications projectives entre deux espaces projectifs distincts. Toutefois, si $f : E \to F$ n'est pas injective, $\mathrm{Ker}(f)$ contient des droites dont l'image n'est pas définie. Il faut donc, ou bien se restreindre aux applications linéaires injectives, ou bien accepter qu'une application projective partant de $\mathbb{P}(E)$ puisse ne pas être défini sur tout $\mathbb{P}(E)$.

Proposition 2.2.24.

- $\mathrm{PGL}(E)$ et $\mathrm{PSL}(E)$ sont des groupes pour la composition.
- Pour tous $f, g \in \mathrm{GL}(E)$, on a $P(f) = P(g)$ ssi il existe $\lambda \in k^*$ tel que $g = \lambda.f$.
- $\mathrm{PGL}(E) \cong {GL(E)}/{Z\big(\mathrm{GL}(E)\big)} \cong {\mathrm{GL}_n(k)}/{\big\{\mathrm{Diag}(\lambda, \dots, \lambda) \mid \lambda \in k^*\big\}}$.
- $\mathrm{PSL}(E) \cong {SL(E)}/{Z\big(\mathrm{SL}(E)\big)} \cong {\mathrm{SL}_n(k)}/{\big\{\mathrm{Diag}(\lambda, \dots, \lambda) \mid \lambda \in k_n^*\big\}}$ où k_n^* est l'ensemble des racines n-ième de l'unité dans k.

Les résultats de générations de $\mathrm{GL}(E)$ et $\mathrm{SL}(E)$ s'étendent bien entendu à $\mathrm{PGL}(E)$ et $\mathrm{PSL}(E)$.

Proposition 2.2.25. Si $n \geq 3$, $\mathrm{PSL}_n(E)$ est simple.

Remarque 2.2.26. La proposition précédente reste vraie si $n = 2$ et $k \neq \mathbb{F}_2, \mathbb{F}_3$.

2.2.1.3 Groupes linéaires sur les corps finis Nous verrons bientôt que, pour tout $q := p^r$, avec p premier et $r \in \mathbb{N}^*$, il existe, à isomorphisme près, un unique corps $\mathbb{F}_q$ de cardinal q. Par exemple, $\mathbb{F}_p \cong {\mathbb{Z}}/{p\mathbb{Z}}$.

Proposition 2.2.27. Si $k = \mathbb{F}_q$ pour un certain q, alors

- $|\mathrm{GL}(E)| = (q^n - 1)(q^n - q) \cdots (q^n - q^{n-1})$;
- $|\mathrm{SL}(E)| = (q^n - 1)(q^n - q) \cdots (q^n - q^{n-2})q^{n-1}$;
- $|\mathrm{PGL}(E)| = |\mathrm{SL}(E)|$;
- $|\mathrm{PSL}(E)| = \frac{|\mathrm{SL}(E)|}{\mathrm{pgcd}(n, q-1)}$.

Proposition 2.2.28. On a

- $\mathrm{GL}_2(\mathbb{F}_2) = \mathrm{SL}_2(\mathbb{F}_2) = \mathrm{PGL}_2(\mathbb{F}_2) = \mathrm{PSL}_2(\mathbb{F}_2) \cong \mathfrak{S}_3$;
- $\mathrm{PGL}_2(\mathbb{F}_3) \cong \mathfrak{S}_4$;
- $\mathrm{PSL}_2(\mathbb{F}_4) \cong \mathcal{A}_4$;
- $\mathrm{PGL}_2(\mathbb{F}_5) \cong \mathfrak{S}_5$;
- $\mathrm{PGL}_2(\mathbb{F}_4) \cong \mathrm{PSL}_2(\mathbb{F}_4) \cong \mathrm{PSL}_2(\mathbb{F}_5) \cong \mathcal{A}_5$.

Remarque 2.2.29. Cette liste n'est pas exhaustive, on pourra citer également $\mathrm{PSL}_2(\mathbb{F}_7) \cong \mathrm{PSL}_3(\mathbb{F}_3) \cong \mathrm{GL}_3(\mathbb{F}_2)$, $\mathrm{PSL}_2(\mathbb{F}_9) \cong \mathcal{A}_6$ ou $\mathrm{GL}_4(\mathbb{F}_2) = \mathrm{PSL}_4(\mathbb{F}_2) \cong \mathcal{A}_8$.