Chapitre 2
Groupes

1 Groupes et sous-groupes

Définition 1.1.
Un groupe est un ensemble G muni d'une loi de composition interne $*$ vérifiant :

- *$*$ est associative.*
- *$*$ admet un élément neutre e ($\forall x \in G, x * e = e * x = x$).*
- *Tout élément de G est inversible ($\forall x \in G, \exists y \in G, x * y = y * x = e$, un tel y est alors unique. On le note x^{-1}).*

Le groupe est dit abélien ou commutatif si $*$ est commutative.

Remarque 1.2.

- *On écrit fréquemment xy pour $x * y$.*
- *Le symbole $+$ est reservé aux lois commutatives. Quand on l'utilise, le neutre est noté 0 (ou 0_G) et l'inverse de x est noté $-x$.*
- *On pose $x^k = \underbrace{x * x * ... * x}_{k \text{ fois}}$ si $k \geq 0$*
  (Le produit de 0 termes est égal à e par convention)
  Et: $x^k = \underbrace{x^{-1} * x^{-1} * ... * x^{-1}}_{-k \text{ fois}}$ si $k < 0$
  On a: $\forall k, l \in \mathbb{Z}, x^k x^l = x^{k+l}$
  En notation additive, on note $k.x = \underbrace{x + x + ... + x}_{k}$
  Et on a: $(k + l).x = k.x + l.x$
- $(xy)^{-1} = y^{-1}x^{-1}$

Définition 1.3.
Soit G un groupe et $H \subset G$.

On dit que H est un sous-groupe de G si: $\begin{cases} e \in H \\ \forall x, y \in H, xy \in H \\ \forall x \in H, x^{-1} \in H \end{cases}$

H muni de la loi induite $\tilde{*}: H \times H \longrightarrow H$ *(qu'on note encore abusivement $*$) est un groupe.*

$(x, y) \longmapsto xy$

Exemple:

- $(\mathbb{Z}, +), (\mathbb{Q}, +), (\mathbb{R}, +), (\mathbb{C}, +), (\{-1, 1\}, *), (\mathbb{Q}^*, *), (\mathbb{R}^*, *), (\mathbb{C}^*, *), (\mathbb{Q}_+^*, *), (\mathbb{R}_+^*, *)$ (Lorsque $(A, +, *)$ est un anneau, l'ensemble des inverses, noté A^*, est un groupe pour $*$)
- S_n = groupe des permutations de $[\![1, n]\!]$
- $\mathbb{U}_n = \{z \in \mathbb{C}^*, z^n = 1\}$ est un sous-groupe de $(\mathbb{C}^*, *)$
- $(\mathbb{Z}/n\mathbb{Z}, +)$
- $\mathbb{K}$ corps. $GL_n(\mathbb{K})$ (ensemble des matrices inversibles à coefficients dans $\mathbb{K}$) est un groupe.

□

Propriété 1.4.
Une intersection de sous-groupes est encore un sous-groupe.

Démonstration:

Soit $(H_i)_{i \in I}$ une famille de sous-groupes d'un groupe G et $H = \bigcap_{i \in I} H_i$.
On a :

- $\forall i \in I, e \in H_i$ donc $e \in H$
- Soit $x \in H, y \in H$,
  On a: $\forall i \in I, x \in H_i$ et $y \in H_i$
  donc $\forall i \in H, xy \in H_i$
  donc $xy \in H$

- Soit $x \in H$
  On a: $\forall i \in I, x \in H_i$
  donc $\forall i \in I, x^{-1} \in H_i$
  donc $x^{-1} \in H$

□

Propriété 1.5.
Soit G un groupe et A une partie de G.
Il existe un plus petit (au sens de $\subset$) sous-groupe de G qui contient A.
On le note $gr(A)$ ou $< A >$.

Démonstration:

La famille de sous-groupes qui contiennent A n'est pas vide (elle contient G)
On peut donc envisager $\bigcap_{\substack{H \text{ sous-groupe de} \\ G \text{ contenant } A}} H$
qui est le plus petit sous-groupe de G contenant A.
On l'appelle le sous-groupe de G engendré par A. □

Exemple:

Soit $a \in G$. $gr(a) = \{a^k, k \in \mathbb{Z}\}$.
En effet: posons $H = \{a^k, k \in \mathbb{Z}\}$

- H est bien un sous-groupe de G, donc $gr(a) \subset H$
- Soit K un sous-groupe de G contenant a.
  Alors: $\forall k, a^k \in K$
  Donc $H \subset K$

H est bien le plus petit sous-groupe de G contenant A. □

Remarque 1.6.
En notation additive: $gr(a) = \{k.a, k \in \mathbb{Z}\}$

Généralisation de l'expression de $gr(A)$

Soit A une partie de G.
On a: $gr(a) = \{x \in G, \exists n \in \mathbb{N}, \exists x_1, ..., x_n \in (A \cup A^{-1})^n, x = x_1 x_2 ... x_n\}$

Démonstration:

Demo en exercice □

2 Morphismes

Définition 2.1.
Soient G_1 et G_2 deux groupes.
Une application $f : G_1 \longrightarrow G_2$ est qualifiée de morphisme si:

$$\forall x, y \in G_1, f(xy) = f(x)f(y)$$

Propriété 2.2.
Si f est un morphisme, alors $\begin{cases} f(e_1) = e_2 \\ \forall x, f(x^{-1}) = f(x)^{-1} \end{cases}$

Remarque 2.3.

- *Si f est un morphisme bijectif, alors f^{-1} est un morphisme.*
- *Un morphisme bijectif est qualifié d'isomorphisme*
- *Un isomorphisme de G dans lui-même s'appelle un automorphisme*

Exemple:

- Soit G un groupe, $a \in G$.
  $\mathbb{Z} \longrightarrow G$ est une application dont l'image est $gr(a)$.
  $k \longmapsto a^k$
  Si cette application est injective, alors: $gr(a) \simeq \mathbb{Z}$
- $\mathbb{Z} \longrightarrow \mathbb{Z}/n\mathbb{Z}$ est un morphisme ($\bar{x}\bar{y} = \overline{xy}$)
  $x \longmapsto \bar{x}$

- $S_n \longrightarrow \{-1,1\}$ est un morphisme
  $\sigma \longmapsto \underbrace{\varepsilon(\sigma)}_{\text{signature}}$
  P_2 désigne l'ensemble des paires de $[\![1,n]\!]$.
  $\varepsilon(\sigma) = \prod_{P\in P_2} \varepsilon_\sigma(P)$ où $\forall i<j, \varepsilon_\sigma(\{i,j\}) = \begin{cases} 1 \text{ si } \sigma(i)<\sigma(j) \\ -1 \text{ si } \sigma(i)>\sigma(j) \end{cases}$

- $$\begin{aligned}\varepsilon(\sigma\circ\sigma') &= \prod_{P\in P_2} \varepsilon_{\sigma\circ\sigma'}(P) \\ &= \prod_{P\in P_2} \varepsilon_\sigma(\sigma'(P))\varepsilon_{\sigma'}(P) \\ &= \prod_{P\in P_2} \varepsilon_\sigma(\sigma'(P)) \prod_{P\in P_2} \varepsilon_{\sigma'}(P) \\ &= \varepsilon(\sigma)\times\varepsilon(\sigma')\end{aligned}$$

- $GL_n(K) \longrightarrow K^*$ est un morphisme
  $M \longmapsto det(M)$

□

Propriété 2.4.
Les sous-groupes de $\mathbb{Z}$ sont de la forme $n\mathbb{Z}$.

Exercice:

Montrer qu'il n'y a que deux morphismes de S_n dans $\mathbb{C}^*$:
$S_n \longrightarrow \mathbb{C}^*$ et ε
$\sigma \longmapsto 1$ □

Propriété 2.5.
Soit $f: G_1 \longrightarrow G_2$ un morphisme

- *L'image d'un sous-groupe de G_1 par f est un sous-groupe de G_2 (en particulier $f(G_1)$, noté $Im(f)$, est un sous-groupe de G_2)*
- *L'image réciproque d'un sous-groupe de G_2 par f est un sous-groupe de G_1 (en particulier $f^{-1}(\{e\})$, noté $Ker(f)$, est un sous-groupe de G_1)*

Remarque 2.6.
Soit $f : G_1 \longrightarrow G_2$ *un morphisme.*
Soit $\mathcal{R}$ *la relation d'équivalence sur* G_1 *associée à* f*:*

$$\begin{aligned} x\mathcal{R}y &\iff f(x) = f(y) \\ &\iff f(x)f(y)^{-1} = e \\ &\iff f(xy^{-1}) = e \\ &\iff xy^{-1} \in Ker(f) \\ &\iff x \in yKer(f) \end{aligned}$$

De même: $x\mathcal{R}y \iff x \in Ker(f)y$
Donc la classe de y *modulo* $\mathcal{R}$ *est* $yKer(f) = Ker(f)y$
En particulier la classe de e *est* $Ker(f)$
Il faut noter que $Ker(f) \longrightarrow yKer(f)$ *est une bijection.*

$$z \longmapsto yz$$

Si G *est fini, toutes les classes ont le même cardinal, à savoir* $|Ker(f)|$.
En outre, le nombre de classes est égal à $|Im(f)|$
Donc $|G| = |Ker(f)||Im(f)|$

Exemple:

Soit p un nombre premier.
$(\mathbb{Z}/p\mathbb{Z}, +, *)$ est un corps.
$((\mathbb{Z}/p\mathbb{Z})^*, *)$ est un groupe de cardinal $p-1$
$f : (\mathbb{Z}/p\mathbb{Z})^* \longrightarrow (\mathbb{Z}/p\mathbb{Z})^*$ est un morphisme car le groupe est abélien.

$$x \longmapsto x^2$$

$$\begin{aligned} x \in Ker(f) &\iff x^2 = \bar{1} \\ &\iff x^2 - \bar{1} = \bar{0} \\ &\iff (x - \bar{1})(x + \bar{1}) = \bar{0} \\ &\iff x = \bar{1} \text{ ou } x = -\bar{1} \end{aligned}$$

Si $p \geq 3$: $|Ker(f)| = 2$ et $|Im(f)| = \frac{p-1}{2}$
Il y a donc $\frac{p+1}{2}$ carrés dans $\mathbb{Z}/p\mathbb{Z}$ □

Remarque 2.7.
Soit E *un* $\mathbb{K}_{ev}$
$(E, +)$ *et* $(\mathbb{K}, +)$ *sont des groupes (abéliens)*
Soit $f \in \mathcal{L}(E, \mathbb{K}), f \neq 0$ *(*f *est une forme linéaire)*
$Ker(f)$ *est un sous espace vectoriel de* E *de dimension* $n-1$.
$\bar{a} = a + Ker(f)$
$a + Ker(f) = \{x \in G, f(x) = f(a)\}$

Définition 2.8.
Soient G et H deux groupes.
$G \times H$, muni de la loi définie par: $(x,y) * (z,t) = (\underbrace{xz}_{\text{produit dans } G}, \underbrace{yt}_{\text{produit dans } H})$
est un groupe appelé groupe produit.

Remarque 2.9.

- *$\{e_G\} \times H$ est un sous-groupe de $G \times H$*
  Il est isomorphe à H
- $\forall x \in G, \forall y \in H, (x, e_H) * (e_G, y) = (x, y) = (e_G, y) * (x, e_H)$

Exemple:

Soit G un groupe et $a \in G$.
L'application $\varphi_a : G \longrightarrow G$, $x \longmapsto axa^{-1}$ s'appelle la conjugaison par a.
C'est un automorphisme de G. On dit encore que c'est un automorphisme intérieur.
En effet:

- $\varphi_a(x)\varphi_a(y) = axa^{-1}aya^{-1} = axya^{-1} = \varphi_a(xy)$
  Donc φ_a est un morphisme
- Clairement, $\varphi_a \circ \varphi_{a^{-1}} = \varphi_{a^{-1}} \circ \varphi_a = Id_G$
  Donc φ_a est une bijection.

□

Remarque 2.10.
Soit X un ensemble et $S(X)$ le groupe des permutations de X.
Soit $a \in S(X)$. La conjugaison par a est: $S(X) \longrightarrow S(X)$, $\sigma \longmapsto a\sigma a^{-1}$.
Dans ce cas, la conjugaison "algébrique" (définie sur un groupe) coincide avec la conjugaison "géométrique".

3 Ordre d'un groupe, d'un élément; groupes monogènes

Définition 3.1.

- *L'ordre d'un groupe est son cardinal (qui peut être infini).*
- *L'ordre d'un élément a d'un groupe G est l'ordre de $gr(a)$*

Définition 3.2.
Un groupe G est dit monogène s'il existe $a \in G$ tel que $gr(a) = G$.
Un tel élément a est qualifié de générateur de G.
Un groupe est dit cyclique s'il est monogène et fini.

Exemple:

1. $\mathbb{Z}$ est monogène: 1 et -1 en sont les deux seuls générateurs.
2. $\mathbb{Z}^2$ n'est pas monogène.
   Quel que soit $(a,b) \in \mathbb{Z}^2, gr(\{(a,b)\}) = \{k.(a,b), k \in \mathbb{Z}\}$
   $= \{(k.a, k.b), k \in \mathbb{Z}\}$
   $\subsetneq \mathbb{Z}^2$
3. $\mathbb{Z}/n\mathbb{Z} = \{\bar{k}, k \in \mathbb{Z}\}$
   $= \{k.\bar{1}, k \in \mathbb{Z}\}$
   $= gr(\bar{1})$
   $\mathbb{Z}/n\mathbb{Z}$ est donc un groupe cyclique d'ordre n.

□

Propriété 3.3.
Lemme:
Soient G un groupe et $\varphi : \mathbb{Z} \longrightarrow G$ un morphisme.
Il existe un morphisme $\psi : \mathbb{Z}/n\mathbb{Z} \longrightarrow G$ tel que: $\forall k, \psi(\bar{k}) = \varphi(k)$, si et seulement si: $n\mathbb{Z} \subset Ker(\varphi)$
En outre, si $n\mathbb{Z} = Ker(\varphi)$ alors ψ est injectif.

Démonstration:

La condition $n\mathbb{Z} \subset Ker(\varphi)$ signifie: $\forall z \in \mathbb{Z}, z \equiv 0[n] \implies \varphi(z) = 0$
Ou encore: $\forall x, y \in \mathbb{Z}, x - y \equiv 0[n] \implies \varphi(x - y) = 0$
Ou encore: $\forall x, y \in \mathbb{Z}, x \equiv y[n] \implies \varphi(x) = \varphi(y)$
C'est donc la condition pour que φ soit compatible avec $\equiv_n$
L'existence d'une application ψ telle que:

$$\mathbb{Z} \xrightarrow{\varphi} G$$

et

$$\mathbb{Z} \xrightarrow{\pi} \mathbb{Z}/n\mathbb{Z} \xrightarrow{\psi} G$$

"commute" ie: $\psi \circ \pi = \varphi$
ie: $\forall k, \psi(\bar{k}) = \varphi(k)$
est équivalente à $n\mathbb{Z} \subset Ker(\varphi)$
Cette condition étant satisfaite, il est immédiat que ψ est un morphisme.

$$\begin{aligned}\forall k, l \in \mathbb{Z}, \psi(\bar{k} + \bar{l}) &= \psi(\overline{k + l}) \\ &= \varphi(k + l) \\ &= \varphi(k) + \varphi(l) \\ &= \psi(\bar{k}) + \psi(\bar{l})\end{aligned}$$

Enfin, si $n\mathbb{Z} = Ker(\varphi)$ alors, pour tout $k \in \mathbb{Z}$,

$$\begin{aligned}\bar{k} \in Ker(\psi) &\iff \psi(\bar{k}) = 0 \\ &\iff \varphi(k) = 0 \\ &\iff k \in Ker(\varphi) \\ &\iff k \in n\mathbb{Z} \\ &\iff \bar{k} = 0\end{aligned}$$

Donc $Ker(\psi) = \{\bar{0}\}$: ψ est injective. □

Propriété 3.4.

- *Tout groupe monogène infini est isomorphe à $\mathbb{Z}$.*
- *Tout groupe cyclique d'ordre n est isomorphe à $\mathbb{Z}/n\mathbb{Z}$.*

Démonstration:

Soit G un groupe monogène et $a \in G$ un générateur de G.
L'application $\mathbb{Z} \longrightarrow G$ est un morphisme surjectif (on sait que $gr(a) = \{a^k, k \in \mathbb{Z}\}$)
$k \longmapsto a^k$
Son noyau est un sous-groupe de $\mathbb{Z}$.
Il existe donc $s \in \mathbb{N}$ tel que $Ker(\varphi) = s\mathbb{Z}$

- Si $s = 0$: φ est un isomorphisme et $G \simeq \mathbb{Z}$
- Si $s \geq 1$:
  D'après le lemme, il existe $\psi : \mathbb{Z}/s\mathbb{Z} \longrightarrow G$ morphisme injectif telle que:
  $\forall k \in \mathbb{Z}, \psi(\bar{k}) = \varphi(k)$
  De même, $Im(\psi) = Im(\varphi) = G$
  ψ est donc un isomorphisme: $G \simeq \mathbb{Z}/s\mathbb{Z}$.

Finalement, un groupe monogène est soit isomorphe à $\mathbb{Z}$, soit isomorphe à $\mathbb{Z}/s\mathbb{Z}$ où $s = Card(G)$ (lorsque G est fini) □

Théorème de Lagrange

Propriété 3.5.
L'ordre d'un sous-groupe d'un groupe fini G divise l'ordre de G.

Démonstration:

Soit G un groupe fini et H un sous-groupe de G.
Appelons congruence à gauche modulo H la relation sur G: $x\mathcal{R}y \iff x^{-1}y \in H$
C'est une relation d'équivalence:

- $\forall x \in G, x^{-1}x = e \in H$ donc $\mathcal{R}$ est réflexive.
- $\forall x, y \in G, x\mathcal{R}y \implies x^{-1}y \in H$
  $\implies (x^{-1}y)^{-1} \in H$
  $\implies y^{-1}x \in H$
  $\implies y\mathcal{R}x$
  Donc $\mathcal{R}$ est symétrique
- $\forall x, y, z \in G, x\mathcal{R}y$ et $y\mathcal{R}z \implies x^{-1}y \in H$ et $y^{-1}z \in H$
  $\implies x^{-1}yy^{-1}z \in H$
  $\implies x^{-1}z \in H$
  $\implies x\mathcal{R}z$

La classe de x pour cette relation est $xH : x\mathcal{R}y \iff x^{-1}y \in H \iff y \in xH$
Les classes pour cette relation s'appellent les classes à gauche modulo H.

- En particulier, la classe de e est H.
- Chaque classe peut être mise en bijection avec xH: $H \longrightarrow xH$.
  $h \longmapsto xh$

On a donc $|G| = |H| \times$ nombre de classes □

Remarque 3.6.

1. *On peut définir la congruence à droite modulo H. La classe à droite modulo H de x est Hx.*
   En général, $xH \neq Hx$
   Même si G est infini, l'ensemble des classes à gauche et l'ensemble des classes à droite ont le même cardinal (ie: peuvent être mis en bijection)
   - $\{$*classes à gauche*$\} \longrightarrow \{$*classes à droite*$\}$
     $C \longmapsto C^{-1} = \{z^{-1}, z \in C\}$
     $H = \{xh, h \in H\}$
     $(xH)^{-1} = \{h^{-1}x^{-1}, h \in H\} = \{hx^{-1}, h \in H\} = Hx^{-1}$
     Ce nombre commun de classes s'appele l'indice de H dans G.
     On le note $[G : H]$
2. *En général, la loi de G n'est pas compatible avec la congruence à gauche modulo H ni avec la congruence à droite modulo H*
   Mais si la congruence à gauche modulo H est compatible alors l'ensemble quotient est un groupe qu'on note G/H et $\pi : G \longrightarrow G/H$ est un morphisme.
   On a alors $H = \bar{e} = \pi^{-1}(\{\bar{e}\}) = Ker(\pi)$
   Donc la congruence à gauche et la congruence à droite coincident.
   On dit dans ce cas que H est distingué dans G.
   On le note $H \lhd G$
   Résumons:
   H étant un sous-groupe de G, les propriétés suivantes sont équivalentes:
   - *La loi de G passe au quotient modulo H à gauche.*
   - *La congruence à gauche notée H est identique à la congruence à droite modulo H*
   - $\forall x \in G, xH = Hx$

   Dans ce cas, la loi de G passe au quotient et on peut parler de groupe quotient.

Propriété 3.7.
Soit G un groupe et $a \in G$.

1. *Si a est d'ordre fini s, alors: $\{k \in \mathbb{Z}, a^k = e\} = s\mathbb{Z}$*
   Si a est d'ordre infini, alors: $\{k \in \mathbb{Z}, a^k = e\} = \{0\}$
   On détermine l'ordre de a en résolvant l'équation $a^k = e$ d'inconnue $k \in \mathbb{Z}$
2. *Si a est d'ordre fini s, alors* $\begin{cases} gr(a) = \{e, a, ..., a^{s-1}\} \\ a^s = e \text{ et } s \text{ est le plus petit } k \in \mathbb{N}^* \text{ tel que } a^k = e \end{cases}$
3. *Soit $a \in G$ et $q \in \mathbb{Z}$*
   Si $a^q = e$, alors a est d'ordre fini s et $s|q$
   Attention: Cela n'entraine pas que a soit d'ordre q !
4. *Si G est d'ordre n alors:*
   L'ordre s d'un élément a divise n
   En particulier: $\forall a \in G, a^n = e$

Démonstration:

1. Soit $a \in G$
   a est un générateur de $gr(a)$
   On a vu ci-dessus que $\varphi : \mathbb{Z} \longrightarrow gr(a)$
   $$k \longmapsto a^k$$
   est un isomorphisme lorsque $gr(a)$ est infini, c'est-à-dire lorsque a est d'ordre infini
   Dans ce cas, $Ker(\varphi) = \{e\}$
   ie: $\{k, a^k = e\} = \{0\}$
   Lorsque $gr(a)$ est d'ordre s, on a vu que $Ker(\varphi) = s\mathbb{Z}$
   ie: $\{k, a^k = e\} = s\mathbb{Z}$
2. Si a est d'ordre fini s, φ induit un isomorphisme $\psi : \mathbb{Z}/s\mathbb{Z} \longrightarrow gr(a)$.
   $\mathbb{Z}/s\mathbb{Z} = \{\bar{0}, \bar{1}, ..., \overline{s-1}\}$
   Donc $gr(a) = \{e, a, ..., a^{s-1}\}$ (car $\psi(\bar{k}) = \varphi(k) = a^k$)
   et on a: $s \equiv 0[s]$ donc $\varphi(s) = \psi(\bar{0}) = e$ et $a^s = e$
3. Conséquence immédiate de ①.
4. D'après le théorème de Lagrange, l'ordre de $gr(a)$ divise l'ordre de G.
   Donc l'ordre de a divise l'ordre n de G.
   Ainsi $n \in s\mathbb{Z}$ et d'après ①, $a^n = e$

□

Propriété 3.8.
Soit G un groupe cyclique d'ordre n.

1. *Soit a un générateur de G.*
   Pour tout $k \in \mathbb{Z}, a^k$ est d'ordre $\frac{n}{k \wedge n}$.
2. *Un groupe cyclique d'ordre n admet $\varphi(n)$ générateur, où φ est l'indicatrice d'Euleur définie par:*
   $\varphi(n) = |\{k \in [\![1, n]\!], n \wedge k = 1\}|$

Démonstration:

1. On résoud $(a^k)^l = e$ d'inconnue $l \in \mathbb{Z}$
$$\begin{aligned}(a^k)^l = e &\iff a^{kl} = e \\ &\iff n | kl \\ &\iff \frac{n}{n \wedge k} | \frac{k}{n \wedge k} l \\ &\iff \frac{n}{n \wedge k} | l\end{aligned}$$
2. Soit G un groupe cyclique d'ordre n et a un générateur de G
On a: $G = \{e, a, ..., a^{n-1}\}$ et, $k \in [\![0, n-1]\!]$ étant fixé,
a^k est un générateur de $G \iff a^k$ est d'ordre n
$$\begin{aligned}&\iff \frac{n}{n \wedge k} = n \\ &\iff n \wedge k = 1\end{aligned}$$
Le nombre de générateurs de G est donc $|\{k \in [\![0, n-1]\!], n \wedge k = 1\}|$

□

Remarque 3.9.
Si a est un générateur de G, les autres sont les a^k, $\begin{cases} k \in [\![0, n-1]\!] \\ n \wedge k = 1 \end{cases}$

Exemple:

$\mathbb{U}_n = \{x \in \mathbb{C}, z^n = 1\} = \{e^{\frac{2ik\pi}{n}}, k \in \mathbb{Z}\}$
$\mathbb{U}_n = gr(e^{\frac{2i\pi}{n}})$
$\begin{cases} e^{\frac{2ik\pi}{n}} \\ n \wedge k = 1 \end{cases}$ est un autre générateur de $\mathbb{U}_n$
Les générateurs de $\mathbb{U}_n$ sont qualifiés de racines n-ièmes primitives de l'unité □

Propriété 3.10.

1. *Tous les sous-groupes d'un groupe cyclique sont cycliques*
2. *Si G est d'ordre n, alors il admet pour chaque $d \in [\![1, n]\!]$ divisant n un et un seul sous-groupe d'ordre d*

Remarque 3.11.

1. *Rappelons que si G d'ordre n admet un sous-groupe d'ordre d, alors $d|n$*
2. *On déduit de ce théorème:*
   $n = \sum_{d|n} \varphi(d)$
   Soit en effet $\omega : G \longrightarrow \{d \in [\![1, n]\!], d|n\}$
   $a \longmapsto$ *ordre de* a
   Pour tout $a \in G$, *en posant* $d = \omega(a)$
   $\{x \in G, \omega(x) = d\} = \{x \in G, x$ *engendre un sous-groupe d'ordre* $d\}$
   $= \{x \in G, x$ *engendre le sous-groupe d'ordre* $d\}$
   Donc $|\{x, \omega(x) = \omega(a)\}| = \varphi(d)$
   On en déduit: $n = \sum_{d|n} \varphi(d)$

Démonstration:

1. Prenons comme "modèle" de groupe cyclique d'ordre n le groupe $\mathbb{U}_n$
   Soit $d|n$ et H un sous-groupe de $\mathbb{U}_n$ d'ordre d.
   On a: $\forall x \in H, x^d = 1$ (corrolaire du théorème de Lagrange)
   Donc $H \subset \mathbb{U}_d$
   D'où, puisque $|H| = d = |\mathbb{U}_d|$
   $H = \mathbb{U}_d$
   Ainsi, $\mathbb{U}_n$ contient un unique sous-groupe d'ordre d, lequel est cyclique.
   (Tous les sous-groupes de $\mathbb{U}_n$ sont donc cycliques).

2. Soit G un groupe cyclique d'ordre n et $a \in G$ un générateur de G.
   Soit $d|n$ et H un sous-groupe de G d'ordre d
   $\varphi : \mathbb{Z} \longrightarrow G$ est un morphisme de groupes.
   $k \longmapsto a^k$
   $\varphi^{-1}(H)$ est un sous-groupe de $\mathbb{Z}$
   Donc il existe $s \in \mathbb{N}$ tel que $\varphi^{-1}(H) = s\mathbb{Z}$
   $H = \varphi(s\mathbb{Z})$ car φ est surjective
   $H = \{a^{ks}, k \in \mathbb{Z}\} = \{(a^s)^k, k \in \mathbb{Z}\} = gr(a^s)$
   H est donc un sous-groupe cyclique.
   Soit $d|n$. Montrons qu'il existe une unique sous-groupe cyclique d'ordre d
   Soit $s \in [\![0, n-1]\!]$
   $$\begin{aligned} a^s \text{ est d'ordre } d &\iff \frac{n}{n \wedge s} = d \\ &\iff \frac{n}{d} = n \wedge s \\ &\iff \exists l, s = l\frac{n}{d} \text{ et } d \wedge l = 1 \end{aligned}$$
   Le nombre de solution est le cardinal de l'ensemble des $l \in \mathbb{N}$ tels que:
   $$\begin{cases} l\dfrac{n}{d} < n \\ l \wedge d = 1 \end{cases}$$
   ie: $\begin{cases} l < d \\ l \wedge d = 1 \end{cases}$
   C'est donc $\varphi(d)$.
   On en déduit que G contient un unique sous-groupe d'ordre d (qui est $gr(a^{\frac{n}{d}})$)
   □

Théorème Chinois

Propriété 3.12.
Le produit de deux groupes cycliques d'ordre n et m est cyclique ssi: $n \wedge m = 1$

Remarque 3.13.
G, H cycliques d'ordre n et m, $n \wedge m = 1$
$a \in G, b \in H$. Alors:
(a, b) générateur de $G \times H \iff$ a générateur de G et b générateur de H.
On en déduit:
$\forall n, m \in \mathbb{N}^*, n \wedge m = 1 \implies \varphi(nm) = \varphi(n)\varphi(m)$
En effet, G étant cyclique d'ordre n, H cyclique d'ordre m, avec $n \wedge m = 1$,
$G \times H$ est cyclique d'ordre nm. Le nombre de générateurs de $G \times H$ est égal à $\varphi(n)\varphi(m)$
Donc $\varphi(nm) = \varphi(n)\varphi(m)$

On en déduit alors:
$\forall n \in \mathbb{N}^*, \varphi(n) = n \prod_{p|n}(1 - \frac{1}{p})$ *où le produit $\prod_{p|n}$ porte sur tous les facteurs premiers de n.*
$\varphi(6) = 6(1 - \frac{1}{2})(1 - \frac{1}{3}) = 2$
En effet, en posant $n = {p_1}^{\alpha_1} {p_2}^{\alpha_2} ... {p_r}^{\alpha_r}$ où les p_i sont 2 à 2 distincts.

$$\begin{aligned} \text{Alors } \varphi(n) &= \prod_{i=1}^{r} \varphi(p_i^{\alpha i}) \\ &= {p_1}^{\alpha_1} ... {p_r}^{\alpha_r} (1 - \frac{1}{p_1}) ... (1 - \frac{1}{p_r}) \\ &= n \prod_{i=1}^{r} (1 - \frac{1}{p_i}) \end{aligned}$$

Propriété 3.14.
Soit G un groupe et $a, b \in G$.
On suppose:

- *a, b d'ordre finis n et m*
- *$n \wedge m = 1$*
- *$ab = ba$*

Alors ab est d'ordre nm.

Démonstration:

On cherche l'ordre de ab.
$(ab)^k = e \iff a^k b^k = e$ car $ab = ba$
$(ab)^k = e \implies (ab)^{nk} = e$
$\implies b^{nk} = e$
Donc $m|nk$. Or $n \wedge m = 1$, donc $m|k$
De même, $n|k$.
On en déduit que $nm|k$.
Par ailleurs, $(ab)^{nm} = e$.
Conclusion: ab est d'ordre nm. □

Démonstration:

Preuve du théorème chinois:
Soit a_G un générateur de G et a_H un générateur de H.
Posons $a = (a_G, e_H), b = (e_G, a_H)$. On a :

- a et b sont d'ordres finis n et m.
- $n \wedge m = 1$
- $ab = (a_G, a_H) = ba$

Donc ab est d'ordre nm. De plus, $card(G \times H) = nm$, donc ab est un générateur de $G \times H$ □

4 Groupe symétrique

Définition 4.1.
Soit X un ensemble.
On note $S(X)$ l'ensemble des permutations de X (les bijections de X dans lui-même)
On vérifie aisément que $(S(X), \circ)$ est un groupe.

Remarque 4.2.

1. *Si $f : X \longrightarrow Y$ est une bijection alors $S(X) \longrightarrow S(Y)$*
$$\sigma \longmapsto f \circ \sigma \circ f^{-1}$$
est un isomorphisme de groupe

2. *Si G est un groupe cyclique, il est isomorphe à un sous-groupe de $S(G)$.*
En effet, l'application $G \longrightarrow S(G)$ *est un morphisme injectif*
$$a \longmapsto \gamma_a : G \longrightarrow G$$
$$x \longmapsto ax$$

Notations:

- $S_n = S([\![1, n]\!])$
- Le tableau $\begin{pmatrix} 1, 2 & , ... & , n \\ a_1, a_2 & , ... & , a_n \end{pmatrix}$ représente la permutation $\sigma : \mathbb{N} \longrightarrow \mathbb{N}$, $i \longmapsto a_i$
- $c = (a_1, a_2, ..., a_p)$ représente le cycle défini par: $\begin{cases} c(a_k) = a_{k+1} \\ c(a_p) = a_1 \\ c(x) = x \text{ si } x \notin \{a_1, ..., a_p\} \end{cases}$

Remarque 4.3.

- *S_n est d'ordre $n!$*
- *Si $a_1, a_2, ..., q_p$ sont dans $[\![1, n]\!]$ et 2 à 2 distincts, $(a_1, ..., a_k)(a_k, ..., a_p) = (a_1, ..., a_p)$*
- *Si $\sigma \in S_n$ et $c = (a_1, ..., a_p)$ est un cycle, alors $\sigma \circ c \circ \sigma^{-1} = (\sigma(a_1), ..., \sigma(a_p))$*

Propriété 4.4.
L'ensemble des transpositions engendre S_n

Remarque 4.5.
Puisqu'une transposition est son propre inverse, cet énoncé signifie que toute permutation peut s'écrire comme produit de transpositions.

Exercice:

Soit $\sigma \in S_N$
Quel est le plus petit p tel qu'il existe des transpositions $\tau_1, ..., \tau_p$ telles que $\sigma = \tau_1 ... \tau_p$ □

Remarque 4.6.
Il n'y a pas unicité d'une décomposition de produit de transpositions.

Définition 4.7.
Pour toute permutation $\sigma \in S_n$, on appelle support de σ:
$Supp(\sigma) = \{x \in [\![1, n]\!], \sigma(x) \neq x\}$

Propriété 4.8.
Pour tout $(\sigma, \sigma') \in {S_n}^2$, $Supp(\sigma) \cap Supp(\sigma') = \varnothing \implies \sigma\sigma' = \sigma'\sigma$

Propriété 4.9.
Théorème:
Toute permutation peut se décomposer en produit de cycles à supports disjoints.
Cette décomposition est unique a l'ordre des facteurs près.

Remarque 4.10.
Id est le produit de 0 cycles.

Exemple:

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 \\ 11 & 7 & 1 & 5 & 9 & 10 & 12 & 2 & 4 & 3 & 6 & 8 \end{pmatrix} = (1, 11, 6, 10, 3)(2, 7, 12, 8)(4, 5, 9)$$

□

Propriété 4.11.
Disons que deux permutions σ et σ' sont conjuguées s'il existe $\eta \in S_n$ telle que $\sigma' = \eta \circ \sigma \circ \eta^{-1}$
σ et σ' sont conjuguées ssi, pour tout $s \in [\![2, n]\!]$, σ et σ' ont le même nombre de cycles de longueur s.

Démonstration:

Si $\sigma = (a_1^1, ..., a_{l_1}^1)(a_1^2, ..., a_{l_2}^2)...(a_1^r, ..., a_{l_r}^r)$
et $\sigma' = (b_1^1, ..., b_{l_1}^1)(b_1^2, ..., b_{l_2}^2)...(b_1^n, ..., b_{l_n}^n)$
Soit $\eta \in S_n$ qui vérifie: $\forall i, j, \eta(a_j^i) = b_j^i$
On a: $\eta \circ \sigma \circ \eta^{-1} = (\eta c_1 \eta^{-1})...(\eta c_r \eta^{-1}) = \eta \circ \sigma' \eta^{-1}$
Réciproque similaire. □

Exercice:

- Quelles sont les classes de conjugaison de S_3 ?
- Combien y-a-t-il d'éléments dans chaque classe ?

- Mêmes questions avec S_4

Classes de conjugaisons de S_3:

- $\{id\}, \# = 1$
- Ensemble des transpositions: $\# = 3$
- 3-cycles: $\# = 2$

Classes de conjugaisons de S_4:

- $\{id\}, \# = 1$
- Ensemble des transpositions: $\# = \binom{2}{4} = 6$
- 3-cycles: $\# = 2 * \binom{3}{4} = 8$
- 4-cycles: $\# = 6$
- produits de 2 transpositions disjointes: $\# = 3$

□

Remarque 4.12.
Il faut distinguer les propriétés "géométriques" et les propriétés "algébriques"
alg = propriétés de groupe
géo = propriétés d'applications
Il est parfois possible d'exprimer géométriquement une propriété algébrique (et vice-versa)

Exemple:

$\sigma^2 = e \iff \sigma$ est un produit de transpositions disjointes □

Exercice:

- Soit $\sigma \in S_n$. On suppose que σ est le produit de cycles 2 à 2 disjoints de longueurs $l_1, ..., l_s$
  Déterminer l'ordre de σ

- Soit $n \in \mathbb{N}^*$.
  Montrer que si $n \neq 6$, tous les automorphismes de S_n sont intérieurs. (Hors programme)

Posons $\sigma = c_1..c_s$ où les c_i sont des cycles 2 à 2 disjoints, c_i de longueur l_i
On a: $\forall k \in \mathbb{Z}, \sigma^k = c_1^k...c_s^k$ (car $c_i c_j = c_j c_i$)
On a: $Supp(c_i^k) \subset Supp(c_i)$
Donc les $Supp(c_i^k)$ sont 2 à 2 disjoints.
On en déduit: $\sigma^k = e \iff \forall i, c_i^k = e$
$\iff \forall i, l_i | k$
$\iff ppcm(l_1, ..., l_s) | k$
Donc σ est d'ordre $ppcm(l_1, ..., l_s)$. □

Rappel: $\varepsilon : S_n \longrightarrow (\{-1, 1\}, \times)$ est un morphisme
Il est surjectif dès que $n \geq 2$
Comme $|Ker(\varepsilon)| \times |Im(\varepsilon)| = |S_n|$, on a: $|Ker(\varepsilon)| = \frac{n!}{2}$ (pour $n \geq 2$)
On note: $A_n = Ker(\varepsilon)$ (groupe alterné)

Exemple:

$A_3 = \{e, (1,2,3), (1,3,2)\}$
$A_4 = \{e\} \cup \{\text{produits de 2 transpositions de supports disjoints}\} \cup \{\text{3-cycles}\}$ □

Remarque 4.13.

1. *A_n étant le noyau d'un morphisme, $A_n < |S_n$ (ie: A_n distingué dans S_n, c'est-à-dire: $\forall \sigma \in S_n, \sigma A_n \sigma^{-1} = A_n$)*

2. *On démontre que pour $n \geq 5$, A_n n'a aucun sous-groupe distingué que les sous-groupes triviaux.*
   C'est fondamentalement la raison pour laquelle il n'y a pas de formule générale de résolution par radicaux de l'équation polynomiale de degré $n, n \geq 5$

Exercice:

Déterminer tous les morphismes de S_n dans $(\mathbb{C}^*, \times)$
Soit $\varphi : S_n \longrightarrow \mathbb{C}^*$ un morphisme.

- Soit τ une transposition
  On a $\tau^2 = e$, donc $\varphi(\tau)^2 = 1$
  Donc $\varphi(\tau) \in \{1, -1\}$

- Soient τ, τ' deux transpositions.
  Il existe $\sigma \in S_n$ tel que $\tau' = \sigma \circ \tau \circ \sigma^{-1}$
  On en déduit: $\varphi(\tau') = \underbrace{\varphi(\sigma)\varphi(\tau)\varphi(\sigma)^{-1}}_{\in \mathbb{C}^*} = \varphi(\tau)$

Ainsi on a:
Soit $\forall \tau, \varphi(\tau) = 1$
Soit $\forall \tau, \varphi(\tau) = -1$
Supposons $\forall \tau, \varphi(\tau) = 1$
Notons $\mathbb{1} : S_n \longrightarrow \mathbb{C}^*$. C'est un morphisme.
$\sigma \longmapsto 1$
$\{\sigma \in S_n, \varphi(\sigma) = \mathbb{1}(\sigma)\}$
C'est donc S_n: $\varphi = \mathbb{1}$
Supposons $\forall \tau, \varphi(\tau) = -1$
Alors $\varphi = \varepsilon$ □

Exercice:

Montrer qu'il existe $n-1$ transpositions de S_n qui forment une famille génératrice.
Montrer que $n-1$ est optimal.
Lemme: Un graphe (non orienté) comportant n sommets et un nombre d'arcs $< n-1$ n'est pas connexe.
$\forall x, y \in [\![1, n]\!], \exists \sigma \in S_n, \sigma(x) = y$
Une famille d'au plus $n-2$ transpositions engendre un sous-groupe G de S_n qui ne peut pas vérifier:
$\forall x, y \in [\![1, n]\!], \exists \sigma \in G, \sigma(x) = y$
De plus, la famille $((1,2),(2,3),...,(n-1,n))$ engendre l'ensemble des transposition, donc engendre le groupe des permutations S_n.
En effet, Soit (a, b) une transposition. On suppose $a < b$.
On a: $(a, b) = (a, a+1)...(b-2, b-1)(b-1, b)(b-1, b-2)...(a+1, a)$ □