Chapitre 6. Théorie des groupes

I. Généralités sur les groupes

Soit E un ensemble

Une **loi de composition interne (l.c.i)** $\cdot$ sur E est une application de $E \times E$ dans E

Une lci est **associative**, / l'ensemble + l.c.i est appelé **demi-groupe** si la priorité des opérations n'a pas d'importance dans un produit, càd $(xy)z = x(yz)$. Dans ce cas les parenthèses peuvent être omises : $(xy)z = x(yz) = xyz$.

Une lci est **commutative** si l'ordre des opérations n'a pas d'importance dans un produit, càd $xy = yx$

Deux termes x, y **commutent** pour la l.c.i si $xy = yx$

On appelle **élément central** un élément qui commute avec tous les autres éléments

On appelle **centre** l'ensemble des éléments centraux.

Tout est central ssi il y a commutativité.

Un élément de E est **neutre** pour la l.c.i si composer un terme de E par l'élement à gauche ou à droite, ne change pas le terme.

$(E, \cdot)$ est qualifié de **monoïde** si sa l.c.i est associative et admet un neutre = demi-groupe + neutre.

Si une lci admet un neutre, celui-ci est unique

Tout terme commute avec le neutre s'il existe.

Si une l.c.i admet neutre, x **symétrique à gauche** de y / y **symétrique à droite** de x signifie que le produit xy est égal au neutre. **Symétrique =** symétrique à gauche ET à droite. **Symétrisable =** $\exists$ symétrique. Parler de symétrique suppose l'existence d'un neutre.

Deux termes symétriques (à gauche ET droite) commutent.

Sous associativité, tout élément a au plus un symétrique.

Si une l.c.i admet un neutre, celui-ci est unique et est son propre symétrique

Un élément a est dit **simplifiable à gauche (resp droite)** (dans toute expression par la lci) si dans toute égalité de produits ou il est à gauche (resp. droite) dans les deux membres, on a toujours égalité si on l'enlève dans les deux membres à gauche (resp droite).

Symétrisable à gauche (resp. droite) implique simplifiable à gauche (resp. droite)

Ensemble Produit.

Le **produit d'un élément** x **par un élément** y est l'élément $x \cdot y$

L'**ensemble produit d'une partie** X **par une partie** Y est l'ensemble des produits $XY = \{x \cdot y : x \in X, y \in Y\}$. Attention a priori $XY \neq YX$. Attention a priori XX, $\{x^2 : x \in X\}$, $X \times X = \{(x, y) : x \in X, y \in X\}$ sont des choses différentes. Il vaudrait mieux préciser à quel def on se réfère en écrivant X^n.

Sous associativité, le **produit d'une famille finie d'éléments** $(x_i)_{i=1..n}$ est l'élément $\prod_{i=1..n} x_i = x_1 \cdot \ldots \cdot x_n$

Sous associativité, le **produit d'une famille finie de parties** $(X_i)_{i=1..n}$ est l'ensemble des produits des n parties. $\prod_{i=1..n} X_i = X_1 \cdot \ldots \cdot X_n = \{x_1 \ldots x_n : x_1 \in X_1, \ldots, x_n \in X_n\}$

L'associativité est présupposée car sinon le produit dépend aussi du placement des parenthèses ce qui rend la notion peu élégante. A priori dépend de l'ordre.

Sous associativité + commutativité, le produit de parties est commutatif, le produit de familles finies est indépendant de l'ordre.

Sous associativité + commutativité + neutre, le **produit d'une famille infinie de parties** $(X_i)_{i \in I}$ est l'ensemble des produits finis provenant d'elle (de n'importe quelles parties dans n'importe quel ordre). La commutativité est présupposée car cette notion ne dépend pas de l'ordre, et sous cette condition généralise plus élégamment le produit fini de parties. L'existence du neutre est supposée pour permettre une autre interprétation comme ensemble des produits infinis de termes dont un nombre fini n'est pas neutre.

$\prod_{i \in I} X_i = \{x_1 \ldots x_n : n \in \mathbb{N}^*, \forall k \exists i \in I \; x_k \in H_i\} = \{\prod_{i \in I} x_i : \forall i \; x_i \in H_i, \exists J \subseteq I \text{ fini } \forall j \notin J \; x_j = 1\}$

Un **groupe** $(G,\cdot)$ est un ensemble G muni d'une lci $\cdot$ sur G tel que 1)2) et 3)
1) la l.c.i est associative (associativité)
2) la l.c.i admet un neutre (il y a un neutre)
3) tout élément est symétrisable par la l.c.i (symétrisabilité) (parler de 3 suppose de toute manière 2)
Dans tout groupe, il y a un unique neutre, et tout élément admet un unique symétrique appelé **inverse** et noté $\boldsymbol{x^{-1}}$ en notation multiplicative ou $-\boldsymbol{x}$ en notation additive. On peut ainsi définir l'application inverse sur tout le groupe.
Un groupe est dit **commutatif/abélien** si sa loi est commutative
Un élément d'un groupe commute toujours avec son symétrique, et avec l'élément neutre.
L'**ensemble inverse** d'une partie d'un groupe, est l'ensemble des inverses d'éléments de la partie. On note $\boldsymbol{S^{-1}}$ l'ensemble inverse d'une partie $S \subseteq G$.
L'inverse d'un groupe est le groupe. $G^{-1} = G$
Regles de calcul.
Sous associativité (dans un demi-groupe à fortiori dans un groupe) on peut définir composer n fois sans se soucier de l'ordre $\boldsymbol{x^n = x \cdot \ldots \cdot x}$ / $\boldsymbol{nx = x + \cdots + x}$
$\boldsymbol{x^0 = 1}$ / $\boldsymbol{0x = 0}$ et $\boldsymbol{x^{-n} = (x^n)^{-1}}$ / $\boldsymbol{-nx = -(nx)}$
Sous associativité, Composer $m+n$ fois revient à faire le produit de composer m fois puis n fois ou l'inverse indistinctement. $x^{m+n} = x^m x^n = x^n x^m$ / $(m+n)x = mx + nx = nx + mx$
Sous associativité, Composer mn fois revient à composer d'abord m fois puis n fois ou l'inverse indistinctement. $x^{nm} = (x^n)^m = (x^m)^n$ / $(nm)x = n(mx) = m(nx)$
Sous associativité, Si deux termes commutent, alors on peut les élever chacun à une puissance différente quelconque, ca commute toujours. $xy = yx \Rightarrow x^m y^n = y^n x^m$
Sous symétrisabilité, tout élément est simplifiable (à gauche/droite) d'une expression.
Dans un groupe, l'inverse du produit est le produit des inverses en inversant l'ordre des lettres.
$(xy)^{-1} = y^{-1}x^{-1}$
I.2. Sous-Groupes. Soit $(G,\cdot)$ un groupe
Définitions équivalentes :
Un **sous-groupe** d'un groupe est une partie non-vide stable par produit et inverse. $H \neq \emptyset, HH \subseteq H, H^{-1} \subseteq H$
Un **sous-groupe** d'un groupe est une partie qui muni de la loi induite, forme encore un groupe.
On note $\boldsymbol{H \leq G}$ si $(H,\cdot)$ sous-groupe de $(G,\cdot)$, $\boldsymbol{H < G}$ si $(H,\cdot)$ sous-groupe propre de $(G,\cdot)$
Tous les sous-groupes sont des groupes et possèdent le même élément neutre, celui du groupe.
G et $\{1_G\}$ sont des sous-groupes de G. Tout groupe ayant au moins deux éléments possède donc au moins deux sous-groupes distincts.
Le centre d'un groupe est un sous-groupe. Propre ssi groupe non abélien.
L'intersection quelconque de sous-groupes d'un groupe est un sous-groupe du même groupe.
L'union d'une famille de sous-groupes totalement ordonnée pour l'inclusion est un sous-groupe du même groupe.
Exemples : $(\mathbb{Z},+) < (\mathbb{Q},+) < (\mathbb{R},+) < (\mathbb{C},+)$, $(\mathbb{Q}^*,\times) < (\mathbb{R}^*,\times) < (\mathbb{C}^*,\times)$, $(\mathbb{Q}_+^*,\times) < (\mathbb{Q}^*,\times)$, $(\mathbb{R}_+^*,\times) < (\mathbb{R}^*,\times)$, $(\mathbb{Q}_+^*,\times) < (\mathbb{R}_+^*,\times)$
Les sous-groupes de $(\mathbb{Z},+)$ sont les $(n\mathbb{Z},+)$, n entier. L'ensemble $\mathbb{U}$ des complexes de module 1 est un sous-groupe propre de $(\mathbb{C}^*,\times)$. Le groupe linéaire général est un sous-groupe du groupe symétrique. Le groupe des similitudes affines/linéaires d'un espace affine/vectoriel euclidien E est un sous-groupe du groupe linéaire général de $\vec{E}$.
Soit $(G,\cdot)$ un groupe, les définitions suivantes sont équivalentes:
Le **sous-groupe engendré** par une partie non vide est le plus petit sous-groupe (au sens inclusion) contenant la partie.
Le **sous-groupe engendré** par une partie non vide est l'intersection de tous les sous-groupes contenant

la partie.
Le **sous-groupe engendré** par une partie non vide est l'ensemble de tous les produits finis d'éléments provenant de la partie ou de son inverse.
On note $< S >$ le sous-groupe engendré par une partie S
Si la partie est égale à son inverse, en particulier si elle s'exprime comme union de sous-groupes. Le sous-groupe engendré par la partie est l'ensemble de tous les produits finis d'éléments de la partie.
$<\cup_{i\in I} H_i > = \{x_1 \dots x_n : n \in \mathbb{N}^*, \forall k \exists i\ x_k \in H_i\}$
Le produit d'un nombre fini de sous-groupes (dans n'importe quel ordre) est inclus dans le sous-groupe engendré par leur union. $\Pi_{i=1..n} H_i = H_1 H_2 \dots H_n \subseteq <\cup_{i=1..n} H_i >$
Il y a égalité ssi le produit est un sous-groupe
Sous commutativité (dans un groupe abélien) il y a toujours égalité. Le produit de la famille est indépendant de l'ordre et est toujours un sous-groupe.
$<\cup_{i=1..n} H_i > = \{x_1 \dots x_n : x_1 \in H_1, \dots, x_n \in H_n\} = H_1 H_2 \dots H_n = \Pi_{i=1..n} H_i$
Théorème. Le produit de deux sous-groupes écrit dans un sens ou l'autre est identique ssi ce produit (dans un sens ou l'autre) est un sous-groupe ssi ce produit (dans un sens ou l'autre) est engendré par l'union de ses 2 sous-groupes.
$HK = KH$ ssi KH sous-groupe ssi HK sous-groupe (ssi $HK =< H \cup K >$ ssi $KH =< H \cup K >$)
Pour une famille finie de sous-groupes, Si le produit de chaque paire de la famille est un sous-groupe alors le produit de la famille est un sous-groupe et est indépendant de l'ordre.
Le sous-groupe engendré par un unique élément est l'ensemble des puissances (resp. multiples) relatives de l'élément. $< a > = \{a^n : n \in \mathbb{Z}\}$
On note de façon compacte $< \boldsymbol{a_1}, \dots, \boldsymbol{a_n} > := <\cup_{i=1..n} \{a_i\} >$
Sous commutativité $< a_1, \dots, a_n > = << a_1 >, \dots, < a_n >> = <\cup_{i=1..n} < a_i >>$
Sous commutativité $< a_1, \dots, a_n > = < a_1 > \cdots < a_n > = \Pi_{i=1..n} < a_i >$
Une **partie génératrice** d'un groupe, est une partie dont le sous-groupe engendré est le groupe lui-même. On dit que la partie **engendre/génère** le groupe. Toute partie engendre son sous-groupe engendré.
Un groupe est dit **monogène** s'il est engendré par un singleton. Un **générateur** est un élément qui engendre le groupe.
Un groupe est dit **de type fini** s'il est engendré par un ensemble fini d'éléments.
Un groupe fini est de type fini, mais réciproque fausse $(\mathbb{Z}, +)$ est engendré par 1)
Un groupe est dit **cyclique** s'il est monogène et fini.
L'**ordre** d'un élément dans un groupe est le cardinal de son sous-groupe engendré. Peut être fini ou infini. Si x est l'élément, on le note $o(x)$
Dans tout groupe l'élément neutre est le seul élément d'ordre 1.
Tout élément non nul de $(\mathbb{Z}, +)$ est d'ordre infini.

I.3. Morphismes de groupes.

Soient $(G,\cdot)$, $(G',*)$ groupes. Un **morphisme de groupes** est une application d'un groupe dans un autre telle que l'image de tout produit est le produit des images. $f(x \cdot y) = f(x) * f(y)$
L'ensemble des morphismes de $(G,.)$ dans $(G',*)$ est noté $\boldsymbol{Hom(G, G')}$
Un **endomorphisme de groupes** est un morphisme d'un groupe dans lui-même.
Soit un morphisme de groupes $f : (G,\cdot) \to (G',*)$
L'image d'un neutre est un neutre. $f(1_G) = 1_{G'}$
L'image de l'inverse est l'inverse de l'image. $f(x^{-1}) = f(x)^{-1}$
L'image d'une puissance (resp. multiple) est la puissance de l'image. $f(x^n) = f(x)^n \ \ \forall n \in \mathbb{Z}$
L'image d'un sous-groupe est un sous-groupe. $H \leq G \Rightarrow f(H) \leq G'$
L'image réciproque d'un sous-groupe est un sous-groupe. $H' \leq G' \Rightarrow f^{-1}(H') \leq G$
L'**image d'un morphisme de groupes $\boldsymbol{Im(f)}$** est l'image de l'application $f(G)$

Le **noyau d'un morphisme de groupes** $\boldsymbol{Ker(f)}$ est l'image réciproque du neutre $f^{-1}(\{1\})$
L'image est un sous-groupe du groupe d'arrivée.
Le noyau est un sous-groupe du groupe de départ.
Morphisme surjectif équivaut à son image = groupe d'arrivée.
Morphisme injectif équivaut à son noyau = singleton neutre.
La composée de morphisme de groupes est un morphisme de groupe.
Un groupe est l'**image homomorphe** d'un autre, si c'est l'image de l'autre par un morphisme de groupes surjectif.
L'**injection canonique** d'une partie X d'un ensemble E est l'application $i : \begin{matrix} X \to E \\ x \mapsto x \end{matrix}$
L'injection canonique d'un sous-groupe dans son groupe est un morphisme injectif de groupes.
Exemples : L'application classe de $(\mathbb{Z},+) \to \left(\frac{\mathbb{Z}}{n\mathbb{Z}},+\right)$ est un morphisme surjectif de groupes.
L'application $x \in G \mapsto x^n \in G$ est un morphisme de groupes.
L'application déterminant du groupe des matrices inversibles d'un corps commutatif $(GL_n(\mathbb{K}),\times)$ dans le groupe $(\mathbb{K}^*,\times)$ est un morphisme de groupe dont le noyau est appelé **groupe linéaire spécial** noté $SL_n(\mathbb{K})$ et est donc un sous-groupe de $(GL_n(\mathbb{K}),\times)$

I.4. Isomorphismes de groupes. Automorphismes

Un **isomorphisme de groupes**, est un morphisme de groupes bijectif càd $\phi : G \to G'$ isomorphisme ssi $\exists \psi : G' \to G \ \phi \circ \psi = \psi \circ \phi = Id$ (definition categorique).
L'ensemble des isomorphismes de groupes entre $(G,\cdot),(G',\cdot)$ est note $\boldsymbol{Iso(G,G')}$
Ex : $exp : (R,+) \to (R^*,\times)$ est un isomorphisme de groupes.
L'application $x \in (R,+) \mapsto \begin{pmatrix} 1 & x \\ 0 & 1 \end{pmatrix} \in \left(\left\{\begin{pmatrix} 1 & t \\ 0 & 1 \end{pmatrix} : t \in R\right\},+\right)$ est un isomorphisme de groupes.
L'application $\sigma \in (S_n,\circ) \mapsto M_\sigma = \left(e_{\sigma(1)},\dots,e_{\sigma(n)}\right) \in (GL_n(R),\times)$ isomorphisme de groupes.
Un **automorphisme de groupes** est un isomorphisme d'un groupe dans lui-même = iso+endomorphisme
Si $\sigma \in S_3$ alors $x \in \{1,\sigma,\sigma^2\} \mapsto x^2 \in \{1,\sigma,\sigma^2\}$ est un automorphisme de groupes.
On note $\boldsymbol{Aut(G)}$ l'ensemble des automorphismes de groupes d'un groupe $(G,\cdot)$.
Si $g \in G$ un groupe, $\alpha_g : h \mapsto ghg^{-1}$ est un automorphisme. C'est un **automorphisme intérieur**
L'inverse d'un automorphisme intérieur est l'automorphisme intérieur de l'inverse $\alpha_g^{-1} = \alpha_{g^{-1}}$
L'ensemble des automorphismes intérieurs est note $\boldsymbol{Int(G)}$ et est un sous-groupe $Int(G) \leq Aut(G)$
Le groupe $Int(G)$ est trivial ssi G est abelien.

II. Sous-groupes distingués et groupes quotients

II.1. Classes à gauche, classes à droite

Soit H sous-groupe de G , la relation d'équivalence **à droite (resp. à gauche) selon/modulo H** est définie par $x \ R_d \ y \Leftrightarrow xy^{-1} \in H$ (resp. $x \ R_g \ y \Leftrightarrow x^{-1}y \in H$)
On note les classes d'équivalences à droite $Hx = \{hx : h \in H\}$ resp. à gauche $xH = \{xh : h \in H\}$, elles forment donc une partition de G. On note $\boldsymbol{\frac{G}{H_d}}$ resp. $\boldsymbol{\frac{G}{H_g}}$ l'ensemble quotient.
L'indice à droite (resp. à gauche) d'un sous-groupe H de G noté $\boldsymbol{[G :_d H]}$ resp. $\boldsymbol{[G :_g H]}$ est le cardinal de l'ensemble quotient $\frac{G}{H_d}$ resp. $\frac{G}{H_g}$
Les classes à droite (resp. à gauche) associées à un sous-groupe H sont en bijection avec H, et donc les une avec les autres, et donc ont toutes même cardinal, celui de H.
Th. de Lagrange. Si H sous-groupe d'un groupe <u>fini</u> G alors $\frac{G}{H}$ fini et $|G| = |H|[G : H]$ (gauche/droite)
Donc le cardinal du sous-groupe H divise celui de G $\frac{|G|}{|H|} = [G : H] \in N$, et donc l'indice ne dépend pas de la convention gauche/droite, il y a autant de classes à gauche que de classes à droite modulo H.

$|H|$ est la taille d'une classe, $[G:H]$ est le nombre de classes.
Un groupe de cardinal premier admet pour seuls sous-groupes G et $\{1\}$.

II.2. Sous-groupe distingués et groupe quotient

II.2.1. Suites exactes

Une **suite exacte** est un diagramme … $\to E_i \to^{f_i} E_{i+1} \to^{f_{i+1}}$ …, ou les E_i sont des groupes, les $f_i: E_i \to E_{i+1}$ sont des morphismes, et de plus $im(f_i) = \ker(f_{i+1})$, l'image d'un morphisme est le noyau du suivant.
Si f_i est injectif, E_i isomorphe a un sous-groupe de E_{i+1}
Si f_i est surjectif, f_{i+1} doit être le morphisme trivial 1 egal au neutre partout d'image 1.
Une section est un morphisme qui admet un morphisme inverse gauche : c'est un $s: H \to G$ tel que $\exists f: G \to H \;\; f \circ s = Id_H$. C'est un morphisme inverse droit.
Une rétraction est un morphisme qui admet un morphisme inverse droit. C'est un morphisme inverse gauche. Une rétraction est donc toujours associée à une section.
Une **suite exacte courte** est une suite exacte de la forme $1 \to A \to^{\alpha} B \to^{\beta} C \to 1$
Dans ce cas β est surjectif, et α est injectif.
Une **extension de groupes** est une suite exacte courte dans le cadre de la théorie des groupes.
Pour $1 \to A \to^{\alpha} B \to^{\beta} C \to 1$ on dit que $\boldsymbol{B}$ **est une extension de** $\boldsymbol{C}$ **par** $\boldsymbol{A}$.
Un **scindage à droite d'une suite exacte courte** est une section de β (du 2eme morphisme, càd droite), c'est donc $s: C \to B$ et $\beta \circ s = Id_C$
Un **scindage à gauche d'une suite exacte courte** est une rétraction de α (du 1er à gauche), c'est donc $r: B \to A$ et $r \circ \alpha = Id_A$
Une suite exacte courte est scindée à gauche (r. droite) si elle admet un scindage à gauche (r. droite)

II.2.2. Sous-groupes distingués

Un sous-groupe H est **distingué/normal** dans G ce qu'on note $\boldsymbol{H \lhd G}$ ou encore « $\frac{\boldsymbol{G}}{\boldsymbol{H}}$ **existe** » ssi les classes a gauches modulo H ne sont plus discernables des classes a droites modulo H ssi $\forall x \in G \; xH = Hx$ ssi $\forall g \in G \; \forall h \in H \; ghg^{-1} \in H$ ssi H est invariant par tout automorphisme intérieur. Dans ce cas on écrira simplement $\frac{\boldsymbol{G}}{\boldsymbol{H}} = G/_d H = G/_g H$.
Si $H \lhd G$ la loi du groupe est compatible avec la relation, on peut définir **loi quotient** $xH \cdot yH = (xy)H$
Ainsi $H \lhd G$ ssi $\frac{G}{H}$ muni de sa loi quotient est un groupe. Il y a donc une certaine analogie entre sous-groupe distingué et diviseur en théorie des nombres.
La loi quotient est aussi l'unique loi sur $\frac{G}{H}$ qui fait de $\pi_H: G \to \frac{G}{H}: x \mapsto xH$ un morphisme de groupes. π_H est la **projection canonique** sur H, c'est un morphisme surjectif de noyau H, et $\frac{G}{\ker(\pi_H)} = im(\pi_H)$
On peut résumer le théorème précèdent par la suite exacte $1 \to^1 H \to^i G \to^{\pi_H} \frac{G}{H} \to^1 1$
Th. factorisation. Un morphisme de groupes $f: G \to G'$, **est factorisable** sur un sous-groupe H de G càd $\exists \overline{f}: \frac{G}{H} \to G'$ tel que $f = \overline{f} \circ \pi$ ssi $f(H) = \{0_{G'}\}$ ssi $H \subseteq \ker(f)$.
Dans ce cas $\overline{f}$ est unique, $\overline{f}$ est un morphisme de groupes et on a $\forall a + H \in \frac{G}{H} \;\; \overline{f}(a+H) = f(a)$, $im(\overline{f}) = im(f), \ker(\overline{f}) = \frac{\ker(f)}{H}$
De plus $\overline{f}$ est surjective ssi f l'est et $\overline{f}$ est injective ssi $\ker(f) = H$.
Th isomorphisme 1 Le noyau d'un morphisme groupes $\phi: G \to G'$ est un sous-groupe distingué de G et ϕ induit un isomorphime de $\overline{\phi}: \frac{G}{\ker(\phi)} \to Im(\phi): xH \mapsto \phi(x)$
Remarque : ce théorème se généralise en dehors de la théorie des groupes, pour tout quotient.
Les sous-groupes distingués d'un groupe G sont exactement les noyaux de morphismes partant de G.

Pour $n \geq 1$, le groupe alterné A_n est sous-groupe distingué du groupe symétrique G_n comme ker de ε
Le groupe special lineaire $SL_n(K)$ est un sous-groupe distingué de $GL_n(K)$ comme noyau du det.
Dans un groupe abélien, tous les sous-groupes sont distingués.
Tout sous-groupe d'indice 2 dans un groupe G est distingué. $[G:H] = 2 \Rightarrow H \lhd G$
Dans un groupe G, les sous-groupes $\{1\}$ et G sont toujours distingués.
Un **groupe simple** est un groupe dont ses seuls sous-groupes distingués sont $\{1\}$ et G.
Un groupe de cardinal premier est simple c'est-à-dire $\frac{Z}{pZ}$ est simple avec p premier.
Si $n \neq 4$, le groupe alterne A_n est simple.
Les groupes simples sont analogues aux nombres premiers. Si un groupe est simple on ne peut pas le décomposer par dévissage en produit de groupes plus petits.

II.3. Centre et groupe dérivé

Le centre d'un groupe G est l'ensemble $\boldsymbol{Z(G)} = \{x \in G \mid \forall g \in G\ xg = gx\}$
Le centre d'un groupe est un sous-groupe distingué de ce groupe. $G/Z(G)$ existe
Tout sous-groupe de $Z(G)$ est distingué dans G.
Un groupe est abélien ssi il coïncide avec son centre.
Si $n \geq 3$, $Z(G_n) = \{1\}$
Le **groupe des quaternions** $\boldsymbol{H_8} = \{\pm 1, \pm i, \pm j, \pm k\}$ est un groupe ou la multiplication est definie par la regle des signes et les formules $i^2 = j^2 = k^2 = -1$; $ij = -ji = k$; $jk = -kj = i$; $ki = -ik = j$
Le centre du groupe des quaternions est $Z(H_8) = \{\pm 1\}$
Le **groupe dérivé d'un groupe** $\boldsymbol{G}$ note $\boldsymbol{G'}$ est <u>le sous-groupe de G engendré</u> par les éléments de la forme $[g,h] = ghg^{-1}h^{-1}, g \in G, h \in G$. Ces éléments sont appelés **commutateurs** du groupe G.
Le groupe dérivé d'un groupe est un sous-groupe distingué càd $\frac{G}{G'}$ existe.
Le groupe dérivé d'un groupe abélien est le groupe trivial $G' = \{1\}$.
On peut « rendre abélien » un groupe en le quotientant par son groupe dérivé G'.
$\frac{G}{G'}$ existe et $\frac{G}{G'}$ est abélien. De plus si pour un autre sous-groupe $\frac{G}{H}$ existe et est abélien, alors $G' \subseteq H$.

II.4. Sous-groupes du quotient et théorème d'isomorphisme

<u>Via la projection canonique</u>,
Si $\frac{G}{H}$ existe, fixer 1 sous-groupe de $\frac{G}{H}$ revient à fixer 1 sous-groupe K de G contenant H. $H \leq K \leq G$
Si $\frac{G}{H}$ existe, fixer un sous-groupe distingué de $\frac{G}{H}$ revient a fixer un sous-groupe distingué de G contenant H. Résultat plus général que le cadre de la théorie des groupes.
Pour tout diviseur d d'un entier $n \in N$, $\frac{Z}{nZ}$ admet un sous-groupe de cardinal d, ce sous groupe est unique et noté $\frac{dZ}{nZ} = \langle \frac{n}{d} \rangle$.
Soit $H, K \leq G$
Si $\frac{G}{H}$ existe et $H \leq K \leq K' \leq G$ alors $\frac{K}{H}$ existe, $\frac{K'}{H}$ existe, et $\frac{K}{H} \leq \frac{K'}{H}$
Th isom. 2. Si $\frac{G}{H}$ existe alors $HK = KH$ est un sous-groupe, $\frac{K}{K \cap H}$ existe, $\frac{KH}{H}$ existe et $\frac{K}{K \cap H} \approx \frac{KH}{H}$
Si $\frac{G}{H}$ existe alors ($\frac{G}{K}$ existe et $H \leq K$) ssi $\frac{\frac{G}{H}}{\frac{K}{H}}$existe)

Th isom. 3. Si $\frac{G}{H}$ existe, $\frac{G}{K}$ existe, et $H \leq K$ c'est-à-dire + simplement si $\frac{\frac{G}{H}}{\frac{K}{H}}$ existe, alors $\frac{G}{K} \approx \frac{\frac{G}{H}}{\frac{K}{H}}$

Le centre d'un groupe est toujours distingué, càd $\frac{G}{Z(G)}$ existe toujours.

Les sous-groupes de H_8 sont $\{1\}, \{\pm 1\}, \{\pm 1, \pm i\}, \{\pm 1, \pm j\}, \{\pm 1, \pm k\}, H_8$ et sont tous distingués.

III. Génération de groupes

III.1. Groupes monogènes cyclique

Un groupe est dit **monogène** s'il est engendré par un singleton. Un **générateur** est un élément qui engendre le groupe. Un groupe est dit **de type fini** s'il est engendré par un ensemble fini d'éléments.

Un groupe est dit **cyclique** s'il est monogène et fini.

Un groupe monogène est abélien.

Un groupe est monogène de cardinal infini ssi il est isomorphe a $(Z, +)$

Un groupe est cyclique ssi il est isomorphe a un $\left(\frac{Z}{nZ}, +\right)$ $n \in N$

L'ordre d'un groupe est le cardinal de son ensemble.

L'ordre d'un élément d'un groupe, est l'ordre du groupe monogène engendre par cet élément. On le note $o(g)$ ou bien $\omega(g)$.

Si $g \in G$ est d'ordre fini alors $g^{o(g)} = 1$.

Dans $\frac{Z}{nZ}$, k est un générateur ssi $k \wedge n = 1$

III.2. Groupes libres

Un groupe libre permet de modéliser les expressions en théorie des groupes. On le formalise comme un langage formel, dans lequel les mots représentent des expressions entre éléments d'un groupe. Si on avait pas l'associativité, a priori pour une expression il faudrait un arbre de syntaxe.

Une lettre de l'alphabet du langage représente l'expression d'un élément d'un groupe. Pour modéliser le fait qu'un élément d'un groupe a toujours un inverse on suppose que chaque lettre est associée à une autre lettre, et correspondent au même symbole, mais l'un représente l'inverse de l'autre. On peut supposer par ex, **l'alphabet de la forme** $\boldsymbol{Y = X \times \{-1, 1\}}$ et on note soit $x = (x, 1)$, soit $x^{-1} = (x, -1)$.

Un **mot du groupe libre** est donc une suite finie de **lettres** de Y. Un mot représente l'expression de composer les symboles éléments dans le même ordre par la l.c.i. du groupe. Ex « ab^{-1} » $= \left('a', 'b^{-1'}\right)$ représente le fait de prendre un premier élément a, puis l'inverse d'un deuxième b, et de calculer leur produit, le mot modélise l'expression ab^{-1}, on confondra la notation d'une expression et de son mot.

Comme dans les langages formels, on peut définir la concaténation, un mot est la concaténation de ses lettres, on peut définir un mot vide note ε.

Un **mot réduit** du groupe libre sur X est un mot dont deux lettres consécutives ne sont jamais associées autrement dit, c'est une expression dans laquelle on a simplifie les xx^{-1}, ou les $x^{-1}x$ consécutifs.

On peut toujours réduire un mot, en supprimant tous ses xx^{-1} ou $x^{-1}x$ consecutifs.

Deux mots sont équivalents ssi ils ont même forme réduite. Autrement dit l'expression qu'ils représentent est la même du point de vue des lois d'un groupe.

Le **groupe libre sur l'ensemble de symboles** $\boldsymbol{X = \{a, b, \dots\}}$ est note $\boldsymbol{M(X)}$ et est forme de l'ensemble des mots réduits, autrement dit on a quotienté par la relation précédente, la forme réduite étant un représentant canonique. On peut munir cet ensemble d'une loi $*$ qui correspond à faire la concaténation puis simplifier l'expression en obtenant le mot réduit correspondant. $\boldsymbol{(M(X),*)}$ **est le groupe libre.**

L'élément neutre du groupe libre est le mot vide ε.

Toute application $\phi : X \to G$ a valeurs dans un groupe G peut s'écrire $\phi = \psi \circ i_X$ avec ψ un unique morphisme de groupes $M(X) \to G$. De plus ψ prolonge ϕ, cad $\psi_{|X} = \phi$. Autrement dit, si on affecte des lettres symboles a certains éléments de G, alors on peut definir ce que veut dire toute expression contenant ces symboles, ψ correspond a <u>évaluer l'expression</u> formée de ces symboles dans G.

Autrement dit $\phi : X \to G$ admet un unique $\psi_\phi : M(X) \to G$ **morphisme d'évaluation** prolongeant ϕ.

Le groupe libre d'un singleton est $M(x) = \{x^n : n \in Z\} =< x >$

Dès que le cardinal de X est ≥ 2 $M(X)$ n'est plus abélien, et est beaucoup plus compliqué.

Le groupe libre d'un ensemble dénombrable est un ensemble dénombrable. (Par $\cup$ denom. de denom.)

III.3. Présentation d'un groupe

L'inclusion d'une partie A d'un groupe G peut être prolongée par l'unique morphisme d'évaluation $\phi_{i_A} : M(A) \to G$, dont l'image n'est autre que le sous-groupe engendre par la partie A.

On a donc toujours $\mathrm{im}(\phi_{i_A}) =< A > \approx \frac{M(A)}{\ker(\phi_{i_A})}$. Si ϕ_{i_A} est bijective, alors $G \approx M(A)$.

Dans le cas non injectif, càd $\neg G \approx M(A)$, une **présentation d'un groupe** G est un couple (A, R) ou A est une partie generatrice de G et R est une partie de $M(A)$ telle que $\ker(\phi_{i_A})$ est le plus petit sous-groupe distingué de $M(A)$ contenant R. (Prendre $R = \ker(\phi_{i_A})$ est trop grand, donc on restreint pour la def).

On note une présentation $< a_1, \dots, a_m ; r_1 = 1, \dots, r_n = 1 >$ avec $r_1, \dots, r_n$ mots reduits. TODO A clarifier.

Tout groupe infini admet un sous-groupe propre non trivial.

Tout groupe fini de cardinal ≥ 2 non premier admet un sous-groupe propre non trivial.

IV. Action d'un groupe sur un ensemble

IV.1. Définitions

Une **action à gauche (resp. à droite) d'un groupe G sur un ensemble X** correspond à une application $G \times X \to X : (g, x) \mapsto g \cdot x$ telle que $\forall x \in G\ 1.x = x$ (resp. $x \cdot 1 = x$) et $g \cdot (h \cdot x) = (gh) \cdot x$ (resp. $(x \cdot h) \cdot g = x \cdot (hg)$.

En posant $\phi(g)(x) = g \cdot x$ (resp. $x \cdot g$), une action peut se voir comme un morphisme de groupes $\phi : (G, .\,_G) \to (G(X), \odot\ \ )$ quelconque ou $G(X)$ est le groupe symétrique de X (ensemble des bijections dans X) muni de la composition orientée $(\sigma, \tau) \mapsto \sigma \odot \tau = \sigma \circ \tau$ (resp. $(\sigma, \tau) \mapsto \sigma \odot \tau = \tau \circ \sigma$ <u>Inverse la composition pour conv. droite!</u>).

Un groupe ***G* agit à gauche (droite) sur un ensemble X** si G admet une action à gauche (droite) sur X.

On considèrera des actions à gauche, mais les résultats sont analogues pour les actions à droites.

Une action est **fidèle** ssi $(\forall x \in X\ \ g \cdot x = x) \Rightarrow g = 1$ ssi son morphisme ϕ est injectif.

Ainsi on peut « rendre » une action fidèle en factorisant son morphisme ϕ associé, sur son noyau, cela modifie le groupe mais pas l'ensemble sur lequel il agit.

Un action est **triviale** si son morphisme ϕ l'est, càd d'image l'identité de $G(X)$, cad $\forall g \forall x\ g \cdot x = x$

Deux éléments de l'ensemble X sont sur une même orbite ssi $\exists g \in G\ g \cdot x = y$.

«Etre sur la même orbite » définit une relation d'équivalence sur X, de classes les **orbites $Gx = \omega_x \subseteq X$**, on peut écrire $\omega_x = \{g \cdot x : g \in G\}$

On note $\frac{X}{G}$ l'ensemble des orbites de X sous l'action de G. $\frac{X}{G} = \{\omega_x : x \in X\}$

Une action est **transitive** ssi $\forall x, y \in X \; \exists g \in G \; g \cdot x = y$ cad ssi il n'y a qu'une seule orbite sur X.
Dans ce cas pour tout point $x \in X$, $G \to X : g \mapsto g \cdot x$ est surjective.
L'action sur une orbite, est donc toujours transitive, et $G \to \omega_x : g \mapsto g \cdot x$ est surjective
Le **stabilisateur de $x \in X$** pour l'action $\cdot$ est le sous-groupe de G : $\boldsymbol{S_x} = \{g \in G \mid g \cdot x = x\} \leq G$
$x \in X$ est un **point fixe de l'action $\cdot$ sur G** si $Stab(x) = G$ cad $\forall g \in G \; g \cdot x = x$ cad $\omega_x = \{x\}$
On note $\boldsymbol{X^G}$ l'ensemble des points fixes de l'action $\cdot$ sur G. $X^G = \{x \in X \mid \forall g \in G \; g \cdot x = x\}$
On note pour $g \in G$, $\boldsymbol{F_g} = \{x \in X \mid g \cdot x = x\}$, Dire $g \in S_x \Leftrightarrow$ dire $x \in F_g$

IV.2. Exemples : groupe symétrique et action d'un groupe sur lui-même

Une action de groupe G sur un ensemble X est **k-transitive** si pour $(x_1, \dots, x_k), (y_1, \dots, y_k)$ deux ensembles de points distincts dans X, $\exists g \in G \; \forall i \; g \cdot x_i = y_i$.
L'action naturelle de G_n sur $X = \{1, \dots, n\}$ correspond au morphisme $Id : G_n \to G(X)$, elle est transitive, et même n-transitive.
Pour cette action, le stabilisateur d'un point de $X = \{1, \dots, n\}$, est isomorphe a G_{n-1} et le quotient $\frac{G_n}{G_{n-1}}$ est en bijection avec l'orbite du point ω_x qui n'est autre que X, donc a n éléments. Ainsi on retrouve $|G_n| = n$!. Les sous-groupes de G_n d'indice n sont toujours isomorphes a G_{n-1}.
Le groupe cyclique engendré par une permutation $\sigma \in G_n$ agit encore sur X mais l'action n'est pas transitive en général.
Th. de Cayley. Tout groupe est isomorphe à un sous-groupe d'un groupe de permutations.
Tout groupe fini de cardinal n est isomorphe a un sous-groupe de G_n
Tout groupe agit sur lui-même en prenant sa l.c.i. comme action : $g \cdot x \coloneqq gx$ (resp. xg)
Cette action est l'**action par translation à gauche** (resp. à droite).
Tout sous-groupe $H \leq G$ agit également sur G en restreignant la l.c.i. de G, les orbites de cette action a gauche (resp. a droite) sont les classes a droite (resp. a gauche) modulo H.
Un groupe G agit sur tout quotient (à gauche/droite) par un sous-groupe : $g \cdot g'H \coloneqq (gg')H$
Cette **action quotient** est transitive mais en général pas fidèle.
Tout groupe agit sur lui-même par conjugaison par automorphisme intérieur : $g \cdot h \coloneqq ghg^{-1} = \alpha_h(g)$.
Une **classe de conjugaison** est une orbite pour cette **action de conjugaison**.
2 éléments d'un groupe sont **conjugués** ssi ils sont dans la même classe de conjugaison ssi $x' = gxg^{-1}$
Le **centralisateur=commutant** de $x \in G$ est le stabilisateur de x pour l'action de conjugaison $C_G(x) = \{g \in G \mid gx = xg\}$, c'est donc aussi l'ensemble des éléments qui commutent avec x.

IV.3. Equation aux classes et formule de Burnside

On précise le lien entre orbite et stabilisateur. Soit G groupe agissant sur un ensemble X, et soit $x \in X$.
Les orbites de X sous l'action de G forment une partition de X et $f_x : \frac{G}{S_x} \to \omega_x : gS_x \mapsto g \cdot x$ est une bijection.
De plus, l'action $\cdot$ est compatible sur ω_x avec l'action quotient $\odot$ de G sur $\frac{G}{S_x}$ dans le sens suivant
$\forall g \in G \; \forall hS_x \in \frac{G}{S_x} \; f_x(g \odot hS_x) = g \cdot f_x(hS_x)$
Si G et X sont finis, la taille d'une orbite $|\omega_x|$ divise la taille du groupe $|G|$.
$\forall g \in G \; \forall x \in X \; S_{g \cdot x} = gS_xg^{-1}$
Deux éléments d'une même orbite ont leur stabilisateur S_x et S_y conjugués, donc de même cardinal.

Formule des classes. Pour G et X finis, $\forall x \in X \quad |G| = |S_x|\,|\omega_x|$

Equation aux classes. Pour G et X finis, $|X| = \sum_{\omega_x \in \frac{X}{G}} |\omega_x| = \sum_{\omega_x} \frac{|G|}{|S_x|} = \#\{\omega_x | \#\omega_x = 1\} + \sum_{\#\omega_x > 1} \frac{|G|}{|S_x|}$

Equation aux classes pour la conjugaison. $|G| = |Z(G)| + \sum_i |\omega_i|$ avec $\forall_i\ |\omega_i| = \frac{|G|}{|S_{x_i}|} \geq 2$

Pour p un nombre premier, un ***p*-groupe** est un groupe fini de cardinal p^k avec $k \in N^*$.

Le centre d'un p-groupe divise p^k et a au moins p éléments $|Z(G)| \geq p$

Tout groupe d'ordre p^2 est abélien.

Soit un p-groupe G agissant sur un ensemble X fini, alors $|X| \equiv |X^G|\ mod\ p$

Si G p-groupe agissant sur un ensemble X fini et p ne divise pas $|X|$, l'action admet au - 1 point fixe

Formule de Burnside. Soit G un groupe fini agissant sur un ensemble X fini.

Alors d'une part $\sum_{g \in G} |F_g| = \sum_{x \in X} |S_x|$

D'autre part, le nombre d'orbites de X est $\left|\frac{X}{G}\right| = \frac{1}{|G|} \sum_{g \in G} |F_g| = \frac{1}{|G|} \sum_{x \in X} |S_x|$

Soit l'action quotient à gauche $\phi \in Hom\left(G, Bij\left(\frac{G}{H_g}\right)\right)$ d'un groupe fini G sur un sous-groupe $H \leq G$.

Alors $\ker(\phi) \subseteq H$ et c'est le plus grand $N \subseteq H$ tel que $\frac{G}{N}$ existe.

V. Produits de groupes

V.1. Produits directs

Produit externe : Relativement à une structure algébrique, on peut toujours définir le produit cartésien de structures, et le munir d'opérations produits, la structure produit hérite des propriétés algébriques. C'est le **produit direct externe**, l'ensemble est le même que celui du produit cartésien.

Le produit direct externe vérifie la propriété universelle : TODO

Le sous-ensemble du produit constitué des familles a support fini (avec un nb fini de termes non neutre) est appelé **produit restreint externe.** Parfois, le terme de somme est utilisé même si on a un produit cartésien. Dans le cas où la famille est finie, il n'a pas de distinction entre restreint et pas restreint.

Le produit restreint externe vérifie la propriété universelle : TODO

Si l'opération est commutative, la prop. universelle se simplifie.

Produit interne : Pour les groupes. Dans un groupe, le **produit interne** de sous-groupes est l'ensemble produit des sous-groupes, les éléments produits le constituant pour qu'ils aient un sens sont nécessairement a support fini.

Le **produit restreint interne** de sous-groupes d'un groupe est un produit interne, telle que le produit externe correspondant à ce produit, doit être isomorphe au produit interne. Cela revient à exiger :

1) 2 éléments provenant de 2 sous-groupes distincts de la famille commutent toujours

2) l'unicité de l'écriture d'un élément sur le produit restreint interne.

Les sous-groupes d'un produit restreint interne sont alors automatiquement distingués dans le groupe et engendrent le groupe.

Dans le cas où la famille est finie et/ou si le groupe est abélien on utilise le terme de **produit direct interne** plutôt que restreint interne.

G est le produit direct interne d'une famille finie de sous-groupes ssi 1)/1') + 2)/2') + 3)/3')

1) 2 éléments provenant de 2 sous-groupes distincts de la famille commutent toujours.

Sous 2)+3), on peut remplacer 1 par 1') Tous les sous-groupes sont distingués, càd tout $\frac{G}{G_i}$ existe.

2) Le groupe est produit des sous-groupes $G = G_1 \dots G_n$ (l'ordre n'importera pas)
Sous 1) on peut remplacer par 2') Le groupe est engendré par les sous-groupes $G = \langle G_1 \cup \dots \cup G_n \rangle$
3) Tout sous-groupe intersecté au produit de tous les autres sous-groupes donne le singleton neutre.
En fait sous 1)2), on peut affaiblir 3 légèrement 3') $\forall i < n \ (G_1 G_2 \dots G_i) \cap G_{i+1} = \{1\}$
Récapitulatif pour 2 sous-groupes :
G est produit direct interne de 2 sous-groupes H et K ssi
Le produit externe $H \times K$ est isomorphe a G càd ssi
1) $\forall h \in H \ \forall k \in K \ hk = kh \quad / \ 1')$ H et K sont distingués dans G.
2) $G = HK \ / \ G = KH \ / \ G = \langle H \cup K \rangle / \ G = \langle K \cup H \rangle$
3) $H \cap K = \{1\}$
Remarque 2) + 3) $\Leftrightarrow \forall x \in G \ \exists \, ! \, h \in H, k \in K \ x = hk$
Dans ce cas on note $G = H \otimes K$.
On peut enlever 2) si on exige juste que H, K sont en produit direct. On peut enlever 1) si grp abéliens.
2 sous-groupes abéliens sont en produits direct interne ssi $H \times K \approx HK$ ssi $H \cap K = \{1\}$
N sous-groupes abéliens sont en produit direct interne ssi $H_1 \times \dots \times H_n \approx H_1 \dots H_n$ ssi $H_i \cap \prod_{j \neq i} H_j = 1$

V.2. Produit semi-direct

On sait que deux sous-groupes H, K distingués dans G, sont en produit direct interne ssi 2)+3)
Deux sous-groupes N, H dont seul l'un est supposé distingué, sont en **produit semi-direct interne** ssi $\begin{cases} G = NH \ / \ G = HN \ / \ G = \langle H \cup N \rangle / \ G = \langle N \cup H \rangle \\ N \cap H = \{1\} \end{cases}$ ssi $\forall x \in G \ \exists \, ! \, n \in N, h \in H \ x = nh$ ssi la restriction a H de la surjection canonique $G \to \frac{G}{N}$ est un isomorphisme de $H \to \frac{G}{N}$ ssi la surjection canonique $G \to \frac{G}{H} \to 1$ se scinde par un morphisme s tel que $s\left(\frac{G}{N}\right) = H$.
Pour $g = nh \in NH = G, \ g' = n'h' \in NH = G$, alors $gg' = (nhn'h^{-1})(hh') \in NH$
Comme H agit par conjugaison sur N, G isomorphe au produit $H \times K$ muni de $\big((n,h),(n',h')\big) \mapsto (n(hn'h^{-1}) = n\alpha_h(n'), hh')$. Avec $\alpha : H \to Aut(N)$ la conjugaison.
Soit un morphisme de groupes $\alpha : H \to Aut(N)$ avec N, H deux groupes, on note α_h l'image d'un $h \in N$.
Le **produit semi-direct externe (à droite) d'un groupe N par un groupe H selon un morphisme $\alpha : H \to Aut(N)$ (càd α action à gauche de H sur N)** est le produit cartésien $N \times H$ muni de la loi $(n,h) \cdot (n',h') = (n\alpha_h(n'), hh')$, on note $N \rtimes_\alpha H$. L'ordre importe contrairement au produit direct.
$N \rtimes_\alpha H$ contient les sous-groupes $N \rtimes_\alpha \{1_H\} \approx N$, et $\{1_N\} \rtimes_\alpha H \approx H$ et s'exprime toujours comme produit semi-direct <u>interne</u> de ces 2 sous-groupes.
$N \rtimes_\alpha H = (N \rtimes_\alpha \{1_H\})(\{1_N\} \rtimes_\alpha H) \approx (N \rtimes_\alpha \{1_H\}) \rtimes (\{1_N\} \rtimes_\alpha H)$ mais pas forcément $\approx N \rtimes H$
$\frac{N \rtimes_\alpha H}{N \rtimes_\alpha \{1\}}$ existe, mais $\frac{N \rtimes_\alpha H}{\{1\} \rtimes_\alpha H}$ n'existe pas forcément.
Résumé:
Si on peut écrire $G = NH$ avec $\frac{G}{N}$ existe, $N \cap H = \{1\}$ alors G est isomorphe au produit semi-direct externe $N \rtimes H$ suivant la conjugaison $\alpha : H \to Aut(N) : h \mapsto (n \mapsto hnh^{-1})$.
Pour un produit semi direct externe $G = N \rtimes_\alpha H$, en identifiant $N \approx N \rtimes_\alpha \{1\}$ et $H \approx \{1\} \rtimes_\alpha H$, N est un sous-groupe distingué dans G, $\frac{G}{N}$ est isomorphe a H. <u>Attention avec cette identification</u>, on ne peut pas toujours conclure $N \rtimes_\alpha H \approx N \rtimes H$ suivant la conjugaison, (sinon α serait inutile).

Différence semi-direct/direct. Un produit semi-direct externe $N \rtimes_\alpha H$ est direct ssi l'action α est triviale ssi $\frac{N \rtimes_\alpha H}{\{1\} \rtimes_\alpha H}$ existe ssi $N \rtimes_\alpha H$ est commutatif.

Il se peut qu'un produit semi-direct associé à une action non triviale soit isomorphe au produit direct qui lui est associé.

Caractérisation d'un produit semi-direct comme suite exacte courte scindée à droite.

Pour un produit semi-direct $N \rtimes_\alpha H$, on a $1 \to N \to^i N \rtimes_\alpha H \to^{\pi_N} H \to 1$ scindée à droite.

Si $1 \to N \to^i G \to^p H \to 1$ est une suite exacte courte scindée à droite de section s, alors $G \approx N \rtimes_\alpha H$ avec $\alpha_h : n \mapsto s(h)ns(h)^{-1}$. s induit un isomorphisme entre H et $s(H) \leq N \rtimes_\alpha H$.

Exemples

Soient G groupe et H sous-groupe de G agissant sur G par automorphismes interieurs. Cela définit un produit semi-direct qu'on note $G \rtimes_\alpha H$ isomorphe a $G \times H$ par $(g, h) \mapsto (gh, h)$

Pour deux groupes G, H on a $Z(G \times H) = Z(G) \times Z(H)$

$GL_n(R) = SL_n(R) \rtimes_\alpha R^*$, si n est impair on peut choisir le produit direct.

Soit N, H groupes et $\alpha, \beta : H \to Aut(N)$ morphismes tels que $\alpha = \beta \circ \phi$ avec $\phi \in Aut(N)$ alors $N \rtimes_\alpha H = N \rtimes_\beta H$

$1 \to A_n \to G_n \to^\varepsilon \{\pm 1\} \to 1$ scindée à droite par $s(-1) = \sigma = (12), s(1) = \sigma^2$ donc $G_n \approx A_n \rtimes_\alpha \{\pm 1\}$

$D_n \approx \frac{Z}{nZ} \rtimes_\alpha \frac{Z}{2Z}$ avec l'action $\alpha(-1): \frac{Z}{nZ} \to \frac{Z}{nZ} : x \mapsto -x$

Si p est premier, le groupe diédral D_{2p} est le seul produit semi-direct non trivial de $\frac{Z}{pZ} \rtimes_\alpha \frac{Z}{2Z}$

$1 \to SL_n(K) \to GL_n(K) \to^{det} K^* \to 1$ scindée par $s(\lambda) = diag(\lambda, 1, \dots, 1)$. $GL_n(K) \approx SL_n(K) \rtimes_\alpha K^*$

Ce produit est direct ssi $K^* \to K^* : x \mapsto x^n$ automorphisme. (vrai pour R et n impair, ou pour K fini de caractéristique p et $n = p^k$).

$1 \to \frac{Z}{2Z} \to \frac{Z}{4Z} \to^p \frac{Z}{2Z} \to 1$ avec p la réduction modulo 2 n'est pas scindée à droite, donc pas un produit semi-direct.

$1 \to \frac{Z}{2Z} \to H_8 \to^p \frac{Z}{2Z} \times \frac{Z}{2Z} \to 1$ n'est pas scindée à droite donc H_8 n'est pas produit semi-direct du groupe de Klein par $\frac{Z}{2Z}$

Pour $G = N \rtimes_\alpha K$ et $K \leq G$, $K \supseteq N$, on a $K = N \rtimes_\alpha (K \cap H)$

Tout groupe d'ordre 255 est cyclique. (par th de Sylow)

CNS pour $N \rtimes_\alpha H \approx N \rtimes_\beta H$

VI. Groupes abéliens de type fini*

VI.1. Structure des groupes abéliens de type fini (notation additive)

La donnée d'un groupe abélien est équivalente à celle d'un Z-module

Un groupe abélien est **Z-libre** s'il existe une famille $(g_i)_{i \in I}$ d'elements de G tel que $Z^{(I)} \to G : (n_i)_{i \in I} \mapsto \sum_{i \in I} n_i g_i$ soit un isomorphisme. La famille $(g_i)_{i \in I}$ est une **base du groupe abélien** G.

Une base d'un groupe abélien est une famille génératrice du groupe abélien.

Il y a des groupes abéliens non Z-libres càd sans base, par ex $(Q, +)$

Tout sous-groupe d'un groupe abélien Z-libre de base finie, est aussi Z-libre avec une base de cardinal inferieur. Toutes les bases du sous-groupe sont en fait de même cardinal fini.

En particulier, si un groupe abélien est Z-libre, toutes ses bases ont même cardinal fini ou $+\infty$.

Le **rang d'un groupe Z-libre** est le cardinal fini ou $+\infty$ de n'importe laquelle de ses bases.

Un groupe Z-libre de rang n est donc isomorphe a $(Z^n, +)$.
Un **élément de Z-torsion d'un groupe** est un élément d'ordre fini dans ce groupe.
On note $\boldsymbol{Tor(G)}$ le **groupe de torsion** de G, càd l'ensemble des éléments de Z-torsion d'un groupe G.
Un groupe est de torsion ssi il est égal à son groupe de torsion. $T(G) = G$
Un groupe est **sans torsion** si son groupe de torsion est trivial. $T(G) = \{0\}$ càd 0 seul elem. d'ordre fini.
Le groupe de torsion d'un groupe est un sous-groupe du groupe.
Un groupe de type fini et de torsion, est de cardinal fini.
Un groupe abélien de type fini a donc un groupe de torsion de cardinal fini.
Un groupe Z-libre est sans torsion.
Un groupe abélien de type fini sans torsion est Z-libre de rang fini.
N Z-modules en produit direct interne ssi $H_1 \times \ldots \times H_n \approx H_1 + \cdots + H_n$ ssi $H_i \cap \sum_{j \neq i} H_j = 0$
Un groupe abélien de type fini G admet toujours un sous-groupe H, Z-libre de rang n ($H \approx Z^n$) tel que $G \approx H \oplus Tor(G)$ et $Tor(G)$ est fini. Cela ramène l'étude de G à celle d'un groupe abélien fini.
On note $\boldsymbol{G(p)}$ l'ensemble des éléments d'un groupe G d'ordre une puissance de p un nombre premier, et on note $\boldsymbol{P(G)}$ l'ensemble des nombres premiers p tels que $G(p) \neq \{0\}$.
Pour un groupe abélien fini G, $G(p)$ est fini et $G = \oplus_{p \in P(G)} G(p)$. Ramène l'étude de G à celle des $G(p)$
Un groupe d'ordre p^2 avec p premier, est soit cyclique isomorphe a $\frac{Z}{p^2 Z}$ soit isomorphe a $\frac{Z}{pZ} \times \frac{Z}{pZ}$, ces deux derniers n'étant pas isomorphes l'un de l'autre.
L'exposant d'un groupe $\boldsymbol{\omega(G)}$ (notation +) est le plus petit entier $n \in N^* \cup \{+\infty\}$ tq $\forall x \in G\ nx = 0$.
Un groupe fini est toujours d'exposant fini, le ppcm des ordres de ses éléments.
Un groupe cyclique est d'exposant fini l'ordre de n'importe lequel de ses générateurs.
Un premier $p|\omega(G)$ ssi $\exists x \in G\ \ p|o(x)$
Pour un groupe abélien fini G, son ordre et son exposant $|G|$ et $\omega(G)$ ont mêmes diviseurs premiers donc l'ordre $|G|$ divise une puissance de l'exposant $\omega(G)$.
Autrement dit un premier $p|\omega(G)$ ssi $p|\#G$
Théorème de Cauchy 1. Pour p diviseur premier de $|G|$ alors $\exists x \in G\ \ o(x) = p$
Pour un groupe abélien fini G, tous les $G(p)$ sont des p-groupes. Ramène l'étude aux p-groupes abéliens
Un p-groupe abélien est isomorphe à $\frac{Z}{p^{n_1} Z} \times \ldots \times \frac{Z}{p^{n_r} Z}$ avec $n_1 \geq \cdots \geq n_r \geq 1$ une suite finie unique.
Finalement un groupe abélien de type fini se décompose $G \approx Z^n \times \prod_{1 \leq i \leq k} \frac{Z}{p_i^{n_{i,1}} Z} \times \ldots \times \frac{Z}{p_i^{n_{i,r}} Z}$ avec $n \in N$ unique, $p_1 < \cdots < p_k$ uniques premiers, et $\forall i\ \ n_{i,1} \geq \cdots \geq n_{i,r} \geq 1$ uniques entiers.
Un groupe abélien fini est isomorphe à $\frac{Z}{d_1 Z} \times \ldots \times \frac{Z}{d_r Z}$ avec $d_1 \geq \cdots \geq d_r \geq 1$ une suite finie unique.
A comparer avec la structure des modules de type fini sur les anneaux principaux.

VI.2. Automorphismes des groupes cycliques

Soit G un groupe cyclique d'ordre $n \in N$ isomorphe à $\left(\frac{Z}{nZ}, +\right)$. On note G multiplicativement.
La classe d'un élément $[x \in Z]_G$ engendre G ssi cet élément x est premier avec n. (Bézout).
On note $\boldsymbol{\frac{Z}{nZ}^\times}$ l'ensemble des générateurs de $\frac{Z}{nZ}$, c'est un groupe pour la loi produit de l'anneau quotient.
L'**indicatrice d'Euler** d'un entier $n \in N$ est le nombre de générateurs de $\frac{Z}{nZ}$ cad $\boldsymbol{\phi(n)} = \left|\frac{Z}{nZ}^\times\right| = \{1 \leq k \leq n \mid k \wedge n = 1\}$

$Aut(G) = Aut\left(\frac{Z}{nZ}\right) \approx \frac{Z}{nZ}^{\times}$ par l'isomorphisme $\alpha \mapsto \alpha(1)$.

Th restes Chinois. Si $m \wedge n = 1$ alors $\frac{Z}{mnZ} \approx \frac{Z}{mZ} \times \frac{Z}{nZ}$, de plus $\frac{Z}{mnZ}^{\times} \approx \frac{Z}{mZ}^{\times} \times \frac{Z}{nZ}^{\times}$, $\phi(mn) = \phi(m)\phi(n)$

Cela ramène l'étude a celle des $\frac{Z}{p^k Z}^{\times}$ avec p premier et $k \in N^*$

Dans le cas $k = 1$ $\frac{Z}{pZ}$ est un corps, $\left|\frac{Z}{pZ}^{\times}\right| = p - 1$, de plus $\frac{Z}{pZ}^{\times}$ est cyclique isomorphe a $\frac{Z}{(p-1)Z}$

Pour p premier et $k \geq 1$, $\phi(p^k) = p^k - p^{k-1} = (p-1)p^{k-1}$

$\forall n \in N^* \; n = \sum_{d|n} \varphi(d)$

Soit p un nombre premier et k un entier

Si $p \geq 3$ et $k \geq 1$ alors $\frac{Z}{p^k Z}^{\times} \approx \frac{Z}{(p-1)p^{k-1}Z}$

Si $p = 2$ et $k \geq 3$ alors $\frac{Z}{2^k Z}^{\times} \approx \frac{Z}{2^{k-2}Z} \times \frac{Z}{2Z}$

Si $p = 2$ et $k = 2$ alors $\frac{Z}{4Z}^{\times} \approx \frac{Z}{2Z}$

Le groupe des inversibles de $\frac{Z}{nZ}$ n'est pas toujours cyclique.

VI.3. Sous-groupes discrets de R^n

Un sous-groupe de R est soit dense, soit de la forme xZ avec $x \in R$. S'il est dense il est non monogène.

Comme $Z + \theta Z$ avec $\theta \in R \setminus Q$, n'est pas monogène, c'est un sous-groupe dense de R.

Un sous-groupe de $(R^n, +)$ est **discret** ssi son intersection avec n'importe quel compact de R^n a un nombre fini de point, cad ssi sa topologie induite par celle de $(R^n, \| \quad \|)$ est discrète.

Un sous-groupe de R est donc soit dense soit discret dans R. Z^n est un sous-groupe discret de R^n.

Un sous-groupe discret de R^n est de la forme $G = Zu_1 + \cdots + Zu_r$ avec $(u_1, \ldots, u_r)$ libre dans R^n $r \leq n$

Cette famille est donc une Z-base de G.

Un **réseau de R^n** est un sous-groupe discret de R^n de rang n.

Réseaux = Objets centraux en mathématiques. Apparaissent en théorie algébrique des nombres, et théorie des groupes algébriques commutatifs complexes.

Le **domaine fondamental d'un réseau Γ associe a une Z-base u** de Γ est l'ensemble

$P_u = \{\sum_{i=1}^n \alpha_i u_i, \forall i \; \alpha_i \in [0,1)\}$

Le domaine fondamental est Lebesgue-mesurable de mesure $\lambda(P_u) = \left|\det_{B_0}(u)\right|$ independant de la base u, car $\lambda(P_v) = \lambda(P_u)|\det(f)|$ avec $f \in GL_n(Z)$ donc $\det(f) = \pm 1$.

Le volume d'un réseau de R^n est donc la mesure de n'importe quel domaine fondamental de ce reseau.

Th. Minkowski. Dans une partie mesurable de R^n de mesure > au volume d'un réseau, on peut trouver deux points distincts de la partie telle que la différence (vecteur les joignant) appartient au réseau.

Si une partie mesurable de R^n est convexe et symétrique par rapport à 0 et sa mesure $\mu(S) > 2^n v(\Gamma)$ avec Γ un reseau, alors l'intersection de la partie S et du reseau Γ contient un point non nul. Cela est encore vrai au cas limite $\mu(S) = 2^n v(\Gamma)$ si on rajoute l'hypothèse que la partie S est compacte.

Ex : Le **minimum essentiel d'un réseau** Γ est la plus petite norme d'un element non nul du reseau.

Le theoreme de Minkowski permet de majorer ce min essentiel. TODO (illisible)

Il existe un 2nd théorème de Minkowski appelé théorème des minima successifs

$\frac{2^n}{n!} v(\Gamma) \leq \lambda_1(\Gamma) \ldots \lambda_n(\Gamma) \leq 2^n v(\Gamma)$

VI.4. Caractères d'un groupe abélien fini (Serre Cours d'arithmétique)

Un caractère d'un groupe abélien fini G, correspond à un morphisme $(G,\cdot) \to (\mathbb{C}^*,\times)$ du groupe vers le groupe multiplicatif des complexes.

Le dual d'un groupe abélien fini, est l'ensemble $\hat{G} = Hom(G,\mathbb{C}^*)$ des caractères de ce groupe.

Pour faire l'analogie avec les formes linéaires, on pourrait noter $\langle \chi, g \rangle = \chi(g)$

L'image d'un élément $g \in G$ d'un groupe abélien fini, par un caractère du groupe, est une racine n-ième de l'unité $\chi(g)^n = 1$ avec $n = \#G$

Dans un groupe cyclique d'ordre n engendré par g, pour une racine n-ième de l'unité fixée $\omega \in \mu_n$, alors il existe un unique caractère χ de ce groupe tel que $\chi(g) = \omega$.

Ainsi, pour un groupe cyclique d'ordre n, $\left(\hat{G},\circ\right) \to (\mu_n,\times): \chi \mapsto \chi(g)$ est un isomorphisme de groupes, et on sait dans ce cas que $\#\hat{G} = \#G = n$. Donc G étant aussi $\approx \mu_n$, on a $G \approx \hat{G}$

Tout caractère d'un sous-groupe H d'un groupe abélien fini G, peut être prolongé en caractère du groupe G.

L'opération de restriction $\rho: \hat{G} \to \hat{H}$ est un morphisme de groupes surjectif, de noyau les caractères de G triviaux sur H, $\ker(\rho)$ est donc isomorphe à $\widehat{\left(\frac{G}{H}\right)}$

On a donc une suite exacte $1 \to \widehat{\left(\frac{G}{H}\right)} \to \hat{G} \to^{\rho} \hat{H} \to 1$

Le dual d'un groupe abélien fini, est aussi un groupe abélien fini de même cardinal. $\#\hat{G} = \#G$

Relations d'orthogonalité.

Pour un caractère $\chi \in \hat{G}$ d'un groupe abélien fini G, $\sum_{g\in G} \chi(g) = \begin{cases} \#G \text{ si } \chi = 1 \\ 0 \text{ si } \chi \neq 1 \end{cases}$

Pour un élément $g \in G$ d'un groupe abélien fini G, $\sum_{\chi\in \hat{G}} \chi(g) = \begin{cases} \#G \text{ si } g = 1 \\ 0 \text{ si } g \neq 1 \end{cases}$

Pour un groupe abélien fini, on a donc $\#G = \#\hat{G} = \#\hat{\hat{G}}$

Pour un élément $g \in G$ d'un groupe abélien fini, $\hat{g} = \langle .,g\rangle: \chi \mapsto \chi(g)$ est un caractère du dual $\hat{G}$.

L'application $\varepsilon: G \to \hat{\hat{G}}: g \mapsto \hat{g} = \left(\chi \mapsto \chi(g)\right)$ est un isomorphisme de groupes.

Exemples de caractères : Pour $a \in \mathbb{Z}$, $\chi_a: \mu_n \to \mathbb{C}^*: e^{\frac{2i\pi k}{n}} \mapsto e^{\frac{2i\pi ka}{n}} \in \widehat{\mu_n}$

$\hat{G} \subseteq F(G,\mathbb{C})$ et $F(G,\mathbb{C})$ est un $\mathbb{C}$ ev isomorphe à $\mathbb{C}^{\#G}$ donc de dimension $\#G$.

Lemme d'indépendance de Dedekind. Une famille finie de caractères distincts sur un groupe fini, forment une famille libre du $\mathbb{C}$ev $F(G,\mathbb{C})$.

Ainsi $\dim\left(Vect\left(\hat{G}\right)\right) = \#\hat{G}$

Pour un groupe fini, $\#\hat{G} = \#G \Rightarrow G$ abélien.

En général $\#\hat{G} = \#\widehat{\left(\frac{G}{D(G)}\right)} = \#\frac{G}{D(G)} = \frac{\#G}{\#D(G)}$

On peut montrer le théorème de classification des groupes abéliens finis.

Un groupe abélien fini est isomorphe à son dual, $\hat{G} \approx G$ (non canoniquement). On le sait dans le cas cyclique et $\widehat{A\times B} = \hat{A} \times \hat{B}$.

Sur un groupe abélien fini, sur $F(G,\mathbb{C})$, $\langle u,v\rangle = \frac{1}{\#G}\sum_{g\in G} u(g)\overline{v}(g)$ est un produit scalaire hermitien.

Pour $\chi_1,\chi_2 \in \hat{G}$, $\langle \chi_1,\chi_2\rangle = \langle \chi_1\chi_2^{-1}, \square\rangle$

Pour ce produit scalaire, les caractères de G forment une base orthonormale, (et donc une famille libre).

VII. Le groupe symétrique

VII.1. Propriétés élémentaires du groupe symétrique

Le groupe symétrique d'ordre n, G_n (ou S_n) est le groupe des bijections de $\{1, \dots, n\}$ muni de la composition. Il est abélien ssi $n \leq 2$

Une **permutation** est un élément du groupe symétrique.

Le **support d'une permutation** est l'ensemble des points non fixes par elle.

Si $(x_1, \dots, x_p)$ avec $2 \leq p \leq n$ sont des elements distincts de G_n le **p-cycle** $(x_1 \dots x_p)$ est la permutation définie par $\sigma(x_i) = x_{i+1}\ \forall i < p,\ \sigma(x_p) = x_1$ et $\sigma(x) = x$ partout ailleurs.

$\{x_1, \dots, x_p\}$ est le **support du p-cycle**.

Un p-cycle est d'ordre p dans le groupe symétrique.

Une **transposition** est un 2-cycle (i, j), se note parfois $t_{n,i,j}$.

Deux cycles à supports disjoints commutent.

Toute permutation $\sigma \in G_n$ du groupe symétrique s'écrit comme produit de cycles à supports disjoints de façon unique à permutation près des cycles.

L'ordre d'une permutation est le ppcm des ordres des cycles de sa décomposition en cycles.

Si $\sigma = (a_1 \dots a_k) \in G_n$ est un k-cycle et $\tau \in G_n$ alors $\tau\sigma\tau^{-1} = (\tau(a_1) \dots \tau(a_k))$ est encore un k-cycle.

Dans G_n, tous les cycles d'ordre fixé $k \in \{1, \dots, n\}$ sont conjugués.

Le centralisateur dans G_n d'un n-cycle est son groupe engendré.

La classe de conjugaison d'une permutation $\sigma \in G_n$ est définie de façon unique par la suite croissante des ordres des cycles de sa décomposition. La somme de ces ordres vaut n. Une classe de conjugaison correspond donc à un élément de $\bigcup_{1 \leq k \leq n} \{1 \leq \alpha_1 \leq \dots \leq \alpha_k \leq n \mid \alpha_1 + \dots + \alpha_k = n\}$

La suite croissante des ordres des cycles de la décomposition de $\sigma \in G_n$ peut être compris comme le type de σ. Une autre façon de le définir est :

Pour $\sigma \in G_n$ il existe un unique $\boldsymbol{a(\sigma)} \in \boldsymbol{E_n} = \{(a_1, \dots, a_n) \in [\![0, n]\!]^n \mid \sum_{k=1}^{n} k a_k = n\}$ appelé **type de σ** tel que $\forall k \in [\![2, n]\!]\ a_k(\sigma)$ est le nombre de k-cycles dans la décomposition de σ en produit de cycles à supports disjoints, et $a_1(\sigma)$ est le nombre de points fixes de σ.

Une classe de conjugaison dans G_n correspond donc à un type fixé. Càd 2 permutations sont conjuguées ssi elles ont même type.

$\forall \sigma \in G_n$ le nombre de permutations de $[\![1, n]\!]$ commutant avec σ est $\prod_{k=1}^{n} a_k(\sigma)!\, k^{a_k(\sigma)}$

$\forall a \in E_n$ le nombre de permutations de $[\![1, n]\!]$ dont le type est a, est $n_a = \frac{n!}{\prod_{k=1}^{n} a_k! k^{a_k}}$

La probabilité pour que deux permutations choisies uniformément et indépendamment dans G_n commutent est $p_n = \frac{|E_n|}{n!}$. $\quad p_n \leq \frac{4^n}{n!} \to_{n \to \infty} 0$

Hardy et Ramanujan 1918. $|E_n| \sim_{n \to \infty} \frac{1}{4\sqrt{3n}} e^{\pi\sqrt{\frac{2n}{3}}}$

Les ensembles suivants engendrent le groupe symétrique d'ordre n :

Les transpositions $(i\ j)$ pour $1 \leq i, j \leq n$

Les transpositions $(1\ i)$ pour $1 \leq i \leq n$

Les transpositions $(i-1\ i)$ pour $2 \leq i \leq n$

La transposition $(1\ 2)$ et le cycle $(1 \dots n)$

Une **inversion d'une permutation $\sigma \in G_n$** est une paire $\{i, j\}$ telle que $i < j$ et $\sigma(i) > \sigma(j)$.

VII.2. Le groupe alterné

La signature est l'unique morphisme de groupes non trivial $\boldsymbol{\varepsilon}$: $(G_n,\circ) \to (C^*,\times)$
La signature d'une permutation est 1 si le nombre d'inversions est paire, -1 sinon, càd $\varepsilon(\sigma) = (-1)^{\#\{\{i,j\}|1\leq i<j\leq n \text{ et } \sigma(i)>\sigma(j)\}}$.
On a $\varepsilon(\sigma) = \prod_{1\leq i<j\leq n} \frac{\sigma(j)-\sigma(i)}{j-i}$
La signature d'une transposition est -1. Donc la signature est à valeurs dans le groupe $(\{\pm 1\},\times)$.
Le produit de k transpositions a donc pour signature $(-1)^k$
Un k-cycle est d'ordre k et de signature $(-1)^{k-1}$. (On peut le décomposer en k transpositions).
Le **groupe alterné d'ordre n** est le noyau de la signature dans le groupe symétrique. $\boldsymbol{A_n} = \ker(\varepsilon)$
Une permutation **paire** est un élément de $A_n \subset G_n$, une permutation **impaire** est élément de $G_n \setminus A_n$.
Autrement dit la parité d'une permutation est la parité de son nombre d'inversions.
Le groupe alterné d'ordre n est un sous-groupe d'indice 2 du groupe symétrique d'ordre n.
G_n agit n-transitivement sur $\{1,\dots,n\}$. A_n agit $(n-2)$-transitivement sur $\{1,\dots,n\}$.
Pour $n \geq 3$ les 3-cycles, engendrent le groupe A_n. Si $n \geq 5$ les 3-cycles sont de plus conjugués dans A_n.
Pour $n \geq 3$ tout 3-cycle est un carré, A_n est engendré par les carrés.
Pour $n \geq 3$ A_n est le seul sous-groupe d'indice 2 du groupe S_n.
Th. du a Galois*. Le groupe alterné d'ordre $n \neq 4$ est un groupe simple. (pas A_4, car $A_4 \approx \frac{Z}{2Z} \times \frac{Z}{2Z}$)
Si $n \geq 5$, les groupes dérivés de A_n et G_n sont donnés par $A'_n = A_n$ et $G'_n = A_n$.
Si $n \neq 4$, les seuls groupes distingués de G_n sont $\{Id\}$, A_n, et G_n
Tout sous-groupe d'indice n de G_n est isomorphe a G_{n-1}

VII.3. Automorphismes de G_n

La connaissance des automorphismes de G_n permet de déterminer les actions d'un groupe sur G_n et par suite les produits semi-directs impliquant G_n
Un automorphisme intérieur $\alpha_\sigma: \tau \mapsto \sigma\tau\sigma^{-1}$ est un automorphisme de G_n, qui est trivial ssi σ commute avec tout element de G_n.
La suite $1 \to Z(G_n) \to^i G_n \to^\alpha Int(G_n) \to 1$ est une suite exacte courte, et des que $n \geq 3$ le centre est trivial $Z(G_n) = 1$, G_n n'est pas abélien, donc
Pour $n \geq 3$ $G_n \approx Int(G_n)$
Pour $n \neq 6$, tout automorphisme du groupe symétrique est un automorphisme intérieur, donc
Pour $n \geq 3, n \neq 6$, on a $Aut(G_n) = Int(G_n) \approx G_n$.
Un automorphisme du groupe symétrique qui transforme les transpositions en transpositions, est un automorphisme intérieur.
Si $n = 6$, $Aut(G_6) \neq Int(G_6)$
Si $n \geq 3$, le groupe G_n n'est ni abélien, ni monogène, ni cyclique.
$G_n \approx A_n \rtimes \frac{Z}{2Z}$ et n'est jamais direct pour $n \geq 3$.
Dans G_n, il y a $\frac{n!}{k!(n-k)!} = C_n^k$ k-cycles $(2 \leq k \leq n)$

VIII. Sous-groupes de Sylow

VIII.0. p-groupes

Pour p un nombre premier, un $\boldsymbol{p}$**-groupe** est un groupe fini de cardinal p^k avec $k \in N^*$.
Le centre d'un p-groupe divise p^k et a au moins p elements $|Z(G)| \geq p$
Théorème de Cauchy 1. Dans un groupe fini, pour tout diviseur premier de son cardinal, on peut trouver

un élément d'ordre ce diviseur. (par récurrence forte et équation aux classes).
Pour p premier, un groupe fini est un p-groupe ssi tous ses elements sont d'ordre une puissance de p.
Tout sous-groupe et tout quotient d'un p-groupe est encore un p-groupe.
Un groupe dont un sous-groupe est un p-groupe normal et le quotient par lui est un p-groupe, est un p-groupe. Un produit semi-direct de deux p-groupes est un p-groupe.
Le produit restreint d'une famille de p-groupes est un p-groupe.
Dans un p-groupe, l'indice d'un sous-groupe est soit infini, soit une puissance de p.
Tout p-groupe est nilpotent donc résoluble.

VIII.1. Sous-groupes de Sylow

La question principale est inverse de Lagrange : étant donné un diviseur d de l'ordre d'un group fini, existe-t-il un sous-groupe de cardinal d ? Pas vrai en général car $|A_4| = 12$ et A_4 n'a pas de sous-groupe d'ordre 6.
Soit p un nombre premier, et G un groupe fini.
Un ***p*-Sylow d'un groupe fini *G***, est un sous-groupe de cardinal p^α, $\alpha \geq 1$ avec $p^\alpha m = |G|$ et $m \wedge p = 1$.
Une autre définition possible est un ***p*-Sylow d'un groupe fini *G*** est un p-sous-groupe maximal de G pour l'inclusion. Un p-Sylow est un p-sous-groupe d'indice premier avec p.
Exemple : Si $F_p = \frac{Z}{pZ}$ corps a p éléments, le groupe $GL_n(F_p)$ est fini de cardinal le nombre de bases de ${F_p}^n$. Càd $\left|GL_n(F_p)\right| = (p^n - 1)(p^n - p\ ) \dots (p^n - p^{n-1}) = p^{\frac{n(n-1)}{2}}(p^n - 1) \dots (p - 1)$.
L'ensemble des matrices triangulaires supérieures de F_p avec des 1 sur la diagonale, est un p-Sylow de $GL_n(F_p)$ car de cardinal $p^{\frac{n(n-1)}{2}}$.

VIII.2. Théorèmes de Sylow

Th. Sylow 1. Un groupe fini G dont p est un diviseur premier de son cardinal, contient au moins un p-Sylow S et alors pour tout sous-groupe H de G, $\exists g \in G$ tel que $gSg^{-1} \cap H$ est un p-Sylow <u>de H</u>.
Soit un groupe fini G, on note $|G| = p^\alpha m$ avec $m \wedge p = 1, \alpha \geq 1$. Alors pour tout $0 \leq i \leq \alpha$, G admet un p-sous-groupe H_i de cardinal p^i.
Tout p-sous-groupe d'un groupe fini G, peut etre inclus dans un p-Sylow du groupe.
Th de Cauchy 2. Un groupe fini G dont p est un diviseur premier de son cardinal, contient au moins un sous-groupe d'ordre p. Ce sous-groupe est cyclique donc on retrouve le théorème de Cauchy 1.
Th. Sylow 2. Pour p fixé, les p-Sylows d'un groupe fini G sont 2 à 2 conjugués.
Th. Sylow 3. Le nombre de p-Sylow distincts de G, $\boldsymbol{n_p(G)}$ divise $|G|$ et $n_p(G) \equiv 1\ (mod\ p)$
Un p-Sylow d'un groupe fini est distingué ssi c'est l'unique p-Sylow pour ce p fixé.

VIII.3. Quelques applications et compléments

Tout groupe de cardinal 45 est isomorphe a l'un des produits directs $\frac{Z}{5Z} \times \frac{Z}{9Z}$ ou $\frac{Z}{5Z} \times \left(\frac{Z}{3Z}\right)^2$
Si G groupe de cardinal pq avec p, q premiers, $p < q$ alors
Si p ne divise pas $q - 1$, $G \approx \frac{Z}{pZ} \times \frac{Z}{qZ}$
Si p divise $q - 1$, $G \approx \frac{Z}{pZ} \times \frac{Z}{qZ}$ ou $G \approx \frac{Z}{pZ} \rtimes_\alpha \frac{Z}{qZ}$ avec α l'unique action non triviale de $\frac{Z}{pZ}$ sur $\frac{Z}{qZ}$
Un groupe simple de cardinal 60 est isomorphe au groupe alterne A_5 d'ordre 5.
Soit G un groupe fini, et p un diviseur premier fixe du cardinal de G, alors
Tous les p-Sylows de G sont distingués ssi le groupe G est produit direct de ses p-Sylows.

Argument de Frattini. Soit G un groupe fini, N un sous-groupe distingué, et S un p-Sylow de N. Alors $G = C(S) \cdot N = N \cdot C(S)$ avec $C(S)$ le centralisateur de S cad $C(S) = \{g \in G \mid gSg^{-1} = S\}$
En particulier, si M est un sous-groupe de G contenant le centralisateur d'un p-Sylow du groupe G, alors M est egal a son centralisateur $C(M)$.

Complément 1. Algorithme de Todd-Coxeter
1.1. Un premier exemple
1.2. Description de l'algorithme
Complément 2. Géométrie diophantienne
2.1. Approximation diophantienne
2.2. L'équation de Pell

Exercices.
Dans un groupe quelconque G, $o(xy) = p \Rightarrow o(yx) = p$
Si l'union de deux sous-groupes est un groupe, alors l'un deux est inclus dans l'autre.
L'intersection de deux sous-groupes de cardinaux finis et premiers entre eux, est le groupe trivial.
Le produit interne de deux sous-groupes d'ordre deux premiers distincts, est un sous-groupe cyclique.
Le produit externe de n sous-groupes de cardinaux $\alpha_1, \dots, \alpha_n$ est cyclique ssi $\forall i \neq j \ \alpha_i \wedge \alpha_j = 1$
Un groupe dans lequel tout carré est nul, est abélien. De plus s'il est fini et non trivial, il est isomorphe a $\left(\left(\frac{\mathbb{Z}}{2\mathbb{Z}}\right)^n, +\right), n \in \mathbb{N}^*$.
Un sous-groupe d'indice $\leq p - 1$ du groupe symétrique S_p avec p premier ≥ 5, est un sous-groupe d'indice 1 ou 2. Montre qu'il n'y a pas de sous-groupe de S_5 d'ordre 30 ou 40, bien que $|S_5| = 120$, donc fournit un contre-exemple réciproque Lagrange.
Dans un groupe abélien si $o(x) < \infty, o(y) < \infty, o(x) \wedge o(y) = 1$ alors $o(xy) = o(x)o(y)$
Un groupe fini tel que $\forall d \geq 1$ l'équation $x^d = 1$ a au plus d solutions, est un groupe cyclique.
Un sous-groupe d'un groupe fini, dont l'indice est le plus petit facteur premier de $card(G)$, est distingué.
Un groupe fini d'ordre n tel que $n \wedge \phi(n) = 1$, est cyclique.
Tchebycheff*. Si $n \in \mathbb{N}, n \geq 4$ alors $\exists p$ premier tel que $n < p < 2n - 2$.
Symbole de Legendre. TODO
Tout entier naturel est somme de quatre carrés d'entiers*.