Théorie des Groupes

David Wiedemann

Table des matières

List of Theorems

Lecture 1: Introduction

Fri 10 Sep

1 Une Introduction à la Théorie des Catégories

Notion Fondamentale : la composition

— Composition d'applications
— l'exemple fondamental d'un groupe est donné par $\mathrm{Aut}(X)$, où la multiplication du groupe est donnée par la composition d'automorphismes.

1.1 Catégories

Definition 1 (Graphe dirigé)
Un graphe dirigé G consiste en un couple de classes G_0 et G_1, muni de deux applications

$$\mathrm{dom} : G_1 \to G_0 \text{ et } \mathrm{cod} : G_1 \to G_0$$

appelées domaine et codomaine. On pense à G_0 comme l'ensemble des sommets et G_1 l'ensemble des arêtes de G.

Par exemple, si $x, y \in G_0, f \in G_1$, alors

$$\mathrm{dom}(f) = x, \quad \mathrm{cod}(f) = y$$

$$X \xrightarrow{\quad f \quad} Y$$

On introduit la notation

$$G(x, y) = \{f \in G_1 | \, \mathrm{dom}(f) = x, \mathrm{cod}(f) = y\}$$

Exemple
Soit X un ensemble, et soit $R \subset X \times X$ une relation sur X. Alors $G_r = (X, R)$ est un graphe dirigé, où

$$\mathrm{dom} : R \to X : (x_1, x_2) \to x_1 \text{ et } \mathrm{cod} : R \to X : (x_1, x_2) \to x_2$$

Observer que $\forall x_1, x_2 \in X$

$$G_R(x_1, x_2) = \begin{cases} \{(x_1, x_2)\} : (x_1, x_2) \in R \\ \emptyset \text{ sinon} \end{cases}$$

Definition 2 (Catégories)
Une catégorie C est un graphe dirigé (C_0, C_1) muni d'applications de composition

$$\gamma_{a,b,c} : C(a, b) \times C(b, c) \to C(a, c) : (f, g) \to g \circ f$$

$$\begin{tikzcd} A \arrow[r, "f"] \arrow[rr, bend right, "f\circ g"'] & B \arrow[r, "g"] & C \end{tikzcd}$$

— *(Existence d'identités) Il existe une application* $\mathrm{Id} : C_0 \to C_1 : c \to \mathrm{Id}_c$ *tel que*
$$f \circ \mathrm{Id}_a = f = \mathrm{Id}_b \circ f \forall f \in C_1(a,b), \forall a, b \in C_0$$
— *(Associativité) Quelque soient* $a, b, c, d \in C_0$ *et* $f \in C(a,b), g \in C(b,c)$ *et* $h \in C(c,d)$
$$(h \circ g) \circ f = h \circ (g \circ f) \in C(a,d)$$

Notation

On note

$$C_0 = \mathrm{Ob}\, C - \text{ les objets de } C$$
$$C_1 = \mathrm{Mor}\, C - \text{ les morphismes}$$

— Si $\mathrm{Ob}\, C, \mathrm{Mor}\, C$ sont des ensembles, alors C est petite.
— Si $C(a,b)$ est un ensemble $\forall a, b \in \mathrm{Ob}\, C$, alors C est localement petite.

Lecture 2: Exemples de Categories

Mon 20 Sep

1.2 Exemples de Catégories

Exemple

— *Des catégories concrètes*
— *des catégories non concrètes*

1.2.1 Catégories concrètes

Les objets sont des ensembles munis de structures supplémentaire :

1. Ens dont les objets sont les ensembles et les moprphismes sont les applications ensemblistes.
$$\mathrm{Ob}\,\mathrm{Ens} = \text{ la classe de tous les ensembles}$$
$$\mathrm{Mor}\,\mathrm{Ens} = \text{ applications ensemblistes}$$
2. La catégorie Gr , dont les objerts sont les groupes et les morphismes sont les homomorphismes de groupe.
$$\mathrm{Ob}\,\mathrm{Gr} = \text{ la classe de tous les groupes}$$
$$\mathrm{Mor}\,\mathrm{Gr} = \text{ la classe de tous les homomorphismes de groupe}$$
La composition est encore donnée par celle des applications ensemblistes et les identites sont celles des groupes vus comme ensembles.

3. La catégorie Ab, dont les objets sont les groupes abeliens et les morphismes sont les homomorphismes de groupe.

$$\operatorname{Ob} \mathrm{A}b = \{A \in \operatorname{Ob} \mathrm{G}r | A \text{ abelien } \}$$
$$\operatorname{Mor} \mathrm{A}b = \{\phi \in \operatorname{Mor} \mathrm{G}r | \operatorname{dom} \phi, \operatorname{cod} \phi \in \operatorname{Ob} \mathrm{A}b\}$$

4. La categorie $\mathrm{Vect}_{\mathbb{K}}$, dont les objets sont les espaces vectoriels sur le corps $\mathbb{K}$ et les morphismes sont les applications lineaires.

$$\operatorname{Ob} \mathrm{Vect}_{\mathbb{K}} = \text{ la classe de tous les } \mathbb{K}\text{-espaces vectoriels}$$
$$\operatorname{Mor} \mathrm{Vect}_{\mathbb{K}} = \text{ la classe de toutes les applications } \mathbb{K}\text{-lineaires}$$

Dans tous ces cas, la composition est bien définie car elle preserve toujours la structure supplementaire (ie. le groupe ou l'espace vectoriel)

1.2.2 Categories pas forcement concretes

1. Soit X un ensemble, $R \subset X \times X$ une relation sur X. Alors le graphe dirigé G_R admet des applications de composition naturelle, qui verifient l'associativité.
Soit $x, y, z \in X$ tel que $(x,y),(y,z) \in R \exists ?(y,z) \circ (x,y)$? Existe-il une arete de x vers $z \iff (x,z) \in R$
Donc on veut que R soit transitive. L'existence de l'identité dans une catégorie implique que $(x,x) \in R \forall x \in X$ ce qui implique que R est reflexive.
2. Pour tout groupe G , il y a une catégorie BG, spécifié par $\operatorname{Ob} BG = \star$ et $BG(\star,\star) = G$, où la composition est donnée par la multiplication de G

$$\operatorname{Ob} BG = \{\star\}$$
$$\operatorname{Mor} G = \{g \in G\}$$

On définit la composition

$$\gamma : BG(\star,\star) \times BG(\star,\star) \to BG(\star,\star) \times BG(\star,\star)$$

et on sait que γ (ie. la composition) est associative car la multiplication dans G est associative.
3. Soient C et D des catégories. Leur produit est la catégorie notée $C \times D$ spécifié par

$$\operatorname{Ob}(C \times D) = \operatorname{Ob} C \times \operatorname{Ob} D$$

et

$$(C \times D)((c,d),(c',d')) = C(c,c') \times D(d,d') \forall c,c' \in \operatorname{Ob} C, d,d' \in \operatorname{Ob} D$$

où la composition est donnée par celle de Cdans la premiere composante et par celle de D dans la deuxieme, et $\mathrm{Id}_{(c,d)} = (\mathrm{Id}_c, \mathrm{Id}_d)$.
$(f, g) : (c, d) \times (c', d') \in \mathrm{Mor}(C \times D)$.
Etant donné $(f, g) : (c, d) \to (c', d'), (f', g') : (c', d') \to (c'', d'')$, on definit

$$(f', g') \circ (f, g) = (f' \circ f, g' \circ g)$$

L'associativité suit de la composition associative dans C et D

Definition 3 (Isomorphisme)
Soit C une catégorie. Un morphisme $f : a \to b$ dans C est un isomorphisme s'il admet un inverse, i.e., il existe un morphisme $g : b \to a$ tel que $g \circ f = \mathrm{Id}_a$ et $f \circ g = \mathrm{Id}_b$. On dit alors que les objets a et b sont isomorphes.
Un isomorphisme dont le domaine est egal au codomaine est un automorphisme.
Une catégorie dont tous les morphismes sont des isomorphiemes est un groupoide.

Lecture 3: Comment comparer 2 categories

Tue 21 Sep

1.3 Foncteurs

On souhaite une application entre categories qui preserve la structure de la composition.

Definition 4 (Foncteur)
Soient C et D des categories. Un foncteur F de C vers D , note $F : C \to D$ consiste en un couple d'applications

$$F_{Ob} : \mathrm{Ob}\, C \to \mathrm{Ob}\, D$$

$$F_{Mor} : \mathrm{Mor}\, C \to \mathrm{Mor}\, D$$

tel que pour tout morphisme $f : a \to b$ dans C

$$F_{\mathrm{Mor}}(f) : F_{\mathrm{Ob}}(A) \to F_{\mathrm{Ob}}(b)$$
$$F_{\mathrm{Mor}}(\mathrm{Id}_c) = \mathrm{Id}_{F_{\mathrm{Ob}(c)}}$$

pour tout $c \in \mathrm{Ob}\, C$, et

$$F_{\mathrm{Mor}}(g \circ f) = F_{\mathrm{Mor}(g)} \circ F_{\mathrm{Mor}}(f)$$

quel que soient $f \in C(a, b), g \in C(b, c),$ et $a, b, c \in \mathrm{Ob}\, C$

Lemme 3
Soient $F : C \to D$ et $F' : D \to E$ des foncteurs. Alors le couple d'applications

$$F'_{\mathrm{Ob}} \circ F_{\mathrm{Ob}} : \mathrm{Ob}\, C \to \mathrm{Ob}\, E$$

et

$$F'_{\mathrm{Mor}} \circ F_{\mathrm{Mor}} : \mathrm{Mor}\, C \to \mathrm{Mor}\, E$$

definit un foncteur de C vers E , que nous notons $F' \circ F : C \to E$.

- (Les foncteurs identites) Pour toute categorie C , il y a un foncteur $\mathrm{Id}_C : C \to C$ dont les composantes sont les identites.
- (Les foncteurs oubli) On travaille souvent (et parfois de maniere implicite) avec des foncteurs en general notes U , qui oublient de la structure sur les objets et morphismes. Par exemple, $U : \mathrm{G}r \to \mathrm{E}ns$.
  Si G est un groupe, $U(G)$ oublie sa mulitplication et ses inverses.
  Si $\phi : G \to H$ est un homomorphisme de groupe, alors $U(\phi) : U(G) \to U(H)$ est simplement l'application sous-jacente.
  U preserve la composition et l'identite, cat elles sont definies exactement de la meme maniere dans les deux categories.
- $U : \mathrm{Vect}_{\mathbb{K}} \to \mathrm{A}b$
  Pour $V \in \mathrm{Ob}\,\mathrm{Vect}_{\mathbb{K}} \Rightarrow U(V)$ oublie la multiplication par scalaire et ne retient que son groupe abelien sous-jacent. Puisque les compositions et les identites sont les memes dans les deux categories, U est bien un foncteur.
- Puisque tout groupe abelien est un groupe, on a un foncteur $\mathrm{Ab} \to \mathrm{Gr}$, etant donne un tel foncteur d'inclusion (qu'on appelle generalement ι) on dit que Ab est une sous-categorie de Gr

Lecture 4: Transformations naturelles

Sun 26 Sep

1.4 Transformations naturelles

Comment comparer deux foncteurs ayant le meme domaine et codomaine ?

Definition 5 (Transformations naturelles)
Soient $F, F' : C \to D$ des foncteurs. Une transformation naturelle τ de F vers F' est une application

$$\tau : \mathrm{Ob}\, C \to \mathrm{Mor}\, D$$

tel que pour tout $f : b \to c$ et et $\tau_c \in D(F(c), F'(c))$, on a

$$F'(f) \circ \tau_b = \tau_c \circ F(f)$$

Si τ_c est un isomorphisme pour tout c , alors τ est un isomorphisme naturel.

Soient $F, F', F" : C \to D$ des foncteurs et soient $\sigma : F \to F'$ et $\tau : F' \to F"$ des transformations naturelles. Alors l'application

$$\mathrm{Ob}\, C \to \mathrm{Mor}\, D : c \to \tau_c \circ \sigma_c$$

On définit alors $\tau \circ \sigma : F \to F"$ par

$$\tau \circ \sigma : \mathrm{Ob}\, C \to \mathrm{Mor}\, D$$

On veut montrer que $\forall f : b \to c$ dans C, on a

$$\tau_c \circ \sigma_c \circ F(f) = \sigma_b \circ \tau_b \circ F\text{"}(f)$$

ce qui suit immédiatement. On construit facilement une transformation naturelle identité. Pour un foncteur $F : C \to D$, il y a une identité donné par

$$\operatorname{Ob} C \to \operatorname{Mor} D : c \to \operatorname{Id}_{F(c)}$$

Il est facile de voir que pour tout autre transformation naturelle $\tau : F \to G$. Notons que ainsi, pour toute catégories C et D , C petit, il y a une catégorie $\operatorname{Fun}(C, D)$, dont les objets sont les foncteurs de C vers D et les morphismes sont les transformations naturelles.

Exemple
Soit $U : \operatorname{Vect}_{\mathbb{K}} \to \operatorname{Ens}$ *le foncteur qui oublie tout la structure algebrique et soit* $L : \operatorname{Ens} \to \operatorname{Vect}_{\mathbb{K}}$ *le foncteur qui envoie un ensemble sur l'ensemble de ses combinaisons linéaires.*
Il y a une transformation naturelle $\eta : \operatorname{Id}_{\operatorname{Ens}} \to U \circ L$*.*
Pour definir $\eta : \operatorname{Id}_{\operatorname{Ens}} \to U \circ L$ *, il nous faut une application* $\eta : \operatorname{Ob} \operatorname{Ens} \to \operatorname{Mor} \operatorname{Ens}$ *tel que*

$$\forall X \in \operatorname{Ob} \operatorname{Ens}, \eta_X : X \to U(L(X))$$

donc $\forall x \in X, \eta_X(x) : X \to \mathbb{K}$*.*
On décide de poser

$$\eta_X(x)(x') = \begin{cases} 1 : x' = x \\ 0 : x' \neq x \end{cases}$$

Est-ce que ce diagramme commute ?

$$\begin{array}{ccc} X & \xrightarrow{\eta_X} & U(L(X)) \\ \Big\downarrow f & & \Big\downarrow U(L(f)) \\ Y & \xrightarrow{\eta_Y} & U(L(Y)) \end{array}$$

On a

$$\begin{aligned} \eta_Y \circ f(x) = \eta_Y(f(x)) : Y \to \mathbb{K} \\ y \to \begin{cases} 1 : y = f(x) \\ 0 : y \neq f(x) \end{cases} \end{aligned}$$

On a aussi

$$U(L(f)) \circ \eta_X(x) : Y \to \mathbb{K}$$

$$y \mapsto \sum_{x' \in f^{-1}(y)} \eta_X(x)(x') = \begin{cases} 1 : y = f(x) \\ 0 : \ sinon \end{cases}$$

On a donc bien une transformation naturelle. De plus, on a une transformation naturelle $\epsilon : L \circ U \to \mathrm{Id}_{\mathrm{Vect}_{\mathbb{K}}}$ *Pour* $V \in \mathrm{Ob}\,\mathrm{Vect}_{\mathbb{K}}$

$$L \circ U(V) = \{\omega : U(V) \to \mathbb{K} | | \{v | \omega(v) \neq 0\} | < \infty\}$$

Enfait, ω *est un élément du dual de* V*.*
Définir $\epsilon_V : L \circ U(V) \to V$ *par*

$$\epsilon_v(\omega) = \sum_{v \in V} \omega(v) \cdot v$$

Cette somme est finie et donc bien définie.
On vérifie facilement que ϵ_V *est linéaire.*
Soit $g : V \to V'$ *une application linéaire, est-ce que le diagramme suivant commute*

$$\begin{array}{ccc} L \circ U(V) & \xrightarrow{\epsilon_V} & V \\ \downarrow{\scriptstyle L\circ U(g)} & & \downarrow{\scriptstyle g} \\ L \circ U(V') & \xrightarrow{\epsilon_{V'}} & V' \end{array}$$

On a

$$g \circ \epsilon_V(\omega) = \sum_{v \in V} \omega(v) \cdot g(v)$$

Dans l'autre sens

$$\begin{aligned} \epsilon_{V'} \circ (L \circ U(g))(\omega) &= \sum_{v' \in V'} L \circ U(g)(\omega)(v') \cdot v' \\ &= \sum_{v' \in V'} \left(\sum_{v \in g^{-1}(v')} \omega(v) \right) \cdot v' \end{aligned}$$

.

Lecture 5: Adjonctions

Sat 02 Oct

1.5 Equivalence de categories

Definition 6 (Equivalence de categories)
Un foncteur $F : C \to D$ *est une Equivalence de categories s'il existe un foncteur* $F' : C \to D$ *tel que*

$$\sigma : \mathrm{Id}_C \overset{\cong}{\Rightarrow} F' \circ F \ \ et \ \tau : \mathrm{Id}_D \overset{\cong}{\Rightarrow} F \circ F'$$

Remarque
Si F *est un isomorphisme de categories, c'est aussi une equivalence de categories.*

Exemple
Soit Un *la categorie avec un seul objet* $*$ *et un seul morphisme* Id. *Soit* C *la categorie* $\mathrm{Ob}\, C = \{a, b\}$ *et deux morphismes non-identite* $f : a \to b$ *et* $g : b \to a$ *qui sont des isomorphismes. Alors les categories* Un *et* C *sont equivalentes.*
On definit $F : \mathrm{Un} \to C$ *par* $F(*) = a, F(\mathrm{Id}) = \mathrm{Id}_a$.
On definit $F' : C \to \mathrm{Un}$ *par* $F'(a) = F'(b) = *$.
On a que $F' \circ F = \mathrm{Id}_{\mathrm{Un}}$ *donc la transformation naturelle* $\sigma = \mathrm{Id}_{\mathrm{Id}_{\mathrm{Un}}}$ *est triviale.*
Dans l'autre sens, $F \circ F' \neq \mathrm{Id}_C$ *, cependant* $\exists \tau : \mathrm{Id}_C \to F \circ F'$ *defini par*

$$\tau : \mathrm{Ob}\, C \to \mathrm{Mor}\, C$$

donne par

$$\tau(a) = \mathrm{Id}_a, \tau(b) = g$$

Verifions la naturalite :
Commencons par $f : a \to b$*, on a*

$$\mathrm{Id}_a \circ \mathrm{Id}_a = g \circ f$$

ce qui est vrai par definition de C.
De meme

$$\mathrm{Id}_a \circ g = \mathrm{Id}_a \circ g$$

1.6 Adjonctions

On veut generaliser la notion d'equivalence de categories, dont il y a beaucoup d'exemples interessants (surtout en theorie des groupes)

Definition 7 (Adjonctions)
Un couple de foncteurs $L : C \to D$ *et* $R : D \to C$ *forme une adjonction s'il existe des transformations naturelles*

$$\eta : \mathrm{Id}_C \to R \circ L \text{ et } \epsilon : L \circ R \to \mathrm{Id}_D$$

tel que les diagrammes suivants commutent

$$\begin{tikzcd} L(c) \arrow[r, "L(\eta_c)"] \arrow[dr, "Id_{L(c)}"'] & L \circ R \circ L(c) \arrow[d, "\epsilon_{L(c)}"] \\ & L(c) \end{tikzcd}$$

$$\begin{tikzcd} R(d) \arrow[r, "\eta_{R(d)}"] \arrow[dr, "\mathrm{Id}_{R(d)}"'] & R \circ L \circ R(d) \arrow[d, "R(\epsilon_d"] \\ & R(d) \end{tikzcd}$$

pour tout $c \in \mathrm{Ob}\, C, d \in \mathrm{Ob}\, D$.

Analysons ces identites triangulaires.
La premiere identite veut dire $\forall c \in \mathrm{Ob}\, C, \eta_c : c \to RL(c)$, on peut lui appliquer L et on trouve

$$L(c) \overset{L(\eta_c)}{\longmapsto} LRL(c)$$

On peut maintenant considerer $\epsilon_{L(c)} : LRL(c) \to L(c)$ pour revenir a $L(c)$

$$L(c) \overset{L(\eta_c)}{\longmapsto} LRL(c) \overset{\epsilon_{L(c)}}{\longmapsto} L(c)$$

et on veut que cette suite de composition soit egale a $\mathrm{Id}_{L(c)}$.
Pour la deuxieme identite, soit $d \in \mathrm{Ob}\, D$, on a alors

$$R(d) \overset{\eta_{R(d)}}{\longmapsto} RLR(d) \overset{R(\epsilon_d)}{\longmapsto} R(d)$$

Si $L : C \leftrightarrow D : R$ est une adjonction avec transformations naturelles associees $\eta : \mathrm{Id}_C \to RL$ et $\epsilon : LR \to \mathrm{Id}_D$, alors on dit que L est un adjoint a gauche de R et R est un adjoint a droite de L.
On notera alors $L \dashv R$.

1.7 Caracterisation des Adjonctions

1.7.1 Preparation

Soit $L : C \leftrightarrow D : R$ un couple de foncteurs entre deux categories petites. On peut y associer deux autres foncteurs interessants
— $D(L(-), -) : C^{op} \times D \to \mathrm{Ens}$
— $C(-, R(-)) : C^{op} \times D \to \mathrm{Ens}$
qui sont definis comme suit
— Sur les objets,

$$\forall (c, d) \in \mathrm{Ob}\, C^{op} \times \mathrm{Ob}\, d \quad D(L(-), -)(c, d) = D(L(c), d)$$

— Sur les morphismes Soient $(f^{op}, g) \in \mathrm{Mor}(C^{op}(c, c') \times D(d, d'))$.
Donc $\exists f \in C(c', c)$, on veut definir une application ensembliste

$$D(L(f^{op}), g) : D(L(c), d) \to D(L(c'), d')$$

On peut resumer ceci dans le diagramme

$$L(c') \overset{L(f)}{\longmapsto} L(c) \overset{h}{\longmapsto} d \overset{g}{\longmapsto} d'$$

Ainsi, $D(L(f^{op}, g)) := g \circ h \circ L(f) : L(c') \to d'$.
Est-ce que ce choix definit bien un foncteur ?

— Identites : Pour $h : L(f) \to d \in C(L(f), d)$ Si $(\mathrm{Id}_c^{op}, \mathrm{Id}_d) \in \mathrm{Mor}(C^{op} \times D)$ alors $D(L(\mathrm{Id}_c^{op}), \mathrm{Id}_d)(h) = \mathrm{Id}_d \circ h \circ \mathrm{Id}_{L_c} = h$.
Donc
$$D(L(\mathrm{Id}_c^{op}, \mathrm{Id}_d)) = \mathrm{Id}_{D(L(c),d)}$$

— Considerons
$$(c, d) \xrightarrow{(f^{op},g)} (c', d') \xrightarrow{(f'^{op},g')} (c", d")$$
et etudions
$$D(L(c), d) \xrightarrow{D(L(f^{op}),g)} D(L(c'), d') \xrightarrow{D(L(f'^{op}),g')} D(L(c"), d")$$
On a donc, pour $h \in D(L(c), d)$
$$D(L(f^{op}), g) \circ D(L(f'^{op}, g'))(h) = g' \circ g \circ h \circ L(f) \circ L(f') \circ g = D(L(f'^{op} \circ f^{op}), g' \circ g)(h)$$

De maniere semblable, $\exists$ foncteur
$$C(-, R(-)) : C^{op} \times D \to \mathrm{Ens}$$
defini sur les objets par
$$\forall (c, d) \in \mathrm{Ob}(C^{op} \times D) \quad C(-, R(-))(c, d) = C(c, R(d))$$
et $\forall (f^{op}, g) : (c, d) \to (c', d')$, alors
$$\begin{aligned} C(f^{op}, R(g)) &: C(c, R(d)) \to C(c', R(d')) \\ &(h : c \to R(d)) \to (R(g) \circ h \circ f) \end{aligned}$$

Lecture 6: Caracterisation des Adjonctions

Sun 10 Oct

1.8 Exemple concret d'adjonction

On considere $L : \mathrm{Ens} \to \mathrm{Vect}_{\mathbb{K}}$ et $U : \mathrm{Vect}_{\mathbb{K}} \to \mathrm{Ens}$.
Ces adjonctions verifient les identites triangulaires et on a une adjonction $L \dashv U$.
Verifions les identites triangulaires.
Soit $V \in \mathrm{Ob}\,\mathrm{Vect}_{\mathbb{K}}$ Considerer
$$U(V) \xrightarrow{\eta_{U(V)}} UL(UV)$$
et
$$U(LU(V)) \xrightarrow{U(\epsilon(V))} U(V)$$
On veut voir que $U(\epsilon_V) \circ \eta_{U(V)} = \mathrm{Id}_{U(V)}$.
Par definition de η ,
$$\begin{aligned} \eta_{U(V)} &\to UL(U(V)) \\ v &\mapsto (\eta_{U(V)}(v) : U(V) \to \mathbb{K}) \end{aligned}$$

ou

$$\eta_{U(V)}(v) : V \to \mathbb{K} : v' \mapsto \delta_{v,v'}$$

Par ailleurs

$$\begin{aligned} U(\epsilon_V) : U(LU(V)) &\to U(V) \\ \omega &\mapsto \sum_{v\in V} \omega(v)\cdot v \end{aligned}$$

Donc, $\forall v \in U(V)$,

$$\begin{aligned} U(\epsilon_V)\circ\eta_{U(V)}(v) &= U(\epsilon_V)(\eta_{U(V)}(v)) \\ &= \sum_{v'\in V} \eta_{U(V)}(v)(v')\cdot v' \\ &= v \end{aligned}$$

Donc $U(\epsilon_V)\circ\eta_{U(V)} = \mathrm{Id}_{U(V)}$.

Montrons l'autre egalite triangulaire.
Soit $X \in \mathrm{Ob}\,\mathrm{Ens}$. Considerons

$$\begin{aligned} L(\eta_X) : L(X) &\to L(UL(X)) \\ \omega &\mapsto L(\eta_X) : UL(X) \to \mathbb{K} \\ L(\eta_X) : \psi &\mapsto \sum_{x\in\eta_X^{-1}(\psi)} \end{aligned}$$

Pour $\psi \in UL(X)$ (donc $\psi : X \to \mathbb{K}$),

$$\eta_X^{-1}(\psi) = \begin{cases} \{x'\} : \text{ si } \psi = \eta_X(x') \\ \emptyset \text{ sinon} \end{cases}$$

donc $L(\eta_X)(\omega) : UL(X) \to \mathbb{K}$

$$\psi \mapsto \sum_{x\in\eta_X^{-1}(\psi)} = \begin{cases} \omega(x') : \psi = \eta_X(x') \\ 0 : \psi \neq \eta_X(x') \forall x' \in X \end{cases}$$

De plus

$$\begin{aligned} \epsilon_{L(X)} : LU(L(X)) &\to L(X) \\ UL(X) \xrightarrow{(} \xi)\mathbb{K} &\mapsto \sum_{\psi\in UL(X)} \xi(\psi)\cdot\psi \end{aligned}$$

Faisons donc le calcul.
Soit $\omega \in L(X)$

$$\epsilon_{L(X)} \circ L(\eta_X)(\omega) = \epsilon_{L(X)}(L(\eta_X)(\omega))$$

$$
\begin{aligned}
&= \sum_{\psi \in UL(X)} L(\eta_X)(\omega)(\psi) \cdot \psi \\
&= \sum_{x \in X} \omega(x) \cdot \eta_X(x)
\end{aligned}
$$

Donc $\forall x' \in X$

$$
\begin{aligned}
\epsilon_{L(X)} \circ L(\eta_X)(\omega)(x') &= \left(\sum_{x \in X} \omega(x) \eta_X(x) \right)(x') \\
&= \sum_{x \in X} \omega(x)(\eta_X(x)(x')) = \omega(x')
\end{aligned}
$$

1.9 Caracterisation des adjonctions

Proposition 7
Un couple de foncteurs $L : C \to D$ et $R : D \to C$ entre categories localement petites est une adjonction si et seulement si il existe un isomorphisme naturel entre les foncteurs

$$D(L(-), -) : C^{op} \times D \to \mathrm{Ens} : (c, d) \to D(L(c), d)$$

et

$$C(-, R(-)) : C^{op} \times D \to \mathrm{Ens} : (c, d) \to C(c, R(d))$$

Nous demontrerons qu'il existe des transformations naturelles $\alpha : D(L(-), -) \to C(-, R(-))$ et $\beta : C(-, R(-)) \to D(L(-), -)$ qui sont mutuellement inverses. On a donc besoin de deux applications

$$\alpha : \mathrm{Ob}(C^{op} \times D) \to \mathrm{Mor\,Ens}$$

et

$$\beta : \mathrm{Ob}(C^{op} \times D) \to \mathrm{Mor\,Ens}$$

tel que $\forall (c, d) \in \mathrm{Ob}(C^{op} \times D)$

$$\alpha_{(c,d)} : D(L(c), d) \to C(c, R(d))$$

et

$$\beta_{(c,d)} : C(c, R(d)) \to D(L(c), d)$$

De plus, on veut que

$$\forall (f^{op}, g) \in C^{op} \times D((c, d), (c', d'))$$

$$D(L(c), d) \xrightarrow{\alpha_{c,d}} C(c, R(d)) \xrightarrow{C(f^{op}, R(g))} C(c', R(d'))$$

$$=D(L(c),d) \overset{D(L(f^{op}),g)}{\longrightarrow} D(L(c'),d') \overset{\alpha_{(c',d')}}{\longrightarrow} C(c',R(d'))$$

et de meme pour l'application naturelle inverse

$$\begin{aligned} &C(c,R(d)) \overset{\beta c,d}{\longrightarrow} D(L(c),d) \overset{D(L(f^{op}),g)}{\longrightarrow} D(L(c'),d') \\ =&C(c,R(d)) \overset{C(f^{op},R(g))}{\longrightarrow} C(c',R(d')) \overset{\beta_{(c',d')}}{\longrightarrow} D(L(c'),d') \end{aligned}$$

Finalement, on soujaite egalement que $\alpha_{(c,d)}$ et $\beta_{(c,d)}$ sont des applications ensemblistes mutuellement inverses.
On va construire α et β a partir des transformations naturelles $\eta : \mathrm{Id}_C \to RL$ et $\epsilon : LR \to \mathrm{Id}_D$.

Preuve
Supposer que $C \dashv D$ soit une adjonction avec transformation naturelle associees η, ϵ.

Premier pas : Construction de α et β

Soit $(c,d) \in \mathrm{Ob}(C^{op} \times D)$

$$\alpha_{(c,d)} : D(L(c),d) \to C(c,R(d))$$

Soit $h : L(c) \to d \in D(L(c),d)$, notons qu'on a

$$c \overset{\eta_C}{\longrightarrow} RL(c) \overset{R(h)}{\longrightarrow} R(d)$$

Definissons donc $\alpha_{(c,d)}(h) = R(h) \circ \eta_C$

Soit $(c,d) \in \mathrm{Ob}(C^{op} \times D)$, on a alors $\forall k : c \to R(d) \in C(c,R(d))$

$$L(c) \overset{L(k)}{\longrightarrow} LR(d) \overset{\epsilon_d}{\longrightarrow}$$

Posons donc

$$\beta_{c,d}(k) = \epsilon_d \circ L(k)$$

Naturalite

Soit $(f^{op}, g) : (c,d) \to (c',d') \in C^{op} \times D$.
Soit $h \in D(L(c),d)$, on a alors

$$\begin{aligned} C(f^{op},R(g)) \circ \alpha_{(c,d)}(h) &= C(f^{op},R(g))(R(h) \circ \eta_c) \\ &= R(g) \circ (R(h) \circ \eta_c) \circ f \\ &= R(g \circ h) \circ \eta_c \circ f \end{aligned}$$

Dans l'autre sens, on a

$$\begin{aligned}\alpha_{(c',d')} \circ D(Lf^{op}, g)(h) &= \alpha_{c',d'}(g \circ h \circ L(f))\\ &= R(g \circ h \circ L(f)) \circ \eta_c\\ &= R(g \circ h) \circ RL(f) \circ \eta_{c'}\end{aligned}$$

Il faut donc montrer que $\eta_c \circ f = RL(f) \circ \eta_{c'}$
Or $f : c' \to c$ *donne*

$$RL(f) \circ \eta_{c'} = \eta_c \circ f$$

commute car η *est une transformation naturelle. De meme, le fait que* ϵ *soit une transformation naturelle implique que* β *en est aussi une.*

α et β sont mutuellement inverses

Considerer pour $(c,d) \in \mathrm{Ob}(C^{op} \times D)$.
On a

$$\begin{aligned}\beta_{(c,d)} \cdot \alpha_{(c,d)}(h) &= \beta_{(c,d)}(R(h) \circ \eta_c)\\ &= \epsilon_d \circ L(R(h) \circ \eta_c)\\ &= \epsilon_d \circ LR(h) \circ L(\eta_c)\end{aligned}$$

On est en train de calculer

$$\begin{aligned}L(c) \xrightarrow{L(\eta_c)} LRL(c) \xrightarrow{LR(h)} LR(d) \xrightarrow{\epsilon_d} R\\ = L(c) \xrightarrow{L(\eta_c)} LRL(c) \xrightarrow{\epsilon_{L(c)}} LR(d) \xrightarrow{h} R(d)\\ = L(c) \xrightarrow{\mathrm{Id}_{L(c)}} \xrightarrow{h} R(d) = h\end{aligned}$$

Donc $h = \epsilon_d \circ LR(h) \circ L(\eta_c)$.
De meme l'autre identite triangulaire implique que $\alpha_{(c,d)} \circ \beta_{(c,d)} = \mathrm{Id}_{C(c,L(d))}$.
Ainsi α *et* β *sont bien des isomorphismes naturels, mutuellements inverses.*

Pour completer la caracterisation, il faudrait aussi montrer l'implication inverse.
Pour definir η, ϵ *a partir de* α, β

— η *: Considere* $\forall c \in \mathrm{Ob}\, C$,

$$\begin{aligned}\alpha_{(c,L(c))} : D(L(c), L(c)) &\to C(c, RL(c))\\ \mathrm{Id}_{L(c)} &\mapsto \alpha_{(c,L(c))}(\mathrm{Id}_{L(c)})\end{aligned}$$

Et on definit alors $\eta_c : c \to RL(c)$ *par* $\eta_c = \alpha_{(c,L(c))}(\mathrm{Id}_{L(c)})$

— ϵ *:Considerer* $\forall d \in \mathrm{Ob}\, D$,

$$\begin{aligned}\beta_{R(d),d} : C(R(d), R(d)) &\to D(LR(d), d)\\ \mathrm{Id}_{R(d)} &\mapsto \beta(R(d), d)(\mathrm{Id}_{R(d)})\end{aligned}$$

□

Lecture 7: Produits et Coproduits

Sat 16 Oct

1.10 Produits et Coproduits

Dans Ens, on a les constructions suivantes :
$\forall f : X \to Y, g : X \to Z \in \operatorname{Mor}\operatorname{Ens}$

$$\exists! h : X \to Y \times Z$$

tel que $\operatorname{pr}_Y \circ h = f, \operatorname{pr}_z \circ h = g$.
De meme $\forall f : X \to Y, g : X \to Z \in \operatorname{Mor}\operatorname{Ens}$

$$\exists! h : X \amalg Y \to Z$$

tel que

$$h \circ i_x = f, h \circ i_y = g$$

Formellement, dans une categorie quelconque

Definition 8
Soit C une categorie, et soient $b, c \in \operatorname{Ob} C$. Un produit de b et c consiste en un objet a de C et de deux morphismes $p : a \to b$ et $q : a \to c$ tel que pour tout couple de morphisme $f : d \to b$ et $g : d \to c$ il existe un unique morphisme $h : d \to a$ tel que $p \circ h = f$ et $q \circ h = g$.

Remarque
En general, le produit de deux objets n'existe pas, mais s'il existe, il est unique a isomorphisme pres.

> **Lemme 9**
> *Soit C une categorie, et soient $b, c \in \operatorname{Ob} C$. Si $b \xleftarrow{p} a \xrightarrow{q} c$ et $b \xleftarrow{p}' a \xrightarrow{q}' c$ sont des produits de b et c, alors il existe un isomorphisme $h : a \to a'$ qui respecte les morphismes de projection.*

Preuve
Puisque $b \xleftarrow{p} a \xrightarrow{q} c$ est un produit de b et c, la propriete universelle du produit nous dit qu'il existe un unique morphisme $h : a' \to a$.
Puisque $b \xleftarrow{p}' a' \xrightarrow{q}' c$ est un produit de b et c, $\exists! k : a \to a'$ tel que

$$p = p' \circ k \text{ et } q = q' \circ k$$

Montrons que h et k sont des isomorphismes mutuellement inverses.
On a que

$$p \circ h \circ k = p' \circ k = p$$

de meme, on a

$$q \circ h \circ k = q$$

L'unicite de la propriete universelle implique que $h \circ k = \operatorname{Id}_A$ et $k \circ h = \operatorname{Id}_{a'}$ $\square$

On introduit la notation pour "le" produit de $b, c \in \mathrm{Ob}\, C$ (s'il existe) est note

$$b \xleftarrow{p}_1 b \times c \xrightarrow{p}_2 c$$

ou parfois simplement $b \times c$.

Definition 9 (Coproduit)
Soit C une categorie. Un coproduit de b et c est un objet a et deux morphismes $i : b \to a$ et $j : c \to a$ tel que pour tout couple de morphismes $f : b \to d$ et $g : c \to d$ il existe un unqiue morphisme $h : a \to d$ tel que $h \circ i = f$ et $h \circ j = g$ ce que nous resumons par le diagramme suivant.

Lemme 10
Soit c une categorie, et soient $b, c \in \mathrm{Ob}\, C$ Si a et a' sont des coproduits de b et c, alors il existe un isomorphismes $h : a \to a'$ tel que $h \circ j = j', h \circ i = i'$

Remarque
Soit C une categorie, et soient $b, c \in \mathrm{Ob}\, C$. Si a est un produit de b et c dans C, alors a est un coproduit dans C^{op}.

1.11 Preservation des produits/coproduits

Proposition 12
Soit $C : L \dashv R : D$

1. *Soient $b, c \in \mathrm{Ob}\, C$, si $b \amalg c$ existe, alors $L(b \amalg c)$ est un coproduit de $L(b)$ et $L(c)$ dans D .*
2. *Soient $d, e \in \mathrm{Ob}\, D$. Si le produit $d \times e$ existe, alors son image sous le foncteur R est un produit de $R(d)$ et $R(e)$*

Preuve
Supposons que $b \xrightarrow{i}_1 b \amalg c \xleftarrow{i}_2 c$ est un coproduit de b et c dans C, considerons son image sous $L : L(b) \xrightarrow{L(i_1)} L(b \amalg c) \xleftarrow{L(i_2)} L(c)$.
Pour montrer que ceci est un coproduit de $L(b)$ et $L(c)$, il faut verifier la propriete universelle.
Soit alors un couple de morphismes $L(b) \xrightarrow{f} d \xleftarrow{g} L(c)$ dans D.
A voir : $\exists! h : L(b \amalg c) \to d$ qui satisfait la propriete universelle.
Observons que $f : L(b) \to d, g : L(c) \to d$ donnent $f^{\#} : b \to R(d)$ et $g^{\#} : c \to R(d)$.
Par la propriete universelle du produit, $\exists! k : b \amalg c \to R(d)$ tel que $k \circ i_2 = g^{\#}$ et $k \circ i_1 = f^{\#}$.
Le morphisme $k : b \amalg c \to R(d)$ correspond a $k^{\flat} : L(b \amalg c) \to d$.
On va montrer que $k^{\flat} \circ L(i_1) = f$ et que $k^{\flat} \circ L(i_2) = g$.

On a $k^\flat = \epsilon_d \circ L(k)$.
De meme, on a $L(f^\sharp) = L(k) \circ L(i_1)$.
Il suffit donc de montrer que $f = \epsilon_d \circ L(f^\sharp)$.
Cependant, $f^\sharp = R(f) \circ \eta_b$, donc $L(f^\sharp) = LR(f) \circ L(\eta_b)$.
Reste a voir que $k^\flat$ est l'unique morphisme faisant commuter ces triangles.
Supposons qu'il existe $l : L(b \amalg c) \to d$ faisant commuter le diagramme, montrons que $l = k^\flat$.
De maniere analogue, on trouve que $l^\sharp \circ i_1 = f^\sharp$ et $l^\sharp \circ i_2 = g$.
Par l'unicite de la propriete universelle du coproduit, on en deduit que $l^\sharp = k^\sharp \Rightarrow l = k$. □

Lecture 8: Groupes Quotients

Sat 23 Oct

2 Groupes Quotients

2.1 Quelques rappels de premiere annee

Soit G un groupe.

- Un sous groupe N de G est normal si $aba^{-1} \in N \forall a \in G, b \in N$, on notera ceci $N \trianglelefteq G$.
- Si $\phi : G \to H$ est un homomorphisme, alors le noyau de ϕ est un sous-groupe normal de G.
  ϕ est injectif si et seulement si $\ker \phi = \{e\}$
- Si $H < G$, on pose $G/H = \{aH | a \in H\}$. De plus on a
  $$aH \cap bH \neq \emptyset \Rightarrow aH = bH$$
  On a une application $q_H : G \to G/H : a \mapsto \overline{a}$
- Si $N \trianglelefteq G$, alors G/N admet une structure de groupe tel que l'application $q_N : G \to G/N$ soit un homomorphisme de groupe
- Soit $N \trianglelefteq G$ et soit $\phi : G \to H$. Si $N < \ker \phi$, il existe un unique homomorphisme $\hat{\phi} : G/N \to H$ tel que $\hat{\phi} \circ q_N = \phi$

2.2 Sens categorique des quotients de groupe

Soient deux homomorphismes de groupe de meme domaine $G_1 \xleftarrow{\phi}_1 G_0 \xrightarrow{\phi}_2 G_2$.
Existe-t'il un groupe G et des homomorphismes $G_1 \xrightarrow{\psi}_1 G \xleftarrow{\psi}_2 G_2$ tel que $\psi_2\phi_2 = \psi_1\phi_1$ et tel que, pour tout couple d'homomorphismes $G_1 \xrightarrow{\omega}_1 H \xleftarrow{\omega}_2 G_2$ tel que $\omega_2\phi_2 = \omega_1\phi_1$, il existe un unique homomorphisme $\omega : G \to H$ tel que $\omega\psi_1 = \omega_1$ et $\omega\psi_2 = \omega_2$.

Remarque
Lorsqu'il existe $G_1 \xrightarrow{\psi}_1 G \xleftarrow{\psi}_2 G_2$ *qui repondent aux criteres de la question, on dit que c'est un pushout de* ϕ_1 *et* ϕ_2.

Un pushout de $\{e\} \xrightarrow{G}_0 \xleftarrow{\phi}_1 G_1$ consiste en

1. un homomorphisme $\psi_1 : G_1 \to G$ tel que $\operatorname{Im}\phi_1 \subset \ker\psi_1$, tel que
2. $\forall$ homomorphisme $\omega_1 : G_1 \to H$ tel que $\operatorname{Im}\phi_1 \subset \ker\omega_1, \exists!\omega : G \to H$ tel que $\omega_1 = \omega \circ \psi_1$

Proposition 14
Soit $\phi : H \to G$ *un homomorphisme de groupe. Soit* $N \trianglelefteq G$ *le plus petit sous-groupe normal de* G *qui contient* $\operatorname{Im}\phi$. *Alors*

$$\{e\} \xrightarrow{i} G/N \xleftarrow{q}_{N_\phi} G$$

ou i *est l'unique homomorphisme du groupe trivial vers* G/N, *est le pushout de*

$$\{e\} \xleftarrow{\pi} H \xrightarrow{\phi} G$$

ou π *est l'unique homomorphisme de* H *vers le groupe trivial.*

Preuve
Il faut montrer que

$$\operatorname{Im}\phi \subset \ker q_N$$

et

$$\forall\psi : G \to G'$$

tel que $\operatorname{Im}\phi \subset \ker\psi$ $\exists!\hat{\psi} : G/N_\phi \to G'$ *tel que*

$$\hat{\psi} \circ q_N = \psi$$

On a

$$\ker q_N = N_\phi \supset \operatorname{Im}\phi$$

Soit $\psi : G \to G'$ *tel que* $\operatorname{Im}\phi \subset \ker\psi$.
On veut trouver un homomorphisme $\hat{\psi} : G/N \to G'$ *tel que* $\hat{\psi} \circ q_N = \psi$.
Or $N_\phi = \bigcap N$ *et* $\operatorname{Im}\phi \subset \ker\psi \trianglelefteq G$ *d'ou* $N \subset \ker\psi$.
Par la propriete universelle du quotient, $\exists!\hat{\psi}$ □

Lecture 9: Theoremes d'isomorphisme

Sat 30 Oct

Theorème 15 (Premier theoreme d'isomorphisme)
Si $\phi : G \to H$ est un homomorphisme de groupe, alors

$$G/\ker\phi \simeq \operatorname{Im}\phi$$

Preuve
Par corestriction de l'homomorphisme $\phi : G \to H$, on obtient un homomorphisme surjectif

$$\phi : G \to \operatorname{Im}\phi$$

Par la propriete universelle du quotient, il existe un unique $\hat{\phi} : {}^{G}\!/_{\ker\phi} \to \operatorname{Im}\phi$ tel que $\hat{\phi} \circ q_{\ker\phi} = \phi$.
Puisque ϕ est surjectif, $\hat{\phi}$ l'est aussi, car $\phi(a) = \hat{\phi}(\overline{a})$.
Pour montrer que $\hat{\phi}$ est injectif, on calcule

$$\ker\hat{\phi} = \left\{\overline{a} \in {}^{G}\!/_{\ker\phi} | \hat{\phi}(\overline{a}) = e\right\} = \{\overline{e}\}$$

□

Theorème 16 (Le deuxieme theoreme d'isomorphisme)
Pour tout $H < G$ et tout $N \trianglelefteq G$

1. $HN = \{ab | a \in H, b \in N\} < G$
2. $H \cap N \trianglelefteq H$; *et*
3. ${}^{H}\!/_{H \cap N} \simeq {}^{HN}\!/_{N}$

Preuve

1. *Pour montrer que HN est un sous-groupe de G, il faut montrer que $\forall ab, a'b' \in HN$,*

$$(ab)^{-1}(a'b') \in HN$$

Or $(ab)^{-1}a'b' = b^{-1}a^{-1}a'b'$; $\exists b" \in N$ tel que $b^{-1}a^{-1} = a^{-1}b"$, donc

$$= a^{-1}b"a'b' = a^{-1}a'b"'b'$$

2. *Soit $a \in H, b \in H \cap N$, on veut montrer que $aba^{-1} \in H \cap N$.*
Or $b \in H \cap N \Rightarrow aba^{-1} \in H$, de meme $b \in H\cap \Rightarrow aba^{-1} \in N$.
Donc $b \in H \cap N$.
3. *$N \trianglelefteq G \Rightarrow N \trianglelefteq HN$, donc $\exists$ un groupe ${}^{HN}\!/_{N}$.*
Considerons la composition

$$H \xrightarrow{\iota} HN \xrightarrow{q} {}^{HN}\!/_{N}$$

Montrons que $q \circ \iota$ surjectif, en effet $\forall ab \in HN$ $\overline{ab} = abN = aN = \overline{a}$.
Montrons que $\ker q \circ \iota = H \cap N$.

$$\ker(q \circ \iota) = \{a \in H | \overline{a} = \overline{e}\}$$

$$
\begin{aligned}
&= \{a \in H | aN = N\}\\
&= \{a \in H | a \in N\}\\
&= H \cap N
\end{aligned}
\qquad \square
$$

On conclut par le premier theoreme d'isomoprhisme.

Notation

Pour G un groupe,

— $\mathcal{S}(G) = \{H \leq G\}$

— $\mathcal{N}(G) = \{H \trianglelefteq N\}$

Theorème 17 (Troisieme theoreme d'isomorphisme)
Soient G un gorupe et $N \trianglelefteq G$. Alors

1. $\mathcal{S}(G/N) = \left\{H/N | H \in \mathcal{S}(G), N < H\right\}$
2. $\mathcal{N}(G/N) = \left\{K/N | K \in \mathcal{N}(G), N < K\right\}$
3. *Si $K \in \mathcal{N}(G)$ et $N < K$, alors* $G/K \simeq {}^{G/N}\!/_{K/N}$

Preuve

1. *Si $N < H < G$, alors $H/N < G/N$.*
   Donc $\left\{H/N | H \in \mathcal{S}(G), N < H\right\}$.
   Soit $\hat{H} < G/N$.
   Alors $q^{-1}(\hat{H}) < G$ est un ss-groupe.

   $$q^{-1}(\hat{H}) = \left\{a \in G | \overline{a} \in \hat{H}\right\}$$

   En particulier $N < q^{-1}(\hat{H})$ puisque $\forall a \in N, \overline{a} = \overline{e} \in \hat{H}$.
   De plus $q^{-1}(\hat{H})/N = \left\{\overline{a} | a \in q^{-1}(\hat{H})\right\} = \hat{H}$
2. *On sait que* $\mathcal{N}(G/N) = \left\{H/N | H \in \mathcal{S}(G), N < H, H/N \trianglelefteq G/N\right\}$.
   Or $H/N \trianglelefteq G/N \iff \forall \overline{a} \in G/N, \overline{b} \in H/N, \overline{a}\overline{b}\overline{a}^{-1}$.
   $\iff \forall \overline{a}\overline{b}, \overline{aba^{-1}} \in H/N \iff aba^{-1} \in H$
3. *Soit $N \trianglelefteq G, K \trianglelefteq G$ tel que $N \trianglelefteq K$.*
   Considerer $G/N \xleftarrow{q}_N G \xrightarrow{q}_K G/K$.
   Puisque $N < K = \ker q_K$, par la propriete universelle du quotient $\exists! \hat{q}$ tel que $\hat{q} \circ q_N = q_K$
   Observons que $\hat{q}$ est surjectif.
   Ensuite calculons $\ker \hat{q}$

   $$\ker \hat{q} = \{aN | \hat{q}(aN) = eK\}$$

$$= \{aN | aK = eK\}$$
$$= {}^{K}\!/_{N}$$ □

On conclut par le premiet theoreme d'isomorphisme

3 Groupes Resolubles

Definition 10 (Groupe resoluble)
Un groupe G est resoluble s'il existe une suite finie de sous-groupes

$$\{e\} = G_r < G_{r-1} < \ldots < G_0 = G$$

tel que
- $G_k \trianglelefteq G_{k-1}$
- ${}^{G_{k-1}}\!/_{G_k}$ *est abelien*

pour tout k.

Remarque
Si G est abelien, alors G est resoluble, car on peut prendre $\{e\} < G$

Remarque
La decomposition n'est pas unique.

Lemme 20
Soient G un groupe et $N \trianglelefteq G$. Alors

$$ {}^{G}\!/_{N} \text{ abelien } \iff \left\{aba^{-1}b^{-1} | a, b \in G\right\} \subset N$$

Preuve
En exercice. □

Proposition 21
Soient G un groupe et $N \trianglelefteq G$. Si N et ${}^{G}\!/_{N}$ sont resolubles, alors G l'est egalement.

Preuve
Si $N, {}^{G}\!/_{N}$ sont resolubles, alors $\exists$ suites de sous-groupes.
Soit N_i la suite resolvant N et K_i la suite resolvant ${}^{G}\!/_{N}$.
$\exists H_i < G$ tel que $q(H_i) = K_i$.
De plus, puisque $K_i \trianglelefteq K_{i-1}$, on sait egalement que $H_i \trianglelefteq H_{i-1}$, par le troisieme theoreme d'isomorphisme.
Donc on a suite de sous-groupes de G

$$q^{-1}(K_s) = H_s \trianglelefteq H_{s-1} \trianglelefteq \ldots \trianglelefteq H_1 \trianglelefteq G_0 = G$$ □

Lecture 10: Introduction aux actions de groupe

Sun 31 Oct

4 Actions de groupe

Definition 11 (Action de groupe)
Une action de groupe G sur l'ensemble X consiste en un homomorphisme de groupe

$$\phi : G \to \operatorname{Aut} X$$

De maniere equivalente, une action de G sur X consiste en une application

$$\phi^\flat : G \times X \to X$$

tel que

$$\phi^\flat(a \cdot b, x) = \phi^\flat(a, \phi^\flat(b, x)) \text{ et } \phi^\flat(e, x) = x \forall a, b \in G, x \in X$$

Definition 12 (Points fixes)
L'ensemble des points fixes par a , note X^a est le sous-ensemble de X defini par

$$X^a = \{x \in X | ax = x\}$$

L'ensemble des points fixes de l'action ϕ, note $(X, \phi)^G$ ou simplement X^G est le sous-ensemble de X defini par

$$X^G = \{x \in X | ax = x \forall a \in G\} = \bigcap_{a \in G} X^a$$

Definition 13 (Orbite)
Soit $\phi : G \to \operatorname{Aut} X$ une action de groupe. Soit $x \in X$

1. *L'orbite de x, note O_x est le sous-ensemble de X defini par*

$$O_x = \{ax | a \in G\}$$

2. *L'ensemble des orbites de l'action est*

$$(X, \phi)_G = \{O_x | x \in X\}$$

que l'on note souvent simplement X_G.

3. *Le stabilisateur de x, note G_x est le sous-groupe de G defini par*

$$G_x = \{a \in G | ax = x\}$$

— Soient $x, x' \in X$, si $O_x \cap O_{x'} \neq \emptyset$, alors $O_x = O_{x'}$.
Donc on peut decomposer X en une reunion disjointe d'orbites, $\exists \overline{X} \subset X$ tel que

$$X = \bigcup_{x \in \overline{X}} O_x$$

— $\forall x \in X \exists$ bijection

$$G/G_x \to O_x : \overline{a} \mapsto a \cdot x$$

— Equation de classe Soit $\phi : G \to \operatorname{Aut} X$ une action de groupe. La bijection du point precedent donne une equation de clsse

$$\#X < \infty \Rightarrow \# = \sum_{x \in \overline{X}} (G : G_x)$$

— Soit $\phi : G \to \operatorname{Aut} X$ une action de groupe, le lemme de Burnside exprime la relation entre orbites et ensembles de points fixes

$$X = \bigcup_{x \in \overline{X}} O_x \Rightarrow \#\overline{X} = \frac{1}{\#G} \sum_{a \in G} \#X^a$$

Lecture 11: Perspectiuve categorique sur les actions de groupe

Sat 06 Nov

4.1 Un cadre categorique pour les actions de groupe

Pour generaliser la notion d'action de groupe a d'autres categories que Ens, quelle definition doit-on essayer de generaliser ?

Definition 14
Soit C une categorie, et soit $c \in \operatorname{Ob} C$. Soit G un groupe. Une action de G sur c consiste en un homomorphisme de groupe

$$\phi : G \to \operatorname{Aut} c$$

Un objet de C muni d'une action de G est un $G-$objet de C.

$\phi : G \to \operatorname{Aut} c$ homomorphisme $\iff$ $\forall a \in G, \phi(a) : c \simeq c$ et $\forall a, b \in G$ $\phi(ab) = \phi(a) \circ \phi(b)$.
Un tel couple, $(c, \phi : G \to \operatorname{Aut} c)$ est un G-objet de C.
On peut decortiquer encore plus lorsque C est concrete

Remarque
Si C est une categorie concrete, $\exists$ foncteur oubli $U : C \to$ Ens.
Si (c, ϕ) est un G-objet de C, alors on a $\phi : G \to \operatorname{Aut} c$.
Appliquons U a la famille des $\phi(a)$

$$U(\phi(a)) : U(c) \xrightarrow{\simeq} U(c)$$

On a alors une action de G sur l'ensemble $U(c)$.
Donc une action de G sur $c \in \operatorname{Ob} C$ consiste en une action de G sur $U(c)$ qui respect la structure supplementaire.

Exemple
Si $V \in \mathrm{Vect}_{\mathbb{K}}$, alors $\operatorname{Aut} V = GL(V)$ le groupe general lineaire de V, ie., le groupe de tous les isomorphismes lineaires de V.

Un G-ev est donc un espace vectoriel muni d'un homomorphisme $\phi : G \to GL(V)$

Comment definir de maniere raisonnable un morphisme entre G-objets dans une categorie C ?
Pour repondre a cette question, on formule la definition d'une action de groupe d'une autre maniere, encore plus categorique.

Lemme 24
Soient C une categorie et G un groupe. Pour tout $c \in \operatorname{Ob} C$, il y a une bijection
$$\operatorname{Gr}(G, \operatorname{Aut} c) \simeq \{F \in \operatorname{Ob} \operatorname{Fun}(BG, C) | F(\star) = c\}$$

Preuve
$\alpha : \operatorname{Gr}(G, \operatorname{Aut} c) \to \{F : BG \to C | F(\star) = c\}$ *Defini comme :*
Etant donne $\phi : G \to \operatorname{Aut} c$ un homomorphisme, on definit $\alpha(\phi)$ comme etant le foncteur
$$\alpha(\phi) : BG \to C$$
precise par
$$\alpha(\phi)(\star) = c$$
$$\alpha(\phi)(a) = \phi(a) : c \simeq c \forall a \in \operatorname{Mor} BG = G$$
$\alpha(\phi)$ est trivialement un foncteur.

On definit l'inverse a α comme
$$\beta(F) : G \to \operatorname{Aut} c$$
est l'application definie par $\beta(F)(a) = F(a) : c \to c$.
On verifie que $\beta(F)(a)$ est un isomorphisme, de plus $\beta(F)$ est un homomorphisme. On montre facilement que $\beta \circ \alpha$ et $\alpha \circ \beta$ sont des identites. □

Definition 15
Soient C une categorie et G un groupe, la categorie $\operatorname{Fun}(BG, C)$ est appelee la categorie des G-objets dans C. Les morphismes dans $\operatorname{Fun}(BG, C)$, sont appeles G-equivariants.

Un morphisme $G-$equivariant est une transformation naturelle $\tau : F \to F'$ ou $F, F' : BG \to C$, ie. une application $\tau : G = \operatorname{Ob} BG \to \operatorname{Mor} C$ telle que pour tout $a \in G$
$$F'(a) \circ \tau_* = \tau_* \circ F(a)$$

Grace au lemme ci-dessus, si $(c, \phi), (c', \phi')$ des G-objets de C, donc $\phi : G \to \operatorname{Aut} c, \phi' : G \to \operatorname{Aut}(c')$ un morphisme $G-$equivariant de (c, ϕ) vers (c', ϕ') consiste en

— un morphisme $f \in C(c, c')$ tel que

$$\phi'(a) \circ f = f \circ \phi(a) \forall a \in G$$

4.2 Generalisation et formalisation du cas $C = \mathrm{Ens}$

Soit C une categorie. Soit G un groupe.
Le foncteur d'action triviale de G est

$$\mathrm{Triv}_G : C \to {}_G C$$

est defini par :

$$triv_G(c) = (c, cst_{\mathrm{Id}})$$

et $\forall f \in C(c, c'), triv_G(f) = f$
Motive par l'analyse du cas $C = \mathrm{Ens}$, on pose

— le foncteur orbite est l'adjoint a gauche de Triv_G, s'il existe

$$(-)_G : {}_G C \to C$$

— Le foncteur point fixe est l'adjoint a droite de Triv_G, s'il existe

$$(-)^G : {}_G C \to C$$

Si $(-)_G$ existe, alors $\exists$ un isomomorphisme naturel

$${}_G C((c, \phi), \mathrm{Triv}_G(c')) \simeq C((c, \phi)_G, c')$$

De meme, si $(-)^G : {}_G C \to C$ existe, alors $\exists$ isomorphisme naturel

$${}_G C(\mathrm{Triv}_G(c'), (c, \phi)) \simeq C(c', (c, \phi)^G)$$

4.3 Creation d'actions libres

$\exists$ adjonction $L : \mathrm{Ens} \dashv \mathrm{Vect}_{\mathbb{K}} : U$.
Il existe egalement un foncteur oublie $U : {}_G C \to C$ $\forall C$ categorie, G groupe, defini par $U(c, \phi) = c$, existe-il un adjoint a gauche de ce foncteur oubli ?
Ie,

$$C(c, U(c', \phi')) \simeq {}_G C(L(c), (c', \phi'))$$

Definition 16 (Action libre)
Soient G un groupe et C une categorie.

— *Le foncteur de G-action libre, note* $\mathrm{Free_G} : C \to {}_{\mathrm{G}}\mathrm{C}$ *est l'adjoint a gauche du foncteur oubli $U : {}_{\mathrm{G}}\mathrm{C} \to C$ lorsqu'il existe.*

Alors, si l'adjoint a gauche de U existe, on aura $\forall c \in \mathrm{Ob}\, C, (c', \phi') \in \mathrm{Ob}\, {}_{\mathrm{G}}\mathrm{C}$

$${}_{\mathrm{G}}\mathrm{C}(\mathrm{Free_G}(cv), (c', \phi')) \simeq C(c, c')$$

4.3.1 Le foncteur $\mathrm{Free_G} : \mathrm{Ens} \to {}_G\,\mathrm{Ens}$

Soit $\mu : G \times G \to G$ la multiplication de G,

Remarque
G est lui meme un G-ensemble, quand on le munite de l'action de translation.

$\forall X \in \mathrm{Ob}\,\mathrm{Ens}$, on pose

$$\mathrm{Free_G}(x) = (G \times X, \phi_X)$$

on on definit

$$\phi_X : G \to \mathrm{Aut}(G \times X) : a \mapsto ((b, x) \mapsto (ab, x))$$

Donc $\mathrm{Free}_G(x) \in \mathrm{Ob}\,{}_G\,\mathrm{Ens}$

Sur les morphismes, on definit

$$\mathrm{Free_G}(f) = \mathrm{Id}_G \times f$$

Lecture 12: Orbites et poiints fixes categoriques

Sat 13 Nov

Lecture 13: Groupes Abeliens

Fri 19 Nov

5 Groupes Abeliens

5.1 Constructions categoriques dans Ab

Comment distinguer les groupes abeliens parmis tous les groupes ?

Lemme 26
Un groupe G est abelien si et seulement si sa multiplication $\mu : G \times G \to G$ est un homomorphisme

Preuve
$\mu : G \times G \to G : (a, b) \mapsto ab.$
Alors μ un homomorphisme de groupe $\iff \forall a, b, a', b' \in G$

$$\mu((a, b) \times (a', b')) = \mu(a, b) \times \mu(a', b')$$

Donc

$$\mu((aa', bb')) = aba'b' = aa'bb' = aba'b' \forall a, b, a', b' \in G$$

Ce qui est equivalent a demandenr que

$$a'b = ba' \forall a', b \in G \qquad \square$$

G est abelien.

5.2 Sommes directes

Comment construire des coproduits dans Ab ?

Lemme 27
Pour tout couple de groupes abeliens A et B,

$$A \xrightarrow{i}_1 A \times B \xleftarrow{i}_2 B$$

ou $i_1(a) = (a, 0)$ et $i_2(b) = (0, b)$ pour tout $a \in A$ et tout $b \in B$ est un coproduit dans Ab.

Preuve
Il suffit de verifier la propriete universelle.
Soient $f \in \mathrm{Ab}(A, C), g \in \mathrm{Ab}(B, C)$, Comment definir $h \in \mathrm{Ab}(A \times B, C)$ tel que $hi_1 = f, hi_2 = g$.
Observer que $hi_1 = f \iff h(a, 0) = f(a) \forall a \in A$ et $hi_2 = g \iff h(0, b) = g(b) \forall b \in B$.
Cependant,

$$h(a, b) = h(a, 0) + h(0, b) = f(a) + g(b)$$ □

Definissons donc $h(a, b) = f(a) + g(b)$

Pour distinguer les deux roles categoriques de $A \times B$ au lieu du produit, on le note $A \oplus B$ et on l'appelle la somme directe et on ecrira les elements comme une somme formelle $a + b \in A \oplus B$.
Quelle est la relation entre la notion de $\oplus$ ci-dessus et celle de $\oplus$ de 2 sous-groupes d'un groupe abelien ?
Parfois on considere la somme directe comme une operation interne a l'ensemble des sous-groupes d'un groupe abelien. Si B et C sont des sous-groupes de A, leur somme, notee $B+C$ est un sous-groupe de A.
Traduisons la propriete universelle de la somme directe de groupes abeliens

Remarque
Selon la propriete universelle du coproduit

$$\forall f \in \mathrm{Ab}(A, C), \in \mathrm{Ab}(B, C), \exists! h \in \mathrm{Ab}(A \oplus B, C)$$

tel que

$$\mathrm{Ab}(A \oplus B, C) \to \mathrm{Ab}(A, C) \times \mathrm{Ab}(B, C) : h \mapsto (h \circ i_1, h \circ i_2)$$

est une bijection.
Ainsi l'existence de α ne depend que de l'existence de i_1 et i_2.
De plus, la propriete universelle de $A \oplus B$ nous donne un inverse a α

$$\beta(f, g) = f + g$$

Definition 17 (Produit quelconque d'ensembles)
Soit X un ensemble et soit $\{Y_x|x \in X\} \subset \operatorname{Ob}\operatorname{Ens}$ Le produit des Y_x note $\prod_X Y_x$ est l'ensemble

$$\left\{\omega \in \operatorname{Ens}(X, \bigcup Y_x)|\omega(x) \in Y_x \forall x \in X\right\}$$

Ceci se generalise naturellement aux groupes

Definition 18 (Produit quelconque de groupes)
Soit $\{G_x|x \in X\} \subset \operatorname{Ob}\operatorname{Gr}$. Le produit des G_x, note $\prod G_x$ est le groupe dont le sous-ensemble sous-jacent est

$$\left\{\omega \in \operatorname{Ens}(X, \bigcup G_x)|\omega(x) \in G_x \forall x \in X\right\}$$

muni de la mulitplication definie par

$$(\omega \cdot \omega')(x) = \omega(x) \cdot \omega'(x)$$

Notons que ici, les projections selon les coordonnees sont en particulier des homomorphismes.

Remarque
Le produit d'une famille quelconque d'ensembles ou de groupes verifie une propriete universelle qui generalise celle de la definition du produit de deux objets, notamment Dans $\operatorname{Gr} : \forall \{f_{x'} \in \operatorname{Gr}(H, G_{x'})|x' \in X\}$,

$$\exists! f \in \operatorname{Gr}(H, \prod G_x)$$

tel que $p_{x'} \circ f = f_{x'} \forall x'$

Generalisons la notion de somme directe aux familles quelconques de groupes abeliens.

Definition 19 (Somme directe quelconque)
Soit X un ensemble, et soit $\{A_x|x \in X\} \subset \operatorname{Ob}\operatorname{Ab}$. Une somme directe des groupes abeliens A_x consiste en un groupe abelien B muni d'homomorphismes $i_x : A_x \to B$ pour tout $x \in X$ tel que l'application

$$\operatorname{Ab}(B, C) \to \prod_{x \in X} \operatorname{Ab}(A_x, C) : h \to (h \circ i_x)_{x \in X}$$

Proposition 30
Soit X un ensemble, et soit $\{A_x|x \in X\} \subset \operatorname{Ob}\operatorname{Ab}$. La somme directe des A_x existe et est unique a isomorphisme pres.

Preuve
Posons $B = \left\{\omega \in \prod_{x \in X} A_x | \# \{x \in X|\omega(x) \neq 0\} < \infty\right\}$ et $\iota_x : A_{x'} \to B : a \mapsto \iota_{x'}(a)$ ou

$$\iota_{x'}(a) : X \to \bigcup_{x \in X} A_x : x \mapsto \begin{cases} a : x = x' \\ 0 : x \neq x' \end{cases}$$

On veut definir un inverse a $\alpha : \mathrm{Ab}(B,C) \to \prod_{x\in X} \mathrm{Ab}(A_x, C)$.
On definit $\beta : \prod_{x\in X} \mathrm{Ab}(A_x, C) \to \mathrm{Ab}(B,C)$ *par*

$$\beta((f_x)_{x\in X}) = f$$

ou $f : B \to C : \omega \mapsto \sum_{x\in X} f_X(\omega(x))$ f *est un homomorphisme, car :*

$$f(\omega+\omega') = \sum_{x\in X} f_x((\omega+\omega')(x)) = \sum_{x\in X} f_x(\omega(x)) + \sum_{x\in X} f_x(\omega'(x)) = f(\omega)+f(\omega')$$

Il reste a voir que c'est bien un inverse

$$\prod_{x\in X} \mathrm{Ab}(A_x, C) \xrightarrow{\beta} \mathrm{Ab}(B,C)$$

$$(f_x)_{x\in X} \mapsto f \mapsto (f \circ \iota_x)_{x\in X}$$

Donc

$$\forall a \in A_{x'} : f \circ \iota_{x'}(a) = \sum_{x\in X} f_x(\iota_{x'}(a)(x)) = f_{x'}(a)$$

On veut montrer que $\beta\alpha = \mathrm{Id}$

$$\mathrm{Ab}(B,C) \xrightarrow{\Pi}_{x\in X} \mathrm{Ab}(A_x, C) \xrightarrow{\mathrm{Ab}} (B,C)$$

On a donc

$$\beta((f\circ\iota_x)_{x\in X})(\omega) = \sum_{x\in X} f\circ\iota_x(\omega(x))$$

$\square$

Lecture 14: Groupes Abeliens libres

Fri 26 Nov

Lemme 31
Soit X *un ensemble, et soit* $\{A_x | x \in X\} \subset \mathrm{Ob}\,\mathrm{Ab}$. *Alors*

$$\#X < \infty \iff \bigoplus_{x\in X} A_x \simeq \prod_{x\in X} A_x$$

Preuve
$\forall X, \bigoplus A_x < \prod_{x\in X} A_x$, *de plus par definition*

$$\bigoplus A_x = \left\{\omega : X \to \bigcup A_x | \omega(x) \neq 0 \text{ pour un nombre fini d'elements}\right\}$$

$\square$

On a donc egalite.

Notation utile pour sommes directes :

$$\omega \in \bigoplus A_x,\ \text{on note } \sum_{x\in X} \omega(x)\cdot x$$

Ou on a a droite une somme finie d'elements

Definition 20 (Groupes abeliens libre)
Soit X un ensemble. La somme directe $\bigoplus_{x\in X}\mathbb{Z}$ est le groupe abelien libre de base X, note $F_{\mathrm{Ab}}(X)$

Theorème 32 (Foncteur libre)
La definition du groupe abelien libre s'etend en un foncteur $F_{\mathrm{Ab}} : \mathrm{Ens} \to \mathrm{Ab}$, qui est adjoint a gauche du foncteur oublie $U : \mathrm{Ab} \to \mathrm{Ens}$

Preuve
Il reste a definir F_{Ab} sur les morphismes.
Soit $f \in \mathrm{Ens}(X, Y)$, alors

$$F_{\mathrm{Ab}}(f) : F_{\mathrm{Ab}}(X) \to F_{\mathrm{Ab}}(Y) : \sum_{x\in X} n_x \cdot x \to \sum_{y\in Y}(\sum_{x\in f^{-1}(y)} n_x)y$$

La preuve que $F_{\mathrm{Ab}}(g \circ f) = F_{\mathrm{Ab}}(g) \circ F_{\mathrm{Ab}}(f)$ ressemble a celle donnee dans le cas du foncteur $\mathcal{L} : \mathrm{Ens} \to \mathrm{Vect}_{\mathbb{K}}$.
Montrons donc que F_{Ab} est l'adjoint a gauche de U.
Etablissons la bijection naturelle $\mathrm{Ab}(F_{\mathrm{Ab}}(X), A) \to \mathrm{Ens}(X, UA)$.
On definit

$$\alpha(\phi) = U(\phi) \circ \eta_X$$

On definit de plus $\forall f : X \to UAl$

$$\beta(f) : F_{\mathrm{Ab}}(X) \to A : \sum_{x\in X} n_x x \mapsto \sum_{x\in X} n_x f(x)$$ □

5.3 Le foncteur hom

Lemme 33
Il y a un foncteur $\mathrm{hom} : \mathrm{Ab}^{op} \times \mathrm{Ab} \to \mathrm{Ab}$ specifie sur les objets par

$$\mathrm{hom}(A, B) = \mathrm{Ab}(A, B)$$

muni de l'addition definie composante par composante pour tout $a \in A$,

Preuve
L'addition $f + g$ est bien un homomorphisme et clairement $f + g = g + f$.
Il faut maintenant montrer que

$$\mathrm{hom}(f^{op}, g) : \mathrm{hom}(A', B) \to \mathrm{hom}(A, B')$$

On a en effet $\forall h, k \in \mathrm{hom}(A', B)$, on a

$$\mathrm{hom}(f^{op}, g)(h + l) = g \circ (h + k) \circ f = g \circ h \circ f + g \circ k \circ f$$ □

On en deduit que hom *est bien un foncteur.*

Proposition 34
Soit X un ensemble, et soit $\{A_x | x \in X\} \subset \mathrm{Ob}\,\mathrm{Ab}$. Pour tout groupe abelien B, il y a un isomorphisme de groupes abeliens

$$\hom(\bigoplus A_x, B) \simeq \prod_{x \in X} \hom(A_x, B)$$

Preuve
On sait deja qu'il y a une bijection

$$\alpha : \mathrm{Ab}(\bigoplus A_x, B) \to \prod_{x \in X} \mathrm{Ab}(A_x, B)$$

Il suffit donc de montrer que α est un homomorphisme.
On a en effet

$$\alpha(h) = (h \circ \iota_x)_{x \in X}$$

Soient $h, k \in \mathrm{Ab}(\bigoplus A_x, B)$.
Alors $\alpha(h+k) = ((h+k) \circ \iota_x) = \alpha(h) + \alpha(k)$ □

5.4 Suites Exactes

Une suite d'homomorphismes de groupe abelien

$$\dots \xrightarrow{\phi_{n+2}} A_{n+1} \xrightarrow{\phi_{n+1}} A_n \xrightarrow{\phi(n)} A_{n-1} \dots$$

est exacte si $\mathrm{Im}\,\phi_{n+1} = \ker \phi_n$ pour tout n.
Une courte suite exacte dans Ab est une suite exacte d'homomorphismes de groupe abeliens dont seulement au plus trois groups, consecutifs, sont non-triviaux. On ecrit une telle suite

$$0 \to A \xrightarrow{\iota} B \xrightarrow{\pi} C \longrightarrow 0$$

Exemple
Pour tout couple de groupes abeliens A et B, il y a une suite exacte

$$0 \to A \xrightarrow{\iota} A \oplus B \xrightarrow{\pi} B \to 0$$

Definition 21 (Suite exacte scindee)
Une suite exacte $0 \to A \xrightarrow{\iota} B \xrightarrow{\pi} C \to 0$ dans Ab est scindee s'il existe $\sigma \in \mathrm{Ab}(C, B)$ tel que $\pi \circ \sigma = \mathrm{Id}$. On dit alors que σ est une section de π.

Lemme 36
Une courte suite exacte est scindee si et seulement si il existe une retraction de l'homomorphisme, ie. il existe $\rho \in \mathrm{Ab}(B, A)$ tel que $\rho \circ \iota = \mathrm{Id}$

Preuve

$\exists\sigma \implies \exists\rho$

Considerer $q : B \to B/\ker\pi$ *et* $\hat{\pi} : B/\ker\pi \to C$.

Observer que

$$\hat{\pi}q\sigma\hat{\pi} = \pi\sigma\hat{\pi} = \hat{\pi}$$

Donc

$$q\sigma\hat{\pi} = \hat{\pi}^{-1}\hat{\pi}q\sigma\hat{\pi} = \mathrm{Id}$$

Par consequent $\forall b \in B$

$$q(b - \sigma\hat{\pi}q(b)) = q(b) - q\sigma\hat{\pi}q(b) = q(b) - q(b) = 0$$

Donc $b - \sigma\hat{\pi}q(b) \in \ker\pi = \operatorname{Im}\iota$.

Ce qui nous permet de definir

$$\rho(b) = \text{ l'unique } a \in A \text{ tel que } \iota = b - \sigma\hat{\pi}q(b)$$

Alors ρ *est un homomorphisme, alors*

$$\iota(a) = b - \sigma\hat{\pi}q(b), \iota(a') = b' - \sigma\hat{\pi}q(b')$$

Alors $\iota(a + a') = b + b' - \sigma\hat{\pi}q(b + b')$.

Et finalement

$$\rho\iota(a) = a$$

car

$$\iota(a) - \sigma\hat{\pi}q\iota(a) = \iota(a)$$

Demontrons maintenant que l'existence de ρ *implique l'existence de* σ.

Pour tout $c \in C$, *choisir* $b_c \in B$ *tel que* $\pi(b_c) = c$.

Normalement, il n'y a aucune raison que $b_{c+c'} = b_c + b_{c'}$, *ie., ces choix de pre-image des elements de* C *ne nous donnent pas un homomorphisme de* C *vers* B.

Modifions ces choix de la maniere suivante pour obtenir un homomorphisme :

Definir $\sigma : C \to B$ *par* $\sigma(c) = b_c - \iota\rho(b_c)$.

Il nous faut voir que $\pi\sigma(c) = c \forall c \in C$.

$$\begin{aligned}\pi\sigma(c) &= \pi(b_c - \iota\rho(b_c)) \\ &= c - \pi\iota\rho(b_c) = c\end{aligned}$$

Si $\pi(b) = c = \pi(b')$, *alors on a* $b - b' \in \ker\pi = \operatorname{Im}\iota$.

Donc il existe un unique $a \in A$ *tel que* $b - b' = \iota(a)$ *d'ou*

$$(b - \iota\rho(b)) - b' - \iota\rho(b) = \iota(a) - \iota\rho\iota(a) = a$$

Montrons finalement que σ est un homomorphisme.
En effet, puisque si $\pi(b) = c$ et $\pi(b') = c'$, alors

$$\pi(b + b') = c + c'$$

donc

$$\sigma(c + c') = (b + b') - \iota\rho(b + b') = b - \iota\rho(b) + b' - \iota\rho(b') = \sigma(b) + \sigma(b') \qquad \square$$

Lecture 15: Lemme des cinqs

Sat 04 Dec

Remarque
$\operatorname{Im}\sigma \leq \ker\rho$ *par construction*

$$\rho(\underbrace{b - \iota\rho(b)}_{\sigma(b)}) = \rho(b) - \rho(b) = 0$$

Par consequent, puisque $b - \sigma\pi(b) \in \ker\pi = \operatorname{Im}\iota$ et donc $\exists! a \in A$ tel que $\iota(a) = b - \sigma\pi(b)$ on a que

$$\rho(b - \sigma\pi(b)) = \rho(b) - \rho\sigma\pi(b) = \rho(b)$$

Et

$$a = \rho\iota(a)$$

d'ou $\iota\rho(b) = b - \sigma\pi(b)$ autrement dit, si la suite $0 \to A \to B \to C \to 0$ est scindee avec section σ et retraction ρ, alors $b = \iota\rho(b) + \sigma\pi(b) \forall b \in B$

Remarque
Si la suite $0 \to A \to B \to C \to 0$ est scindee, avec section σ et retraction ρ, alors il y a des isomorphismes mutuellement inverses

$$A \oplus C \to B : a + c \to \iota(a) + \sigma(c) \text{ et } B \to A \oplus C : b \to \rho(b) + \pi(b)$$

On a

$$\alpha\beta(b) = \alpha(\rho(b) + \pi(b)) = \iota\rho(b) + \sigma\pi(b) = b$$

De meme

$$\beta\alpha(a+c) = \beta(\iota(a)+\sigma(c)) = \rho(\iota(a)+\sigma(c))+\pi(\iota(a)+\sigma(c)) = \rho\iota(a)+\rho(\sigma(c))+\pi\iota(a)+\pi\sigma(c) = a+c$$

Proposition 39 (Lemme des Cinq)
Soit

$$\begin{tikzcd} 0 \arrow[r] & A \arrow[r, "\iota"] \arrow[d, "\phi"'] & B \arrow[r, "\pi"] \arrow[d, "\psi"'] & C \arrow[r] \arrow[d, "\omega"'] & 0 \\ 0 \arrow[r] & A' \arrow[r, "\iota'"] & B' \arrow[r, "\pi'"] & C' \arrow[r] & 0 \end{tikzcd}$$

un diagramme commutatif dans Ab, *ou les deux suites horizontales sont exacts. Si ϕ et ω sont des isomorphismes, alors ψ est aussi un isomor-*

phisme.

Preuve
Puisque ψ est un homomorphisme, il suffit de voir que ψ est bijectif.

— *ψ est surjectif.*
  Soit $b' \in B'$, $\exists! c \in C$ tel que $\omega(c) = \pi'(b')$.
  Puisque π est surjectif, $\exists b \in B$ tel que $\pi(b) = c$.
  Si $\psi(b) = b'$, on a fini. En general, $\psi(b) \neq b'$, mais on peut le "corriger" pour obtenir une pre-image de b.
  Observer que
  $$\pi'\psi(b) = \omega\pi(b) = \pi'(b')$$
  D'ou $b' - \psi(b) \in \ker \pi' = \operatorname{Im} \iota'$.
  Donc $\exists! a' \in A'$ tel que $\iota'(a') = b' - \psi(b)$.
  Puisque $\phi : A \to A'$ est un iso, $\exists! a \in A$ tel que $\phi(a) = a'$.
  Alors $b + \iota(a) \in \psi^{-1}(b')$, car
  $$\psi(b + \iota(a)) = \psi(b) + \psi\iota(a) = \psi(b) + \iota'\phi(a) = \psi(b) + b' - \psi(b) = b'$$

— *ψ est injectif.*
  Soit $b \in B$, si $\psi(b) = 0$, alors
  $$\omega\pi(b) = \pi'\psi(b) = 0$$
  Puisque ω est un iso, cela implique que $\pi(b) = 0$, ie. que $b \in \ker \pi = \operatorname{Im} \iota$.
  Donc $\exists! a \in A$ tel que $b = \iota(a)$.
  Par consequent,
  $$0 = \psi(b) = \psi\iota(a) = \iota'\phi(a),$$
  d'ou $\phi(a) = 0$ car ι' injectif et donc $a = 0$ car ϕ injectif.
  On en deduit que $b = \iota(a) = 0$ □

5.5 Torsion et divisibilite

Soit $(A, +, 0)$ un groupe abelien.
But : Distinguer des sous-groupes importants d'un groupe abelien qui nous aident a comprendre sa structure.

Definition 22
Soit $a \in A$. L'element a est un element de torsion s'il existe $n \in \mathbb{N}$ tel que $na = 0$.
Si a est un element de torsion, alors l'ordre de a est
$$o(a) = \min\{n | na = 0\}$$

Definition 23 (Elements de torsion)
On pose

$$T(A) = \{a \in A | a \textit{ element de torsion } \}$$

et pour $n \in \mathbb{N}$

$$T_n(A) = \{a \in A | na = 0\}$$

Observer que $T(A) = \bigcup T_n(A)$

Lemme 40
$T_n(A)$ *et* $T(A)$ *sont des sous-groupes.*

Definition 24
Soit p un premier. On pose

$$A(p) = \bigcup_{k \in \mathbb{N}} T_{p^k}(A) = \left\{a \in A | \exists k \textit{ tel que } p^k a = 0\right\}$$

et on l'appelle le sous-groupe de p-torsion de A.

Definition 25
Soit p un premier. Un groupe abelien A est p-divisible si pour tout $a \in A$*, il exists* $b \in A$ *tel que* $pb = a$*. Il est divisible s'il est p-divisible pour tout premier p.*

5.6 La structure des p-groupes abelien

Restricition a une classe speciale de groupes abeliens, ce qui nous permet d'en faire une analyse plus fine de leur structure.

Definition 26
Un groupe abelien A est un p-groupe abelien s'il existe $k \in \mathbb{N}$ *tel que* $|A| = p^k$.

Remarque
Si A est un p-groupe abelien, alors $A = A(p)$ *puisque* $o(a) || A | \forall a \in A$.
Si A est un p-groupe abelien et $B < A$*, alors* ${}^{A}\!/_{B}$ *est aussi un p-groupe abelien.*

Lemme 42
Si $|A(p)| < \infty$*, alors* $A(p) = T_{p^N}(A)$ *ou*

$$N = \max\left\{k | \exists a \in A(p) \textit{ tel que } o(a) = p^k\right\}$$

Si $|A(p)| < \infty$*, alors* $A(p)$ *est un p-groupe abelien.*

Preuve
Le premier point est evident.
Par recurrence sur $|A(p)|$.

Si $|A(p)| = 1$, *alors* $A(p) = 0$.
Si vrai $\forall |A(p)| < N$, *supposons que* $|A(p)| = N$. *Alors* $\exists a \in A(p) \setminus \{0\}$.
Par le premier theoreme d'isomorphisme, on a

$$A(p)\diagup_{\langle a\rangle} \simeq (A\diagup_{\langle a\rangle})(p)$$

Par l'hypothese de recurrence, $\exists k$ *tel que*

$$|(A\diagup_{\langle a\rangle}(p))| = p^k$$

Par consequent

$$|A(p)| = |(A\diagup_{\langle a\rangle})||\langle a\rangle| = p^{k+o(a)}$$

□

Lemme 43
Soit A *un* p*-groupe abelien et soit* $b \in A \setminus \{0\}$. *S'il existe un entier positif* k *tel que* $p^k b \neq 0$ *et* $o(p^k b) = p^m$, *alors* $o(b) = p^{k+m}$

Lemme 44
Soit A *un* p*-groupe abelien, et soit* $a \in A$ *tel que* $o(a)$ *soit maximal. Pour tout* $\bar{b} \in A\diagup_{\langle a\rangle}$, *il existe* $b \in \bar{b}$ *tel que* $o(b) = o(\bar{b})$.

Preuve
Soit $q : A \to A\diagup_{\langle a\rangle}$ *l'homomorphisme quotient.*
Observer que si $b \in A$ *et* $p^k b = 0$, *alors* $p^k \bar{b} = 0$, *d'ou*

$$o(\bar{b}) \leq o(b)$$

On veut donc montrer que $\forall b \in A \exists b' \in A$ *tel que* $\bar{b} = \overline{b'}$ *et*

$$o(b') = o(\bar{b})$$

Poser $p^s = o(a)$ *et* $p^r = o(\bar{b})$ *d'ou* $p^r \bar{b} = 0$.
Si $p^r b = 0$, *on en deduit que* $o(b) = p^r$ *et on a fini.*
Si $p^r b \neq 0$, *on doit trouver* $b' \in A$ *tel que* $p^r b' = 0$ *et* $\overline{b'} = \bar{b}$, *ie.,* $b - b' \in \langle a\rangle$.
Or $p^r b \neq 0 \implies \exists 0 < n < p^s$ *tel que* $p^r b = na$.
Ecrivons $n = p^t m$ *avec* $p \not| m$, *alors*

$$p^r b = p^t ma$$

Puisque $p \not| m$, $(p^s, m) = 1$, *donc* $\exists u, v \in \mathbb{Z}$ *tel que*

$$up^s + vm = 1$$

d'ou $a = 1a = (up^s + vm)a = up^s a + vma = vma$.
Par ailleurs, ceci implique que $(p^s, v) = 1$.

En particulier $p \not| v$ et donc $p \not| vm$.
Donc $o(ma) = o(a) = p^s$.
Par consequent

$$o(p^r b) = o(na) = o(p^t ma) = p^{s-t}$$

Donc par le lemme precedent, on a

$$o(b) = p^{s-t+r}$$

□

Puisque p^s est l'ordre maximal d'un element de A, il s'ensuit que $s - t + r \leq s$, ie., $r \leq t$.
Poser $b' = b - p^{t-r} ma$.
Alors $p^r b' = p^r b - p^t ma = 0$

Lecture 16: Classification des groupes Abeliens Finis

Fri 10 Dec

5.7 Classification des groupes abeliens finis

Theorème 45 (Classifiaction)
Si A est un groupe abelien fini d'ordre n, alors pour tout nombre premier p qui divise n, il existe une unique suite d'entiers

$$r_{p,1} \geq r_{p,2} \ldots \geq r_{p,m_p}$$

tels que

$$A = \prod_{p \in P_n} \mathbb{Z}/_{p^{r_{p,1}}\mathbb{Z}} \times \ldots \times faktor \mathbb{Z} p^{r_{p,m_p}} \mathbb{Z}$$

ou $P_n = \{p \text{ premier } |p|n\}$

Il nous faut deux lemmes techniques necessaires pour la demonstration du theoreme.

Lemme 46
Si A est un groupe abelien tel que $A = T_n(A)$ et $n = lm$ ou $(l, m) = 1$, alors

$$A = T_l(A) \oplus T_m(A)$$

Preuve
$(l, m) = 1$ implique $\exists r, s \in \mathbb{Z}$ tel que $rl + sm = 1$.
Ainsi

$$\forall a \in A, a = rla + sma \in T_m(A) + T_l(A)$$

Par ailleurs, si $a \in T_m(A) \cap T_l(A)$, alors

$$la = 0 = ma$$

d'ou $rla + sma = 0$, donc $a = 0$.
Donc $T_m(A) \cap T_l(A) = \{0\}$, donc on a bien une somme directe. □

Une consequence du lemme ci-dessous est

Lemme 47
Si A est un groupe abelien, tel que $A = T_n(A)$, alors $A = \bigoplus_{p \in P_n} A(p)$

Preuve
On ecrit $n = p_1^{l_1} \ldots p_k^k$, ou $P_n = \{p_1, \ldots, p_k\}$.
Par recurrence sur k, on conclut. □

Preuve (du theoreme de classification)
Notons que, si A est abelien fini, et $|A| = n$ alors

$$A = T_n(A)$$

Donc par le lemme precedent

$$A = \bigoplus_{p \in P_n} A(p)$$

On sait aussi que chaque $A(p)$ est un p groupe abelien, puisque $|A(p)| < \infty$.
Ainsi, il suffit de demontrer que si A est un p groupe abelien, il existe une suite unique $r_1 \geq \ldots \geq r_m$ tel que

$$A \simeq \mathbb{Z}/_{p^{r_1}\mathbb{Z}} \times \ldots \times \mathbb{Z}/_{p^{r_m}\mathbb{Z}}$$

Existence

Par recurrence sur $|A|$.
Si $|A| = 1$, on a fini.
Si $|A| = p$, alors $A = \mathbb{Z}/_{p\mathbb{Z}}$
Supposons qu'une telle decomposition en produit de groupes cycliques existe pour tout p-groupe abelien A tel que $|A| = p^k, \forall k < n$.
Soit A un p-groupe abelien tel que $|A| = p^n$.
Soit maintenant $a \in A$ d'ordre maximal, $o(a_1) = p^{r_1}$, alors

$$|A/_{\langle a_1 \rangle}| = p^{n-r_1} < p^n$$

Par l'hypothese de recurrence, il existe une suite $r_2 \geq \ldots \geq r_m$ tel que $\exists$ iso

$$\phi : A/_{\langle a_1 \rangle} \to \mathbb{Z}/_{p^{r_2}\mathbb{Z}} \times \ldots$$

Posons $\overline{a_i} = \phi^{-1}((0, \ldots, 1, \ldots))$ avec un 1 a la $i-1$ eme place.
Alors $o(\overline{a_i}) = p^{r_i} \forall i$ et

$$A/_{\langle a_1 \rangle} \simeq \bigoplus_{i=2}^{m} \langle \overline{a_i} \rangle$$

Par le lemme 4.5, il existe un representant de $\overline{a_i}$ dont l'ordre est p^{r_i}.
Sans perte de géneralité, $o(a_i) = p^{r_i}$.

On affirme que

$$A = \bigoplus_{i=1}^{m} \langle a_i \rangle \simeq \prod_{i=1}^{m} \mathbb{Z}/p^{r_i}\mathbb{Z}$$

Considerons l'homomorphisme quotient $q : A \to A/\langle a_1 \rangle$.
$\forall b \in q$, *il existe* $s_2, \ldots, s_m$ *tel que* $\overline{b} = q(b) = s_2\overline{a_2} + \ldots + s_m\overline{a_m}$
Par consequent

$$\overline{b} = \overline{s_2 a_2 + \ldots + s_m a_m}$$

Donc il existe $s_1 \in \mathbb{Z}$ *tel que*

$$b - s_2 a_2 - \ldots - s_m a_m = s_1 a_2$$

ie, $b = \sum_i s_i a_i$

Finalement on observe que $\langle a_i \rangle \cap \langle a_j \rangle = \{0\}$

Unicite

Recurrence sur $|A|$.
Si $|A| = 1, p$, *on a un seul choix.*
Ensuite, si

$$\mathbb{Z}/p^{r_1}\mathbb{Z} \times \ldots \times \frac{\mathbb{Z}}{p^{r_m}} \simeq \mathbb{Z}/p^{s_1}\mathbb{Z} \times \ldots \times \frac{\mathbb{Z}}{p^{s_m}} \qquad \square$$

avec r_1 *et* s_1 *maximal.*
Alors $r_1 = s_1$ *car a gauche l'ordre maximal est* p^{r_1} *et a droite, l'ordre maximal est* p^{s_1}.
Et on a fini par recurrence.

Lecture 17: Sous-groupes de Sylow

Sat 11 Dec

6 Theoremes de Sylow

6.1 Les p-groupes

Dorenavant, p sera toujours un premier fixe.

Definition 27
Si G *est un groupe fini,* $|G|$ *est l'ordre de* G.
Si H *st un sous-groupe d'un groupe fini* G, *alors* $(G : H)$ *est l'index de* H *dans* G, *ie.,* $|G|/|H|$

Definition 28 (p-groupes)
Un groupe fini G *est un p-groupe si* $|G|$ *est une puissance de* p.
Un p-sousgroupe d'un groupe G *est un sous-groupe non-trivial* H *de* G *tel que*

$|H|$ est une puissance de p.
Un p-sous-groupe fini G est dit de Sylow si $|H|$ est la puissance maximale de p qui divise $|G|$.

Definition 29
Pour tout groupe G, on pose

$$\mathcal{S}_p(G) = \{H \in \mathcal{S}(G) | H \text{ un } p\text{-sous-groupe } \}$$

Si p divise $|G|$, on note l'ensemble des p-sous-groupes de Sylow par

$$Syl_p(G) = \{H \in \mathcal{S}_p(G) | H \text{ de Sylow } \}$$

6.2 Existence des p-sous-groupes

> **Theorème 48 (Existence de p-sous-groupes)**
> *Si G est un groupe fini tel que p divise $|G|$, alors $Syl_p(G) \neq 0$*

On a deja vu que dans le cas ou G est abelien, $Syl_p(G)$ est non-vide.

Definition 30 (Centre d'un groupe)
Le centre d'un groupe G est le sous-groupe

$$Z(G) = \{a \in G | ab = ba \forall b \in G\}$$

Remarque
Le centre d'un groupe est toujours abelien. Par ailleurs pour tout groupe G

$$Z(G) = \ker \gamma_G$$

ou γ_G est l'homomorphisme de representation adjointe.

Observer que

$$b \in Z(g) \iff ab = ba \forall a \in G \iff C_G(b) = G \iff (G : G_b) = 1$$

Par consequent, l'equation de classe devient

$$|G| = \sum_{b \in Z(G)} (G : G_b) + \sum_{b \in \overline{G} \setminus Z(G)} (G : G_b) = |Z(G)| + \sum_{b \in \overline{G} \setminus Z(G)} (G : C_G(b))$$

Lecture 18: Existence des groupes de Sylow

Fri 17 Dec

Grace a cette version de l'equation de classe, on a

> **Lemme 50**
> *Soit G un groupe tel que p divise $|G|$. Si p divise $(G : H)$ pour tout sous-groupe propre H de G, alors p divise aussi l'ordre du centre $Z(G)$ de G*

Preuve

$$|G| = |Z(G)| + \sum_{b \in \overline{G} \setminus Z(G)} (G|C_G(b))$$

$\square$

Or par hypothese, la somme a droite est divisible par p, alors la somme est aussi divisible par p.
Donc $\sum_{b \in \overline{G} \setminus Z(G)} (G : C_G(b))$ *est divisible par p.*
Puisque $p||G|$*, on en deduit que* $p||Z(G)|$*.*

> **Lemme 51**
> *Si* G *est un groupe abelien fini tel que* p *divise* $|G|$*, alors il existe* $a \in G$ *tel que* $o(a) = p$*.*

Preuve
$G = G(p) \oplus G'$ *ou* $p \not| |G'|$ *Puisque* $p||G|$*, on doit avoir que* $p||G(p)|$ *donc* $\exists a \in G(p) \setminus \{0\}$*, donc il existe* $k > 0$ *tel que* $o(a) = p^k$*, donc* $o(p^{k-1}a) = p$*.* $\square$

6.3 Preuve du theoreme d'existence

Par recurrence sur $|G|$.
Rappel : G un groupe fini tel que $|G| < \infty$ et tel que $p||G|$.

Preuve
Base de la recurrence $|G| = p$*, alors* $G \simeq \mathbb{Z}/p\mathbb{Z}$ *et donc* $Syl_p(G) = \left\{\mathbb{Z}/p\mathbb{Z}\right\}$.
Pas de recurrence : Supposons vrai $\forall G$ *groupe fini tel que* $|G| < N$ *ou (* $N > p$*) et tel que* $p||G|$*.*
Soit G *un groupe fini tel que* $|G| = N$ *et tel que* $p|N$*.*
Posons $n = \max\left\{k|p^k|N\right\}$*.*
On veut montrer qu'il existe un sous-groupe $P < G$ *tel que* $|P| = p^n$*.*

1. *Supposons qu'il existe un sous-groupe propre* $H \leq G$ *tel que* $p \not| (G : H)$*.*
   Alors $p^n||H|$ *et puisque* $|H| < |G| = N$*, on a fini par recurrence.*

2. *Supposons donc que* $p|(G : H) \forall H < G$*, alors le lemme implique que* $p||Z(G)|$ *ce qui implique que* $\exists a \in Z(G)$ *tel que* $o(a) = p$*.*
   Puisque $a \in Z(G)$*,* $\langle a \rangle$ *est un sous-groupe normal.*
   Ainsi $G/\langle a \rangle$ *est un groupe.*
   Par ailleurs $|G/\langle a \rangle| = \frac{N}{p} < N$ *et* $n-1$ *est la puissance maximale de p qui divise l'ordre du groupe quotient.*
   Ainsi par recurrence $Syl_p(G/\langle a \rangle)$ *et il existe donc* $P < G/\langle a \rangle$ *tel que*

$|P| = p^{n-1}$.
Par le 3eme theoreme isomorphisme, il existe donc $\tilde{P} < G$ $\langle a \rangle < \tilde{P}$ et $|\tilde{P}| = |P| \cdot |\langle a \rangle| = p^n$.

6.4 Proprietes des p-sous-groupes de Sylow

Pour formuler les proprietes, on a besoin du normalisateur

Definition 31 (Normalisateur)
Soient G un groupe et $H < G$. Le normalisateur de H dans G, note $N_G(H)$ est le sous-groupe de G specifie par

$$N_G(H) = \left\{a \in G | aba^{-1} \in H \forall b \in H\right\}$$

Remarque
Quelques soient G et $H < G$, le normalisateur est le plus grand sous-groupe de G par rapport auquel H est un sous-groupe normal.

Theorème 53 (Proprietes importantes)
Soit G un groupe tel que p divise $|G|$

1. *Quelques soient $H \in \mathcal{S}_p(G)$ et $P \in Syl_p(G)$, il existe $Q \in Syl_p(G)$ et $a \in G$ tels que*
$$Q = aPa^{-1} \text{ et } H < Q$$
2. *Quelques soient $P, Q \in Syl_p(G)$, il existe $a \in G$ tel que $Q = aPa^{-1}$*
3. *La cardinalite de $Syl_p(G)$ est egale a $(G : N_G(P))$ quelque soit $P \in Syl_p(G)$*
4. *Il existe $m \in \mathbb{N}$ tel que la cardinalite de $Syl_p(G)$ est egale a $mp + 1$*

Remarque
Soit G un groupe et soit $T \subset \mathcal{S}$. Si $aKa^{-1} \in T$ pour tout $a \in H$ et tout $K \in T$, alors il y a une action de H sur T

$$\beta_{H,T} : H \to \text{Aut}(T)$$

specifie par

$$\beta_{H,T}(a) : T \to T : K \to aKa^{-1}$$

pour tout $a \in H$.
Pour tout $K \in T$, on notera l'obrite de K sous l'action $\beta_{H,T}$ par

$$O_K^H = \left\{aKa^{-1} | a \in H\right\}$$

et son stabilisateur par

$$H_K = \left\{a \in H | aKa^{-1} = K\right\}$$

Si T est fini, l'equation de classe pour cette action devient

$$|T| = \sum_{i \in I} (H : H_{K_i})$$

Par exemple, pour $\beta_{G,Syl_p(G)}$ puisque

$$P < N_G(P) = G_p$$

on sait que $p \not| (G : G_p)$ ce qui implique que

$$p \not| |O_p|$$

car $|O_p| = (G : G_p)$.

Lemme 55
Soient G un groupe tel que p divise $|G|$, $P \in Syl_p(G)$ et $H \in \mathcal{S}_p(G)$. Si $H < N_G(P)$ alors $H < P$

Preuve
Strategie : Montrer que $HP = P$ car si $HP = P$, alors $\forall a \in H, b \in P \exists c \in P$ tel que $ab = c$ d'ou $a = cb^{-1} \in P$, ie. $H < P$.
Pour y arriver

1. $HP < G$

$$\forall a_1, a_2 \in H, b_1, b_2 \in P$$

$$(a_1b_1)(a_2b_2)^{-1} = a_1a_2^{-1}(a_2b_1a_2^{-1})(a_2b_2^{-1}a_2^{-1})$$

   Donc $(a_1b_1)(a_2b_2)^{-1} \in HP$

2. $P < HP$ *est un sous-groupe normal :*
   $\forall b \in P \forall ac \in HP$, *alors*

$$(ac)b(ac)^{-1} = a(cbc^{-1})a^{-1}$$

3. $H \cap P < H$ *est un sous-groupe normal car* $\forall b \in H \cap P, \forall a \in H : aba^{-1} \in H \cap P$.

4. *Donc par le 3eme theoreme d'isomorphisme*

$$H/_{H \cap P} \simeq HP/_{P}$$

   D'ou HP est un p-groupe qui contient $P \in Syl_p(G)$.
   Par la maximalite des p-sous-groupes de Sylow, on en deduit que $HP = P$

6.5 Preuve des proprietes de $Syl_p(G)$

1. *Soit $H \in \mathcal{S}_p(G)$, soit $P \in Syl_p(G)$, on doit montrer que $\exists Q \in Syl_P(G)$ et $a \in G$ tel que $Q = aPa^{-1}$ et $H < Q$.*
   Considerons $\beta_{H,O_P^G} : H \to Aut(O_p^G)$.
   Si $P' \in O_P^G$, alors
   — soit $H_{p'} = H$
   — Soit $H_{p'} < H$
   Si $H_{p'} < H$, alors $p|(H : H_{p'})$.
   Ecrivons $O_P^G = \bigcup O_{P_i}$ ou $\{P_1, \ldots\} \subset O_P^G$.
   L'equation de classe dit alors quee

$$|O_P^G| = \sum_{i|H_{p_i}=H} (H : H_{p_i}) + \sum_{i|H_{P_i}<H} (H : H_{p_i})$$

   car la somme a droite est divisible par p et $|O_P^G$ n'est pas divisible par p $\sum_{i|H_{p_i}=H}(H : H_{p_i})$ est non-nul.
   Il existe donc un p_i tel que $H_{p_i} = H$, ie. $aP_ia^{-1} = P_i \forall a \in H$.
   Autrement dit $H < N_G(P_i)$ et donc $H < P_i$.
   Ainsi, on a bien que $H < P_i$ et il existe $a \in G$ tel que $P_i = aPa^{-1}$ puisque $P_i \in O_P^G$.

2. *On fixe $P, Q \in Syl_p(G)$, on doit montrer que $Q \in O_P^G$.*
   Puisque $Q \in Syl_p(G)$, on sait que $Q \in \mathcal{S}_p$, on applique 1 a Q et on a donc qu'il existe $Q' \in Syl_p(G)$ et $a \in G$ tel que $Q' = aPa^{-1}$ et $Q \leq Q'$ d'ou $Q = Q'$ en comparant les cardinalites.
3. *Calculer $|Syl_p(G)|$ en termes de $N_G(P)$ avec $P \in Syl_p(G)$.*
   Considere $\beta_{Syl_p(G),G} : G \to \mathrm{Aut}(Syl_p(G))$.
   Par 2, $\forall P \in Syl_p(G), O_P^G = Syl_p(G)$.
   D'ou par l'equation de classe

$$|Syl_p(G)| = |O_P^G| = (G : G_p) = (G : N_G(P))$$

4. *Un autre calcul de $|Syl_p(G)|$.*
   On considere maintenant pour $P \in Syl_P(G)$

$$\beta_{P,Syl_p(G)} : P \to \mathrm{Aut}(Syl_p(G))$$

   Alors

$$O_P^P = \left\{aPa^{-1}|a \in P\right\} = \{P\}$$

   et si $P \neq Q$ alors $p|(P : P_Q)$ car si $p \not|(P : P_G)$, alors $P = P_Q = \left\{a \in P|aQa^{-1} = Q\right\}$ ce qui veut dire que $P < N_G(Q)$ et donc $P = Q$ ce

qui est impossible.
Et alors l'equation de classe donne

$$|Syl_p(G)| = |O_P^P| + \sum_i O_{Q_i}^P = 1 + pm$$

□