Générateurs et relations

Proposition : Soit G un groupe et $\{H_i\}_{i\in I}$ une famille des sous-groupes (respectivement sous-groupes normaux) de G. Alors $\bigcap_{i\in I} H_i$ est un sous-groupe (respectivement, un sous-groupe normal) de G.

Preuve : exercice facile.

Proposition : Soit X un sous-ensemble d'un groupe G (X pas nécessairement un groupe). Alors il existe un **plus** petit sous-groupe $\langle X\rangle$ de G contenant X et il existe un plus petit sous-groupe normal N_G^X de G contenant X.

Preuve Soit $\mathcal{X} = \{H \leq G \mid X \subseteq H\}$ et soit $\mathcal{X}^N = \{H \trianglelefteq G \mid X \subseteq H\}$. Alors

$$\langle X\rangle = \bigcap_{H\in\mathcal{X}} H \quad \text{et} \quad N_G^X = \bigcap_{H\in\mathcal{X}^N} H$$

Il est facile de voir que ce sont les plus petits sous-groupes de G avec le propriétés voulues. (utiliser raisonnement par l'absurde) □

En fait on peut décrire les éléments de $\langle X\rangle$ et N_G^X (voir les propositions suivantes).

Définitions

$\langle X\rangle$ est appelé le sous-groupe de G engendré par X

X est appelé l'ensemble de générateurs de X

N_G^X est appelé la clôture normale de X dans G.

Remarques

1) $\langle \emptyset \rangle = \{1\}$.

2) $\#X = 1$ alors $\langle x \rangle$ est un sous-groupe cyclique.

Soit $X \subseteq G$ et notons $X^{-1} := \{x^{-1} \mid x \in X\}$.

Soit $S(X) := \{u \in G \mid u = x_1 x_2 \cdots x_n,\ x_i \in X \cup X^{-1}\}$

Proposition $\langle X \rangle = S(X)$.

Preuve : A voir que $S(X)$ est un sous-groupe de G.

$1 \in S$ ✓ ; l'inverse de $x_1 \cdot x_2 \cdots x_u$ est $x_u^{-1} x_{u-1}^{-1} \cdots x_1^{-1} \in S(X)$.

$u = x_1 x_2 \cdots x_u$, $v = y_1 y_2 \cdots y_m$ alors $uv^{-1} \in S(X)$.

De plus $X \subseteq S(X)$.

Si $H \leq G$ contient X alors forcement il contient X^{-1} (car tout inverse d'un élément de H est dans H), et il contient tout produit fini de éléments dans $X \cup X^{-1}$ (car tout produit des 2 éléments de H est contenu dans H). Donc $S(X) \leq H$, ce qui entraine que $S(x)$ est minimal contenant X.

Donc $\langle X \rangle = S(X)$. □

Notons l'orbite par conjugaison de X dans G par.

$X^G := \{g x g^{-1} \mid g \in G,\ x \in X\}$.

Proposition $N_G^X = S(X^G)$.

Preuve On sait que $S(X^G)$ est un sous-groupe de G. On veut voir qu'il est normal :

Soit $u = g_1 x_1 g_1^{-1} g_2 x_2 g_2^{-1} \cdots g_u x_u g_u^{-1}$, $g_i \in G$, $x \in X \cup X^{-1}$

Alors $a u a^{-1} = a g_1 x_1 g_1^{-1} a^{-1} a g_2 x_2 g_2^{-1} a^{-1} a \cdots a^{-1} a g_u x_u g_u^{-1} a^{-1}$

$= (ag_1) x_1 (ag_1)^{-1} (ag_2) x_2 (ag_2)^{-1} \cdots (ag_u) x_u (ag_u)^{-1} \in S(X)$

Donc $S(X^G) \trianglelefteq G$.

Pour tester la minimalité on procède comme dans la proposition précédente. □

Définition : Soit G un groupe.

S'il existe un sous-ensemble X de G tel que $\langle X \rangle = S(X) = G$ on dit que X est un ensemble de générateurs de G.

S'il existe X un ensemble de générateurs de G, tel que $\#X < \infty$, alors on dit que G est de type fini ou G est de génération finie.

Remarque G fini $\Rightarrow$ G de type fini

Exemples

1) $G = \langle G \rangle$.

2) $G = S_n$ alors $G = \langle X \rangle$ où $X = \{\text{transpositions}\}$

3) $G = C_n$ alors $G = \langle g \rangle$, g - générateur.

4) $G = \mathbb{Z}$ alors $G = \langle 1 \rangle$.

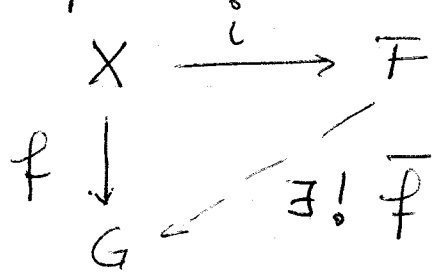
Donc on remarque qu'il est naturel d'engendrer un sous-groupe à l'intérieur d'un groupe ambient (donc la loi de multiplication est définie) pour toute paire d'éléments. On essaye maintenant de construire des groupes sans avoir un groupe ambient. Pour cela le concept crucial est celui de groupe libre qu'on définira et construira par la suite.

Groupe libre et présentations

Déf Soit X un ensemble

Un <u>groupe libre sur X</u> est un couple (F, i) où F est un groupe et $i : X \longrightarrow F$ est une application, tels que la propriété universelle suivante est satisfaite :

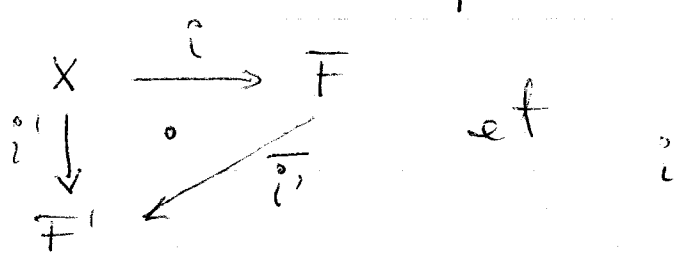
Pour tout groupe G et pour toute application $f : X \longrightarrow G$, il existe un unique homomorphisme de groupes $\overline{f} : F \longrightarrow G$ tel que $\overline{f} \circ i = f$.



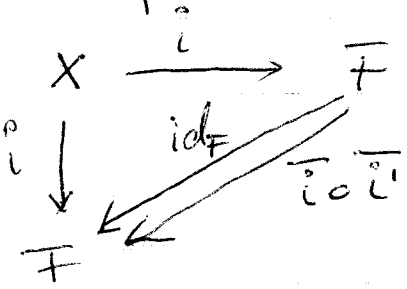
<u>Lemme</u> : Si (F, i) existe (pour un X fixé) alors il est unique à isomorphisme près.

<u>Preuve</u> Soit (F', i') un autre groupe libre sur X

Alors on a qu'il existe $\overline{i}$ est $\overline{i'}$ tels que



Donc $\overline{i} \circ \overline{i'}$ est un homomorphisme de F dans F tel que le diagramme suivant commute ;



Comme id_F fait aussi commuter le diagramme, par unicité on a que $\overline{i} \circ \overline{i'} = id_F$.

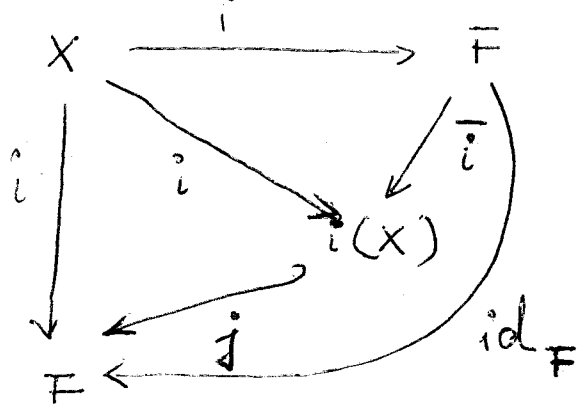
De même on obtient que $\bar{i}' \circ \bar{i} = id_{F'}$
Donc $\bar{i}$ est un isomorphisme et $F \cong F'$. □

Lemme (propriétés de (F, i)).
Soit (F, i) un groupe libre sur X. Alors
1) $F = \langle i(X) \rangle$
2) i est injective.

Preuve

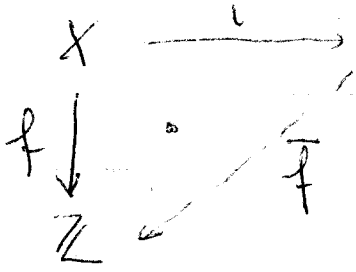
1) Soit $H = \langle i(X) \rangle \leq F$

Donc on a :



où $j : \langle i(X) \rangle \hookrightarrow F$ est l'inclusion.
Par propriété universelle $j \circ \bar{i} = id_F$. En particulier j est surjective donc un isomorphisme.

2) Si $X = \{*\}$ a un élément, alors i est clairement injective. Supposons que $\#X \geq 2$.
Soit $x \neq y$, $x, y \in X$.
On définit $f : X \longrightarrow \mathbb{Z}$ par $f(x) = 1$ et $f(z) = 0$, $\forall\, z \in X \setminus \{x\}$. En particulier, $f(y) = 0$.



Par propriété universelle, il existe $\bar{f} : F \longrightarrow \mathbb{Z}$ tel que $\bar{f} \circ i = f$. En particulier.
$\bar{f}(i(x)) = f(x) = 1 \neq 0 = f(y) = \bar{f}(i(y))$
Donc $i(x) \neq i(y)$ et i est injective □

Théorème (existence du groupe libre).
Pour tout ensemble X, il existe un groupe libre sur X.

Preuve

Considérons l'ensemble $X^{-1} := \{ x^{-1} \mid x \in X \}$.
C'est tout simplement un ensemble isomorphe à X et disjoint à X.

Soit $\mathcal{W} = \{ x_1 x_2 \cdots x_n \mid x_i \in X \amalg X^{-1} \} \cup \{\phi\}$ l'ensemble des mots finis avec lettres en $X \amalg X^{-1}$.
Sur $\mathcal{W}$ on considère l'opération de concaténation des mots $(x_1 x_2 \cdots x_n, y_1 y_2 \cdots y_m) \longmapsto x_1 x_2 \cdots x_n y_1 y_2 \cdots y_m$
Soit ϕ le mot vide et considérons sur $\mathcal{W}$ la relation d'équivalence engendrée par
$\{ x x^{-1} \sim \phi \mid x \in X \} \amalg \{ x^{-1} x \sim \phi \mid x \in X \}$.

Alors $W = \mathcal{W}/\sim$ est un groupe pour l'opération de concaténation.

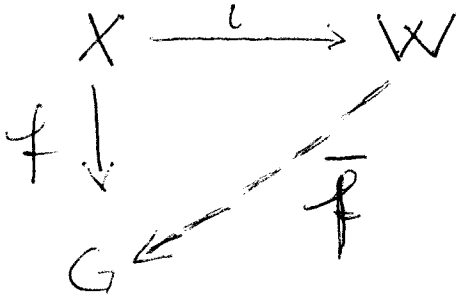
En effet $\overline{\phi}$ est l'élément neutre et $x_n^{-1} x_{n-1}^{-1} \cdots x_1^{-1}$ est l'inverse de $x_1 x_2 \cdots x_n$

De plus, l'opération de concaténation est clairement associative.

Maintenant X est un sous-ensemble de W par l'inclusion $i : X \longrightarrow W$, $x \longmapsto \overline{x}$.

A voir (W, i) est un groupe libre sur X.

Soit G un groupe et $f : X \to G$ une application.



Alors $\bar{f}$ doit satisfaire :

$$\bar{f}(\bar{x}) = f(x) \quad , \quad \bar{f}(\bar{\phi}) = 1_G$$

$$\bar{f}(\overline{x^{-1}}) = f(x)^{-1} \overset{\text{notation}}{=:} f(x^{-1})$$

Donc $\bar{f}$ est uniquement déterminé comme morphisme de groupes par :

$$\bar{f}(\overline{x_1 x_2 \cdots x_n}) = f(x_1) f(x_2) \cdots f(x_n).$$

et il est bien défini car

$$f(\overline{x x^{-1}}) = f(x) \cdot f(x)^{-1} = 1_G = \bar{f}(\phi)$$

Donc (W, i) satisfait la propriété universelle. □

Définition Ce groupe (W, i), qui est unique à isomorphisme près, par le lemme précédent, est appelé le groupe libre sur X et est noté $F(X)$ ou F_X.

Exemples

1) $\bar{F}_\phi = \{1\}$

2) $\bar{F}_{1*} = \mathbb{Z}$

Remarque : (voir le théorème suivant)
Tout groupe est le quotient d'un groupe libre.

Théorème : Soit G un groupe. Il existe alors une suite exacte courte des groupes

$$1 \longrightarrow N \longrightarrow F \longrightarrow G \longrightarrow 1$$

telle que F est un groupe libre (d'où la remarque précédente).

Preuve :

Soit X un ensemble de générateurs de G. Il existe toujours, quitte à prendre G lui-même, le but est bien sûr de le prendre aussi petit que possible. Soit F_X le groupe libre sur X. Alors il existe un unique homomorphisme de groupes $\bar{j} : F_X \longrightarrow G$ avec $\bar{j} \circ i = j$ où $i : X \to F_X$ et $j : X \to G$ sont les inclusions canoniques. Comme $G = \langle j(X) \rangle$ et $F = \langle i(X) \rangle$ on a que $\bar{j}$ est surjective. Notons $N := \ker \bar{j}$. Alors on a la suite exacte courte :

$$1 \longrightarrow N \hookrightarrow F \xrightarrow{\bar{j}} G \longrightarrow 1.$$

□

Remarque N 'contient' les relations entre les générateurs de G. Donc F et N décrivent $G \left(\simeq F/N\right)$ d'où la définition suivante.

Définition Soit G un groupe, soit X un ensemble et soit R un sous-ensemble de F_X. On dit que $\langle X \mid R \rangle$ est une présentation de G par générateurs et relations et on écrit $G = \langle X \mid R \rangle$ si

1) Il existe une application $f : X \to G$ tel que $G = \langle f(X) \rangle$. (donc $\bar{f} : F_X \to G$ est surjective)
2) $\ker \bar{f} = N_{F_X}^R$

Autrement dit, on a une suite exacte courte :

$$1 \to N_{F_X}^R \hookrightarrow F_X \xrightarrow{\bar{f}} G \longrightarrow 1$$

Remarques

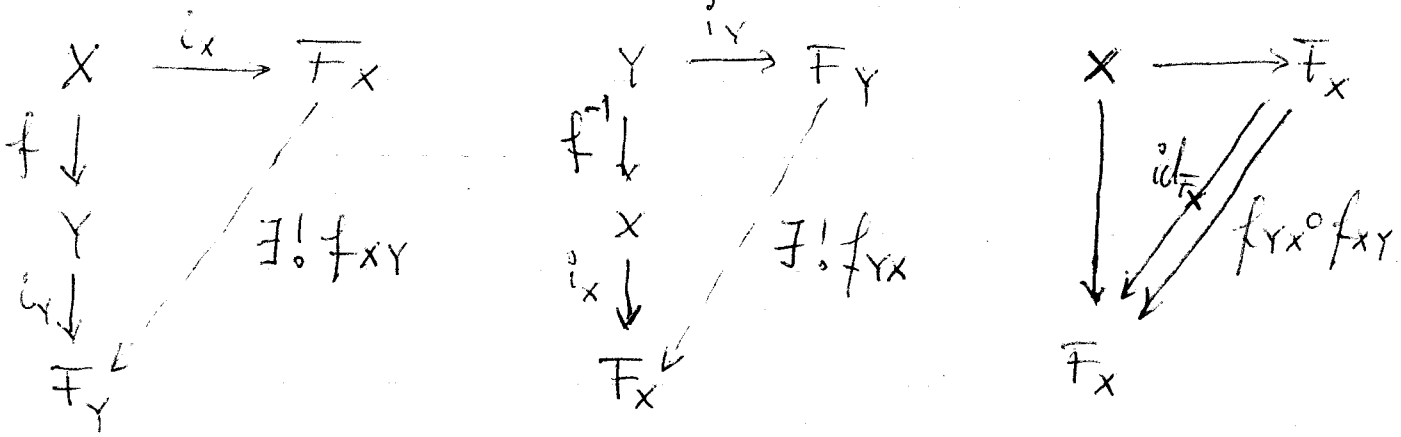
1) $G = \langle X | R \rangle \Rightarrow G \simeq F_X / N_{F_X}^R$

2) Si $r \in R$ alors $\overline{f}(r) = 1$
Donc $N_{F_X}^R$ contient tous les mots de X qui feront 1 dans G (regardés à travers $\overline{f}$).
Donc G est l'ensemble de classe d'équivalence des mots de F_X pour la relation $r = 1$ pour $r \in R$.

On dit que <u>G est de présentation finie</u> si $\#X < \infty$ et $\#R < \infty$.

3) En général il n'y a pas d'algorithme pour résoudre le problème des mots suivant : étant donné $G = \langle X | R \rangle$ est-ce que $w \in F_X$ est 1 dans G.
Pas d'algorithme même si G est de présentation finie.

4) Toute bijection $f : X \to Y$ induit un isomorphisme $\tilde{f} : F_X \longrightarrow F_Y$. Ceci est facile à voir en utilisant la propriété universelle du groupe libre.



Par unicité dans le troisième diagramme $id_{F_X} = f_{YX} \circ f_{XY}$
De même $f_{XY} f_{YX} = id_{F_Y}$ donc f_{XY} est un isomorphisme qu'on note $\tilde{f}$. □

On peut maintenant comparer deux présentations.

Théorème (Van Dyk)

Soit $G = \langle X | R \rangle$ et soit $H = \langle Y | S \rangle$.
Supposons qu'on a une bijection $f : X \to Y$ telle que $\tilde{f}(R) \subset S$ (où $\tilde{f} : F_X \to F_Y$ est l'isomorphisme définit auparavant).
Alors il existe un epimorphisme $\varphi : G \to H$.

Preuve Il faut completer le diagramme suivant ou les lignes sont des suites exactes courtes et le premier carré commute.

$$\begin{array}{ccccccccc} 1 & \longrightarrow & N_{F_X}^{R} & \hookrightarrow & F_X & \xrightarrow{i_X} & G & \longrightarrow & 1 \\ & & \tilde{f}\downarrow & & \downarrow\tilde{f} & & \downarrow\varphi & & \\ 1 & \longrightarrow & N_{F_Y}^{S} & \hookrightarrow & F_Y & \xrightarrow{i_Y} & H & \longrightarrow & 1 \end{array}$$

En effet, comme $\tilde{f}$ est un isomorphisme et $\tilde{f}(R) \subset S$ on a que $N_{F_Y}^{\tilde{f}(R)} \subseteq N_{F_Y}^{S}$. De plus $\tilde{f}\left(N_{F_X}^{R}\right) = N_{F_Y}^{\tilde{f}(R)}$ donc le premier carré commute.

Construction de $\varphi : G \to H$

Tout $g \in G$ s'écrit $g = i_X(w)$
On définit $\varphi(g) := i_Y \circ \tilde{f}(w)$.
On vérifie :

a) φ est bien défini :

$i_X(w) = i_X(v)$ alors $w = v \cdot s$, $s \in N_{F_X}^{R}$

$\Rightarrow \tilde{f}(w) = \tilde{f}(v) \cdot \underbrace{\tilde{f}(s)}_{\in N_{F_Y}^{S}}$

$\Rightarrow i_Y \circ \tilde{f}(w) = i_Y \circ \tilde{f}(v)$ (car $i_Y \circ \tilde{f}(s) = 1$)

b) Ψ est un homomorphisme de groupes (facile)

c) Ψ fait commuter le 2ème carré !

Donc Ψ est surjectif car $\tilde{f}$ et i_Y sont surjectifs. □

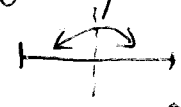
Exemple (illustration du théorème de Van Kampen)

Le groupe diédral $D_{2N} = \langle x, y \mid x^N = 1, y^2 = 1, (xy)^2 = 1 \rangle$

$N = 1$ $\quad D_2 = \langle x, y \mid x^2 = 1, y = 1, (xy)^2 = 1 \rangle$
$= \langle x \mid x^2 = 1 \rangle \simeq C_2$

C_2 peut-être vu géométriquement comme engendré par la symmétrie d'un segment

Donc D_2 est isomorphe au groupe d'isométries d'un segment

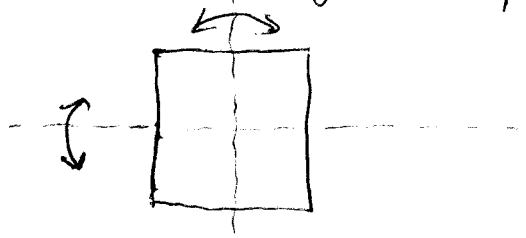


$N = 2$ $\quad D_4 = \langle x, y \mid x^2 = 1, y^2 = 1, (xy)^2 = 1 \rangle$

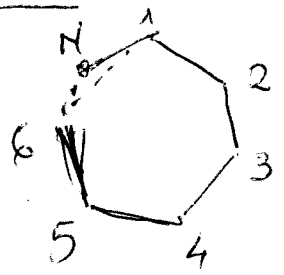
$(xy)^2 = 1 \iff xy = y^{-1}x^{-1} = yx$ (car $x^2 = 1, y^2 = 1$).

Donc $D_4 \simeq C_2 \times C_2$ est isomorphe au groupe de Klein.

De plus, D_4 est isomorphe au groupe des isométries planaires d'un carré (engendré par les symmétries axiales)



$N \geq 3$ Soit P_N un N-gône régulier dans le plan.



Isométries (P_N) = groupe des isométries du plan qui préservent globalement le N-gone.

Si T est une isométrie du P_N, alors T est complètement déterminée par les images des sommets 1 et 2. On a :

$T(1) = i$ (N choix possibles.)

$T(2) =$ voisin de i (2 choix possibles)

Donc $|\mathrm{Isom}(P_N)| = 2N$.

On définit R et S dans $\mathrm{Isom}(P_N)$ par :

$R(1) = 2$, $R(2) = 3$ (rotation de $\frac{2\pi}{N}$)

$S(1) = 1$, $S(2) = N$ (symmetrie autour de l'axe passant par le centre de P_N et par le sommet 1)

Exercice : R et S engendrent $\mathrm{Isom}(P_N)$.

On vérifie que R et S satisfont les relations du groupe diédral $R^N = 1$, $S^2 = 1$, $(RS)^2 = 1$.

La bijection $\{x, y\} \longrightarrow \{R, S\}$ envoye les relations dans D_{2N} sur des relations dans $\mathrm{Isom}(P_N)$

Par le théorème de Van Dyk on a une surjection

$$\varphi : D_{2N} \twoheadrightarrow \mathrm{Isom}(P_N).$$

Mais tout élément de D_{2N} s'écrit comme $x^a y^b$ avec $0 \leq a \leq n-1$ et $0 \leq b \leq 1$ (utiliser les relations)

Donc D_{2N} a au plus $2N$ éléments et on a que φ est un isomorphisme de groupes.