CHAPITRE 1 :

NOTIONS PRELIMINAIRES

I.1 PRESENTATION DE GROUPE

Soit X un ensemble dénombrable non vide .On considère X',copie de X .Il y a une bijection naturelle $\varphi : X \longrightarrow X'$ .X' sera noté X^{-1} et pour un élément $x \in X$,$\varphi(x)$ sera noté x^{-1} ,x sera éventuellement noté x^{+1} .

On appelle **mot sur l'alphabet X** (ou **sur X**) ,tout suite finie d'éléments de $X \cup X^{-1}$ .On notera une telle suite $x_1^{\varepsilon_1}\ldots x_n^{\varepsilon_n}$ où $x_1,\ldots,x_n \in X$ et $\varepsilon_1,\ldots,\varepsilon_n \in \langle -1;1\rangle$ .n est appelé **longueur du mot** .Le mot de longueur nulle est appelé **le mot vide** et sera noté 1 .Un mot de longueur n est dit **positif** si pour tout $i = 1 \ldots n$,$\varepsilon_i = +1$. L'ensemble des mots sur X sera noté $\mathfrak{M}(X)$.$\mathfrak{M}(X)$ muni de la loi de concaténation est un monoïde ,noté M(X) ayant pour élément neutre le mot vide .Soient ω et ω' ,deux mots sur un même alphabet ,on note $\omega \equiv \omega'$ si ω et ω' sont identiques .On dit qu'un mot μ est un **sous-mot** de ω ,si il existe deux mots (éventuellement vides) α et β tels que $\omega \equiv \alpha\,\mu\,\beta$ .On dit que μ est un sous-mot **initial** (resp^t **terminal**) de ω ,si il existe un mot α tel que $\omega \equiv \mu\,\alpha$ (resp^t $\omega \equiv \alpha\,\mu$) .Deux mots ω et ω' sont dits **conjugués cycliques** si il existe des mots α et β (éventuellement vides) tels que $\omega \equiv \alpha\,\beta$,et $\omega' \equiv \beta\,\alpha$.

On considère les opérations suivantes sur $\mathfrak{M}(X)$

(1) On note $\omega \xrightarrow{(1)} \omega'$ lorsque il existe deux mots α et β tels que $\omega \equiv \alpha\,x\,x^{-1}\beta$,ou $\omega \equiv \alpha\,x^{-1}x\,\beta$;et $\omega' \equiv \alpha\,\beta$ (où $x \in X$) .

(2) On note sous les même conditions $\omega' \xrightarrow{(2)} \omega$.

On note $\omega \longrightarrow \omega'$ si $\omega \xrightarrow{(1)} \omega'$,ou $\omega \xrightarrow{(2)} \omega'$.
Deux mots ω et ω' sont dits **librement égaux** si ω' peut être obtenu à partir de ω par une suite finie d'opérations (1) et (2) ,i.e. si il existe une suite finie de mots $(\omega_0,\ldots,\omega_n)$ où $\omega_0 \equiv \omega$,$w_n \equiv \omega'$,et $\forall\, i \in \langle 0,..,n-1\rangle$, $\omega_i \longrightarrow \omega_{i+1}$ .Un mot est dit **librement réduit**

,si on ne peut pas lui appliquer l'opération (1) (c'est à dire si il ne contient pas un sous-mot de la forme $x\,x^{-1}$,ou $x^{-1}x$ .On appelle **réduction libre** d'un mot une suite finie d'opérations (1) appliquée au mot ,tel que le mot obtenu soit librement réduit.

Il est aisé de vérifier qu'être librement égal est une relation d'équivalence sur M(X) ,compatible avec la loi de concaténation .Le quotient de M(X) par cette relation a une structure de groupe ,où l'inverse de la classe d'équivalence de $x_1^{\varepsilon_1}\ldots x_n^{\varepsilon_n}$,est la classe d'équivalence de $x_1^{-\varepsilon_1}\ldots x_n^{-\varepsilon_n}$ .Ce groupe sera noté F(X) ,et sera appelé **groupe libre engendré par X** (ou **sur X**) .Dans la suite on commettra l'abus de langage consistant à identifier un mot sur X avec sa classe d'équivalence dans F(X) .

PROPOSITION I.1.1 : Soit F(X) un groupe libre .Si ω et ω' sont deux mots librement réduits ,$\omega = \omega'$ dans F(X) ssi $\omega \equiv \omega'$ .En particulier si ω est réduit ,et $\omega = 1$ dans F(X) ,alors $\omega \equiv 1$.

Démonstration : Remarquons que si un mot ω donné peut être librement réduit en un unique mot ω_0,il en est de même du mot obtenu à partir de ω par une opération (1) ou (2) .Pour une opération de la forme (1) le résultat est trivial .Appliquons (2) à $\omega \equiv A\,B$ .On obtient $\omega_1 \equiv A \times x^{-1}B$ (l'autre cas étant similaire) ,que l'on réduit librement .Une opération (1) intervenant sur un sous-mot de A ou de B ,pourrait être appliquée sur ω ,et donc donc d'après ce qui précède n'altère pas le résultat .On peut donc sans perte de généralités supposer que A et B sont librement réduits.On a alors un des cas suivants :

$$\omega_1 \equiv A \times x^{-1}B \xrightarrow{(1)} A\,B \equiv \omega$$

$$\omega_1 \equiv A \times x^{-1}B \equiv A'(x^{-1}x)x^{-1}B \xrightarrow{(1)} A'x^{-1}B \equiv A\,B \equiv \omega$$

$$\omega_1 \equiv A \times x^{-1}B \equiv A \times (x^{-1}x)B' \xrightarrow{(1)} A \times B' \equiv A\,B \equiv \omega$$

Donc dans tout les cas ,si ω peut être librement réduit en un unique élément ω_0 il en est de même de ω_1 .

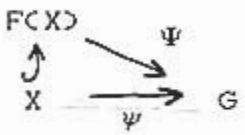
Considérons deux mots librement réduits ω et ω',librement égaux .Il existe donc une suite de transformations de la forme (1) et (2) changeant ω en ω' .Or ω ne peut être librement réduit qu'en lui-même.Donc ω' ne peut être librement réduit qu'en ω .Or ω' est librement réduit ,et donc $\omega \equiv \omega'$. ■

Remarque : Le procédé de réduction libre est déterministe ,i.e le résultat d'une réduction libre est indépendant de la façon de procéder .Pour un groupe libre ,donné par ses générateurs ,on a une solution au problème du mot ,par application de réductions libres .

Etant donné un groupe G ,et une S famille génératrice de G ,on peut se donner les éléments de G ,par des mots sur les générateurs .On dira que G est **Libre sur S** ,si tout mot réduit sur S ,représentant un élément l'élément neutre de G ,est vide .On vérifie aisément qu'alors G est le groupe libre sur S ,$G \cong F(S)$ .Un groupe est dit **Libre** ,si il est libre sur une de ses familles génératrices .

$|X|$ sera appelé le rang de F(X) .Si X est fini ,on dira que F(X) est de rang fini .Un résultat important est le fait qu'un groupe libre est uniquement déterminé par son rang (à isomorphisme près).

PROPOSITION I.1.2 : Soient un groupe G et $\psi : X \longrightarrow G$ .Alors il existe un unique homomorphisme Ψ ,tel que le diagramme suivant commutte .



Remarques Il s'agit même d'une caractérisation des groupes libres .

Les groupes libres sont des objets universels dans la catégorie des groupes .

Considérons un groupe G quelconque ,et S une famille génératrice de G .Alors d'après la proposition I.1.2 ,il existe un unique homomorphisme surjectif $\Psi : F(S) \longrightarrow G$,dont la restriction à S est l'inclusion sur les générateurs de G .On a donc $G \cong F(S)_{/\ker\Psi}$ .Toute groupe est donc quotient d'un groupe libre par un sous-groupe normal .Appelons R un sous-ensemble de F(S),dont la clôture normale dans F(S) est ker Ψ (elle sera notée $gp_{F(S)}(R)$) .On appelle **présentation** de G la donnée de $< S / R >$,où R est donné comme un ensemble de mots sur S .F(S) s'appelle le sous-groupe libre sous-jacent à G

Réciproquement considérons un ensemble S ,et R un ensemble de

mots sur S . Alors il existe un groupe , unique à isomorphisme près ayant pour présentation $\langle S / R \rangle$. En effet les éléments de R sont éléments du groupe libre sur S , et $F(S)_{/gp_{F(S)}(R)}$ définit un unique groupe.

Les éléments de S sont appelés les **générateurs** , et les élément de R , les **relateurs** . Un relateur de la forme $\alpha \beta^{-1}$ sera éventuellement noté $\alpha = \beta$ (et alors sera appelé relation) . Un élément de la forme $x x^{-1}$ ou $x^{-1}x$ ($x \in S$) sera appelé relateur trivial.

Etant donné une présentation $\langle S / R \rangle$, on note $gp(\langle S / R \rangle)$ le groupe ayant cette présentation . Un groupe admet une infinité de présentations . En effet , si $\langle S / R \rangle$ est une présentation de G , il en est de même de $\langle S \cup \{a\} / R \cup \{a\} \rangle$ si $a \notin S$. Si le contexte le permet , on confondra un groupe et une de ses présentations .

une présentation est dite **finie** , si S et R sont finis . Un groupe est dit **finiment présenté** (**f.p.**) , si il admet une présentation finie . Un groupe est dit **finiment engendré** (**f.e.**) , si il admet une famille génératrice finie (dans ce cas il admet une présentation $\langle S / R \rangle$ où S est fini) .

De la même façon que pour les groupes libres , lorsque l'on se donnera un groupe par une présentation , on verra les mots sur les générateurs comme éléments du groupe , i.e. , on confondra un mot avec sa classe d'équivalence . Lorsque le contexte l'exigera , on notera $\bar{\omega}$, l'élément de groupe représenté par ω . Pour un groupe G , nous noterons $=_G$ pour exprimer une égalité dans G . L'écriture $=_F$ sera réservée à la relation être librement égal .

PROPOSITION I.1.3 : Si un groupe G admet une présentation finie

$$\langle x_1, \ldots, x_n / r_1, \ldots, r_m \rangle$$

, ainsi qu'une présentation finiment engendrée

$$\langle a_1, \ldots, a_N / R_1, \ldots \rangle$$

alors tous les relateurs , sauf un nombre fini d'entre eux sont superflus , i.e

$$\langle a_1, \ldots, a_N / R_i \ ; i \in I \rangle$$

est une présentation de G , où $I \subset \mathbb{N}$ est fini .

Démonstration : Appelons F_1/N_1 et F_2/N_2 les quotient correspondant resp^t à la première et deuxième présentation . Il

existe un isomorphisme ψ : $F_1/N_1 \longrightarrow F_2/N_2$,qui envoie les générateurs $x_1,..,x_n$ sur des mots en $a_1,..,a_N$ (de longueur bornée) .Les images de $r_1,..,r_m$,sont dans le sous-groupe normal engendré par R_1,..etc... ;c'est à dire s'écrivent comme produit de conjugués sur ces relateurs .Puisque les mots $\psi(r_1),..,\psi(r_m)$ sont de longueur bornée ,seul un nombre fini de R_i sont utiles à leur écriture comme produit de conjugués de relateurs .De plus $\psi(r_1),..,\psi(r_m)$ engendrent N2 .En effet soit un mot ω en $a_1,..,a_n$,trivial .Alors $\psi^{-1}(\omega)$,est trivial ,et s'écrit donc comme produit de conjugués de $r_1,..,r_m$.Ainsi ω s'écrit comme produit de conjugués de $\psi(r_1),..,\psi(r_m)$ .Et donc seul un nombre fini de R_i est utile à engendrer N2 . ■

Etant donné un groupe G donné par une présentation $< S / R >$,deux mots ω et ω' sont égaux dans G (i.e. sont représentants de la même classe d'équivalence),si et seulement si $\omega\ \omega'^{-1}$ est librement égal à un élément de $gp_{F(S)}(R)$,soit si ω est librement égal à $\prod_{i=1..k} p_i\ r_i\ p_i^{-1}$,où les r_i sont des éléments de R ,et les p_i sont des mots sur S .On peut donc passer de ω' à ω par une suite finie d'opérations de la forme suivante :

(1) Insertion d'un sous-mot de la forme $x\ x^{-1}$,$x^{-1}x$ ($x \in S$) ,r_i ($r_i \in R$) .
(2) Suppression d'un sous-mot de la forme $x\ x^{-1}$,$x^{-1}x$,r_i .

De plus il est clair que si l'on applique une des opérations précédentes à un mot ,on obtient un mot de la même classe d'équivalence .Ceci a donné à la théorie s'intéressant aux groupes par la donnée de présentation le nom de *combinatoire des groupes* .

I.2 TRANSFORMATIONS DE TIETZE

Notations : On note $\omega(a_1,..,a_n)$ lorsque le mot ω s'écrit sur $a_1,..,a_n$ .Si l'on a une correspondance $a_i \longleftrightarrow b_i$ pour $i = 1..n$,on note $w(b_i)$ le mot obtenu à partir de ω ,en remplaçant toutes les occurences de a_i ,par b_i ,$i = 1 .. n$.

Soit $< x_1,..,x_n / r_1,..,r_m >$ une présentation finie d'un groupe G .On considère les transformations suivantes ,appelées transfor--mations de Tietze .

T_1 : Ajouter à la présentation de G ,un relateur r_{m+1} ,qui appartient à la clôture normale de $\langle r_1,..,r_m \rangle$.

T_1^{-1}: Opération inverse de T_1 .

T_2 : Ajouter à la présentation de G ,un générateur x_{n+1} ,ainsi qu'une relation $x_{n+1} = \omega(x_1,..,x_n)$.

T_2^{-1}: Opération inverse de T_2 .

THEOREME I.2.1 : *(Tietze)*

Deux présentations finies sont des présentations du même groupe ssi on peut passer de l'une à l'autre par une suite finie de transformations de Tietze .

Démonstration : *Condition suffisante*

La transformation T_1 laisse le groupe libre sous-jacent et son sous-groupe normal inchangés et donc le groupe reste identique

Soient G donné par $\langle x_1,..,x_n / r_1,..,r_m \rangle$ et G' dont la présentation est obtenu à partir de celle de G par une transformation T_2 .Considérons $\varphi : \langle x_1,..,x_n,x_{n+1} \rangle \longrightarrow \langle x_1,..,x_n \rangle$ dont la restriction à $\langle x_1,..,x_n \rangle$ est l'identité et tel que l'image de x_{n+1} soit $\omega(x_1,..,x_n)$ intervenant dans T_2 .Alors il existe un unique homomorphisme surjectif du groupe libre sous-jacent à G' dans G(prop. I.1.2).Les relateurs de G' sont dans $\ker \varphi$,et donc φ passe au quotient en $\tilde{\varphi} : G' \longrightarrow G$,homomorphisme surjectif. De plus soit un mot ζ en $\langle x_1,..,x_{n+1} \rangle$ tel que $\tilde{\varphi}(\zeta) =_G 1$.Alors en utilisant $x_{n+1} = \omega(x_1,..,x_n)$,on a un mot ζ' en $\langle x_1,..,x_n \rangle$ tel que $\zeta' =_{G'} \zeta$ .L'image de ζ' par $\tilde{\varphi}$ est le même mot ,qui est librement égal à un élément de la forme $p_1 r_{i_1}^{\varepsilon_1} p_1^{-1} \ldots p_k r_{i_k}^{\varepsilon_k} p_k^{-1}$ où les r_i sont des relateurs de G .Or tout relateur de G est un relateur de G' et donc $\zeta =_{G'} \zeta' =_{G'} 1$ .Ainsi $\ker \tilde{\varphi} \leq gp_{G'}(\langle r_1,..,r_{m+1} \rangle)$,et donc $\tilde{\varphi}$ est un isomorphisme de G' dans G . □

Condition nécessaire

Supposons que G admette deux présentations finies π et π' que l'on notera $\langle a_i / r_j(a_i) \rangle$ et $\langle a'_i / r'_j(a'_i) \rangle$.

Puisque les deux présentations représentent le même groupe il y a des mots α'_i en a_i représentant les a'_i .Alors les $r'_j(\alpha'_i)$ sont conséquences des $r_j(a_i)$ (i.e. sont dans le sous-groupe normal engendré par les $r_j(a_i)$) .De même il y a des mots α_i en a'_i

représentant les a_i ,et les $r_j(\alpha_i)$ sont conséquences des $r'_j(a'_i)$.
On effectue alors les transformations de Tietze suivantes :

$$< a_i \,/\, r_j(a_i) >$$

$$< a_i \,/\, r_j(a_i) \,;\, r'_j(\alpha'_i) > \qquad \text{par } T_1$$

$$< a_i \,;\, a'_i \,/\, r_j(a_i) \,;\, r'_j(\alpha'_i) \,;\, a'_i = \alpha'_i > \qquad \text{par } T_2$$

$$< a_i \,;\, a'_i \,/\, r_j(a_i) \,;\, r'_j(a'_i) \,;\, r'_j(\alpha'_i) \,;\, a'_i = \alpha'_i > \quad \text{par } T_1$$

$$< a_i \,;\, a'_i \,/\, r_j(a_i) \,;\, r'_j(a'_i) \,;\, a'_i = \alpha'_i > \qquad \text{par } T_1^{-1}$$

$$(*) \quad < a_i \,;\, a'_i \,/\, r_j(a_i) \,;\, r'_j(a'_i) \,;\, a'_i = \alpha'_i \,;\, a_i = \alpha_i > \quad \text{par } T_2$$

De même on peut tranformer la présentation π' en (*) par une suite finie de transformations de Tietze .Et ,en considérant les transformations inverses ,(*) se transforme π' .On a alors une suite finie de transformations de Tietze :

$$\pi \longrightarrow \ldots \longrightarrow (*) \longrightarrow \ldots \longrightarrow \pi' \qquad \text{C.Q.F.D.} \blacksquare$$

Remarques Si l'on se permet de faire intervenir dans les transformation ,une infinité de générateurs ou relateurs ,le théorème se généralise aux présentations quelconques .La démonstration est en tout point similaire .

Ce résultat caractérise combinatoirement des présentations (finies) d'un même groupe ,tout en fournissant des opérations élémentaires permettant de changer une présentation d'un groupe ,en une autre .Il ne fournit néamoins pas de procédure effective permettant de décider si deux présentations données ,définissent un même groupe.Cependant pour une présentation finie d'un groupe G,les transformations de Tietze permettent d'établir un algorithme énumérant toutes les présentations finies de G .Ainsi pour des groupes dont on connait une présentation finie canonique ,on peut énumérer toutes ses présentations finies .C'est le cas des groupes libres de rang fini (avec pour présentation $<x_1 \ldots x_n / >$,des groupes abéliens (théorème de Kronecker) ,des groupes finis (relateurs $x_i x_j = x_k$) ,du groupe trivial (<a / a>) ,etc ... .

COROLLAIRE I.2.1 : On peut construire un algorithme ,qui pour une présentation finie quelconque ,énumère toutes les présentations finies du même groupe .

Démonstration : Nous allons construire un tel algorithme .

Considérons les transformations élémentaires de Tietze $T_1, T_1^{-1}, T_2, T_2^{-1}$ .Une telle transformation sera dite de **rang k** (k ∈ ℕ),lorsqu'une des conditions suivantes est satisfaite :

-Il s'agit d'une transformations T_1 ou T_1^{-1} portant sur un relateur R **dérivable en k étapes** ,i.e obtenu à partir du mot vide par au plus k opérations consistant à insérer ou à supprimer un relateur (autre que R) de la présentation ,ou un relateur trivial .

-Il s'agit d'une transformation T_2 ou T_2^{-1} ,portant sur un générateur α_{n+1} et un relateur $\alpha_{n+1} = \omega(\alpha_1,..,\alpha_n)$,tel que le mot ω soit de longueur au plus k .

Pour une transformation T quelconque ∃ k ∈ ℕ ,tel que T soit de rang k .De plus T est de rang k' pour tout k'≥ k .

Si l'on se donne une présentation finie ,alors pour k ∈ ℕ ,il y a un nombre fini de transformations de rang k pour cette présentation .De plus il y a une procédure finie les déterminant toutes :

-On détermine toutes les opérations T_1 réalisables ,en énumérant tous les éléments dérivables en k étapes .Il y a un nombre fini de relateurs et de générateurs et donc aussi d'opération T_1 .

-On détermine toutes les opérations T_1^{-1},En considérant pour chaque relateur de la présentation ,tous les mots dérivables en k étapes à partir des autres relateurs .Puisqu'il y a un nombre fini de générateurs et de relateurs on peut décider(après réduction libre des mots obtenus) pour chaque relateur s'il est dérivable des autres en moins de k étapes ,et ainsi déterminer toutes les transformations T_1^{-1}.

-On détermine toutes les transformation T_2 ,en considérant tous les mots de moins de k lettres ,qui bien sûr sont en nombre fini .

-Pour déterminer les opérations T_2^{-1},on repère les générateurs n'apparaissant que dans un unique relateur .On peut alors appliquer T_2^{-1},uniquement lorsqu'après réduction cyclique du relateur ,le générateur considéré à une unique occurence ,et le relateur est de longueur k + 1 .De même que précedemment il n'y a qu'un nombre fini de possibilités .

L'algorithme d'énumération est le suivant :

-Etape 1 : Enumérer et appliquer à la présentation toutes les transformations de rang 1 . On obtient un ensemble fini de présentations (finies) $\mathfrak{P}_1$

-Etape i : Enumérer toutes les transformations de rang i appliquables à des éléments de $\mathfrak{P}_{i-1}$,et les appliquer . On obtient un ensemble fini de présentations (finies) $\mathfrak{P}_i$.

Considérons deux présentations finies d'un même groupe , Π et Π' . Alors il y a une suite finie de présentations (f.) ,$(\Pi_0;..;\Pi_n)$ telle que $\Pi = \Pi_0$ et $\Pi' = \Pi_n$,et une suite finie de changements de Tietze $(t_1;..;t_n)$,tels que $\forall\ i \in \langle 1,..,n\rangle$ t_i change Π_{i-1} en Π_i . On note $(rg_1;..;rg_n)$ la suite finie d'entiers ,telle que rg_i est le rang de t_i . On applique l'algorithme précédent à Π_0 . Alors :

- Π_1 est obtenu à l'étape rg_1
- si $rg_2 \leq rg_1$ alors Π_2 est obtenu à l'étape $rg_1 + 1$
- sinon Π_2 est obtenu à l'étape rg_2

-etc ...

Et ainsi soit M tel que $rg_m = \max (rg_1,..,rg_n)$. Alors Π_n est obtenu exactement à la $(rg_m + n - m)^{ème}$ étape . Toute présentation finie présentant le même groupe que Π est donc énumérée au bout d'un temps fini. L'algorithme néamoins tourne indéfiniment et l'on ne sera jamais en possession de toutes les présentations finies du même groupe . ■

COROLLAIRE I.2.2 : On peut construire un algorithme ,qui pour deux présentations finies d'un même groupe permet d'exprimer tout élément du groupe donné par un mot dans une des présentations ,comme mot dans l'autre présentation .

Démonstration : Nous allons construire un tel algorithme .

Etant données deux présentations Π et Π' finies d'un même groupe . On peut utiliser l'algorithme précédent pour énumérer toutes les présentations finies ,représentant le même groupe que Π'. Alors au bout d'un temps fini ,on obtiendra Π' . Cet algorithme permet en outre d'expliciter une suite de changements de Tietze $(t_1,..,t_N)$ ainsi qu'une suite de présentations $(\Pi_0,..,\Pi_N)$,menant

de Π à Π' (i.e. $\Pi = \Pi_0$; $\Pi' = \Pi_N$) .

Considérons un mot ω exprimé dans Π .L'algorithme suivant permet d'écrire un mot de Π en un mot représentant du même élément dans Π' .

- Soit un mot ω exprimé dans Π_i .Si t_i est une opération de la forme T_2^{-1} ,de générateur α et de relateur $\alpha = m$ où m est un mot sur les générateurs autres que α,alors ω' est le mot obtenu à partir de ω en remplaçant dans ω les occurences de α par m Sinon $\omega' \equiv \omega$.ω' est exprimé dans Π_{i+1} ,et représente le même élément du groupe que ω .

Soit un mot exprimé dans Π_0 ,On réitère l'opération l'opération précédente .On fini par aboutir à un mot dans Π_N ,exprimant le même élément que ω . ■

I.3 PROBLEMES DE DEHN

On considère un groupe G donné par une présentation finie Π . Les problèmes de Dehn sont les suivants .

-Problème de l'égalité Existe-t-il un algorithme permettant de décider pour tout couple de mots sur les générateurs ,s'ils représent le même élément du groupe .

-Problème du mot Existe-t-il un algorithme permettant de décider pour tout mot ω sur les générateurs ,si $\bar{\omega} = 1$.

-Problème de la conjugaison Existe-t-il un algorithme permettant de décider pour tout couple de mot ,s'ils représentent des éléments conjugués du groupe (i.e si pour x et y ,$\exists$ $h \in G$ tel que $h^{-1}\bar{x}\,h = \bar{y}$ dans G) .

-Problème du mot généralisé Existe-t-il un algorithme qui pour $n + 1$ mots $a_1,\ldots,a_n,x$,décide si x est dans le sous-groupe engendré par $a_1,\ldots,a_n$.

-Problème de l'isomorphisme Existe-t-il un algorithme permettant de décider pour tout couple de présentations finies Π et Π' ,si $gp(\Pi) \cong gp(\Pi')$.

Il faut remarquer que les problèmes de Dehn portent sur une présentation d'un groupe et non sur le groupe. Nous verrons néamoins que pour les 4 premiers ,leur résolution est indépendante de la présentation f.e. choisie .

On distingue dans les problèmes de décision sur les présentations ,un problème **local** ,d'un problème **global** ,i.e. portant sur les mots ,ou sur les présentations .Le problème de l'isomorphisme est global ,alors que les autres problèmes de Dehn sont locaux. Le problème de l'isomorphisme semble être un analogue global du problème de l'égalité .Dans les deux cas ,deux mots ou deux présentations sont équivalentes,si l'on peut aller de l'un(e) à l'autre par une finie de transformations élémentaires .Dans les deux cas le problème de décision consiste à décider si l'on peut construire entre deux éléments un cheminement .Dans la pratique ,cependant la résolution du problème de l'isomorphisme s'avère être bien plus complexe .

Ces problèmes n'ont de sens que pour des présentations que l'on peut expliciter ,c'est pourquoi on les définit pour des présentations finies .Les problèmes locaux peuvent néamoins être étendus à une classe plus large ,les présentations récursives .Une présentation est dite récursive si elle admet un nombre fini de générateurs ,et si l'on peut énumérer ses relateurs (la notion d'énumération sera formalisée dans le paragraphe I.4) . En particulier ,toute présentation finie est récursive .

Pour de telles présentations ,on a des algorithme de semi-décision (i.e. d'énumération) .On a déjà vu (corollaire I.2.1)que l'on peut énumérer toutes les présentations finies d'un groupe f.p. .Pour les problème locaux ,on peut pour un groupe f.e. ,énumérer sous une forme canonique ,tous les éléments du groupe triviaux ,égaux à un même élément ,conjugués d'un élément ,ou s'écrivant sur des générateurs donnés .Si la présentation est récursive ,alors on peut énumérer tous les changements élémentaires ,et ainsi tous les mots vérifiant les propriétés respectives .

Si l'on veut cependant décider ,par exemple, si un mot est trivial ,un algorithme de semi-décision laissera l'utilisateur devant des indécisions .En effet pour tout élément non trivial ,l'utilisateur à un temps donné ne pourra décider si l'élément

n'est pas trivial ou bien si ,tout simplement la procédure ne l'a pas encore déterminé (les procédures d'énumération sont en général infinies) .De façon générale il en est de même pour tout les autres problèmes ,un algorithme d'énumération ne résoud pas le problème : il permet d'énumérer une liste perpétuellement incom--plète .Remarquons néamoins que dans la cas d'une classe de groupe f.p. pour laquelle tout groupe admet une (unique) écriture canonique ,l'algorithme d'énumération établit au corollaire I.2.1 ,nous permet de résoudre le problème de l'isomorphisme dans cette classe .En effet étant données deux présentations ,on peut énumérer toutes les autres présentations des même groupes .On finira par aboutir à deux présentations canoniques ,et l'on pourra décider si elles représentent le même groupe .Ainsi ,c'est le cas des groupes finis ,abéliens ,libres .En pratique cette algorithme ,ainsi que tout autre algorithme ,utilisant une énumération par changements de Tietze ,n'est pas effectif .

Dans la suite ,étant donnée une présentation Π ,on note respectivement , $\mathcal{WP}(\Pi)$,$\mathcal{Sg}(\Pi)$,$\mathcal{CP}(\Pi)$,$\mathcal{GWP}(\Pi)$,$\mathcal{Iso}\mathcal{P}(\Pi)$;le problème du mot ,le problème d'égalité ,le problème de conjugaison ,le problème du mot généralisé ,et le problème de l'isomorphisme (resp^t) ,sur Π .

Etant donnés deux problèmes de décision A et B ,on dit que A est **réducible** à B ,et l'on note $A \leq B$,si un algorithme pour B permet d'établir un algorithme pour A ,c'est à dire si une réponse positive au problème A est nécessaire à une réponse positive au problème B .Ainsi $\mathcal{WP}(\Pi) \leq \mathcal{Sg}(\Pi)$,puisque si l'on peut décider si deux mots sont égaux ,on peut décider lorsqu'un mot est trivial .Réciproquement deux mots ω et μ sont égaux ssi $\omega\,\mu^{-1} = 1$,ainsi $\mathcal{Sg}(\Pi) \leq \mathcal{WP}(\Pi)$.On note $\mathcal{Sg}(\Pi) \equiv \mathcal{WP}(\Pi)$ .La relation $\equiv$ est une relation d'équivalence sur l'ensemble des problèmes de décision ,les classes d'équivalences admettent un ordre partiel $\leq$,et sont appelées **degrés** (cette notion se formalise en théorie des fonctions récursives .Etant donnés ,deux sous-ensemble de $\mathbb{N}^p$,A et B ,on écrit $A \leq B$,si χ_A est construit à partir de χ_B et des fontions élémentaires ,grâce aux schémas de construction des fonctions récursives .On démontre que $\equiv$ est une relation d'équivalence sur les sous-ensembles de $\mathbb{N}^p$,$p \in \mathbb{N}$,qu'il existe

une infinité de classes d'équivalence ,et que la relation $\leq$ établit une structure d'ordre partiel sur les classes d'équivalence ,avec une borne maximale $0'$ degré du problème d'arrêt de la machine de Turing universelle ,et une borne minimale 0 ,classe des ensembles récursifs) .

On ne s'interessera plus au problème de l'égalité,sa décidabilité est dans tous les cas équivalente à celle du problème du mot ,et de plus un algorithme pour le problème du mot fournit (de façon explicite) ,un algorithme pour le problème d'égalité .On peut remarquer d'autres cas de réducibilité dans les problèmes de Dehn

$\mathcal{WP}(\Pi) \leq \mathcal{EP}(\Pi)$,ceci car pour décider si un mot est trivial ,il suffit de décider s'il est conjugué au mot vide .

$\mathcal{WP}(\Pi) \leq \mathcal{GWP}(\Pi)$,car pour décider si un mot est trivial ,il suffit de décider s'il appartient au sous-groupe engendré par le mot vide .

Ainsi ,si l'on démontre que le problème de conjugaison ,ou le problème du mot généralisé sont résolubles pour Π ,alors le problème du mot est résoluble pour Π (et par la même le problème de l'égalité) .Dualement ,si l'on montre que le problème du mot n'est pas résoluble il en est de même pour les problèmes de conjugaisons ,et du mot généralisé .

LEMME I.3.1 : Dans la classe des présentations récursives ,les problèmes du mot généralisé ,du mot ,et de conjugaison sont des invariants algébriques ,i.e ,pour deux présentations récursives Π_1 ,et Π_2 d'un même groupe $\mathcal{WP}(\Pi_1) \equiv \mathcal{WP}(\Pi_2)$; $\mathcal{EP}(\Pi_1) \equiv \mathcal{EP}(\Pi_2)$; $\mathcal{GWP}(\Pi_1) \equiv \mathcal{GWP}(\Pi_2)$.

Démonstration : Considérons deux présentations $\Pi_1 = \langle S_1/R_1 \rangle$ et $\Pi_2 = \langle S_2/R_2 \rangle$,d'un même groupe .Alors ,il existe un isomorphisme $\varphi : F(S_1)/gp(R_1) \longrightarrow F(S_2)/gp(R_2)$ qui envoie les générateurs de Π_1 disons a_i,sur des mots de Π_2 disons α_i .Remarquons que générateurs sont en nombre fini .

Si il existe un algorithme résolvant $\mathcal{WP}$, $\mathcal{EP}$,$\mathcal{GWP}$,pour Π_2 ,alors il existe un algorithme les résolvant dans Π_1 .Puisque les générateurs de Π_1 ,sont en nombre fini il existe un algorithme changeant un mot de Π_1 ,en un mot de Π_2 (Il suffit de se doter

d'une table de correspondance $a_i \longleftrightarrow \alpha_i$) ,et alors puisque ces éléments représentent le même élément de groupe ,et que la validité des propriétés (être trivial ,conjugué d'un élément ...) ne dépend pas de la présentation ,pour des mots ω de Π_1 , on détermine leur écriture dans Π_2 ,et puisque l'on peut alors décider de tous les problèmes dans Π_2 ,on le peut aussi dans Π_1 .

De façon similaire on peut voir que si des algorithmes existent pour Π_1 ,alors il en est de même pour Π_2 . ■

Les algorithmes en question ne sont pas donnés constructivement ,c'est à dire que si l'on se dote ,d'un algorithme résolvant ,par exemple ,le problème du mot pour une présentation récursive d'un groupe G donné ,alors on sait qu'il existe un tel algorithme pour toute présentation récursive de G ,mais on ne sait en général pas l'expliciter .En fait la constructivité de cet algorithme est réductible à la constructivité d'un isomorphisme donné explicitement ,c'est à dire par l'image des générateurs (et inversement) .

Dans la classe des présentations finies ,le corollaire I.2.2 nous permet étant données deux présentations ,de construire un tel isomorphisme .On a ainsi un résultat plus fort :

LEMME I.3.2 : Si l'on dispose d'un algorithme pour résoudre le problème du mot généralisé (resp^t du mot ,de la conjugaison) ,pour une présentation finie d'un groupe G ,alors on peut construire un tel algorithme pour toute présentation finie de G .

Ainsi l'on peut parler pour un groupe G f.p.(ou rec.p.) de $\mathcal{WP}(G)$,$\mathcal{CP}(G)$,$\mathcal{GWP}(G)$.Dans la suite nous parlerons de ces problèmes pour des classes particulières de groupe f.p. .Lorsque l'on donnera explicitement un algorithme ,on le donnera pour une présentation finie canonique d'un groupe ;un algorithme pourra alors être construit pour chaque présentation finie de ce groupe ,grâce aux algorithmes donnés dans le corollaire I.2.2 et le lemme I.3.1 .Cet algorithmes ne sont néamois pas effectifs .

Definition : On dit d'une propriété de groupe qu'elle est **héréditaire** dans une classe de groupe C ,lorsque si un groupe de C vérifie cette propriété ,il en est de même de tous ses

sous-groupes qui appartiennent à C .

LEMME I.3.3 : Avoir un problème du mot résoluble est un propriété héréditaire dans la classe des groupes recursivement présentés .

Démonstration : Etant données deux groupes H et G par une présentation récursive ,tel que H est un sous-groupe de G ,alors il existe une application injective qui envoie les générateurs de H ,sur des mots de G.Le noyau de cet application est trivial ,et ainsi un mot de H est trivial ssi son image est trivial .Si le problème du mot est résoluble dans G ,alors de même que pour le lemme I.3.1 ,il est résoluble dans H . ■

Remarque Le problème de la conjugaison ,n'est pas héréditaire dans la classe des groupes récursivement présentés ,comme nous le verrons dans la suite .

Définition : On dit d'une propriété de groupe P ,que c'est une **poly-propriété** ,si pour tout groupe G ,tout sous-groupe normal de G ,N ,si N et $G/_N$ vérifient P ,alors il en est de même de G .

Hall a démontré ,qu'être finiment présenté ,est une poly-propriété .

Lemme I.3.5 : être finiment présenté ,et avoir un problème du mot soluble est une poly-propriété .

Démonstration : Considérons un sous-groupe normal N de G .SI N et G/N sont finiment présentés,il en est de même de G (Hall) .On considère le plongement naturel $\Pi : G \longrightarrow G/_N$ .Etant donnée une une présentation finie $< S / R >$ de G ,on peut prendre une présentation finie (proposition I.1.3) de $G/_N$ ayant pour générateurs les images par Π des éléments de S ,et une présentation finie de N où les générateurs sont des mots sur S .De plus d'après le lemme I.3.2 ,la résolution du problème du mot ,est indépendante de la présentation .Supposons que N et $G/_N$ aient un problème du mot soluble .

Etant donnés un mot ω sur S ,$\omega =_G 1$ ssi $\Pi(\omega) = 1$ dans $G/_N$,et $\bar{\omega} = 1$ dans N .Pour décider si un mot $\omega = 1$ dans G ,on teste si $\Pi(\omega) = 1$ dans $G/_N$ .Si ce n'est pas le cas ,alors $\omega \neq_G 1$.

Si c'est le cas ,alors $\bar{\omega} \in N$ .Puisque N est f.p. ,on peut énumérer tous les éléments de N ,et leurs écritures dans G (simplement ,en énumérant tous les mots de N ,et en leur appliquant toutes les transformations utilisant des éléments de R) .Alors on finit par trouver une écriture de $\bar{\omega}$ sur les générateurs de N .On peut alors décider si $\bar{\omega} =_N 1$,et donc si $\omega =_G 1$. ■

Remarque : En particulier toute extension d'un groupe ayant un problème du mot soluble ,par un groupe ayant un problème du mot soluble ,a un problème du mot soluble .(en particulier ,pour les produits directs ,et semi-directs (ou split extension)).

Avoir un problème du mot généralisé (resp^t de la conjugaison) ,soluble n'est pas une poly-propriété (Nous établiront en III.2 ,l'existence d'une split extension de 2 groupes ayant ces problèmes soluble ,pour laquelle ils ne sont pas solubles).

I.4 MACHINES DE TURING

Pour discuter de l'existence d'algorithme ,nous avons d'abord besoin de formaliser la notion intuitive d'algorithme .C'est ce que nous nous proposons de faire dans cette partie .

Un algorithme est un procédé permettant de décider pour des éléments donnés explicitement (par une suite finie de symbôle ,de telle qu'un utilisateur ,peut pour chaque élément ,l'écrire sous sa forme explicite) ,s'ils vérifient ou non une certaine propriété ,c'est à dire s'ils appartiennent à un certain sous-ensemble de l'ensemble de ces éléments .L'existence de tels algorithmes ne dépend pas de la façon d'expliciter les éléments ,mais de la propriéte étudiée .On dit intuitivement qu'une propriété (resp^t un ensemble) est calculable ,si l'on peut reconnaître grâce à un procédé mécanique (ou "machine") ,si un élément la vérifie (resp^t lui appartient) ,ou non .Cette notion de calculable a été formalisée dans les années 30 ,en la notion de récursivité ,par *Turing* ,*Godel* ,*Church* (...) de diverses façon qui sont toutes équivalentes .La thèse de *Church* affirme que la récursivité est une définition rigoureuse de la calculabilité

.Elle est vérifiée par l'expèrience depuis plus de 50 ans ,on n'a encore jamais trouvé un ensemble qui soit calculable (au sens intuitif du terme) ,et qui ne soit pas récursif (On ne peut démontrer la thèse de Church ,puisque ce n'est pas une assertion mathématique) .

Nous utilisons la définition de Turing ,qui n'est pas la plus maniable ,mais qui dans notre cas sera la plus pratique .La théorie des fonctions récursives aurait ,par exemple ,été plus naturelle pour définir la notion de réducibilité .

Dans la suite nous continuerons à parler informellement d'algorithme .Par exemple on établira des algorithmes ,plutôt que de démontrer que l'ensemble en question est récursif .Ce serait un travail très laborieux ,et en fait la théorie ne sert qu'à démontrer qu'un problème de décision est **récursivement insoluble** ,i.e. qu'il n'existe pas d'algorithme permettant de décider (on emploiera aussi le terme **récursivement soluble**) .C'est la raison pour laquelle ,il a fallu attendre 1930 ,pour que ces notions apparaissent ,puisque l'on pensait avant les travaux de Gödel que des algorithmes existaient toujours .

Turing utilise des "machines" formelles idéales ,et élémentaires ,permettant (en principe) d'effectuer tout ce qu'une machine peut faire .De telles machines sont appelées **machines de Turing .**

Dans cette partie ,parallèlement au discours formel ,nous nous donnerons une interprétation intuitive des notions employées.

De façon informelle ,on peut se représenter une machine de turing comme une boite ; composée d'une tête de lecture-écriture ,parcourant par une bande de longueur illimitée .La bande est constituée d'une suite de cases , chaque case contenant un symbôle ,pris sur un alphabet fini $S=(s_0,...,s_n)$ (on considèrera que le symbôle so représente un "blanc").(c.f. fig.1).Les actions de la machine consistent à scanner une case ;lire ou écrire sur une case scanné ;déplacer sa tête de lecture sur la bande (de façons à scanner une autre case) .

La machine possède un nombre fini d'états $q_0, q_1, \ldots, q_m$. A chaque instant , elle se trouve dans un état donné ,sa tête de lecture-écriture positionnée sur une case de la bande .Son action est alors déterminée par sa structure initiale , son état ,et le symbôle scanné sur la case .La machine peut alors effectuer une des actions suivantes :

(i) Remplacer le symbôle scanné s par le symbôle s' ,et passer à l'état q' .

(ii) Se déplacer d'une case vers la droite et passer à l'état q' .

(iii) Se déplacer d'une case vers la gauche et passer à l'état q' .

où $s, s' \in S$; $q' \in \{q_0, \ldots, q_m\}$.

La machine se trouve initialement à l'état q_1 , sa tête étant positionnée sur la première case ,à gauche ,non vide .Pour effectuer le calcul d'un mot ω de $\mathcal{G}^*$ (ensemble des mots sur l'alphabet $\mathcal{G}$), l'utilisateur fait démarrer la machine avec ω inscrit sur la bande .

Dans la suite on considère $\mathcal{G} = \{s_0, \ldots, s_n\}$ et $\mathcal{Q} = \{q_0, \ldots, q_n\}$

Définitions : Un **Quadruple** sur l'alphabet $\mathcal{G}$,et l'ensemble d'états $\mathcal{Q}$,est un 4-uplet d'une des formes suivantes

q s s'q'
q s R q'
q s L q' où $q, q' \in \mathcal{Q}$, $s, s' \in \mathcal{G}$

On appelle **préfixe** d'un quadruple ,le 2-uplet formé de ses 2 premiers éléments (q,s) .

Définition : Une **machine de Turing** ,est un ensemble fini de quadruples sur un alphabet et un ensemble d'états ; tel que pour tout couple de quadruples ,leur préfixe sont distincts (on dit qu'il n'y a pas d'ambiguité) .

Remarque Lorsque l'on parlera d'une machine T sur un alphabet $\mathcal{S}$ et un ensemble d'état Ω ,on prendra $\mathcal{S}$ et Ω minimum ,i.e tels que tout élément de $\mathcal{S} \cup \Omega$ ait une occurence dans un quadruple de T .

Informellement ,le quadruple q s s'q' ; (respectivement q s R q' ,q s L q') correspond à l'instruction : "lorsque l'état est q ,le symbôle lu est s ;effectuer l'action (i) (respectivement (ii) ,(iii)) .Ainsi la définition d'une machine de Turing formelle ,correspond informellement à ce que nous avons appelé structure initiale de la machine i.e. ,les règles déterminant les actions de la machine .

Définition : Une **description instantanée** est un mot sur $\mathcal{S} \cup \Omega$ ayant exactement une occurence d'un élément de Ω .

Une description instantanée $\alpha \equiv s_i \ldots s_k q_l s_j \ldots s_n$ doit être informellement interprétée comme "description instantanée" de la machine i.e., le mot inscrit sur la bande est $s_i \ldots s_n$,l'état est q_l, le symbôle lu est s_j (symbôle se trouvant immédiatement à droite de q_l).

Définition : Considérons une machine de Turing T , α et β deux descriptions instantanées ; on dit que $\alpha \longrightarrow \beta$ est un **mouvement élémentaire** si il existe P et Q mots sur S (éventuellement vides) ,tel que l'on a une des conditions suivantes :

(i) $\begin{cases} \alpha \equiv P\ q_i s_j\ Q \\ \beta \equiv P\ q_l s_k\ Q \end{cases}$ où $q_i s_j s_k q_l \in T$

(ii) $\begin{cases} \alpha \equiv P\ q_i s_j s_k\ Q \\ \beta \equiv P\ s_j q_l s_k\ Q \end{cases}$ où $q_i s_j\ R\ q_l \in T$

(iii) $\begin{cases} \alpha \equiv P\ q_i s_j \\ \beta \equiv P\ s_j q_l s_o \end{cases}$ où $q_i s_j\ R\ q_l \in T$

(iv) $\begin{cases} \alpha \equiv P\ s_k q_i s_j\ Q \\ \beta \equiv P\ q_l s_k s_j\ Q \end{cases}$ où $q_i s_j\ L\ q_l \in T$

$$(v)\ \begin{cases} \alpha \equiv q_i s_j Q \\ \beta \equiv q_i s_o s_j Q \end{cases} \qquad \text{où} \quad q_i s_j L\, q_l \in T$$

Remarques On interpretera $\alpha \longrightarrow \beta$,comme une opération élémentaire de la machine .

Les cas (iii) et (v) formalisent la présence d'une bande infinie à droite et à gauche .

Etant donné qu'il n'y a jamais d'ambiguité ,$\alpha \longrightarrow \beta$ et $\alpha \longrightarrow \gamma \Longrightarrow \beta = \gamma$.

Définitions : **Un calcul de T** est une suite finie de descriptions instantanées $\alpha_1,\ldots,\alpha_n$ avec $\alpha_i \longrightarrow \alpha_{i+1}$ pour tout i de $\langle 1,..,n-1\rangle$,et tel que pour toute description instantanée δ , on n'a pas $\alpha_n \longrightarrow \delta$. α_1 (resp^t α_n) est alors appelé **description initiale** (resp^t **terminale**).

Soit ω un mot sur $\mathcal{G}$,on dit que $T(\omega)$ existe si il existe un calcul de T ,avec pour description initiale , $q_1\omega$.

Soit $e(T) = \left\{ \omega \in \mathcal{G}^* \ / \ T(\omega) \text{ existe} \right\}$ .On dit que T **énumère** e(T) .

Définition : $E \subseteq \mathcal{G}^*$,est dit **récursivement énumérable** si il existe une machine de turing qui énumère E .

Définition : $E \subseteq \mathcal{G}^*$ est dit **récursif** si E et $\mathcal{G}^* \setminus E$ sont récursivement énumérables .

Si un ensemble E est récursif alors il existe un algorithme décidant pour un élément donné écrit sur $\mathcal{G}$ s'il appartient à E .En effet il existe deux machine de Turing énumérant E ,et ainsi on peut savoir pour un élément donné ω si il appartient à E ou non ,simplement en énumérant E et $\mathcal{G}^* \setminus E$ .Au bout d'un temps fini ,ω sera listé ,soit comme élément de E ,soit comme élément de $\mathcal{G}^* \setminus E$

THESE DE CHURCH : La récursivité est une définition rigoureuse de la calculabilité .

On se donne une présentation finie Π de G ,de famille génératrice S .Ainsi les problèmes de Dehn deviennent :

Problème du mot : $\{ \omega \in \mathcal{M}(S) / \omega =_G 1 \}$ est-il récursif ?

Problème de la conjugaison : $\{ \omega,v \in \mathcal{M}(S) / \exists h \in G ; h^{-1}\omega h = v \}$ est-il récursif ?

Problème du mot généralisé : pour chaque famille génératrice $a_1,..,a_n$,$\{ \omega \in \mathcal{M}(S) / \omega =_G$ mot $(a_1,..,a_n) \}$ est-il récursif ?

Problème de l'isomorphisme : $\{ (\Pi,\Pi') / gp(\Pi) \cong gp(\Pi') \}$ est il récursif ?

Nous avons déjà vu que l'on dispose d'un algorithme d'énumération ,ce qui signifie avec la thèse de Church ,que ces ensembles sont récursivement énumérables .Néamoins pour un ensemble récursivement énumérable non récursif ,on peut décider lorsqu'un élément est O.K. ,mais pas s'il ne l'est pas .En effet un tel ensemble est toujours infini (car sinon aprés énumération ,on connait tous les éléments qui ne le sont pas) tout ce que l'on peut faire c'est énumérer cet ensemble ,et pour un élément qui ne sera jamais énuméré ,l'utilisateur ne peut pas savoir s'il le sera un jour .De tels ensembles existent .Ce résultat est la source de tous les problèmes d'indécidabilité en Mathématiques .

Proposition I.4.1 : Il existe un ensemble récursivement énumérable ,non récursif .

Pour une démonstration voir par exemple [35]

Proposition I.4.2 : L'intersection ou la réunion de deux ensembles récursivement énumérables (resp^t récursif) est r.e. (resp^t rec.) .

Démonstration : La notion de r.e. et de recursif peut se formaliser par la théorie des fonctions récursives .Alors le résultat est trivial puisque :

$\chi_{A\cap B} = \chi_A \cdot \chi_B$,et $\chi_{A\cup B} = \chi_A + \chi_B - \chi_{A\cap B}$ ■

Définition : On appelle **état d'arrêt** d'une machine T ,tout état ayant une occurence dans une description instantanée

terminale .

Le résultat suivant sera utile à la suite .

LEMME I.4.1 : Pour toute machine de Turing ,il existe une machine énumérant le même ensemble ,et dont tous les états d'arrêt sont q_0 .On dit alors que q_0 est l'état d'arrêt de la machine .

Démonstration : Remarquons qu'une machine de Turing s'arrête ,lorsque pour un état q est un symbôle s ,il n'existe pas de quadruple ayant pour préfixe (q,s) .Pour de tels couples (q,s) contruisons une nouvelle machine d'ensemble d'état $Q \cup \langle q_0 \rangle$ et de même alphabet ,ayant même quadruples que T ,plus les quadruples q s s q_0 ,ils sont en nombre fini .De plus la machine a alors pour état d'arrêt q_0 . ■

Remarque : Pour formaliser la notion de présentation récursive ,on a besoin que R soit un ensemble de mots positifs .Mais étant donné une présentation de groupe ,on peut la transformer en une présentation ou les relateurs sont des mots positifs .Il suffit de rajouter des générateurs x_i ,et des relateurs $x_i = a_i^{-1}$,où les a_i sont les générateurs ,et changer dans les relateurs ,des occurences de a_i^{-1} ,par x_i .

I.5 EXTENSIONS DE BRITTON ET HNN EXTENSIONS

Notations : Soient une présentation $G = \langle S / D \rangle$,des lettres $t_1,\ldots,t_n$ n'appartenant pas à S ,et des mots $r_1,\ldots,r_m$,sur $S \cup \langle t_1,\ldots,t_n \rangle$ .On note $\langle S ; t_1,\ldots,t_n / D ; r_1,\ldots,r_m \rangle$,ou plus simplement $\langle G ; t_1,\ldots,t_n / r_1,\ldots,r_m \rangle$,la présentation suivante $\langle S \cup \langle t_1,\ldots,t_n \rangle / D \cup \langle r_1,\ldots,r_m \rangle \rangle$ .Dans cette partie nous confondrons groupes et présentations de groupe .

Soient $E = \langle S / D \rangle$ une présentation ,et $V = \langle 1,\ldots,n \rangle$ $I = \langle 1,\ldots,m \rangle$ .Une seconde présentation E^* ,a pour lettres stables $\langle p_v ; v \in V \rangle$,et pour base E ,si :

$$E^* = \langle S ; p_v , v \in V / D ; p_{v(i)}^{-1} A_i p_{v(i)} = B_i , i \in I \rangle$$

où v ,w : $I \longrightarrow V$,et A_i et B_i sont des mots sur S .

On note $p_y \simeq p_z$ $(y,z \in V)$,si $p_y = p_z$,dans le groupe obtenu à en rajoutant les relateurs $s = 1$,$\forall s \in S$ à la présentation de E^*. $\simeq$ est une relation d'équivalence sur $\langle p_v , v \in V \rangle$,qui induit une relation d'équivalence sur I .Soit $K(v) = \langle i \in I / p_i \simeq p_v \rangle$ $(v \in V)$,classe d'équivalence de la relation induite sur I .$A(v)$ dénote le sous-groupe de E engendré par $\langle A(i) , i \in K(v) \rangle$,$B(v)$ le sous-groupe de E engendré par $\langle B(i) , i \in K(v) \rangle$ .On dit que E^*(défini comme précédemment) satisfait la **condition de l'isomorphisme généralisée** (G.I.C),si pour tout $v \in V$,la fonction $\varphi : A(v) \longrightarrow B(v)$,telle que $\forall i \in I$ $\varphi(A(i)) = B(i)$,s'étend en un isomorphisme entre $A(v)$ et $B(v)$.

Définition : E^* est une **extension de Britton** de E si E^* a pour base E ,pour lettres stables $(p_1,..,p_n)$,et si E^* satisfait la condition de l'isomorphisme généralisé .

Remarque Dans ce cas les relateurs additionnels ,sont appelés relateurs de l'extension .

Soient S et T ,des mots sur S ,et $y,z \in V$ .On dit que S p_y produit $p_z T$,si S p_y peut être transformé en $p_z T$ par une suite d'opérations de la forme :

$$X\ A_i p_{z(i)} Y \longrightarrow X\ p_{y(i)}\ Y$$

$$X\ A_i^{-1} p_{y(i)} Y \longrightarrow X\ p_{z(i)}\ B_i^{-1}\ Y$$

où X et Y sont des mots de S .

Théorème I.5.1 : *(Lemme de Britton)*

Soit E^* une extension de Britton de E ,ayant pour lettres stables P .Alors

(i) E est plongé dans E^* par l'inclusion sur les générateurs

(ii) Si $\omega = 1$ dans E^* ,alors ω contient un sous-mot d'une des formes (1) $p_y^{-1}\ C\ p_z$ ou (2) $p_y\ C\ p_z^{-1}$;où $p \in P$ et C est un mot sur S (générateurs de E) .Dans le cas (1) C est égal dans E à un mot $\mu(A_i) \in A(y)$,et $\mu(A_i)\ p_z$ produit $p_y\ \mu(B_i)$ .Dans le cas (2) ,C est égal dans E à un mot $\mu(B_i) \in B(y)$,et $\mu(A_i)\ p_z$ produit $p_y\ \mu(B_i)$.

Remarque C'est le théorème fondamental de cette partie .Il est dû sous une forme simplifiée à J.L.Britton .

Démonstration : Soit $< a_v , v \in V >$ le groupe libre engendré par les a_v .Dans cette démonstration nous noterons $< X >_G$ le sous-groupe de G engendré par X .

On considère : $F = < a_v , v \in V > * E$

$G = < b_v , v \in V > * E$

et les sous-groupes $M_v = < a_{y(i)}^{-1} A_i a_{z(i)} ; i \in K(v) >_F$

$N_v = < b_{y(i)} B_i b_{z(i)}^{-1} ; i \in K(v) >_G$.

Alors $M_v = M_t$ ssi $K(v) = K(t)$ .De plus $< M_v ; M_t >_F \cong M_v * M_t$ si $K(v) \neq K(t)$,et à M_v sinon ; et $< M_v ; E >_F \cong M_v * E$,et ce pour tout $v \in V$ .Les considérations analogues sont valables pour N_v .

Puisque E^* vérifie G.I.C. ,alors $M_v \cong N_v$,par l'isomorphisme canonique .Nous prenons $Y = < a_{y(i)}^{-1} A_i a_{z(i)} ; i \in I >_F * E \subseteq F$

et $Z = < b_{y(i)} B_i b_{z(i)}^{-1} ; i \in I >_G * E \subseteq G$

et alors $Y \cong Z$ en étendant les fonctions $E \longrightarrow E$,et $M_v \longrightarrow N_v$ $\forall v \in V$(propriété des produits libres) ,qui envoie $a_{y(i)}^{-1} A_i a_{z(i)}$,sur $b_{y(i)} B_i b_{z(i)}^{-1}$ pour tout i .

Considérons $\bar{E} = < S ; a_v , b_v , v \in V / D ; a_{y(i)}^{-1} A_i a_{z(i)} = b_{y(i)} B_i b_{z(i)}^{-1} ; i \in I >$

Avec ce qui précède ,il est clair que $\bar{E} = F *_{Y=Z} G$.

L'application $S \longrightarrow S$,et $p_v \longrightarrow a_v b_v$,s'étend en un homomorphisme $E^* \longrightarrow \bar{E}$,puisque les relateurs de E^* ,sont envoyés sur les relateurs de $\bar{E}$.De plus il est injectif .Si si un mot $\omega (S, a_v b_v)$ est trivial dans $\bar{E}$,il l'est aussi dans le groupe obtenu à partir de $\bar{E}$,en rajoutant les relations $b_v = 1$ $\forall v \in V$ .Or ce groupe est clairement isomorphe à E^* ,avec $S \longrightarrow S$,et $a_v \longrightarrow p_v$ et si l'on compose ces deux homomorphismes on obtient l'identité .Ainsi ω^{-1} est trivial dans E^* .Ainsi puisque E se plonge dans $\bar{E}$,dans l'image de E^* ,E est plongé dans E^* par l'inclusion sur les générateurs .

Considérons le mot ω intervenant dans le théorème .On peut prendre ω librement réduit .

$$\omega \equiv S_1\, p_{v1}^{\alpha_1}\, S_2\, p_{v2}^{\alpha_2} \ldots S_{n-1}\, p_{vn}^{\alpha_n}\, S_n$$

où $n \geq 1$,$\alpha_i \neq 0$,et les S_i sont des mots dans E .
Puisque $\omega = 1$ dans E^* ,son image $\omega' \equiv S_1 (a_{v1} b_{v1})^{\alpha_1} \ldots (a_{vn} b_{vn})^{\alpha_n}$,est égal à 1 dans $\bar{E}$ .Or $a_i \in F \setminus Y$,$b_i \in G \setminus Z$,et les $S_i \in Y = Z$ donc le produit libre amalgamé $\bar{E} = F *_{Y=Z} G$,ω' a une écriture unique sous forme normale . Et alors pour tout i seul un des cas suivants est possible :

(1) $\alpha_i < 0$, $\alpha_{i+1} > 0$ et $a_{vi}^{-1} S_{i+1} a_{vi+1} \in Y$.

(2) $\alpha_i > 0$, $\alpha_{i+1} < 0$ et $b_{vi} S_{i+1} b_{vi+1}^{-1} \in Z$.

Considérons le cas (1) .Puisque Y est engendré par les $a_{y(i)}^{-1} A_i a_{z(i)}$,$i \in I$ et S ,et que ces un produit libre ,forcément $\exists\, v \in V$ tel que $a_{vi}^{-1} S_{i+1} a_{vi+1} \in M_v$ (puisqu'il doit avoir une écriture sous forme normale de longueur 1 et que les réductions entre a_i ne peut se faire que pour des indices i du même K(v)).De plus $S_{i+1} = \mu(A_l)$ où $\forall\, l$, $A_l \in A(v)$ .Nous avons alors :

$$a_{vi}^{-1} S_{i+1} a_{vi+1} = \prod_{j=1}^{m} a_{tj}^{-1} A_{lj}^{\varepsilon_j} a_{tj+1}$$

et
$$\mu(A_l) = \prod_{j=1}^{m} A_{lj}^{\varepsilon_j} \qquad \text{avec } \varepsilon_j = \pm 1$$

et $a_{vi} = a_{t1}$,$a_{vi+1} = a_{tm+1}$,et les $a_{tj}^{-1} A_{lj}^{\varepsilon_j} a_{tj+1}$ sont les générateurs de M_v ou leur inverse .De plus K(vi)=K(vi+1)
Donc ω' contient un sous-mot de la forme $b_{vi}^{-1} a_{vi}^{-1} \mu(A_l) a_{vi+1} b_{vi+1}$
où $\exists$ v $A_l \in A(v)$ .Donc ω contient un sous-mot de la forme $p_{vi}^{-1} \mu(A_l) p_{vi+1}$.
Or dans E^* ,nous avons $a_{vi}^{-1} \mu(A_l) a_{vi+1} = b_{vi} \mu(B_l) b_{vi+1}^{-1}$ .De plus $p_{vi}^{-1} \mu(A_l) p_{vi+1} = \mu(B_l)$,donc $\mu(A_l) p_{vi+1}$ produit $p_{vi} \mu(B_l)$ .Ce qui dans le cas (1) ,démontre la partie (1) du théorème .Dualement ,le cas (2) démontre la partie (2) . ■

On note $E \leq E^*$,si E^* a pour base E ,et si pour tout mot ω de E , $\omega = 1$ dans E ,ssi $\omega = 1$ dans E^* .

Lemme I.5.1 : Si E^* est une extension de Britton ayant pour base E ,alors $E \leq E^*$.

Démonstration : Le résultat est clair puisque (avec le théo.I.5.1) ,E est plongé naturellement dans E^* . ■

Considérons une extension de Britton ayant pour lettres stables P .Un sous-mot tel que dans le théorème I.5.1 ,est appelé un **pinch** .Si un mot contient un pinch ,on peut lui appliquer la réduction suivant : $\omega \equiv U\ p_y^{-1} C\ p_z\ V = U\ p_y^{-1}\ \mu(A_i)\ p_z V$

(théo I.5.1 (1)) $= U\ p_y^{-1}\ p_y\ \mu(B_i)\ V$

$= U\ \mu(B_i)\ V$

Cette opération s'appelle **extraction d'un pinch** ,nous l'avons appliquée dans le cas (1) ,mais elle similaire dans l'autre cas .Une telle opération diminue le nombre d'occurences de lettres stables dans un mot .
Un mot qui n'est pas égal à un mot ayant moins d'occurences d'éléments de P ,est dit **P-réduit** .

Lemme I.5.2 : Un mot sur E^* ,extension de Britton ayant pour lettres stables P est P-réduit ssi ,on ne peut pas extraire un pinch .

Démonstration : La condition nécessaire est triviale ,puisque un pinch réduit le nombre d'occurence d'éléments de P .

Prenons W ne contenant pas de pinchs ,et supposons que W = U où U contient moins d'éléments de P que W .Si U n'en contient pas ,alors avec le théorème I.5.1 ,W contient un pinch ce qui est contradictoire ,sinon ,on peut considérer que U ne contient pas de pinch .Alors $W\ U^{-1}$,d'après le théorèmeI.5.1 contient un pinch ,qui est forcément à la jonction puisque W et U n'en contiennent pas .Ainsi de suite ,on retire toutes les occurences d'éléments de P,jusqu'à ce qu'il n'y en ait plus .Mais puisque tous les pinchs sont à la jonction ,on a retiré autant d'éléments de P dans W que dans U ,ce qui est contradictoire . ■

Définition : E^* est une **HNN extension** de E ,si E^* ,a pour base $E = \langle S / D \rangle$,pour lettres stables $P = \langle p_v , v \in V \rangle$,et si $E^* = \langle S ; p_v , v \in V / D ; p_{v(i)}^{-1} A_i\ p_{v(i)} = B_i , i \in I \rangle$,où I est fini ,V est fini A_i et B_i ,sont des mots sur S , $v : I \longrightarrow V$,et E^* satisfait C.I.G. .

Remarque Il est clair que les HNN extensions sont un cas particulier des extensions de Britton .En particulier tous les résultats démontrés pour les extensions de Britton sont valables pour les HNN extensions .

Dans ce cas $p_y \simeq p_z$,si et seulement si $p_y = p_z$ .La condition de l'isomorphisme généralisé s'appelle alors condition de l'isomorphisme .Le théorème I.5.1 devient le *lemme de Britton* .

Les HNN extensions sont aussi appellées extensions forte de Britton .

Lemme I.5.3 : Si E^* est une HNN extension de E ,ayant pour lettres stables P ,alors le sous-groupe de E^* engendré par P est libre sur P .

Démonstration : Soit F le groupe libre engendré par P .Considérons l'application φ : $E^* \longrightarrow$ F telle que $\varphi(p) = p$ $\varphi(s) = 1$;$\forall$ p $\in$ P ,et $\forall$ s $\in$ S .Il est clair au vu des relateurs de E^* ,que φ s'étend en un homomorphisme .Alors tout relateur sur P dans E^* ,serait un relateur sur F ,qui est libre . ■

Lemme I.5.4 : Soit E^* ,HNN extension de E avec pour lettres stables ,$P = \langle p_v , v \in V \rangle$ .Soient deux mots U et W tels que ,$U \equiv S_0 p_{v_1}^{\varepsilon_1} S_1 \ldots S_{n-1} p_{v_n}^{\varepsilon_n} S_n$,et $V \equiv T_0 p_{v_1}^{\zeta_1} T_1 \ldots T_{m-1} p_{v_m}^{\zeta_m} T_m$,sont deus mots P-réduits ,tels que $S_0, \ldots S_n$ et $T_0, \ldots, T_m$ sont des mots dans E ;$v_1, \ldots, v_n, w_1, \ldots, w_m \in V$;$\varepsilon_1, \ldots \varepsilon_n, \zeta_1, \ldots, \zeta_m \in \langle -1;1 \rangle$ .Alors si U = V dans E^* ,n = m ;$\forall$ i = 1...n , $v_i = w_i$, $\varepsilon_i = \zeta_i$,et de plus $p_{v_n}^{\varepsilon_n} S_n T_m^{-1} p_{v_m}^{-\zeta_m}$ est un pinch .

Démonstration : On a $U V^{-1} = 1$ dans E^* .Donc d'après le théorème I.5.1 ,il contient un pinch .Puisque U et V sont P-réduits ,(lemme I.5.2) ,le pinch est $p_{v_n}^{\varepsilon_n} S_n T_m^{-1} p_{v_m}^{-\zeta_m}$,et donc $v_n = w_m$ et $\varepsilon_n = \zeta_m$ .Le mot obtenu est encore trivial dans E^* . En appliquant le même raisonnement jusqu'à ce qu'il n'y ait plus d'occurences d'éléments de P ;on a n = m (puisque chaque extraction de pinch se fait à la jonction) ,$v_i = w_i$,et $\varepsilon_i = \zeta_i$ ■