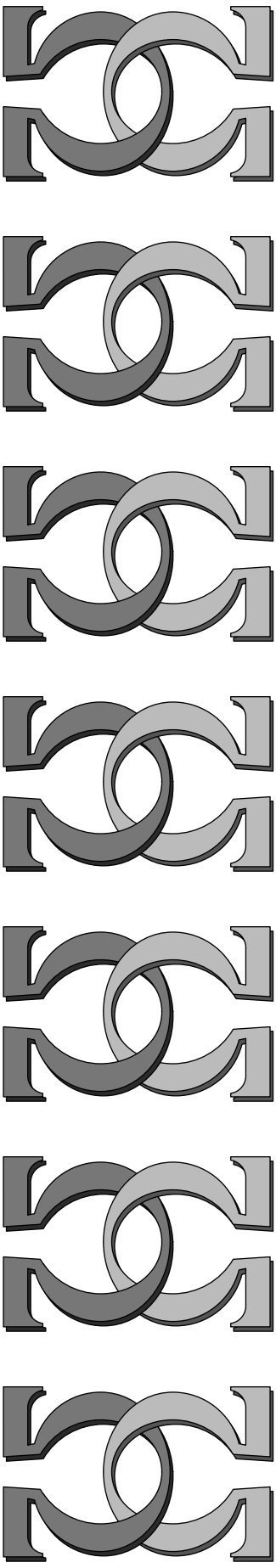

CDMTCS
Research
Report
Series

Higman's Embedding Theorem. An Elementary Proof

Luminiţa Dediu
University "Dunărea de Jos", Romania

CDMTCS-010
December 1995

Centre for Discrete Mathematics and
Theoretical Computer Science

Higman's Embedding Theorem. An Elementary Proof*

Luminiţa Dediu†

Abstract

In 1961 G. Higman proved a remarkable theorem establishing a deep connection between the logical notion of recursiveness and questions about finitely presented groups.

The basic aim of the present paper is to provide the reader with a rigorous and detailed proof of Higman's Theorem. All the necessary preliminary material, including elements of group theory and recursive functions theory, is systematically presented and with complete proofs. The aquainted reader may skip the first sections and proceed immediately to the last.

1 Subgroups

We assume familiarity with the concept of subgroup. We shall use the standard notation, i.e. $H \leq G$ means that H is a subgroup of G.

Fact 1.1. If H is a subgroup of a group G and K is a subset of H, then K is a subgroup of H iff K is a subgroup of G.

Fact 1.2. For any family $\{H_i\}_{i\in I}$ of subgroups of a group G the intersection $\bigcap_{i\in I} H_i$ is also a subgroup of G.

Proof. First, we have $\bigcap_{i\in I} H_i \neq \emptyset$. Indeed, if $H_i \leq G$, for all $i \in I$, then $1 \in H_i, i \in I$, so $1 \in \bigcap_{i\in I} H_i$. Let $x, y \in \bigcap_{i\in I} H_i$. Then $x, y \in H_i$ for all $i \in I$. As $H_i \leq G$, for all $i \in I, xy^{-1} \in H_i$, hence $xy^{-1} \in \bigcap_{i\in I} H_i$. □

Fact 1.3. Let $f : G \longrightarrow G'$ be a group morphism, $H \subseteq G$ and $K \subseteq G'$.

a) If H is a subgroup of G, then $f(H)$ is a subgroup of G'.

b) If K is a subgroup of G', then $f^{-1}(K)$ is a subgroup of G.

*Paper written to be admitted for PhD studies at Bucharest University under the guidance of Professor Cristian Calude.

†Department of Mathematics, University "Dunărea de Jos" of Galatzi, Romania

Proof. Since $H \leq G$ we have $1_G \in H$ and $f(1_G) = 1_{G'} \in f(H)$ (f is a morphism). Hence $f(H) \neq \emptyset$. Let $x, y \in f(H)$. There exist two elements $h_1, h_2 \in H$ such that $x = f(h_1), y = f(h_2)$. Then we can write (using the properties of f):

$$xy^{-1} = f(h_1)[f(h_2)]^{-1};$$

since $H \leq G$ it follows that $h_1 h_2^{-1} \in H$, so $xy^{-1} = f(h_1 h_2^{-1}) \in f(H)$.

The proof of the second statement is similar: if $K \leq G'$, then $1_G \in K$, so $1_G = f^{-1}(1_{G'}) \in f^{-1}(K)$ and $f^{-1}(K) \neq \emptyset$. Accordingly, if $x, y \in f^{-1}(K)$, then for some $k_1, k_2 \in K$ we have $x = f^{-1}(k_1), y = f^{-1}(k_2)$ and $xy^{-1} = f^{-1}(k_1)[f^{-1}(k_2)]^{-1} = f^{-1}(k_1 k_2^{-1}) \in f^{-1}(K)$ ($K \leq G'$ and $k_1 k_2^{-1} \in K$). □

From Fact 1.3 the preimage under the morphism f of the trivial subgroup $\{1_{G'}\}$ of G' is a subgroup of G. This is a special subgroup and it is called the *kernel* of the morphism f. We denote it by $Kerf$:

$$Kerf = \{x \in G : f(x) = 1_{G'}\}.$$

In the same way, the image by f of the group G, denoted by Imf or $f(G)$, is a subgroup of G'.

2 Generated Subgroups. Generators

Let E be a subset of a group G.

Definition 2.1 *The subgroup generated by the subset E (in G) is the intersection of all the subgroups of G containing E.*

Such subgroups do exist: for instance, the trivial subgroup G.

Proposition 2.2 *The subgroup G' generated by a subset E consists of all finite products of elements of E and inverses of these elements.*

Proof. Following the definition we have:

$$G' = \bigcap_{\substack{H \leq G \\ H \supseteq E}} H.$$

Let G'' be the set of all finite products of elements of E and their inverses. We shall prove that $G' = G''$.

By definition it follows that $E \subseteq G'$. On the other hand, from Fact 1.2, G' is a subgroup of G and it is immediate now that $G'' \subseteq G'$.

Conversely, it is sufficient to show that $G'' \leq G$ and $G'' \supseteq E$. First, note that G'' contains the "simple products", i.e. all products formed by a single element x of E or x^{-1}, so $E \subseteq G''$. Let $a = x_1 x_2 \dots x_m$ and $b = y_1 y_2 \dots y_n$ be two elements of G'', where $x_i, y_j \in E$, $1 \leq i \leq m, 1 \leq j \leq n$. Therefore we have:

$$ab^{-1} = (x_1 \dots x_m)(y_1 \dots y_n)^{-1} = x_1 \dots x_m y_n^{-1} \dots y_1^{-1},$$

and this is a finite product of elements of E and inverses of elements of E, hence $ab^{-1} \in G''$. □

From 2.2 it follows that if H_1, H_2 are subgroups of a group G, then the subgroup generated by H_1, H_2 is formed by all finite products of elements in H_1, H_2 and their inverses. We shall denote this subgroup by $\langle H_1, H_2 \rangle$ or $Gp\{H_1, H_2\}$. As a particular case, if G is a commutative group, then the subgroup $\langle H_1, H_2 \rangle$ consists of all elements of the form $h_1 h_2$ with $h_1 \in H_1, h_2 \in H_2$. This subgroup is denoted by $H_1 H_2$ and we call it the *product of subgroups* H_1, H_2.

Definition 2.3 *A group G is said to be finitely generated if there exists a finite set E of elements of G that generates it. If E generates G we say that E is a set of generators for G.*

Example 1. The aditive group of integers $(\mathbb{Z}, +)$ can be generated by the element 1 or by its oposite -1, since every integer $n \neq 0$ can be written as a sum of n terms equal to 1 if $n > 0$ or as a sum of $-n$ terms equal to -1 if $n < 0$.

Groups that can be generated by a single element are called *cyclical groups.*

3 Equivalence Relations. Quotient Set

Let A be a set.

Definition 3.1 *A binary relation, usually denoted by "$\sim$", is said to be an equivalence relation on A provided the following three conditions hold:*

i) $a \sim a$ *(reflexivity),*

ii) $a \sim b \Longrightarrow b \sim a$ *(symmetry),*

iii) $a \sim b, b \sim c \Longrightarrow a \sim c$ *(transitivity).*

Examples 2.

1. Let n be a positive integer and define on $\mathbb{Z}$ the following binary relation denoted by "$\equiv \mod n$": for every $a, b \in \mathbb{Z}$
$$a \equiv b \bmod n \Longleftrightarrow n/(a-b).$$
2. The divisibility relation on $\mathbb{N}$ is not an equivalence relation since it is not symmetric.

If "$\sim$" is an equivalence relation on A, then for each $a \in A$ we define the set:

$$\hat{a} = \{b \in A : b \sim a\}$$

called the *equivalence class of the element* $\hat{a}$.

Theorem 3.2 *The equivalence classes determined by "$\sim$" on A have the following properties:*

1) $a \in \hat{a}$, *for all* $a \in A$ *(hence* $\hat{a} \neq \emptyset$*),*

2) $\hat{a} = \hat{b} \Longleftrightarrow a \sim b$,

3) for all $a, b \in A : \hat{a} = \hat{b}$ *or* $\hat{a} \bigcap \hat{b} = \emptyset$,

4) $A = \bigcup_{a \in A} \hat{a}$.

Proof. 1). Since $a \sim a$ it follows that $a \in \hat{a}$ and so $\hat{a} \neq \emptyset$.

2). From 1) we have $a \in \hat{a}$. If $\hat{a} = \hat{b}$, then $a \in \hat{b}$ i.e. $a \sim b$. Assume now that $a \sim b$. Let $x \in \hat{a}$, then $x \sim a$ and, by transitivity, $x \sim b$, i.e. $x \in \hat{b}$. This way we have $\hat{a} \subseteq \hat{b}$. Changing roles between a and b we obtain $\hat{b} \subseteq \hat{a}$. Hence $\hat{a} = \hat{b}$.

3). Let $a, b \in A$ such that $\hat{a} \bigcap \hat{b} \neq \emptyset$. Then there exists $x \in \hat{a} \bigcap \hat{b}$, i.e. $x \sim a$ and $x \sim b$. Using transitivity we have $a \sim b$ and from 2) it follows $\hat{a} = \hat{b}$.

4). For every set A we can write $A = \bigcup_{a \in A} a$. From 1) $a \in \hat{a}$, then $A = \bigcup_{a \in A} \hat{a}$. □

One can note that using 3) we can write A as a union of sets pairwise disjoint. In this case, we say that the equivalence classes of A realise a *partition* of A. The set of equivalence classes determined by the relation "$\sim$" on A is denoted by $A/\sim$ and is said to be the *quotient set* of A relative to "$\sim$". The map $p : A \longrightarrow A/\sim$ which carries every element a of A into his equivalence class $\hat{a}$ is a surjection that we call the *canonical surjection.*

Definition 3.3 *Let H be a subgroup of a group G. We define on G the relation "$\equiv_l \bmod H$" given by:*

$$x \equiv_l y \bmod H \Longleftrightarrow x^{-1}y \in H \text{ for all } x, y \in G,$$

and we call it the left congruence modulo H.

We shall prove that the above relation is an equivalence on G. For all $x, y, z \in G$ we have (using the properties of a subgroup):

i) $x^{-1}x = 1 \in H \Longrightarrow x \equiv_l x \bmod H$.

ii) By definition

$$x \equiv_l y \bmod H \Longleftrightarrow x^{-1}y \in H$$

so,

$$(x^{-1}y)^{-1} \in H \Longleftrightarrow y^{-1}x \in H \Longleftrightarrow y \equiv_l x \bmod H.$$

iii) By definition

$$x \equiv_l y \bmod H,\ y \equiv_l z \bmod H \Longleftrightarrow x^{-1}y \in H,\ y^{-1}z \in H$$

so,

$$(x^{-1}y)(yz^{-1}) \in H \Longleftrightarrow x^{-1}z \in H \Longleftrightarrow x \equiv_l z \bmod H.$$

□

Thus we can construct the quotient set $G/\equiv_l \bmod H$, which is usually denoted by $(G/H)_l$; its elements are called *left equivalence classes modulo H.* Following the definition, the class of an element $x \in G$ is the set defined by

$$\{y \in G : x^{-1}y \in H\} = \{y \in H : y \in xH\} = xH.$$

If $X \in (G/H)_l$, i.e. X is an equivalence class, an element $x \in X$ is called a *representative* of X. Obviously, $x \in G$ is a representative of X iff $X = xH$.

Note that if $x, y \in G$ and $xH = yH$, then $x \equiv_l y \bmod H$ and $x^{-1}y \in H$. Similarly we can define the right congruence modulo H by

$$x \equiv_r y \bmod H \Longleftrightarrow xy^{-1} \in H.$$

The right equivalence class modulo H of an element $x \in G$ is Hx and the quotient set $G/\equiv_r \bmod H$ is denoted by $(G/H)_r$.

Proposition 3.4 *The quotient sets $(G/H)_l$ and $(G/H)_r$ have the same cardinal.*

Proof. Let $X \in (G/H)_l$, $X = xH$ with $x \in G$. Then we have:

$$X^{-1} = (xH)^{-1} = H^{-1}x^{-1} = Hx^{-1} \in (G/H)_r.$$

(We have used the relation $H^{-1} = H$. Indeed, if $x \in H$ we can put $x = (x^{-1})^{-1}$ and since $x^{-1} \in H$ (H is a subgroup), then $x = (x^{-1})^{-1} \in H^{-1}$. If $x^{-1} \in H^{-1}$, then $x \in H$, so $x^{-1} \in H$. Hence $H^{-1} = H$.)

In the same manner as above we can prove that for every $Y \in (G/H)_r$ one has $Y \in (G/H)_l$. In fact we can define the maps $\Phi : (G/H)_l \longrightarrow (G/H)_r$ carrying X onto X^{-1} and $\Psi : (G/H)_r \longrightarrow (G/H)_l$ carrying Y onto Y^{-1}.

These maps are inverse one to the other:

$$\Phi(\Psi(Y)) = \Phi(Y^{-1}) = (Y^{-1})^{-1} = Y,$$

$$\Psi(\Phi(X)) = \Psi(X^{-1}) = (X^{-1})^{-1} = X,$$

so that they establish a bijection between $(G/H)_l$ and $(G/H)_r$. □

Example 3. Consider S_3 the group of all permutations of a 3 element set and

$$H = \left\{ \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} \right\}$$

a subgroup of S_3.

We shall construct the left and right equivalence classes modulo H. For all $\sigma, \tau \in S_3$ we have: $\sigma \equiv_l \tau \bmod H \iff \sigma^{-1}\tau \in H$. On the other hand one can note that $\sigma \in H$ iff $\sigma(3) = 3$, hence $\sigma^{-1}\tau \in H \iff (\sigma^{-1}\tau)(3) = 3 \iff \tau(3) = \sigma(3)$.

In this way we get the following relation: $\sigma \equiv_l \tau \bmod H \iff \sigma(3) = \tau(3)$. The left equivalence classes modulo H are:

$$C_1^l = H,$$

$$C_2^l = \left\{ \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} \right\},$$

$$C_3^l = \left\{ \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} \right\}.$$

Similarly, we deduce that $\sigma \equiv_r \tau \bmod H \iff \sigma^{-1}(3) = \tau^{-1}(3)$.

Since for every transposition $\tau = (i, j) \in S_3$ we have $\tau^{-1} = \tau$, the inverses of the elements of S_3 are: $e^{-1} = e$, $(1,2)^{-1} = (1,3)$, $\begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}^{-1} = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$, and we obtain the following right classes modulo H:

$$C_1^r = \left\{ \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}, (1,3) \right\},$$

$$C_2^r = \left\{ \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}, (2,3) \right\},$$

$$C_3^r = \left\{ \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}, (1,2) \right\}.$$

We can see now that the quotient sets $(S_3/H)_l$ and $(S_3/H)_r$ are not equal.

4 Normal Subgroups. Quotient Groups

Proposition 4.1 *Let H be a subgroup of a group G. The following statements are equivalent:*

a) $xHx^{-1} \subseteq H$, *for all* $x \in G$,

b) $xHx^{-1} = H$, *for all* $x \in G$,

c) $xH = Hx$, *for all* $x \in G$,

d) $(G/H)_l = (G/H)_r$.

Proof.

- a) $\Longrightarrow$b): For all $x \in G$ we have $xHx^{-1} \subseteq H$; but $x^{-1} \in G$ and thus $x^{-1}Hx \subseteq H$. Putting $H = x(x^{-1}Hx)x^{-1}$ we obtain $H \subseteq xHx^{-1}$ (from the last inclusion), hence $H = xHx^{-1}$.
- b) $\Longrightarrow$a) is immediate.
- b) $\Longrightarrow$c): $xHx^{-1} = H$ and by multiplication to right by x we obtain $xH = Hx$.
- c) $\Longrightarrow$b): $xH = Hx \Longrightarrow xHx^{-1} = (Hx)x^{-1} = H$.
- c) $\Longrightarrow$d): For all $x \in G$ we denote by $\hat{x}_l$ (and respectively $\hat{x}_r$) the left (right) equivalence class modulo H. We saw that $\hat{x}_l = xH$ ($\hat{x}_r = Hx$). From c) we obtain $\hat{x}_l = \hat{x}_r$, for all $x \in G$, hence $(G/H)_l = (G/H)_r$.

- d) $\Longrightarrow$c): Let $x \in G$. Then $\hat{x}_l = xH \in (G/H)_l = (G/H)_r$, so we can find $y \in G$ such that $\hat{x}_l = y_r$, i.e. $xH = Hy$. Putting $x = x.1 \in xH = Hy$ it follows that $x \in Hy$, i.e. $x \equiv_r y \bmod H$. Hence x is a representative of Hy and so we can write $Hx = Hy$. Now we have $Hx = Hy = xH$, i.e. $xH = Hx$. □

Definition 4.2 *A subgroup H of a group G is said to be normal if it satisfyes one of the equivalent conditions in Proposition 4.1. We write this by $H \trianglelefteq G$.*

Examples 4.

1. G and e are (trivial) normal subgroups of G.
2. If G is an abelian group, then for all $x \in G$ and for any subgroup H of G we have $xH = Hx$. Therefore, any subgroup of an abelian group is a normal subgroup.
3. Let H be the subgroup considered in Example 3. As we have seen, the sets of left and right equivalence classes modulo H are not equal, hence H is not a normal subgroup.
4. Any intersection of normal subgroups is a normal subgroup.

Definition 4.3 *Let R be a subset of a group G. The normal subgroup*

$$\overline{R} = \bigcap_{\substack{N \trianglelefteq G \\ N \supseteq R}} N.$$

is called the normal closure of R in G.

If N is a normal subgroup of G, then by definition the left and right congruence relations modulo N on G coincide, hence we can simply talk about the congruence relation on G modulo N. We shall denote it by "$\equiv \bmod N$" and the quotient set by G/N.

Proposition 4.4 *If N is a normal subgroup of a group G, then G/N can be organized with a group structure and the canonical surjection $p : G \longrightarrow G/N$, $p(x) = \hat{x}$, for all $x \in G$ becomes a group morphism.*

Proof. For all $x, y \in G$ we define the product of two elements $\hat{x}, \hat{y} \in G/N$ by $\hat{x}.\hat{y} = \widehat{xy}$. First we have to check that the operation given above makes sense: if $\hat{x} = \hat{x}'$ and $\hat{y} = \hat{y}'$, then $x^{-1}.x' \in N$ and $y^{-1}.y' \in N$, hence there exist $h_1, h_2 \in N$ such that $h_1 = x^{-1}x'$ and $h_2 = y^{-1}y'$. It follows that $x' = xh_1, y' = yh_2$, so we deduce that $x'y' = (xh_1)(yh_2) = x(h_1y)h_2$.

Since N is a normal subgroup we get $Ny = yN$, i.e. there exists $h_3 \in N$ such that $h_1y = yh_3$:

$$x'y' = x(yh_3)h_2 = (xy)(h_3h_2) \in (xy)N.$$

Accordingly $x'y' \equiv (xy) \bmod N$, and so the definition of the internal operation is correctly defined.

We show now that G/N is a group:

- Associativity: for all $\hat{x}, \hat{y}, \hat{z} \in G/N$ we have $(\hat{x}\hat{y})\hat{z} = (\widehat{xy})\hat{z} = \widehat{(xy)z} = \widehat{x(yz)} = \hat{x}(\widehat{yz}) = \hat{x}(\hat{y}\hat{z})$.
- If e denotes the identity element of G, then for each $x \in G/N$ we have $\hat{x}\hat{e} = \widehat{xe} = \hat{x} = \widehat{ex} = \hat{e}\hat{x}$, hence $\hat{e}$ is the identity element of G/N.
- The inverse of an element $\hat{x}$ is $\widehat{x^{-1}}$. Indeed: $\widehat{x^{-1}}\hat{x} = \widehat{x^{-1}x} = \hat{e} = \widehat{xx^{-1}} = \hat{x}\widehat{x^{-1}}$.

To finish the proof we have to verify that the canonical surjection p that carries an element $x \in G$ into his class $\hat{x} \in G/N$ is a group morphism: $p(xy) = p(x)p(y)$. Indeed: $p(xy) = \widehat{xy} = \hat{x}\hat{y} = p(x)p(y)$ and this concludes the proof. □

Definition 4.5 *The group G/N costructed above is called the quotient group of G relative to the normal subgroup N.*

Example 5. Let us construct the quotient groups of the aditive group $(\mathbb{Z}, +)$.

We assume familiarity with the fact that all the subgroups of $\mathbb{Z}$ have the form $n\mathbb{Z}$ with $n \geq 0$. In the same time, $(\mathbb{Z}, +)$ is an abelian group, so it is clear that any subgroup of it is normal. Hence we want to construct a quotient group of the form $\mathbb{Z}/n\mathbb{Z}, n \geq 0$. Then, we consider two cases:

- $n = 0 :\ \mathbb{Z}/(0) = \mathbb{Z}$.
- $n > 0$:

$$x \equiv y \bmod n\mathbb{Z} \Longleftrightarrow x - y \in n\mathbb{Z} \Longleftrightarrow n/(x-y) \Longleftrightarrow x \equiv y \bmod n,$$

so the congruence modulo $n\mathbb{Z}$ on $\mathbb{Z}$ is reduced to the congruence modulo n on $\mathbb{Z}$. Finally,

$$\mathbb{Z}/n\mathbb{Z} = \mathbb{Z}/(\equiv \bmod n) = \mathbb{Z}_n.$$

5 The Fundamental Isomorphism Theorem for Groups

As we have seen before if f is a group morphism from G into G', then $Kerf$ is a subgroup of G. We shall prove here that $Kerf$ is a normal subgroup (that is $Kerf$ satisfies one of the equivalent conditions of 4.1) and then we shall construct the quotient group $G/Kerf$.

Let $x \in G$ and $y \in Kerf$. Then $xyx^{-1} \in xKerfx^{-1}$ and $f(xyx^{-1}) = f(x)f(y)f(x^{-1})$. Since $y \in Kerf,\ f(y) = e'$ (where e' is the identity element of G') and

$$f(xyx^{-1}) = f(x)e'f(x^{-1}) = f(xx^{-1}) = f(e) = e'.$$

Hence $xyx^{-1} \in Kerf$ for all $x \in G$ and $y \in Kerf$, thus $Kerf$ is normal in G.

Now we may consider the quotient group $G/Kerf$ and present one of the theorems which play a major role in what will follow.

Theorem 5.1 *(***The Fundamental Isomorphism Theorem***) If $f : G \longrightarrow G'$ is a group morphism, then there exists a group isomorphism between $G/Kerf$ and Imf, i.e.*

$$G/Kerf \simeq Imf.$$

Proof. Define $\overline{f} : G/Kerf \longrightarrow Imf \subseteq G'$ by $\overline{f}(\hat{x}) = f(x)$. First verify that the definition makes sense: let $\hat{x}, \hat{y} \in G/Kerf$ such that $\hat{x} = \hat{y}$. That means that $x \equiv y \bmod (Kerf)$, hence $x^{-1}y \in Kerf$ and so $f(x^{-1}y) = e'$. Since f is a morphism we can write:

$$e' = f(x^{-1}y) = [f(x)]^{-1}f(y);$$

it follows that $f(x) = f(y)$, therefore $\overline{f}(\hat{x}) = \overline{f}(\hat{y})$.

By definition $Imf = \{\overline{f}(\hat{x}) : \hat{x} \in G/Kerf\} = \{f(x) : x \in G\} = Imf$, thus $\overline{f}$ is a surjection.

In order to show that $\overline{f}$ is injective, let $\hat{x}, \hat{y} \in G/Kerf$ be such that $\overline{f}(\hat{x}) = \overline{f}(\hat{y})$. It follows that $f(x) = f(y)$ and hence

$$f(x)[f(y)]^{-1} = e' \Longleftrightarrow f(xy^{1}) = e' \Longleftrightarrow xy^{-1} \in Kerf \Longleftrightarrow \hat{x} = \hat{y},$$

proving that $\overline{f}$ is bijective. All that remains to do is to prove that $\overline{f}$ is a group morphism. Indeed, since f is a morphism we get:

$$\overline{f}(\hat{x}\hat{y}) = \overline{f}(\widehat{xy}) = f(xy) = f(x)f(y) = \overline{f}(\hat{x})\overline{f}(\hat{y}),$$

for all $\hat{x}, \hat{y} \in G/Kerf$. □

As a corrollary we note that in case f is a surjective group morphism, then $G' = Imf$, and thus G' is isomorphic to $G/Kerf$. This result is very often used to establish isomorphisms between groups.

Example 6. Let $(\mathbb{C}^*,.)$ be the multiplicative group of the non-zero complex numbers and let $f:\mathbb{C}^* \longrightarrow \mathbb{R}_+^*$ be the morphism defined by $f(z)=|z|$, for all $z\in\mathbb{C}^*$. It is immediate that f is a surjective group morphism: for all $a\in\mathbb{R}_+^*$ there exists $z\in\mathbb{C}^*, z=a+0i$, such that $f(z)=f(a+0i)=a$. For all $z_1,z_2\in\mathbb{C}^*$ we have

$$f(z_1z_2)=|z_1z_2|=|z_1||z_2|=f(z_1)f(z_2),$$

thus f is a surjective group morphism from $(\mathbb{C}^*,.)$ into $(\mathbb{R}_+^*,.)$ and from the fundamental theorem we deduce that $\mathbb{R}_+^*\simeq\mathbb{C}^*/Kerf$ where

$$Kerf=\{z\in\mathbb{C}^*:|z|=1\}.$$

6 Free Groups. Defining Relations

Let $\mathcal{M}$ be a finite (or not) set of symbols (letters) $x_\alpha, x_\beta,\ldots$ and assign to these symbols (by an one-to-one correspondence) another set of symbols denoted by $x_\alpha^{-1}, x_\beta^{-1},\ldots$ called *inverses* of symbols in $\mathcal{M}$.

Definition 6.1 *A word is a finite ordered sequence of symbols (letters) of the form* $w=x_{\alpha_1}^{\varepsilon_1}\ldots x_{\alpha_n}^{\varepsilon_n}$, $\varepsilon_i=\underline{+}1, 1\le i\le n$, *where no succesive symbols are inverse one to the other, i.e.* $x_{\alpha_i}^{\varepsilon_i}\neq x_{\alpha_{i-1}}^{-\varepsilon_{i-1}}$, $2\le i\le n$.

The number n is called the *length* of the word and is usually denoted by $|w|=n$. The word that contains no symbol is called the *empty word* and is denoted by 1 or λ. Its length is obviously 0.

Example 7. Consider $\mathcal{M}=\{a,b,c\}$. Then $w_1=ab^{-1}, w_2=ba^{-1}cb^{-1}a$ are words and $|w_1|=2, |w_2|=5$.

Let X be the set containing the symbols of $\mathcal{M}$ and their inverses. The set of all words written with the symbols in X becomes a group together with the following internal operation called juxtaposition: if $w_1=x_{\alpha_1}^{\varepsilon_1}\ldots x_{\alpha_n}^{\varepsilon_n}$, $\varepsilon_i=\underline{+}1, 1\le i\le n$, $w_2=x_{\beta_1}^{\delta_1}\ldots x_{\beta_m}^{\delta_m}$, $\delta_j=\underline{+}1, 1\le j\le m$ are words, their product is defined by

$$w_1w_2=x_{\alpha_1}^{\varepsilon_1}\ldots x_{\alpha_n}^{\varepsilon_n}x_{\beta_1}^{\delta_1}\ldots x_{\beta_m}^{\delta_m},$$

i.e. by joining the second word to the first.

If $x_{\alpha_n}=x_{\beta_1}$ and $\varepsilon_n+\delta_1=0$ (i.e. $x_{\alpha_n}^{\varepsilon_n}$ and $x_{\beta_1}^{\delta_1}$ are inverse) we can *cancel* the sequence involved and repeat the operation with the next symbols if necessary. Letter cancelation in a word product is also called *reduction.* For instance, if $w_1=x_\alpha x_\beta^{-1}x_\delta$ and $w_2=x_\delta^{-1}x_\beta x_\alpha x_\delta$, then $w_1w_2=x_\alpha x_\beta^{-1}x_\delta x_\delta^{-1}x_\beta x_\alpha x_\delta=x_\alpha x_\alpha x_\delta$.

As we see in this example, some sequences of identical repeated letters of the form

$$\underbrace{xx\ldots x}_{n\ times}\ \text{or}\ \underbrace{x^{-1}x^{-1}\ldots x^{-1}}_{n\ times}$$

may appear. We agree to denote these sequences by x^n and, respectively, x^{-n}. Thus, a word can be defined as beeing an ordered finite sequence of letters of the form $w=x_{\alpha_1}^{\varepsilon_1}\ldots x_{\alpha_n}^{\varepsilon_n}$, with $\varepsilon_i\in\mathbb{Z}$, $1\le i\le n$ and $x_{\alpha_i}^{\varepsilon_i}\neq x_{\alpha_{i-1}}^{-\varepsilon_{i-1}}$ (no cancelation is possible). In this way the word $w=x_\alpha x_\alpha x_\beta x_\delta^{-1}x_\delta^{-1}x_\delta^{-1}$ can be represented as $w=x_\alpha^2x_\beta x_\delta^{-3}$.

The juxtaposition operation is associative. The empty word 1 is considered to be the identity element of the set of all words. The inverse of a word $w=x_{\alpha_1}^{\varepsilon_1}\ldots x_{\alpha_n}^{\varepsilon_n}$ is the word $w^{-1}=x_{\alpha_n}^{-\varepsilon_n}\ldots x_{\alpha_1}^{-\varepsilon_1}$. So we can speak by now of the group of words written with the symbols of X, called the *free group generated by* $\mathcal{M}$. The elements of $\mathcal{M}$ are called *free generators* of the free group. The cardinality of $\mathcal{M}$ is said to be the *rank* of the free group.

Theorem 6.2 *Any group is isomorphic to some quotient group of a free group.*

Proof. Let G be a group and $\mathcal{M}$ a set of generators of G. Denote those generators by $a_\alpha, a_\beta, \ldots$. Consider a free group F whose generators system has the same cardinality as $\mathcal{M}$. Between the elements of $\mathcal{M}$ and the free generators of F we can establish a bijection and we agree to denote by x_α the element of F associated to a_α in $\mathcal{M}$. The map $a_\alpha \rightleftharpoons x_\alpha$ defines a group morphism which associates to each element $g \in G,\ g = a_{\alpha_1}^{\varepsilon_1} \ldots a_{\alpha_n}^{\varepsilon_n}$ a word $w = x_{\alpha_1}^{\varepsilon_1} \ldots x_{\alpha_n}^{\varepsilon_n},\ \varepsilon_i = \underline{+}1, 1 \leq i \leq n$ (or $\varepsilon_i \in \mathbb{Z}$). According to the fundamental isomorphism theorem we have $G \simeq F/N$, where N is the kernel of the above morphism. □

Remarks.

1) The normal subgroup N contains the words whose image in G is equal to the identity.

2) The representation of a group as a quotient group of a free group is not unique: it depends on the choice of $\mathcal{M}$.

Keeping the same notations as above, consider a group G. We have seen that there exists a free group F and a normal subgroup N of F such that $G \simeq F/N$. Let $w \in N, w = x_{\alpha_1}^{\varepsilon_1} \ldots x_{\alpha_n}^{\varepsilon_n},\ \varepsilon_i \in \mathbb{Z},\ 1 \leq i \leq n$. The image in G of w is the identity element and so we obtain an equality of the form

$$a_{\alpha_1}^{\varepsilon_1} \ldots a_{\alpha_n}^{\varepsilon_n} = e \tag{1}$$

called *relation* between the generators $a_{\alpha_1}, a_{\alpha_2}, \ldots$ of the group G.

If we consider in N a subset R such that the normal subgroup generated by R in F coincides to N, then the system of relations of the form (1) which corresponds in G to elements of R is called a set of *defining relations* of the group G. All remaining relations between the generators of G are considered as *consequences* of the defining relations, since every element of N can be generated by the elements of R and their conjugates.

We state that the group G is completely defined when the defining relations are given. Since R generates N, then the quotient group F/N is completely determined. We conclude that any group can be described by a set of defining relations between some given generators. Thus, a group can be viewed as a pair of sets (X, R), where X is a set of generators and R is the set of defining relations (by a mild abuse of notation we use the letter R also for the set of defining relations). Section 8 deals with some more details.

Examples 8.

1. Let us define a group that has a single generator a and a single defining relation $a^n = e$. The free group F generated by the symbol x, $x \longleftrightarrow a$, is the cyclical infinite group $F = \langle x \rangle$. The set of words corresponding to the defining relation contains a single element: $R = \{x^n\}$. The normal subgroup generated by x^n in F is $N = \langle x^n \rangle$. Thus $G = \langle a \rangle \simeq \langle x \rangle / \langle x^n \rangle$. But since any cyclical infinite group is isomorphic to the aditive group of integers $(\mathbb{Z}, +)$ and this isomorphism brings $\langle x^n \rangle$ onto $n\mathbb{Z}$, we conclude that:

$$G \simeq \langle x \rangle / \langle x^n \rangle \simeq \mathbb{Z}/n\mathbb{Z} = \mathbb{Z}_n.$$

2. The symmetric group S_3 can be defined by two generators a and b and the defining relations

$$a^3 = e, b^2 = e, abab = e,$$

where $a = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix},\ b = (1,2)$. The reader can easily check that $ab = (1,3),\ ba = (2,3)$. Since any permutation is a product of transpositions it follows that a and b generate S_3.

If we consider the free group F generated by a and b, then $S_3 \simeq F/H$ and F will contain the following 6 elements:

$$a, b, a^2, b^2 = e, ab, ba = a^2 b.$$

Indeed, since $abab = e$ we get:

$$ab = b^{-1}a^{-1} \Longrightarrow a = b^{-1}a^{-1}b^{-1} \Longrightarrow ba = a^{-1}b^{-1};$$

on the other hand,

$$a^3 = e \Longrightarrow a^{-1} = a^2 \text{ and } b^2 = e \Longrightarrow b = b^{-1},$$

so $ba = a^2b$; any other combination of a's and b's gives one of the above 6 elements.

Thus we can represent S_3 by its generators and defining relations as follows:

$$S_3 = \langle a, b; a^3 = e, b^2 = e, abab = e \rangle.$$

7 Recursive Functions and Sets

Historically, the notion of a computable function has been developed between 1931-1947 by different, but equivalent, tools: formal equations (J. Herbrand, K. Gödel, S. C. Kleene), Turing machines (A. M. Turing), Post systems (E. L. Post), and Markov normal algorithms (A. Markov).

A remarkable fact is that all these notions are equivalent, in the sense that they "generate" the same class of functions defined on $\mathbb{N}$, the *recursive functions* .

Definition 7.1 *A function $f : \mathbb{N}^k \longrightarrow \mathbb{N}$ is said to be computable if there exists an algorithm which computes $f(n_1, \ldots, n_k)$, for every $(n_1, \ldots, n_k) \in \mathbb{N}^k$.*

Examples 9.

1. Let $f(x)$ be the $x^{\underline{th}}$ prime number. Using as algorithm the method described by the sieve of Eratostheneses we can compute f.
2. Let $f(x, y)$ be the greatest common divisor (g.c.d.) of the positive integers x, y. This function, as we all kwow, can be computed by Euclid's algorithm (considering $f(x, 0) = f(0, y) = 0$).

Definition 7.2 *The following functions are said to be initial (basic) functions:*

1. *The projection functions: $P_m^{(n)}$, $1 \leq m \leq n$, defined by $P_m^{(n)}(x_1, \ldots, x_n) = x_m$.*
2. *The constant functions: $C_m^{(n)}$, $m \in \mathbb{N}$ fixed, defined by $C_m^{(n)}(x_1, \ldots, x_n) = m$.*
3. *The succesor function defined by $Succ(x) = x + 1$.*

Definition 7.3 *A function defined on $\mathbb{N}$ or $\mathbb{N}^k$ is said to be recursive if it is an initial function or if it can be generated by an initial function in a finite number of steps, using the following three rules:*

a) **Functional composition (substitution)**. *If f is a k-variables function, and $g_1, \ldots, g_k$ are functions of n variables then*

$$g(x_1, \ldots, x_n) = f(g_1(x_1, \ldots, x_n), \ldots, g_k(x_1, \ldots, x_n))$$

determinates a n-variables function.

b) **Primitive recursion**. *If f is a $(k+1)$-variables function and g is a $(k-1)$-variables function, then the following system of equations defines an unique k-variables function:*

$$f(x_1, \ldots, x_{k-1}, 0) = g(x_1, \ldots, x_{k-1}),$$

$$f(x_1, \ldots, x_{k-1}, y+1) = h(x_1, \ldots, x_{k-1}, y, f(x_1, \ldots, x_{k-1}, y)).$$

(Dedekind proved the existence and the unicity of these functions.)

c) **Minimization**. *If f is a $(k+1)$-variables function such that for every k-tuple $(x_1, \ldots, x_k)$ of natural numbers there exists a number y with $f(x_1, \ldots, x_k, y) = 0$, then one can determine a new function g by the condition:*

$$g(x_1, \ldots, x_k) = \mu y[f(x_1, \ldots, x_k, y) = 0],$$

where $\mu y[\ldots]$ means "the least y such that ...".

Examples 10.

1. The sum function $f(x,y) = x + y$ can be obtained by primitive recursion from $h(x,y,z) = z + 1$ and $P_1^{(1)}(x) = x$ as follows:
$$f(x,0) = x + 0 = P_1^1(x) = x,$$
$$f(x,y+1) = x + (y+1) = (x+y) + 1 = h(x,y,x+y).$$
On the other hand we can write:
$$h(x,y,z) = Succ(P_3^{(3)}(x,y,z)),$$
hence we conclude that h is recursive and therefore f will be recursive too.

2. The product function $f(x,y) = xy$ is recursive:
$$f(x,0) = x.0 = C_0^{(1)}(x) = 0,$$
$$f(x,y+1) = x(y+1) = x.y + x.1 = g(x,y,xy),$$
where $g(x,y,z) = P_1^{(3)}(x,y,z) + P_3^{(3)}(x,y,z) = x + z$ is a recursive function.

3. In the same manner, the exponential function $f(x,y) = x^y$ is recursive:
$$f(x,0) = x^0 = C_1^{(1)}(x) = 1,$$
$$f(x,y+1) = x^{y+1} = x^y.x = t(x,y,x^y),$$
where $t(x,y,z) = P_1^{(3)}(x,y,z)P_3^{(3)}(x,y,z)$ is recursive (we agree that $0^0 = 1$).

Fix a set $S \subseteq I\!N$. Following Leibniz there are two basic algorithmically ways to "define" S: a decision method and a generating method. Using the notion of recursive function, we can give a precise version of these two techniques:

- **The generating method**

  Definition 7.4 *A set S of natural numbers is called recursively enumerable if $S = \emptyset$ or if there exists a recursive function $f : I\!N \longrightarrow I\!N$ whose range coincides with S.*

  We shall say in this case that the function f generates (enumerates) the elements of S.

- **The decision method**

  Definition 7.5 *A set S of natural numbers is said to be decidable (recursive) if its characteristic function f_S,*
$$f_S(n) = \begin{cases} 1, & \text{if } n \in S, \\ 0, & \text{otherwise} \end{cases},$$
  is recursive. If f_S is recursive, one can decide whether an arbitrary natural number n is or not an element of S.

Examples 11. The following sets are recursive:

1. $S = \{2n : n \geq 0\}$,
2. $S = \{n : n \text{ is prime}\}$.

Remark. A set S is recursive iff both S and its complement $\mathbb{N} - S$ are recursively enumerable. So, if S is a recursive set, then S is recursively enumerable. The converse is not true (see Section 9).

The notions of recursive function, recursive and recursively enumerable set can be extended from $\mathbb{N}$ to $\mathbb{N}^n$ and, then, to $\mathbb{Z}^n$, for every $n > 0$.

Theorem 7.6 *Cantor's function $J : \mathbb{N}^2 \longrightarrow \mathbb{N}$ defined by*

$$J(x, y) = (x + y)(x + y + 1)/2 + x$$

is a recursive bijection.

The reader interested on the proof is referred to [3].

Thus we have got an encoding scheme which allows us to identify, in a recursive manner, the sets $\mathbb{N}$ and $\mathbb{N}^2$. J is called the *Cantor numbering* and the number $J(x, y)$ is referred to as the *Cantor number* associated to the pair (x, y). The decoding associates of J are usually denoted by K and L and so we have:

$$J(K(z), L(z)) = z,$$
$$K(J(x, y)) = x,$$
$$L(J(x, y)) = y.$$

Cantor's function can be extended to a recursive bijection $J^{(n)} : \mathbb{N}^n \longrightarrow \mathbb{N}$, for every $n \geq 3$ with decoding associates denoted by $I_1^{(n)}, \ldots, I_n^{(n)}$.

Definition 7.7 *A function $\Phi : \mathbb{N}^n \longrightarrow \mathbb{N}^n$ is recursive if there exists a recursive funtion $f : \mathbb{N} \longrightarrow \mathbb{N}$ such that*

$$\Phi \circ I = I \circ f,$$

where $I : \mathbb{N} \longrightarrow \mathbb{N}^n$, $I = (I_1^{(n)}, \ldots, I_n^{(n)})$ is the inverse of the generalized Cantor's bijection.

Consider now a bijection $\alpha : \mathbb{N} \longrightarrow \mathbb{Z}$ and its extension $\alpha^{(n)} : \mathbb{N}^n \longrightarrow \mathbb{Z}^n$,

$$\alpha^{(n)}(x_1, \ldots, x_n) = (\alpha(x_1), \ldots, \alpha(x_n)).$$

Definition 7.8 *A function $\Psi : \mathbb{Z}^n \longrightarrow \mathbb{Z}^n$ is recursive if there exists a recursive function $\Phi : \mathbb{N}^n \longrightarrow \mathbb{N}^n$ such that*

$$\Psi \circ \alpha^{(n)} = \alpha^{(n)} \circ \Phi.$$

Thus, the definitions for recursively enumerable and recursive sets can be extended for the subsets of $\mathbb{N}^n$ and, respectively, of $\mathbb{Z}^n$.

Let F be a non-empty set such that there exists a one-to-one correspondence f between F and the natural numbers. We say that f is a *Gödel numbering* for F and the set $Im\ f$ is called the *set of code-numbers* (or Gödel numbers) of F.

Definition 7.9 *The set F is said to be recursive (recursively enumerable) if the corresponding set of code-numbers is recursive (recursively enumerable).*

8 Recursively Presented Groups. Free Products with Amalgamation. HNN-Extensions

Groups are often described as quotient groups of some free groups: $G \simeq F/N$. If F is a free group with basis X and N is the normal closure in F of a set R, then we say that the pair $(X; R)$ is a *presentation* for G, and - by convention - we write $G = (X; G)$ (see examples given in Section 6).

If $\overline{X}$ is the set of images $\overline{x}$ in G of all elements x of X by the canonical surjection $(x \mapsto \overline{x} \in F/N)$ then, since a surjective morphism carries systems of generators into systems of generators, $\overline{X}$ is generating G. If $r = r(x_1, \ldots, x_n)$ is an element of R (hence a word written with generators $x_1, \ldots, x_n$), then we get $r(\overline{x}_1, \ldots, \overline{x}_n) = e$ in G, that is a defining relation. The elements of R will be called *relators.*

A presentation $(X; R)$ is *finitely generated* if X is finite and is *finite* if both X and R are finite sets. In this last case we often say that the group G has a *finite presentation* or is *finitely presented.*

We say that a presentation $(X; R)$ is *recursive* if X is finite and R is recursively enumerable.

8.1 Free Product of Groups

We shall use the notation $\langle a_1, a_2, \ldots; r_1, r_2, \ldots\rangle$ to denote (X, R), for a group presentation, where $X = \{a_1, a_2, \ldots\}$ and $R = \{r_1, r_2, \ldots\}$.

Let A and B be two groups having, respectively, the presentations $A = \langle a_1, \ldots; r_1, \ldots\rangle, B = \langle b_1, \ldots; s_1, \ldots\rangle$; assume that the sets of generators are disjoint. The *free product $A \star B$ of the groups A and B* is the group defined by

$$A \star B = \langle a_1, \ldots, b_1, \ldots; r_1, \ldots, s_1, \ldots\rangle.$$

The groups A and B are called the *factors* of the product.

One can prove that the free product $A \star B$ does not depend on the presentations chosen for A and B and, more, $A \star B$ is generated by subgroups $\overline{A}$ and $\overline{B}$ which are isomorphic to A and, respectively, B, such that $\overline{A} \bigcap \overline{B} = \{e\}$.

In the general case, if $\{A_i; i \in I\}$ is any family of groups, we define the free product of the groups A_i, written $\star_{i\in I} A_i$, to be the group with presentation the union of disjoint presentations of the A_i.

8.2 Free Products with Amalgamation. HNN-Extensions

These are two constructions which are basic to combinatorial group theory.

Let $G = \langle x_1, \ldots; r_1, \ldots\rangle$ and $H = \langle y_1, \ldots; s_1, \ldots\rangle$ be two groups and let $A \leq G, B \leq H$ be subgroups such that there exists an isomorphism $\Phi : A \longrightarrow B$. The *free product of G and H amalgamating the subgroups A and B by the isomorphism Φ* is the group

$$\langle x_1, \ldots, y_1, \ldots; r_1, \ldots, s_1, \ldots, a = \Phi(a), a \in A\rangle.$$

If G is a group with a given presentation, then by the notation

$$\langle G, z, \ldots; u, \ldots\rangle$$

we mean the group defined by the generators and the relators of G together with whatever additional generators and relators are indicated. The additional generators will be disjoint from those of G. Thus we can write the free product with amalgamation as

$$\langle G \star H; a = \Phi(a), a \in A\rangle,$$

or, simply,

$$\langle G \star H, A = B, \Phi\rangle.$$

The basic ideea, as one can see in the last notation, is that the subgroup A is identified with its isomorphic image $\Phi(A) = B$ in H.

The free product with amalgamation depends on G, H, A, B and Φ; G and H are called the *factors* of the product, while A and B are called the *amalgamated subgroups.*

Let G be a group and A and B two subgroups which are isomorphic. We define the *Higman-Neumann-Neumann extension of G relative to A, B and Φ* to be the group

$$G^* = \langle G, t; t^{-1}at = \Phi(a), a \in A\rangle,$$

where Φ is the isomorphism between A and B (shortly we shall say "HNN-extension".)

The group G is called the *base of G^*, t* is the *stable letter, A* and B, the *associated subgroups.*

Of course, both constructions can be generalized. Let $\{A_i\}_{i\in I}, \{B_i\}_{i\in I}$ be families of subgroups of G with $\{\Phi_i : i \in I\}$ a family of maps such that each $\Phi_i : A_i \longrightarrow B_i$ is an isomorphism. The HNN-extension with base G, stable letters $t_i, i \in I$, and associated subgroups A_i and $B_i, i \in I$, is the group

$$G^* = \langle G, t_i, i \in I; t_i^{-1}at_i = \Phi(a), a \in A_i\rangle.$$

Similarly, let $\{G_i\}_{i\in I}$ be a family of groups. If A is a group and $\{\Phi_i : i \in I\}$ is a family of injective morphisms $\Phi_i : A \longrightarrow G_i, i \in I$, then we define the free product of the groups G_i amalgamating the subgroups $\Phi_i(A)$ to be the group

$$P = \langle \star_{i\in I} G_i; \Phi_i(a) = \Phi_j(a), a \in A, i, j \in I\rangle.$$

9 Higman's Embedding Theorem

Theorem 9.1 *(**Higman**)* A finitely generated group G can be embedded in some finitely presented group iff G can be recursively presented.

We shall prove, for the beginning, only the direct implication, as the converse one needs some new concepts and results.

Thus, assume that G is a finitely generated group which can be embedded in a finitely presented group H. Hence there exists a subgroup $G' \leq H$ which is isomorphic to G. This implies that a finitely generated subgroup of a finitely presented group admits a recursive presentation.

We use the fact that any group can be described as a quotient group of some free group $G' = F/R$ where R is a normal subgroup of the free group F representing the defining relations of G'. We shall construct both F and R such that $G' = F/R$ and we shall prove that R is a recursively enumerable set.

Let $\{x_1, \ldots, x_m\}$ be the set of generators of G'. As $G' \leq H$ we can presume that the symbols $x_1, \ldots, x_m$ belong to the set of generators of H. Thus we can consider that $\{x_1, \ldots, x_m, x_{m+1}, \ldots, x_n\}$ is the set of generators of H.

Now, let $\{a_1, \ldots, a_m, \ldots, a_n, \ldots\}$ be another set of symbols and K be the free group generated by it. Define the group morphism (given on generators) $\Phi : K \longrightarrow H$ by

$$\Phi(a_i) = x_i,\ 1 \leq i \leq n,$$

$$\Phi(a_j) = 1,\ j \geq n+1.$$

We are interested on $Ker\ \Phi$. By definition we have $Ker\ \Phi = \{w \in K : \Phi(w) = 1\}$. It is clear that $a_{n+1}, a_{n+2}, \ldots$ belong to the set of generators of $Ker\ \Phi$, since any word of the form $a_{n+1}^{m_{n+1}} a_{n+2}^{m_{n+2}} \ldots$ will belong to $Ker\ \Phi$:

$$\Phi(a_{n+1}^{m_{n+1}} a_{n+2}^{m_{n+2}} \ldots) = (\Phi(a_{n+1}))^{m_{n+1}} (\Phi(a_{n+2}))^{m_{n+2}} \ldots = 1.$$

Now, a word written with the other symbols $a_1, \ldots, a_n$ is in $Ker\ \Phi$ iff between these symbols holds a relation of the form $\Phi(a_1^{m_1} \ldots a_n^{m_n}) = 1$, that is the generators $x_1, \ldots, x_n$ of H are satisfying $x_1^{m_1} \ldots x_n^{m_n} = 1$. Such a relation holds in H only if it is a consequence of the defining relations of H. Since H is finitely presented there exists only a finite number of such relations, hence we have a finite number of relations between the generators of $Ker\ \Phi$ and that means $Ker\ \Phi$ is recursively enumerable.

Let F be the free subgroup of K generated by the elements $\{a_1, \ldots, a_m\}$ and let $\overline{\Phi}$ be the restriction of Φ to F, that is $\overline{\Phi} : F \longrightarrow G'$. Now,

$$Ker\ \overline{\Phi} = Ker\ \Phi \bigcap F$$

and we can check that $\overline{\Phi}$ is a surjective morphism: indeed, for every $x_i \in G', 1 \leq i \leq m$, there exists $a_i \in F, 1 \leq i \leq m$, such that $x_i = \overline{\Phi}(a_i), 1 \leq i \leq m$, from the above definition of Φ. We conclude, using the fundamental isomorphism theorem, that $G' \simeq F/Ker\ \overline{\Phi}$ and thus the set of defining relations of G' is $Ker\ \overline{\Phi}$. But

$$R = Ker\ \overline{\Phi} = Ker\ \Phi \bigcap F$$

and $Ker\ \Phi$ is recursively enumerable so, in order to prove that R is recursively enumerable, we have to show that F is recursively enumerable.

As F has a finite set of generators we conclude that F is recursively enumerable. Then the intersection $Ker\ \Phi \bigcap F$ is also recursively enumerable. □

For the converse implication of the theorem we shall give equivalent definitions for the notions of "recursive set" and "recursively enumerable set" using polynomials with integer coefficients.

Let $P(X_1, \ldots, X_k)$ be a polynomial in k variables with integer coefficients. A k-tuple of integers such that $P(z_1, \ldots, z_k) = 0$ is said to be a *root* of P.

Definition 9.2
A subset S of $\mathbb{Z}^n$ is called Diophantine if there exists a polynomial $P(X_1, \ldots, X_n; Y_1, \ldots, Y_m)$ such that

$$(s_1, \ldots, s_n) \in S\ iff\ P(s_1, \ldots, s_n; Y_1, \ldots, Y_m)\ \textit{has an integer root in}\ Y_1, \ldots, Y_m.$$

In this case we say that P enumerates S.

Example 12. The set $\mathbb{N}$ is Diophantine. Indeed, by the theorem of Lagrange we know that an integer is non-negative iff it can be written as the sum of four squares. Thus, the polynomial $P(X; Y_1, \ldots, Y_4) = Y_1^2 + \ldots + Y_4^2 - X$ enumerates $\mathbb{N}$, that is $s \in \mathbb{N} \Longleftrightarrow P(s; Y_1, \ldots, Y_4)$ has a root.

One can note that every Diophantine set S is intuitively effectively enumerable. Let $P(X_1, \ldots, X_n; Y_1, \ldots, Y_m)$ be the polynomial which enumerates S. Then, consider all the $(n+m)$-tuples of integers of the form $(s_1, \ldots, s_n; d_1, \ldots, d_m)$ and it can be effectively enumerated. For every enumerated $(n+m)$-tuple we can compute $P(s_1, \ldots, s_n; d_1, \ldots, d_m)$. If its value is 0 then we put $(s_1, \ldots, s_n)$ on the list of elements of S. If not, we compute the value of P for the next $(n+m)$-tuple.

The following theorem is an important result obtained in 1970 by Matijasevich (see [10] for a recent presentation).

Theorem 9.3 *A subset S of $\mathbb{Z}^n$ is recursively enumerable iff it is Diophantine.*

Next we shall prove that there exist recursively enumerable sets which are not recursive. We shall construct such a set and on this purpose we shall use a "code" for the objects we are working with, following Gödel's method: to each polynomial we assign a natural number. Consider the map

$$\alpha : \mathbb{Z} \longrightarrow \mathbb{N}^*, \alpha(z) = \begin{cases} 2|z| + 1, & \text{if } z \leq 0, \\ 2|z|, & \text{if } z > 0. \end{cases}$$

The construction indicates that α is a one-to-one correspondence between $\mathbb{Z}$ and $\mathbb{N}^*$.

Denote by $X_0, X_1, \ldots, X_m, \ldots$ the variables we shall work with, and assign to each monomial term

$$T = cX_{i_1}^{e_1} X_{i_2}^{e_2} \ldots X_{i_n}^{e_n}$$

with $c \in \mathbb{Z}^*, e_i \geq 1, i_1 < \ldots < i_n$, the number

$$\beta(T) = 2^{\alpha(c)} p_{i_1+2}^{e_1} \ldots p_{i_n+2}^{e_n},$$

where p_j is the $j^{\underline{th}}$ prime number.

Example 13. If $T = 5X_0^3 X_3 X_4^2$ then $\beta(T) = 2^{2.5}.3^3.11^1.13^2 = 2^{10}.3^3.11.13^2$.

Since any non-zero polynomial in m variables can be written as a sum of monomial terms

$$P = T_1 + T_2 + \ldots + T_k,$$

$\beta(T_1) < \ldots < \beta(T_k)$, we assign to P the number

$$\Gamma(P) = 2^{\beta(T_1)} 3^{\beta(T_2)} \ldots p_k^{\beta(T_k)}.$$

Theorem 9.4 *The set*

$$S = \{e \in \mathbb{Z} : e = \Gamma(P(X_{i_1}, \ldots, X_{i_n})) \text{ and } P(e, X_{i_2}, \ldots, X_{i_n}) \text{ has a root } \}$$

is a recursively enumerable set which is not recursive.

Proof. The set S contains code numbers of those polynomials P for which, substituting the first variable by their own Gödel number, we obtain a polynomial which has a root. The set S is intuitively effectively enumerable. Indeed, we can effectively enumerate the polynomials $P(X_{i_1}, \ldots, X_{i_n})$. We compute then $\Gamma(P(X_{i_1}, \ldots, X_{i_n})) = e$ for the enumerated polynomial P and enumerate the n-tuples $(e, d_2, \ldots, d_n)$ with $d_2, \ldots, d_n \in \mathbb{Z}$. For each enumerated n-tuple compute $P(e, d_2, \ldots, d_n)$ and if it is zero we put e on the list of elements of S; if not, we compute the value of P for the next n-tuple.

We shall prove that S cannot be recursive, that is, its complement $S^* = \mathbb{Z} - S$ is not recursively enumerable. We have:

$$S^* = \{z \in \mathbb{Z} : z \text{ is not in the range of } \Gamma \text{ or } z = \Gamma(P(X_{i_1}, \ldots, X_{i_n})) \\ \text{but } P(z, X_{i_2}, \ldots, X_{i_n}) \text{ does not have a root}\}.$$

Assume that S^* is recursively enumerable, that is Diophantine. Let Q be the polynomial which enumerates S^*, hence $z \in S^*$ iff $Q(z, X_{i_2}, \ldots, X_{i_l})$ has a root. Let $e^* = \Gamma(Q)$. The question is: $e^* \in S$ or $e^* \in S^*$? Following the definitions of S and Q we have

$$e^* \in S^* \Longleftrightarrow Q(e^*, X_{i_2}, \ldots, X_{i_l}) \textit{ has a root}$$

and since $e^* = \Gamma(Q)$, then $e^* \in S$. We have got a contradiction! □

The following definition introduces one of Higman's key concepts.

Definition 9.5 *A subgroup H of a finitely generated group G is called* **benign** *in G if the group*

$$G_H = \langle G, t; t^{-1}ht = h, h \in H \rangle$$

can be embedded in a finitely presented group.

We shall often use in our proof the following fact: if G, K are finitely generated groups, H is benign in K and $H \subseteq G \subseteq K$, then H is benign in G.

Indeed, if H is benign in K, then

$$K_H = \langle K, t; t^{-1}ht = h, h \in H \rangle$$

can be embedded in a finitely presented group M. Then

$$G_H = \langle G, s; s^{-1}hs = h, h \in H \rangle$$

can be embedded in K_H by the map $g \mapsto g$, for all $g \in G$, and $s \mapsto t$. Hence G_H embeds in K_H which embeds in M and thus H is benign in G.

The following lemma - due to Higman too - establishes the role that benign subgroups will play in our proof.

Lemma 9.6 *(The Higman Rope Trick) If R is a benign normal subgroup of a finitely generated group F, then the quotient group F/R can be embedded in a finitely presented group.*

Proof. Let $x_1, \ldots, x_n$ be the generators of the group F. By hypothesis, since R is benign in F, it follows that

$$F_R = \langle F, t; t^{-1}rt = r, r \in R \rangle$$

is embeddable in a finitely presented group H. Denote by $\overline{F}$ the subgroup of H which is isomorphic to F and by $\overline{R}$ the subgroup of $\overline{F}$ which is isomorphic to R.

Without altering the finite presentation of H we can assume that the generators $\overline{x_1}, \ldots, \overline{x}_n$ of the group $\overline{F}$ are included among the generators of H. If $w \in F$ is a word on generators $x_1, \ldots, x_n$, its image in $\overline{F}$ will be denoted by $\overline{w}$ and it will represent a word on generators $\overline{x}_1, \ldots, \overline{x}_n$.

Viewed in F_R, R is a subgroup both for F and for $t^{-1}Ft$ because of the defining relations of F_R; then the group $L = \langle F, t^{-1}Ft \rangle$ generated by F and $t^{-1}Ft$ can be considered as the free product of the above groups with R amalgamated. Define a morphism $\Phi : L \longrightarrow \overline{F}/\overline{R}$ by $w \mapsto \overline{\overline{w}}$ and $t^{-1}wt \mapsto 1$, where $\overline{\overline{w}}$ denotes the class of $\overline{w} \in \overline{F}$ in the quotient group $\overline{F}/\overline{R}$. One can note that the definition of Φ makes sense:

$$\Phi(r) = \overline{\overline{r}} = 1 \text{ in } \overline{F}/\overline{R}, \text{ for all } r \in R,$$

and

$$t^{-1}rt = r \Longrightarrow \Phi(r) = \Phi(t^{-1}rt) = 1, \text{ for all } r \in R;$$

hence the two definitions agree on the amalgamated part of L.

Consider now the group $H \times \overline{F}/\overline{R}$ whose elements will be written as ordered pairs. Since $L = F \star_R t^{-1}Ft$ is a subgroup of F_R and F_R is embeddable in H, we can view L as a subgroup of H. Define then

$$\Psi : L \longrightarrow L \times \overline{F}/\overline{R} \text{ by } l \mapsto (l, \Phi(l)),$$

where Φ is the above morphism. It is immediate that $Ker\ \Psi = \{1\}$, hence Ψ is one-to-one. We conclude that L is isomorphic to $Im\ \Psi$ (by the fundamental isomorphism theorem). Since $Im\ \Psi$ is a subgroup of $L \times \overline{F}/\overline{R}$, then $L \times \{1\}$ is isomorphic to the subgroup $Im\ \Psi$ of $L \times \overline{F}/\overline{R}$:

$$(l, 1) \mapsto l \mapsto (l, \Phi(l)),$$

and we can costruct the HNN-extension

$$K = \langle H \times \overline{F}/\overline{R}, s; s^{-1}(l,1)s = (l, \Phi(l), l \in L\rangle$$

of the group $H \times \overline{F}/\overline{R}$, with stable letter s and associated subgroups $L \times \{1\}$ and $Im\ \Psi$ (we have seen that L can be viewed as a subgroup of H).

We shall prove that K is exactely the finitely presented group in which F/R can be embedded. The set of defining relations of K is given by:

- the defining relations of H which form a finite set, since H is finitely presented;
- the defining relations of $\overline{F}/\overline{R}$;
- the relations saying that the generators of H commute with the generators of $\overline{F}/\overline{R}$ (by definition of a direct product of groups). These relations form a finite set since H and $\overline{F}/\overline{R}$ are finitely generated ($\overline{F}/\overline{R}$ is a quotient group of a finitely generated group, hence it is finitely generated);
- the relations $s^{-1}(l,1)s = (l, \Phi(l)), l \in L$ form a set of generators of L. Since F is finitely generated and $L = F \star_R t^{-1}Ft$ is finitely generated, this set of defining relations is finite.

In order to prove that the set of defining relations of K is finite, it suffices to prove that the set of defining relations of $\overline{F}/\overline{R}$ is finite or it follows from the other relations.

A defining relation for a group G finitely generated by $y_1, \ldots, y_n$ has the form $r(y_1, \ldots, y_n) = 1$. In our case, a defining relation for $\overline{F}/\overline{R}$ is of the form $\overline{\overline{w}} = 1$ where $\overline{\overline{w}}$ is a word on generators $\overline{\overline{x}}_1, \ldots, \overline{\overline{x}}_n$.

We shall prove that the above relation can be written using the relations:

$$s^{-1}(l,1)s = (l, \Phi(l)),\ l \in L,$$

$$t^{-1}rt = r,\ r \in R.$$

Thus, if $w \in F$, we have:

$$s(w,1)s^{-1} = (w, \Phi(w)) = (w, \overline{\overline{w}}). \tag{2}$$

From the second group of relations it follows:

$$w = t^{-1}wt \Longrightarrow (w,1) = (t^{-1}wt, 1) \Longrightarrow s(w,1)s^{-1} = s(t^{-1}wt,1)s^{-1} = \\ = (t^{-1}wt, \Phi(t^{-1}wt)) = (t^{-1}wt, 1) = (w,1). \tag{3}$$

From (2) and (3) we have $\overline{\overline{w}} = 1$, hence the set of defining relations of K is finite. The set of generators is given by the generators of H and those of $\overline{F}/\overline{R}$ (all of them in a finite number) and s. Thus K is a finitely presented group. □

How can we use this lemma for our goal? We know that every group can be written as a quotient group of some free group and more, that every recursively presented group G has the form F/R where R is a recursively enumerable normal subgroup of F. The lemma shows that it remains to prove that every recursively enumerable normal subgroup of a finitely generated free group is benign.

To do this, first we need some initial examples and some ways to construct benign subgroups from subgroups already known to be benign.

The notation $\langle G, t; t^{-1}Ht = H\rangle$ will be used for the HNN-extension of G with stable letter t and amalgamated subgroups equal to H, while $Gp\{H, K\}$ will denote the subgroup generated by subgroups H and K of a group G.

Lemma 9.7 *Let G be a finitely generated group which can be embedded in a finitely presented group. Then, the following statements are true:*

a) *Any finitely generated subgroup of G is benign in G.*

b) *If H and K are benign in G, then $H \bigcap K$ and $Gp\{H, K\}$ are benign in G.*

Proof. a) By hypothesis we know that G can be embedded in a finitely presented group M. Let H be a finitely generated subgroup of G. Then the group

$$G_H = \langle G, t; t^{-1}ht = h, h \in H\rangle$$

is embeddable in

$$N = \langle M, t; t^{-1}ht = h, h \in H\rangle.$$

The group N is finitely presented since M is finitely presented and H is finitely generated and every relation $t^{-1}ht = h, h \in H$, is a consequence of the relations $t^{-1}h_it = h_i, h_i \in B$, where B is the finite system of generators of H. Hence H is benign in G.

b) One has

$$G_{H\bigcap K} = \langle G, u; u^{-1}(H\bigcap K)u = H\bigcap K\rangle.$$

Let M and N be the finitely presented groups in which $G_H = \langle G, t; t^{-1}Ht = H\rangle$ and, respectively, $G_K = \langle G, s; s^{-1}Ks = K\rangle$ embed. Hence G can be viewed as a subgroup both in M and N and we can construct the free product with amalgamation

$$P = \langle M * N; G = G\rangle$$

denoted also by $M *_G N$.

This is a finitely presented group since M and N are finitely presented groups and, on the other hand, G is finitely generated, the set of "aditional" defining relations is finite.

Now define a map

$$\Phi : G_{H\bigcap K} \longrightarrow Gp\{G, ts\}$$

on generators:

$$g \mapsto g, u \mapsto ts,$$

and we establish an isomorphism between the group $G_{H\bigcap K}$ and the subgroup $Gp\{G, ts\}$ of the group P. The fact that Φ is bijective is immediately by its definition. We shall only check that Φ preserves the defining relations:

- this is true for the defining relations holding in G since $g \mapsto g$;
- for the relations $u^{-1}xu = x$ with $x \in H\bigcap K$ we have:

  $$\Phi(u^{-1}xu) = \Phi(u^{-1})\Phi(x)\Phi(u) = (\Phi(u))^{-1}\Phi(x)\Phi(u) = (ts)^{-1}x(ts) = s^{-1}t^{-1}xts = s^{-1}(t^{-1}xt)s.$$

  Since $x \in H\bigcap K$ and the defining relations of G_H and, respectively, of G_K still hold in P, we have $t^{-1}xt = x$ in H and more, $s^{-1}xs = x$ in K, and thus $\Phi(u^{-1}xu) = x = \Phi(x)$.

Thus Φ embeds $G_{H\bigcap K}$ into a finitely presented group, hence $H\bigcap K$ is benign in G.

For the second part of b) we shall prove that in P we have:

$$Gp\{H, K\} = Gp\{t^{-1}Gt, s^{-1}Gs\}\bigcap G. \tag{4}$$

Since $Gp\{t^{-1}Gt, s^{-1}Gs\}$ and G are finitely generated, then by a) they will be benign subgroups and (using the above result) their intersection will be benign in P, hence it will be benign in G.

It remains to prove the equality (4):

"$\subseteq$" Working on generators: if $h \in H$ belongs to the set of generators of H, and $k \in K$ belongs to the generators set of K, obviously h and k are in G. On the other hand, the relations $t^{-1}ht = h, h \in H$ and $s^{-1}ks = s, k \in K$ hold in P, hence $h, k \in Gp\{t^{-1}Gt, s^{-1}Gs\}$.

"$\supseteq$" Let $t^{-1}g_1t, s^{-1}g_2s$ be two elements of the generators set of $Gp\{t^{-1}Gt, s^{-1}Gs\}$, with $g_1, g_2 \in G$. Then:

$$(t^{-1}g_1t \in G, s^{-1}g_2s \in G) \Longleftrightarrow (t^{-1}g_1t = g_1, s^{-1}g_2s = g_2).$$

Since we are working in P, those two relations hold for the elements of H, respectively of K. Hence $t^{-1}g_1t = g_1 \Longrightarrow g_1 \in H$ and $s^{-1}g_2s = g_2 \Longrightarrow g_2 \in K$. □

Lemma 9.8 *(Principal Lemma) If S is a recursively enumerable set of integers, then the subgroup $Gp\{a_0^z b_0 c_0^z : z \in S\}$ is a benign subgroup of the free group $\langle a_0, b_0, c_0\rangle$.*

Proof. If S is recursively enumerable then S is Diophantine. Let $P(X_0 \ldots, X_t)$ be the polynomial with integer coefficients that enumerates S:

$$z_0 \in S \Longleftrightarrow \exists z_1, \ldots, z_t \in \mathbb{Z} : P(z_0, z_1, \ldots, z_t) = 0. \tag{5}$$

We can still simplify this characterization of a recursively enumerable set by converting (5) to:

$$z_0 \in S \Longleftrightarrow \exists z_1, \ldots, z_m \in \mathbb{Z} : \mathcal{M}(z_0, \ldots, z_m) \tag{6}$$

where $\mathcal{M}(z_0, \ldots, z_m)$ is a system of elementary formulas of one of the forms:

1. $X_i = c,\ c \in \mathbb{Z}$,
2. $X_i = X_j$,
3. $X_i + X_j = X_k,\ i \neq j \neq k \neq i$,
4. $X_l = X_i X_j,\ 0 < l < i < j \leq m$.

(the last restriction for the subscipts will be used latter.)

For a better understanding we present an example. Let $P = 6X_1 - X_2^2 + X_0$ and suppose that $z_0 \in S$ iff $P(z_0, X_1, X_2)$ has a root. Using auxillary variables and the elementary formulas, we have:

- for $6X_1 :\ X_4 = 6,\ X_5 = X_1,\ X_4 X_5 = X_3$,
- for $X_2^2 :\ X_7 = X_2,\ X_8 = X_2,\ X_7 X_8 = X_6$,
- for $-X_2^2 :\ X_{10} = -1,\ X_{11} = X_6,\ X_{10} X_{11} = X_9$,
- for $6X_1 - X_2^2 + X_0 :\ X_3 + X_9 = X_{12},\ X_{12} + X_{10} = X_{13}$,
- for $P = 0 :\ X_{13} = 0$.

Denoting by $\mathcal{M}(X_0, \ldots, X_{14})$ the conjunction of the above formulas, we can write:

$$z_0 \in S \Longleftrightarrow \exists z_1, \ldots, z_{13} \in \mathbb{Z} : \mathcal{M}(z_0, \ldots, z_{13}).$$

Back to our proof, using (6) we shall introduce the symbols $a_i, b_i, c_i, 1 \leq i \leq m$, and we shall establish that some particular subgroups of the free group $F = \langle a_0, b_0, c_0, \ldots, a_m, b_m, c_m \rangle$ are benign.

To each $(m+1)$-tuple $(z_0, \ldots, z_m)$ we shall associate a code-word of F denoted by $w_{(z_0,\ldots,z_m)}$ having the form:

$$w_{(z_0,\ldots,z_m)} = c_m^{-z_m} b_m^{-1} a_m^{-z_m} \ldots c_1^{-z_1} b_1^{-1} a_1^{-z_1} a_0^{z_0} b_0 c_0^{z_0} a_1^{z_1} b_1 c_1^{z_1} \ldots a_m^{z_m} b_m c_m^{z_m}.$$

Consider

$$A = Gp\{w_{(z_0,\ldots,z_m)} : (z_0, \ldots, z_m) \in \mathbb{Z}^{m+1}\}.$$

The generators $w_{(z_0,\ldots,z_m)}$ of this group are free. Indeed, the reductions to be done cannot alter the middle part $a_0^{z_0} b_0 c_0^{z_0}$ since the generators $a_i, b_i, c_i,\ 1 \leq i \leq m$, of F are free. Thus A is freely generated by the code-words.

We shall use from now on the letter Γ to denote the system of elementary formulas $\mathcal{M}$ or one of the formulas involved in $\mathcal{M}$. If $\Gamma(X_0, \ldots, X_m)$ is a formula, let A_Γ be the group generated by those code-words $w_{(z_0,\ldots,z_m)}$ for which $\Gamma(z_0, \ldots, z_m)$ is true:

$$A_\Gamma = Gp\{w_{(z_0,\ldots,z_m)} : \Gamma(z_0, \ldots, z_m) \textit{ is true}\}.$$

We introduce also the notations: $A_i^c, A_{i,j}^=, A_{i,j,l}^+, A_{i,j,l}^:$ with respect to the elementary formulas. For instance

$$A_{i,j}^= = Gp\{w_{(z_0,\ldots,z_m)} : z_i = z_j\}.$$

Let us prove now that if $A_i^c, A_{i,j}^=, A_{i,j,l}^+, A_{i,j,l}^:$ are benign subgroups of F, then the subgroup

$$Gp\{a_0^{z_0} b_0 c_0^{z_0} : z_0 \in S\}$$

has the same property.

Let $\Gamma_1, \ldots, \Gamma_p$ be the elementary formulas that give the system $\mathcal{M}$. Then:

$$(6) \Longleftrightarrow z_0 \in S \Longleftrightarrow \exists z_1, \ldots, z_m : \Gamma_q(z_0, \ldots, z_m) \; is \; true, \; 1 \leq q \leq p,$$

and more, we shall show that

$$A_{\mathcal{M}} = \bigcap_{1 \leq q \leq p} A_{\Gamma_q}$$

that is:

$$Gp\{w_{(z_0,\ldots,z_m)} : \Gamma_q(z_0, \ldots, z_m) \; is \; true, \; 1 \leq q \leq p\} = \bigcap_{1 \leq q \leq p} Gp\{w_{(z_0,\ldots,z_m)} : \Gamma_q(z_0, \ldots, z_m) \; is \; true\}.$$

"$\subseteq$" We are working only on generators. Let $w_{(z_0,\ldots,z_m)} \in A_{\mathcal{M}}$. Then $\Gamma_q(z_0, \ldots, z_m)$ is true for every $1 \leq q \leq p$, hence $w_{(z_0,\ldots,z_m)} \in A_{\Gamma_q}$, $1 \leq q \leq p$, i.e. $w_{(z_0,\ldots,z_m)} \in \bigcap_{1 \leq q \leq p} A_{\Gamma_q}$.
"$\supseteq$" If $w \in \bigcap_{1 \leq q \leq p} A_{\Gamma_q}$, then $w \in A_{\Gamma_q}, 1 \leq q \leq p$. Hence w is written with the generators of $A_{\Gamma_q}, 1 \leq q \leq p$. Since the generators $w_{(z_0,\ldots,z_m)}$ are free we conclude that w has the same form for all A_{Γ_q} (if not, we could establish - for two different forms - a relation between the generators $w_{(z_0,\ldots,z_m)}$ of the involved subgroups A_{Γ_q}). Hence w contains only generators $w_{(z_0,\ldots,z_m)}$ that belong to all groups A_{Γ_q}, that is $\Gamma_q(z_0, \ldots, z_m)$ is true for every $1 \leq q \leq p$ and so $\mathcal{M}(z_0, \ldots, z_m)$ is true.

We next establish the equality:

$$Gp\{a_0^{z_0} b_0 c_0^{z_0} : z_0 \in S\} = Gp\{A_{\mathcal{M}}, a_1, b_1, c_1, \ldots, a_m, b_m, c_m\} \bigcap \langle a_0, b_0, c_0 \rangle.$$

"$\subseteq$" Let $w = a_0^{z_0} b_0 c_0^{z_0}$, $z_0 \in S$. Then $w \in \langle a_0, b_0, c_0 \rangle$ and there exist $z_1, \ldots, z_m \in \mathbb{Z}$ such that $\mathcal{M}(z_0, \ldots, z_m)$. Putting

$$w = a_0^{z_0} b_0 c_0^{z_0} = a_1^{z_1} b_1 c_1^{z_1} \ldots a_m^{z_m} b_m c_m^{z_m} w_{(z_0,\ldots,z_m)} c_m^{-z_m} b_m^{-1} a_m^{-z_m} \ldots c_1^{-z_1} b_1^{-1} a_1^{-z_1}, \tag{7}$$

with $w_{(z_0,\ldots,z_m)} \in A_{\mathcal{M}}$ we obtain $w \in Gp\{A_{\mathcal{M}}, a_1, b_1, c_1, \ldots, a_m, b_m, c_m\}$.
"$\supseteq$" Any word of $Gp\{A_{\mathcal{M}}, a_1, b_1, c_1, \ldots, a_m, b_m, c_m\}$ that belongs to the group $\langle a_0, b_0, c_0 \rangle$ will be written only with the symbols a_0, b_0, c_0. Working on generators, from every word $w_{(z_0,\ldots,z_m)} \in A_{\mathcal{M}}$ and from the symbols a_i, b_i, c_i, $1 \leq i \leq m$, we can uniquely construct words containing the symbols a_0, b_0, c_0 and having the reduced form $a_0^{z_0} b_0 c_0^{z_0}$ as shown in (7). Note that these words truely reduce to $a_0^{z_0} b_0 c_0^{z_0}$ since $w_{(z_0,\ldots,z_m)} \in A_{\mathcal{M}}$ and hence $\mathcal{M}(z_0, \ldots, z_m)$. On the other hand, every word having the form $a_0^{z_0} b_0 c_0^{z_0}$ where $z_0 \in S$ belongs to the set of generators of the group $Gp\{a_0^{z_0} b_0 c_0^{z_0} : z_0 \in S\}$, hence the equality is true.

Let us sum up: to use Lemma 9.7 we have to prove the following statements:

a) the finitely generated group F is embeddable in a finitely presented group;

b) $Gp\{A_{\mathcal{M}}, a_1, b_1, c_1, \ldots, a_m, b_m, c_m\}$ and $\langle a_0, b_0, c_0 \rangle$ are benign subgroups of F.

We shall begin with b) which is easier to show. First of all, $\langle a_0, b_0, c_0 \rangle$ is benign in F since it is finitely generated and F is too (from Lemma 9.7 a)); in the second place $Gp\{A_{\mathcal{M}}, a_1, b_1, c_1, \ldots, a_m, b_m, c_m\}$ is the group generated by $A_{\mathcal{M}}$ and by $\langle a_1, b_1, c_1, \ldots, a_m, b_m, c_m \rangle$ which is a finitely generated subgroup of F and, hence, is benign. It remains to prove that $A_{\mathcal{M}}$ is benign and thus, from Lemma 9.7 b), we shall get the desired conclusion.

Since $A_{\mathcal{M}} = \bigcap_{1 \leq q \leq p} A_{\Gamma_q}$ it will suffice to our goal to prove that all subgroups A_{Γ_q} are benign in F.

In what will follow we shall obtain also the result claimed above in a). Namely, we shall construct a finitely presented group M that contains F (or in which F is embeddable) such that for each formula Γ_q there exists a finitely generated subgroup L_{Γ_q} of M with $L_{\Gamma_q} \bigcap F = A_{\Gamma_q}$. Note that L_{Γ_q} and F are benign in M since they are finitely generated and, hence, A_{Γ_q} will be benign in M. On the other hand, we have $A_{\Gamma_q} \subset F \subset M$ and thus A_{Γ_q} becomes benign in F.

We construct M in two stages:

First stage. Let

$$F^* = \langle F, t_0, t_1, \ldots, t_m; R^* \rangle,$$

where R^* is the set of defining relations of the form:

$$t_i^{-1} b_i t_i = a_i b_i c_i, \; 0 \leq i \leq m,$$

$$and \; t_i \; commutes \; with \; all \; the \; other \; generators \; of \; F. \tag{8}$$

We shall prove that F^* is an HNN-extension of F. Thus, $t_0, t_1, \ldots, t_m$ are the stable letters and the associated subgroups will all be equal to F, the corresponding morphisms $\Phi_i : F \longrightarrow F,\ 0 \leq i \leq m$, being given by

$$b_i \mapsto a_i b_i c_i, \lambda \mapsto \lambda,$$

where λ is any generator of F except b_i. Note that the morphisms Φ_i leave unchanged all the generators of F except b_i and this last one has as unique inverse image the element $a_i^{-1} b_i c_i^{-1}$ of F. Hence Φ_i are bijective (since the generators $a_i, b_i, c_i,\ 0 \leq i \leq m$, are free $a_i b_i c_i$ cannot coincide to one of them).

In this way we have shown that F^* is an HNN-extension of F and this completes the first stage.

Second stage. Using the above constructed group F^* we shall extend it as follows: let M be the group given by

$$M = \langle F^*, p_{j,l}, 0 < l < j \leq m; R_M \rangle,$$

where R_M is the union of R^* with the following defining relations holding for every ordered pair (j, l):

$$p_{j,l}^{-1} c_j p_{j,l} = t_l c_j,$$

$$p_{j,l} \textit{ commutes with all the other generators of } F \textit{ and with } t_l. \tag{9}$$

We check now that M is an HNN-extension of F^*. If we present relations (9) in all details, then we get:

$$p_{j,l}^{-1} c_j p_{j,l} = t_l c_j,$$

$$p_{j,l}^{-1} \lambda p_{j,l} = \lambda, \text{where } \lambda \text{ is any generator of } F \text{ except } c_j,$$

$$p_{j,l}^{-1} t_l p_{j,l} = t_l.$$

We can deduce now that the associated subgroups are all equal to $Gp\{F, t_l\}$ and the corresponding automorphisms (given on generators) are

$$\Phi_{j,l} : Gp\{F, t_l\} \longrightarrow Gp\{F, t_l\}$$

defined by $c_j \mapsto t_l c_j, \lambda \mapsto \lambda$, where λ is t_l or any generator of F except c_j.

It is clear that $\Phi_{j,l}$ are bijective. It still remains to prove that both $\Phi_{j,l}$ and $\Phi_{j,l}^{-1}$ preserve the defining relations of F^* (note that $\Phi_{j,l}^{-1}$ brings c_j into $t_l^{-1} c_j$ and leaves unchanged all the other generators of F and t_l):

- the relations that do not contain c_j are identically verified since both $\Phi_{j,l}$ and $\Phi_{j,l}^{-1}$ leave unchanged t_l and the generators of F except c_j;
- the relations that contain c_j in F have the form $t_l^{-1} c_j t_l = c_j$. Then:

$$\Phi_{j,l}(t_l^{-1} c_j t_l) = \Phi_{j,l}(t_l^1)\Phi_{j,l}(c_j)\Phi_{j,l}(t_l) = t_l^{-1}(t_l c_j)t_l = c_j t_l = t_l c_j = \Phi_{j,l}(c_j).$$

$$\begin{aligned}
\Phi_{j,l}^{-1}(t_l^{-1} c_j t_l) &= \Phi_{j,l}^{-1}(t_l^{-1})\Phi_{j,l}^{-1}(c_j)\Phi_{j,l}^{-1}(t_l) \\
&= t_l^{-1}(t_l^{-1} c_j)t_l \\
&= t_l^{-1} t_l^{-1} c_j t_l \\
&= t_l^{-1} t_l^{-1} t_l c_j \\
&= t_l^{-1} c_j \\
&= \Phi_{j,l}^{-1}(c_j).
\end{aligned}$$

So M is an HNN-extension of F^*. Since F is finitely generated, the set of defining relations R^* will be finite; we conclude that M is finitely generated and R_M is finite, hence M is finitely presented.

Thus F embeds in F^* and F^* embeds in M, hence there exists a subgroup of M which is isomorphic to F. We shall identify this subgroup with F.

Prove now that for every elementary formula there exists a finitely generated subgroup L_{Γ_q} of M such that $L_{\Gamma_q} \bigcap F = A_{\Gamma_q}$. We shall effectively construct these subgroups. Namely we claim that:

1. $L_i^c = Gp\{w_{(0,\ldots,0,c,0,\ldots,0)}, t_s, s \neq i\}$ where c is on the i^{th} position,

2. $L^{=}_{i,j} = Gp\{w_{(0,\dots,0)}, t_s, t_it_j, s \neq i,j\}$,

3. $L^{+}_{i,j,l} = Gp\{w_{(0,\dots,0)}, t_s, t_it_l, t_jt_l, s \neq i,j,l\}$,

4. $L^{:}_{i,j,l} = Gp\{w_{(0,\dots,0)}, t_s, t_ip_{j,l}, t_jp_{i,l}, s \neq i,j,l\}$,

and we shall study each of them.

1. From relations (8) we have:

$$\begin{aligned} t_i^{-1}w_{(z_0,\dots,z_m)}t_i &= t_i^{-1}(c_m^{-z_m}b_m^{-1}a_m^{-z_m}\dots c_1^{-z_1}b_1^{-1}a_1^{-z_1}c_0^{z_0}b_0a_0^{z_0}a_0^{z_0}b_0c_0^{z_0}a_1^{z_1}b_1c_1^{z_1}\dots a_m^{z_m}b_mc_m^{z_m})t_i \\ &= c_m^{-z_m}b_m^{-1}a_m^{-z_m}\dots c_i^{-z_i}(t_i^{-1}b_i^{-1})a_i^{-z_i}\dots a_0^{z_0}b_0c_0^{z_0}\dots a_i^{z_i}(b_it_i)c_i^{z_i}\dots a_m^{z_m}b_mc_m^{z_m} \end{aligned}$$

and

$$\begin{cases} t_i^{-1}b_i^{-1} &= c_i^{-1}b_i^{-1}a_i^{-1}t_i^{-1} \\ b_it_i &= t_ia_ib_ic_i \end{cases}$$

and thus we get:

$$\begin{aligned} t_i^{-1}w_{(z_0,\dots,z_m)}t_i &= c_m^{-z_m}b_m^{-1}a_m^{-z_m}\dots c_i^{-z_i}(c_i^{-1}b_i^{-1}a_i^{-1}t_i^{-1})a_i^{-z_i} \\ &\quad \dots a_0^{z_0}b_0c_0^{z_0}\dots a_i^{z_i}(t_ia_ib_ic_i)c_i^{z_i}\dots a_m^{z_m}b_mc_m^{z_m} \\ &= c_m^{-z_m}b_m^{-1}a_m^{-z_m}\dots c_i^{-(z_i+1)}b_i^{-1}a_i^{-(z_i+1)} \\ &\quad \dots a_0^{z_0}b_0c_0^{z_0}\dots a_i^{z_i+1}b_ic_i^{z_i+1}\dots a_m^{z_m}b_mc_m^{z_m} \\ &= w_{(z_0,\dots,z_{i-1},z_i+1,z_{i+1},\dots,z_m)}. \end{aligned}$$

Hence the conjugation by t_i increases with one unit the i^{th} element z_i of $w_{(z_0,\dots,z_m)}$. That means that starting with a word $w_{(0,\dots,0,c,0,\dots,0)}$ we can construct a word $w_{(z_0,\dots,z_{i-1},c,z_{i+1},\dots,z_m)}$ conjugating by t_0 the initial word z_0 times, then by t_1, z_1 times etc. (no conjugation by t_i since c remains on the i^{th} position!).

Similarly as above one can prove that

$$t_iw_{(z_0,\dots,z_m)}t_i^{-1} = w_{(z_0,\dots,z_{i-1},z_i-1,z_{i+1},\dots,z_m)},$$

constructing in this way the negative numbers z_i.

2. Assume that $i < j$. From above we get: $(t_it_j)^{-1}\ w_{(z_0,\dots,z_m)}(t_it_j) = w_{(z_0,\dots,z_i+1,\dots,z_j+1,\dots,z_m)}$.

Thus conjugation z_i times by t_it_j of a word $w_{(0,\dots.0)}$ will introduce z_i on the i^{th} and j^{th} positions and the initial word will become $w_{(0,\dots,0,z_i,0,\dots,0,z_j,0,\dots,0)}$. Next, the other z_s' will be obtained by conjugating z_s times the last word by t_s.

3. We know by now that conjugation z_i times by t_it_l will introduce z_i on the i^{th} and l^{th} positions and then, the conjugation z_j times by t_jt_l will introduce z_j on the j^{th} and l^{th} positions. Finally we get $z_i + z_j$ on the l^{th} position, i.e. $z_l = z_i + z_j$. All the other $z_s^{'}$, $s \neq i,j,l$ will be introduced by conjugation by t_s.

4. Using relations (9) we can write:

$$\begin{aligned} {p_{j,l}}^{-1}\ w_{(z_0,\dots,z_m)}p_{j,l} &= {p_{j,l}}^{-1}(c_m^{-z_m}b_m^{-1}a_m^{-z_m}\dots c_j^{-z_j}b_j^{-1}a_j^{-z_j}\dots a_0^{z_0}b_0c_0^{z_0}\dots a_j^{z_j}b_jc_j^{z_j}\dots a_m^{z_m}b_mc_m^{z_m})\ p_{j,l} \\ &= c_m^{-z_m}b_m^{-1}a_m^{-z_m}\dots {p_{j,l}}^{-1}\ c_j^{-z_j}b_j^{-1}a_j^{-z_j}\dots\ a_0^{z_0}b_0c_0^{z_0}\dots\ a_j^{z_j}b_jc_j^{z_j}p_{j,l}\dots a_m^{z_m}b_mc_m^{z_m}. \end{aligned}$$

Also from (9) we get:

$${p_{j,l}}^{-1}c_j^{\alpha} = t_lc_j\ {p_{j,l}}^{-1}c_j^{\alpha-1} = \dots = t_l^{\alpha}c_j^{\alpha}\ {p_{j,l}}^{-1}$$

and

$$c_j^{\alpha}\ p_{j,l} = c_j^{\alpha-1}\ p_{j,l}t_lc_j = \dots = p_{j,l}c_j^{\alpha}t_l^{\alpha}.$$

Thus:

$$\begin{aligned} {p_{j,l}}^{-1}w_{(z_0,\dots,z_m)}p_{j,l} &= c_m^{-z_m}b_m^{-1}a_m^{-z_m}\dots t_l^{-z_j}c_j^{-z_j}b_j^{-1}a_j^{-z_j}\dots a_j^{z_j}b_j\ p_{j,l}c_j^{z_j}t_l^{z_j}\dots a_m^{z_m}b_mc_m^{z_m} \\ &= c_m^{-z_m}b_m^{-1}a_m^{-z_m}\dots c_j^{-z_j}b_j^{-1}a_j^{-z_j}\dots t_l^{-z_j}c_l^{-z_l}b_l^{-1}a_l^{-z_l} \\ &\quad \dots a_l^{z_l}b_lc_l^{z_l}t_l^{z_j}\dots a_j^{z_j}b_jc_j^{z_j} \\ &\dots\ a_m^{z_m}b_mc_m^{z_m}. \end{aligned}$$

From (8) we get:

$$\left\{\begin{array}{rcl} b_l t_l^{\alpha} & = & t_l^{\alpha} a_l^{\alpha} b_l c_l^{\alpha} \\ t_l^{-\alpha} b_l^{-1} & = & c_l^{-\alpha} b_l^{-1} a_l^{-\alpha} t_l^{-\alpha} \end{array}\right.$$

hence

$$\begin{array}{rcl} {p_{j,l}}^{-1} w_{(z_0,\ldots,z_m)} p_{j,l} & = & c_m^{-z_m} b_m^{-1} a_m^{-z_m} \ldots c_l^{-z_l} (c_l^{-z_j} b_l^{-1} a_l^{-z_j} t_l^{-z_j}) a_l^{-z_l} \\ & & \ldots a_l^{z_l} (t_l^{z_j} a_l^{z_j} b_l c_l^{z_j}) c_l^{z_l} \\ & & \ldots a_m^{z_m} b_m c_m^{z_m} \\ & = & c_m^{-z_m} b_m^{-1} a_m^{-z_m} \ldots c_l^{-(z_j+z_l)} b_l^{-1} a_l^{-(z_j+z_l)} t_l^{-z_j} \\ & & \ldots t_l^{z_j} a_l^{z_j+z_l} b_l c_l^{z_j+z_l} \ldots \ a_m^{z_m} b_m c_m^{z_m} \\ & = & w_{(z_0',\ldots,z_m')}, \end{array}$$

where $z_k^{'} = z_k$ for $k \neq l$ and $z_l^{'} = z_j + z_l$.

Using the same method one can prove that

$$p_{j,l} w_{(z_0,\ldots,z_m)} {p_{j,l}}^{-1} = w_{(z_0',\ldots,z_m')}$$

where $z_k^{'} = z_k$ for $k \neq l$ and $z_l^{'} = z_l - z_j$.

We conclude that for $0 < l < i < j$ the following equalities hold:

$$(t_i p_{j,l})^{-1} w_{(0,\ldots,0)} (t_i p_{j,l}) = w_{(0,\ldots,0,1,0,\ldots,0)} \text{ with 1 on the } i^{th} \text{ position;}$$

$$\begin{array}{rcl} (t_j p_{i,l})^{-1} w_{(0,\ldots,0,1,0,\ldots,0)} (t_j p_{i,l}) & = & p_{i,l}^{-1} w_{(0,\ldots,0,1,0,\ldots,0,1,0,\ldots,0)} p_{i,l} \text{ (1 on the } i^{th} \text{ and } j^{th} \text{ positions)} \\ & = & w_{(0,\ldots,0,1,0,\ldots,0,1,0,\ldots,0,1,0,\ldots,0)} \text{ with 1 on the } i^{th} \text{ and } j^{th} \text{ positions;} \end{array}$$

$$\begin{array}{rcl} (t_i p_{j,l})^{-1} w_{(0,\ldots,0,1,0,\ldots,0,1,0,\ldots,0,1,0,\ldots,0)} (t_i p_{j,l}) & = & {p_{j,l}}^{-1} w_{(0,\ldots,0,1,0,\ldots,0,2,0,\ldots,0,1,0,\ldots,0)} p_{j,l} \\ & = & w_{(0,\ldots,0,2,0,\ldots,0,2,0,\ldots,0,1,0,\ldots,0)}, \end{array}$$

and so on.

Hence conjugation by $t_i p_{j,l}$ increases z_i with one unit and adds z_j to z_l while conjugation by $t_j p_{i,l}$ increases z_j with one unit and adds z_i to z_l. Starting from $w_{(0,\ldots,0)}$ we shall finally get $w_{(z_0,\ldots,z_m)}$ with $z_l = z_i z_j$ and $z_k = 0,\ k \neq i, j, l$ and it can be easily verified by complete induction. First step was verified above. Suppose we have $w_{(0,\ldots,0,z_l,0,\ldots,0,z_i,0,\ldots,0,z_j,0,\ldots,0)}$ with $z_l = z_i z_j$ and we continue with the following transformations:

$$\begin{array}{rcl} w_{(0,\ldots,0,z_i z_j,0,\ldots,0,z_i,0,\ldots,0,z_j,0,\ldots,0)} & \longrightarrow & w_{(0,\ldots,0,z_i z_j+z_j,0,\ldots,0,z_i+1,0,\ldots,0,z_j,0,\ldots,0)} \\ & \longrightarrow & w_{(0,0,\ldots,0,z_i z_j+z_j+z_i+1,0,\ldots,0,z_i+1,0,\ldots,0,z_j+1,0,\ldots,0)}, \end{array}$$

and we get on the l^{th} position the product $(z_i + 1)(z_j + 1)$ of the elements laying on the i^{th} and j^{th} positions.

Now we can state that every word $w_{(z_0,\ldots,z_m)}$ satisfying the elementary formula Γ (hence a word from $A_\Gamma \subset F$) belongs to L_Γ, i.e. $A_\Gamma \subseteq F \bigcap L_\Gamma$. The reverse inclusion is also true because every word from L_Γ that belongs to F is a word $w_{(z_0,\ldots,z_m)}$ satisfying Γ. Hence this word is obtained by succesive stable letter reductions and that means $w_{(z_0,\ldots,z_m)} \in A_\Gamma$. This concludes the proof of the principal lemma. □

We are able to complete now the proof of the theorem. We saw that if G is a recursively presented group, then it can be viewed as a factor group $\overline{F}/\overline{R}$, where F is a finitely generated free group and R is a recursively enumerable normal subgroup of F. According to Lemma 9.6 we have to show that any recursively enumerable normal subgroup of a finitely generated free group is benign. But we can simplify the problem by working in a two-generators group: the Higman-Neumann-Neumann Embedding Theorem states that we can embed F into a two-generators group preserving the recursiveness of presentations (see for the proof the papers by Higman or [8]). Hence, it suffices to prove that any recursively enumerable normal subgroup N of a free group $L = \langle a, b \rangle$ is benign in L.

We need to precise what we mean by "set of words on the generators a and b recursively enumerable". We shall use again Gödel's method, assigning to each word $w \in L$ a number $\gamma(w)$ and we shall say that a set W of words is recursively enumerable iff the set of Gödel numbers

$$\Gamma(W) = \{\gamma(w) : w \in W\}$$

is recursively enumerable.

Let the empty word have the Gödel number 0. If w is a non-empty word on the generators a, b, a^{-1}, b^{-1} then $\gamma(w)$ will be the number represented in the base 10 obtained from w by changing a, b, a^{-1}, b^{-1} into respectively 1, 2, 3 and 4. For instance $\gamma(ab) = 12,\ \gamma(b^{-1}a^2) = 411$.

Let K be the free group $\langle a, b, c, d, e, h\rangle$ where generators a, b are the same as above. To each word $w \in L$ we assign a code-word $g_w \in K$ defined by:

$$g_w = whc^{\gamma(w)}de^{\gamma(w)}.$$

Consider

$$H = Gp\{g_w : w \ is \ a \ word \ on \ a, b, a^{-1}, b^{-1}\}$$

the subgroup of K generated by all the g_w's. Note that H is freely generated by the set of all g_w's. Indeed, there are no reductions in a product of the form $g_{w_1}g_{w_2}$ or $g_{w_1}g_{w_2}^{-1}$ since, in the first case, g_{w_1} ends on $e^{\gamma(w_1)}$ while w_2 is written only on a, b, a^{-1}, b^{-1} and, in the second case, two different words w_1, w_2 have different Gödel numbers and hence $e^{\gamma(w_1)}$ cannot reduce with $e^{-\gamma(w_2)}$. Therefore we have no relation between the generators g_w, i.e. they define a system of free generators for H.

Denote by N the subgroup generated by a subset X of L and assume that X is recursively enumerable. Our task is to prove that N is benign in L.

Let $Y = Gp\{h, a, b, c^ide^i : i \in \Gamma(X)\}$. Since a, b, c, d, e, h are free, Y is free generated in K and more, we can show that:

$$N = Gp\{H \bigcap Y, h, c, d, e\} \bigcap Gp\{a, b\} \text{ in } K.$$

"$\subseteq$" $N \subseteq Gp\{a, b\}$ for $X \subseteq L$. It remains to prove that $Gp\{H \bigcap Y, h, c, d, e\}$ is a subgroup of K which contains X. Thus, if $w \in X$, then we can put:

$$w = whc^{\gamma(w)}de^{\gamma(w)}e^{-\gamma(w)}d^{-1}c^{-\gamma(w)}h^{-1} \Longleftrightarrow w = g_w[hc^{\gamma(w)}de^{\gamma(w)}]^{-1}$$

with $\gamma(w) \in \Gamma(X)$, hence $w \in Gp\{H \bigcap Y, h, c, d, e\}$. Since N is defined by the intersection of all the subgroups of K that contain X we conclude that "$\subseteq$" holds.

"$\supseteq$" Let $w \in Gp\{H \bigcap Y, h, c, d, e\}$. Then $w \in Gp\{a, b\}$ iff all h, c, d, e reduce. But any generator of $H \bigcap Y$ is a code-word g_w with $\gamma(w) \in \Gamma(X)$ (i.e. with $w \in X$) and thus every $w \in Gp\{H \bigcap Y, h, c, d, e\} \bigcap Gp\{a, b\}$ has the form $w = g_w[hc^{\gamma(w)}de^{\gamma(w)}]^{-1}$ with $w \in X$.

Now we have to prove that N is benign in K. From Lemma 9.7, it suffices to show that H and Y are benign in K.

If we put $Y = Gp\{\langle h, a, b\rangle,\ \langle c^ide^i, i \in \Gamma(X)\rangle\}$ from the same lemma we have to show that $\langle h, a, b\rangle$ and $\langle c^ide^i,\ i \in \Gamma(X)\rangle$ are benign in K. Thus, $\langle h, a, b\rangle$ is benign in K since it is finitely generated; $\langle c^ide^i, \in \Gamma(X)\rangle$ is benign in $\langle c, d, e\rangle$ for we have X recursively enumerable and hence $\Gamma(X)$ is recursively enumerable and the conditions of the lemma are fulfilled. It remains to prove that $\langle c^ide^i, i \in \Gamma(X)\rangle$ is benign in K too.

We shall use the HNN-extensions and for this we denote $A = \langle c^ide^i, i \in \Gamma(X)\rangle$ and $C = \langle c, d, e\rangle$. Since A is benign in C (Lemma 9.7) then

$$C_A = \langle C, t; t^{-1}(c^ide^i)t = c^ide^i, i \in \Gamma(X)\rangle$$

embeds in a finitely presented group M_1 while

$$K_C = \langle K, s; s^{-1}gs = g, g \in \{c, d, e\}\rangle$$

embeds in finitely presented group M_2.

Let $P = \langle M_1 * M_2; C = C\rangle$. In order to show that A is benign in K we shall prove that

$$K_A = \langle K, x; x^{-1}(c^ide^i)x = c^ide^i, i \in \Gamma(X)\rangle$$

embeds in P. For that, define $\Phi : K_A \longrightarrow P$ by $x \mapsto ts,\ y \mapsto y$, where $y \in \{a, b, c, d, e, h\}$ and thus we get an isomorphism between K_A and the subgroup $Gp\{K, ts\}$ of P. We need to verify that Φ preserves the defining relations:

$$\begin{aligned}
\Phi(x^{-1}(c^i de^i)x) &= \Phi(x^{-1})\Phi(c^i)\Phi(d)\Phi(e^i)\Phi(x) \\
&= s^{-1}t^{-1}(c^i de^i)ts \\
&= s^{-1}[t^{-1}(c^i de^i)t]s \\
&= s^{-1}(c^i de^i)s \ (in\ M_1) \\
(s^{-1}c^i s)(s^{-1}ds)(s^{-1}e^i s) & \\
&= c^i de^i \ (in\ M_2) \\
&= \Phi(c^i)\Phi(d)\Phi(e^i) \\
&= \Phi(c^i de^i).
\end{aligned}$$

Thus K_A is isomorphic to a subgroup of the finitely presented group P. (Note that P is finitely presented since it is defined as a free product with amalgamation and the amalgamated part C is finitely generated.) It results that A is benign in K. Now we can state that Y is benign in K.

We have also to prove that H is benign in K. For this, let

$$K^* = \langle K, t_\lambda, \lambda \in \{a, b, a^{-1}, b^{-1}\}; R^* \rangle$$

where the set R^* of defining relations is given by:

$$\begin{aligned}
t_\lambda^{-1} a t_\lambda &= a, \\
t_\lambda^{-1} b t_\lambda &= b, \\
t_\lambda^{-1} c t_\lambda &= c^{10}, \\
t_\lambda^{-1} d t_\lambda &= c^{\gamma(\lambda)} de^{\gamma(\lambda)}, \\
t_\lambda^{-1} e t_\lambda &= e^{10}, \\
t_\lambda^{-1} h t_\lambda &= \lambda h,
\end{aligned}$$

with $\lambda \in \{a, b, a^{-1}, b^{-1}\}$.

One can easily see that if we define $\Phi_\lambda : K \longrightarrow C_\lambda$ by $a \mapsto a,\ b \mapsto b, c \mapsto c^{10},\ d \mapsto c^{\gamma(\lambda)} de^{\gamma(\lambda)},\ e \mapsto e^{10},\ h \mapsto \lambda h$, where $\lambda \in \{a, b, a^{-1}, b^{-1}\}, C_\lambda = \langle a, b, h, c^{10}, e^{10}, c^{\gamma(\lambda)} de^{\gamma(\lambda)} \rangle$ then K^* becomes an HNN-extension of K with stable letter λ and associated subgroups K and C_λ.

Using the relations that define R^* we can prove that:

($\star$) If $w = \lambda_1 \lambda_2 \dots \lambda_n$ is a word on generators a, b, a^{-1}, b^{-1}, then

$$t_{\lambda_n}^{-1} \dots t_{\lambda_1}^{-1} h d t_{\lambda_1} \dots t_{\lambda_n} = g_w.$$

($\star\star$) If $w = u\lambda$ is a word ending in the letter λ with $\lambda \in \{a, b, a^{-1}, b^{-1}\}$, then

$$t_\lambda g_w t_\lambda^{-1} = g_u.$$

Thus we have:

$$\begin{aligned}
t_{\lambda_n}^{-1} \dots t_{\lambda_1}^{-1} h d t_{\lambda_1} \dots t_{\lambda_n} &= t_{\lambda_n}^{-1} \dots (t_{\lambda_1}^{-1} h t_{\lambda_1})(t_{\lambda_1}^{-1} d t_{\lambda_1}) \dots t_{\lambda_n} \\
&= t_{\lambda_n}^{-1} \dots t_{\lambda_2}^{-1} (\lambda_1 h)(c^{\gamma(\lambda_1)} de^{\gamma(\lambda_1)}) t_{\lambda_2} \dots t_{\lambda_n} \\
&= \lambda_1 t_{\lambda_n}^{-1} \dots t_{\lambda_2}^{-1} h c^{\gamma(\lambda_1)} de^{\gamma(\lambda_1)} t_{\lambda_2} \dots t_{\lambda_n} \\
&= \lambda_1 t_{\lambda_n}^{-1} \dots (t_{\lambda_2}^{-1} h t_{\lambda_2})(t_{\lambda_2}^{-1} c^{\gamma(\lambda_1)} t_{\lambda_2}(t_{\lambda_2}^{-1} d t_{\lambda_2})(t_{\lambda_2}^{-1} e^{\gamma(\lambda_1)} t_{\lambda_2}) \dots t_{\lambda_n} \\
&= \lambda_1 t_{\lambda_n}^{-1} \dots \lambda_2 h c^{10\gamma(\lambda_1)} c^{\gamma(\lambda_2)} de^{\gamma(\lambda_2)} e^{10\gamma(\lambda_1)} t_{\lambda_3} \dots t_{\lambda_n}.
\end{aligned}$$

One can easily check that since $t_\lambda^{-1} c t_\lambda = c^{10}$, then $t_\lambda^{-1} c^\alpha t_\lambda = c^{10\alpha}$ for every $\alpha \in I\!N$ and the same relation is also true for e.

Also note that if $w = \lambda_1 \dots \lambda_n$, then by definition we get:

$$\gamma(w) = \gamma(\lambda_1 \dots \lambda_n) = 10^{n-1}\gamma(\lambda_1) + 10^{n-2}\gamma(\lambda_2) + \dots + 10\gamma(\lambda_{n-1}) + \gamma(\lambda_n)$$

in the base 10.

Continuing the calculus of $t_{\lambda_n}^{-1} \dots t_{\lambda_1}^{-1} h d t_{\lambda_1} \dots t_{\lambda_n}$ using the same technics as above it follows:

$$\begin{aligned} t_{\lambda_n}^{-1} \dots t_{\lambda_1}^{-1} h d t_{\lambda_1} \dots t_{\lambda_n} &= \lambda_1\lambda_2 \dots \lambda_{n-1} t_{\lambda_n}^{-1} h c^{10^{n-2}\gamma(\lambda_1)+\dots+\gamma(\lambda_{n-1})} d e^{10^{n-2}\gamma(\lambda_1)+\dots+\gamma(\lambda_{n_1})} t_{\lambda_n} \\ &= \lambda_1 \dots \lambda_n h c^{10^{n-1}\gamma(\lambda_1)+\dots+10\gamma(\lambda_{n-1})+\gamma(\lambda_n)} d e^{10^{n-1}\gamma(\lambda_1)+\dots+10\gamma(\lambda_{n-1})+\gamma(\lambda_n)} \\ &= wh\ c^{\gamma(w)} d e^{\gamma(w)}\ = g_w. \end{aligned}$$

Thus $(\star)$ is true.

In order to prove $(\star\star)$, consider $w = u\lambda$ and then

$$t_\lambda g_w t_\lambda^{-1} = t_\lambda u\lambda h c^{\gamma(u\lambda)} d e^{\gamma(u\lambda)} t_\lambda^{-1} = u\lambda(t_\lambda h) c^{\gamma(u\lambda)} d e^{\gamma(u\lambda)} t_\lambda^{-1} = u\lambda\lambda^{-1} h t_\lambda c^{\gamma(u\lambda)} d e^{\gamma(u\lambda)} t_\lambda^{-1}.$$

On the other hand we have:

$$\gamma(u\lambda) = 10\gamma(u) + \gamma(\lambda) \text{ in the base } 10$$

and

$$t_\lambda^{-1} c^\alpha t_\lambda = c^{10\alpha} \Longrightarrow t_\lambda c^{10\alpha} = c^\alpha t_\lambda \text{ for every } \alpha \in \mathbb{N},$$

and we get

$$t_\lambda c^{10\gamma(u)+\gamma(\lambda)} = t_\lambda c^{10\gamma(u)} c^{\gamma(\lambda)} = c^{\gamma(u)} t_\lambda c^{\gamma(\lambda)}.$$

Note that the analogous relations hold for the generator e.

Hence we can write:

$$t_\lambda g_w t_\lambda^{-1} = uhc^{\gamma(u)} t_\lambda c^{\gamma(\lambda)} d e^{\gamma(\lambda)} t_\lambda^{-1} = uhc^{\gamma(u)} t_\lambda t_\lambda^{-1} d t_\lambda t_\lambda^{-1} = uhc^{\gamma(u)} d e^{\gamma(u)} = g_u.$$

Now we claim that in K^*

$$H = Gp\{hd, t_\lambda, \lambda \in \{a, b, a^{-1}, b^{-1}\}\} \bigcap K. \tag{10}$$

If we establish this equality we can see that H is the intersection of two finitely generated subgroups of K^*, hence they are benign subgroups and from Lemma 9.7 H will be benign in K^*. Since $H \subset K \subset K^*$ it follows that H is benign in K.

Thus the subgroup N of L generated by a recursively enumerable subset X is benign in K, and since $N \subset L \subset K$, N will be benign in L. This will conclude the proof of the theorem.

The last part of the proof that remains to be done is to establish the equality (10).

"$\subseteq$" Let $g_w \in H$ be a code-word of an element w on the generators a, b, a^{-1}, b^{-1} hence $w = \lambda_1 \dots \lambda_n$ with $\lambda_i \in \{a, b, a^{-1}, b^{-1}\},\ 1 \le i \le n$. From $(\star)$ we deduce that $g_w \in Gp\{hd, t_\lambda, \lambda \in \{a, b, a^{-1}, b^{-1}\}\}$. Since $H \subseteq K$ it is clear that $g_w \in K$ and hence " $\subseteq$" is true.

"$\supseteq$" Let $T \in Gp\{hd, t_\lambda, \lambda \in \{a, b, a^{-1}, b^{-1}\}\} \bigcap K$. $T \in K$ means that no stable letter of K^* is contained in T. There will be a sequence of succesive reductions of the stable letters t_λ and namely, we denote by $T_0 = T,\ T_1, \dots, T_m$ a sequence of words such that every T_{i+1} is obtained from T_i by a single stable letter reduction and T_m contains no stable letters.

Consider z a subword of T_i between succesive occurrences of the stable letters, that is $T_i = S_1 t_\lambda^\epsilon z t_\mu^\delta S_2$ where z contains no t_λ. Note that the defining relations of K^* require $\epsilon\delta = -1$ and $\lambda = \mu$. In that case T_i will contain sequences of the form $t_\lambda^{-1} z t_\lambda$ and $t_\lambda z t_\lambda^{-1}$.

We prove that if $z \in H$ then $t_\lambda^{-1} z t_\lambda \in H$. For $T = T_0$ the statement is true since the subwords z between two succesive occurrences of t_λ are generated by hd and hence, from $(\star)$, we have:

$$t_\lambda^{-1}(hd)^\alpha t_\lambda = \underbrace{(\ t_\lambda^{-1}(hd)t_\lambda)(\ t_\lambda^{-1}(hd)t_\lambda) \dots (\ t_\lambda^{-1}(hd)t_\lambda)}_{\alpha \text{ times}} = g_\lambda^\alpha \in H.$$

For T_i, if z is any word of H, $z = g_{w_1}^{\epsilon_1} \dots g_{w_n}^{\epsilon_n},\ \epsilon_i \in \{-1, 1\},\ 1 \le i \le n$, we have:

$$t_\lambda^{-1} g_{w_1}^{\epsilon_1} \dots g_{w_n}^{\epsilon_n} t_\lambda = (t_\lambda^{-1} g_{w_1}^{\epsilon_1} t_\lambda) \dots (t_\lambda^{-1} g_{w_n}^{\epsilon_n} t_\lambda).$$

Since $w_i = \lambda_{i_1} \dots \lambda_{i_k}$, with $\lambda_{i_j} \in \{a, b, a^{-1}, b^{-1}\},\ 1 \le j \le k$, we deduce that each sequence $t_\lambda^{-1} g_{w_i}^{\epsilon_i} t_\lambda$ from the above product can be written as follows (see $(\star)$):

$$t_\lambda^{-1} g_{w_i}^{\epsilon_i} t_\lambda = t_\lambda^{-1}(t_{\lambda_{i_k}}^{-1} \dots t_{\lambda_{i_1}}^{-1} h dt_{\lambda_{i_1}} \dots t_{\lambda_{i_k}})^{\epsilon_i} t_\lambda = (t_\lambda^{-1} t_{\lambda_{i_k}}^{-1} \dots t_{\lambda_{i_1}}^{-1} h dt_{\lambda_{i_1}} \dots t_{\lambda_{i_k}} t_\lambda)^{\epsilon_i} = g_{w_i\lambda}^{\epsilon_i}$$

and we get

$$t_\lambda^{-1} z t_\lambda = g_{w_1\lambda}^{\epsilon_1} \dots g_{w_n\lambda}^{\epsilon_n} \in H.$$

If the sequences $t_\lambda z t_\lambda^{-1}$ with $z \in H$ reduce also to elements of H, then it is clear that T_m, after all these reductions, will be a product of elements belonging to H. Since H is a subgroup T_m will be an element of it.

Consider $z \in H,\ z = g_{w_1}^{\epsilon_1} \dots g_{w_n}^{\epsilon_n},\ \epsilon_i \in \{-1, 1\},\ 1 \le i \le n$, and there are no succesive g_w and g_w^{-1}. Note that we can put

$$z = (w_1 h c^{\gamma(w_1)} d e^{\gamma(w_1)})^{\epsilon_1} \dots (w_n h c^{\gamma(w_n)} d e^{\gamma(w_n)})^{\epsilon_n}$$

and the sequences $(c^{\gamma(w)} d e^{\gamma(w)})^\epsilon$ do not reduce.

On the other hand, if $z \in H \subseteq K$, the image of z through the isomorphism Φ_λ will belong to C_λ (the subgroup associated to K in the HNN-extension K^*). Since C_λ is freely generated by $h, a, b, c^{10}, e^{10}, c^{\gamma(\lambda)} d e^{\gamma(\lambda)}$ (see the defining relations of R^*) we conclude that $z \in C_\lambda$ iff the power exponents of c and e are congruent modulo 10 to 0 or $\underline{+}\gamma(\lambda)$. Thus

$$\gamma(w_i) \equiv 0 (\mathrm{mod} 10)$$

or

$$(\gamma(w_i))^{\epsilon_i} \equiv \underline{+}\gamma(\lambda) (\mathrm{mod} 10),\ 1 \le i \le n.$$

If $w = u\lambda$ is a word ending on λ then $\gamma(w) = 10\gamma(u) + \gamma(\lambda)$ and hence $\gamma(w) \equiv \gamma(\lambda) (\mathrm{mod} 10)$. It results that $z \in C_\lambda$ iff all words w_i (whose code-words g_{w_i} determinate the element z) end on λ. In the same time, for any other letter $\beta \neq \lambda$, the congruences $\gamma(\beta) \equiv \gamma(\lambda) (\mathrm{mod} 10)$ and $\gamma(\beta) \equiv 0 (\mathrm{mod} 10)$ are false (the definition of the function γ says that $\gamma(\alpha) \in \{1, 2, 3, 4\}$ with $\alpha \in \{a, b, a^{-1}, b^{-1}\}$). If all w_i end in λ we can write $w_i = u_i\lambda$ and using $(\star\star)$

$$t_\lambda z t_\lambda^{-1} = (t_\lambda g_{w_1}^{\epsilon_1} t_\lambda^{-1}) \dots (t_\lambda g_{w_n}^{\epsilon_n} t_\lambda^{-1}) = (t_\lambda g_{w_1} t_\lambda^{-1})^{\epsilon_1} \dots (t_{la} g_{w_n} t_\lambda^{-1})^{\epsilon_n} = g_{u_1}^{\epsilon_1} \dots g_{u_n}^{\epsilon_n}$$

and finally $t_\lambda z t_\lambda^{-1} \in H$. □

References

[1] C. Calude, *Theories of Computation Complexity*, North-Holland, Amsterdam, Tokyo, Oxford, New York, 1988.

[2] G. Higman, Subgroups of finitely presented groups, *Proc. Royal Soc. London* Ser. A262, 455-475, 1961.

[3] G. Higman and B. H. Neumann and H. Neumann, Embedding theorems for groups, *J. London Math. Soc.* 24, 247-254, 1949.

[4] Ion D. Ion and N. Radu, *Algebra*, Editura Didactică şi Pedagogică, Bucharest, 1981. (in Romanian)

[5] N. Jacobson, *Basic Algebra*, Freeman, San Francisco, 1965.

[6] A. G. Kurosh, *The Theory of Groups*, Chelsea Pub. Co., New York, 1956.

[7] C. Lyndon and P. Schupp, *Combinatorial Group Theory*, Springer-Verlag, Berlin, Heidelberg, New York, 1977.

[8] Yu. Y. Manin, *A Course in Mathematical Logic*, Springer-Verlag, New York, Heidelberg, Berlin, 1977.

[9] V. Yu. Matijasevich, *Hilbert's Tenth Problem*, MIT Press, Cambridge, MA, 1993.

[10] C. Năstăsescu, C. Niţă and C. Vraciu, *Basic Algebra*, Editura Academiei R.S.R., Bucharest, 1986. (in Romanian)

[11] J. Rotman, *The Theory of Groups*, Allyn and Bacon, Inc., Boston, 1973.