The proof of this lema proceed by the following two lemmas:

Lemma 1.7.17: Let r, s be distinct elements of $\{1, 2, \dots, n\}$. Then A_n $(n \geq 3)$ is generated by the 3-cycles $\{(rsk) \; 1 \leq k \leq n, \; k \neq r, s\}$.

proof: Assume $n > 3$ (the case $n = 3$ is trivial). Every element of A_n is a product of terms of the form $(ab)(cd)$ or $(ab)(ac)$, where a, b, c, d are distinct elements of $\{1, 2, \dots, n\}$. Since $(ab)(cd) = (acb)(acd)$ and $(ab)(ac) = (acb)$, A_n is generated by the set of all 3-cycles. Any 3-cycle is of the form (rsa), (ras), (rab), (sab), or (abc), where a, b, c are distinct and $a, b, c \neq r, s$. Since $(ras) = (rsa)^2$, $(rab) = (rsb)(rsa)^2$, $sab = (rsb)^2(rsa)$, and $(abc) = (rsa)^2(rsc)(rsb)^2(rsa)$, A_n is generated by

$$\{(rsk) \mid 1 \leq k \leq n, \; k \neq r, s\}.$$

Lemma 1.7.18: If N is a normal subgroup of A_n $(n \geq 3)$ and N contains a 3-cycle, then $N = A_n$.

proof: $(rsc) \in N \Rightarrow (rsk) = (rs)(ck)(rsc)^2(ck)(rs) = [(rs)(ck)](rsc)^2[(rs)(ck)]^{-1} \in N$ for any $k \neq r, s, c$. Hence $N = A_n$ by Lemma 1.7.17.

proof of Lemma 1.7.16 is a reading assignment:

Def 1.7.19: The subgroup D_n of S_n $(n \geq 3)$ generated by

i) $a = (123 \ldots n)$ and

ii) $b = \begin{pmatrix} 1 & 2 & 3 & \ldots & i & \ldots & n-1 & n \\ 1 & n & n-1 & \ldots & n+2-i & \ldots & 3 & 2 \end{pmatrix}$

$$= \prod_{2 \leq i < n+2-i} (i \quad n+2-i)$$

is called the dihedral group of degree n.

Remark 1.7.20:

a) The group D_n is isomorphic to and usually identified with the group of all symmetries of a regular polygon with n sides.

b) D_4 is (isomorphic to) the group D_4^* of symmetries of the square, see Example 1.2.9:

Thm 1.7.21: For each $n \geq 3$, the dihedral group D_n is a group of order $2n$ whose generators a and b satisfy

i) $a^n = (1)$; $b^2 = (1)$; $a^k \neq (1)$ if $0 < k < n$;

ii) $ba = a^{-1}b$.

Any group G which is generated by elements $a, b \in G$ satisfying i) & ii) for some $n \geq 3$ (with $e \in G$ in place of (1)) is isomorphic to D_n.

b) Let $\mathcal{G}$ be the category whose objects are all groups; hom (A, B) is the set of all group homomorphisms $f: A \to B$. A morphism f is an equivalence iff f is an isomorphism.

c) A (multiplicative) group G can be considered as a category with one object G. Let hom (G, G) be the set of elements of G; composition of morphisms a, b is simply the composition ab given by the binary operation in G. Since every element of G has an inverse every morphism is an equivalence. Note that 1_G is the identity element e of G.

Def 1.8.4: Let $\mathcal{C}$ be a category and $\{A_i \mid i \in I\}$ a family of objects of $\mathcal{C}$. A product for the family $\{A_i \mid i \in I\}$ is an object P of $\mathcal{C}$ together with a family of morphisms $\{\pi_i : P \to A_i \mid i \in I\}$ such that for any object B and family of morphisms $\{\phi_i : B \to A_i \mid i \in I\}$, there is a unique morphism $\varphi: B \to P$ such that $\pi_i \circ \varphi = \varphi_i$ for all $i \in I$.

▷ A product P for $\{A_i \mid i \in I\}$ is usually denoted $\prod_{i \in I} A_i$.

Def 1.8.5: A coproduct (or sum) for the family $\{A_i \mid i \in I\}$ of objects in a category $\mathcal{C}$ is an object S of $\mathcal{C}$, together with a family of morphisms $\{\iota_i : A_i \to S \mid i \in I\}$ such that for any object B and family of morphisms $\{\psi_i : A_i \to B \mid i \in I\}$ there is a unique morphism $\psi : S \to B$ such that $\psi \circ \iota_i = \psi_i$ for all $i \in I$.

Def 1.8.6: A concrete category is a category $\mathcal{C}$ together with a function σ that assigns to each object A of $\mathcal{C}$ a set $\sigma(A)$ (called the underlying set of A) in such a way that:

i) every morphism $A \to B$ of $\mathcal{C}$ is a function on the underlying sets $\sigma(A) \longrightarrow \sigma(B)$;

ii) the identity morphism of each object A of $\mathcal{C}$ is the identity function on the underlying set $\sigma(A)$;

iii) composition of morphisms in $\mathcal{C}$ agrees with composition of functions on the underlying sets.

Def 1.8.7: Let F be an object in a concrete category $\mathcal{C}$, X a non empty set, and $i : X \to F$ a map (of sets). F is free on the set X provided that for any object A of $\mathcal{C}$ and map (of sets) $f : X \to A$, there exists a unique morphism of $\mathcal{C}$, $\bar{f} : F \to A$, such that $\bar{f} i = f$ (as a map of sets $X \to A$).

1.9 Direct Products and Direct Sums

In this section we study products in the category of groups and coproducts in the category of abelian groups. These products and coproducts are important not only as a means of constructing new groups from old, but also for describing the structure of certain groups in terms of particular subgroups (whose structure, for instance, may already be known).

Let us start by extending the definition of the direct product $G \times H$ of groups G and H to an arbitrary (possibly infinite) family of groups $\{G_i \mid i \in I\}$.

Def: Define a binary operation on the Cartesian product (of sets) $\prod_{i \in I} G_i$ as follows: If $f, g \in \prod_{i \in I} G_i$, that is,

$(f, g : I \longrightarrow \bigcup_{i \in I} G_i$ and $f(i), g(i) \in G_i$ for each $i)$,

then $fg : I \longrightarrow \bigcup_{i \in I} G_i$ is the function given by

$i \mapsto f(i)g(i)$. Since each G_i is a group, $f(i)g(i) \in G_i$ for every i whence $fg \in \prod_{i \in I} G_i$. If we identify

$f \in \prod_{i \in I} G_i$ with its image $\{a_i\}$ ($a_i = f(i)$ for each $i \in I$) as is usually done in the case when I is finite, then the binary operation in $\prod_{i \in I} G_i$ is the familiar component-wise multiplication: $\{a_i\}\{b_i\} = \{a_ib_i\}$.

Def 1.9.1: The set $\prod_{i \in I} G_i$ together with the above binary operation is called the direct product (or complete direct sum) of the family of groups $\{G_i \mid i \in I\}$. If $I = \{1, 2, \ldots, n\}$ $\prod_{i \in I} G_i$ is usually denoted $G_1 \times G_2 \times \ldots \times G_n$ (or in additive notation, $G_1 \oplus G_2 \oplus \ldots \oplus G_n$).

Thm 1.9.2: If $\{G_i \mid i \in I\}$ is a family of groups, then

i) the direct product $\prod_{i \in I} G_i$ is a group

ii) for each $k \in I$, the map

$$\pi_k : \prod_{i \in I} G_i \to G_k$$

$$f \mapsto f(k) \quad (\text{or } \{a_i\} \mapsto a_k)$$

is an epimorphism of groups.

NB The maps π_k are called the cannonical projections of the direct product.

1.9 Direct Products and Direct Sums

In this section we study products in the category of groups and coproducts in the category of abelian groups. These products and coproducts are important not only as a means of constructing new groups from old, but also for describing the structure of certain groups in terms of particular subgroups (whose structure, for instance, may already be known).

Let us start by extending the definition of the direct product $G \times H$ of groups G and H to an arbitrary (possibly infinite) family of groups $\{G_i \mid i \in I\}$.

: Define a binary operation on the Cartesian product (of sets) $\prod_{i \in I} G_i$ as follows: If $f, g \in \prod_{i \in I} G_i$, that is, ($f, g : I \longrightarrow \bigcup_{i \in I} G_i$ and $f(i), g(i) \in G_i$ for each i), then $fg : I \longrightarrow \bigcup_{i \in I} G_i$ is the function given by $i \mapsto f(i)g(i)$. Since each G_i is a group, $f(i)g(i) \in G_i$ for every i whence $fg \in \prod_{i \in I} G_i$. If we identify

Thm 1.9.3: Let $\{G_i \mid i \in I\}$ be a family of groups and $\{\varphi_i : H \to G_i \mid i \in I\}$ a family of group homs. Then there is a unique hom $\varphi : H \longrightarrow \prod_{i\in I} G_i$ such that $\pi_i \varphi = \varphi_i$ for all $i \in I$ and this property determines $\prod_{i\in I} G_i$ uniquely up to isomorphism. In other words, $\prod_{i\in I} G_i$ is a product in the category of groups.

R) Since the direct product of abelian groups is clearly abelian, it follows that the direct product of abelian groups is a product in the category of abelian groups also.

Def 1.9.4: The (external) weak direct product of a family of groups $\{G_i \mid i \in I\}$, denoted $\prod^{w}_{i\in I} G_i$ is the set of all $f \in \prod_{i\in I} G_i$ such that $f(i) = e_i$, the identity in G_i, for all but a finite no of $i \in I$. If all the groups G_i are (additive) abelian, $\prod^{w}_{i\in I} G_i$ is usually called the (external) direct sum & is denoted $\sum_{i\in I} G_i$.

Def 1.9.5: Let $\{N_i \mid i \in I\}$ be a family of normal subgroups of a group G such that $G = \langle \bigcup_{i \in I} N_i \rangle$ and for each $k \in I$,

$$N_k \cap \langle \bigcup_{k \neq i} N_i \rangle = \langle e \rangle.$$

Then G is said to be the internal weak direct product of the family $\{N_i \mid i \in I\}$ (or the internal direct sum if G is (additive) abelian).

(ii) There is a distinction between internal and external weak direct products. If a group G is the internal weak direct products of groups N_i, then by defn each N_i is actually a subgroup of G and G is isomorphic to the external weak direct product $\prod_{i \in I}^{w} N_i$. However, the external weak direct product $\prod_{i \in I}^{w} N_i$ does not actually contain the groups N_i, but only isomorphic copies of them (namely the $\iota_i(N_i)$)

1.10: Free Groups, Free Products and Generators & Relations

In this section, we show that free objects (free groups) exists in the (concrete) category of groups, and we shall use these to develop a method of describing groups in terms of generators & relations.

In the following, we see how to construct free group on a given set X.

Constructing Free group on ~~b~~ a set ~~X~~

Given a set X, we shall construct a group F that is free on the set X in the sense of Defn 1.8.7.

Constructing free group on the set X.

Given

If $X = \phi$, F is the trivial group $\langle e \rangle$.
If $X \neq \phi$, let X^{-1} be a set disjoint from X such that $|X| = |X^{-1}|$. Choose a bijection $X \longrightarrow X^{-1}$ and denote the image of $x \in X$ by x^{-1}. Finally choose a set that is disjoint from $X \cup X^{-1}$ and has exactly one element; denote this element by 1.

Def^n 1.10.1: A word on X is a sequence $(a_1, a_2, \ldots)$ with $a_i \in X \cup X^{-1} \cup \{1\}$ such that for some $n \in \mathbb{N}^*$, $a_k = 1$ for all $k \geq n$. The constant sequence $(1, 1, \ldots)$ is called the empty word and is denoted 1.

Def^n 1.10.2: A word $(a_1, a_2, \ldots)$ on X is said to be reduced provided that

i) for all $x \in X$, x and x^{-1} are not adjacent (that is, $a_i = x \Rightarrow a_{i+1} \neq x^{-1}$ and $a_i = x^{-1} \Rightarrow a_{i+1} \neq x$ for all $i \in \mathbb{N}^*$, $x \in X$) and

ii) $a_k = 1 \Rightarrow a_i = 1$ for all $i \geq k$.

In particular, the empty word 1 is reduced.

Every nonempty reduced word is of the form $(x_1^{\lambda_1}, x_2^{\lambda_2}, \dots, x_n^{\lambda_n}, 1, 1, \dots)$, where $n \in \mathbb{N}^*$, $x_i \in X$ and $\lambda_i = \pm 1$

Convention: $x^{\lambda} = x$ if $\lambda = 1$

: We denote the reduced word by $x_1^{\lambda_1} \dots x_n^{\lambda_n}$

Def^n 1.10.3: Two reduced words $x_1^{\lambda_1} \dots x_n^{\lambda_n}$ and $y_1^{\delta_1} \dots y_m^{\delta_m}$ are equal iff both are 1 or $m = n$ and $x_i = y_i$, $\lambda_i = \delta_i$ for each $i = 1, 2, \dots, n$.

Consider ~~the~~ the map

the set of all reduced words on X

$$\varphi : X \to F(X)$$
$$x \mapsto x^1 = x.$$

~~that maps~~

The map φ is injective.

Define a binary operation on the set $F(X) = F$ of all reduced words on X. The empty word 1 is to act as an identity element ($w1 = 1w = w$ for all $w \in F$).

Let $x, y \in F$. Then

$$x = x_1^{\lambda_1} \dots x_n^{\lambda_n} \text{ and } y = y_1^{\delta_1} \dots y_m^{\delta_m}$$

$$xy = x_1^{\lambda_1} \dots x_n^{\lambda_n} \cdot y_1^{\delta_1} \dots y_m^{\delta_m} = x_1^{\lambda_1} \dots x_n^{\lambda_n} y_1^{\delta_1} \dots y_m^{\delta_m}$$

But xy need not be reduced for example if $x_n^{\lambda_n} = y_1^{-\delta_1}$

For example, $(x_1 x_2^{-1} x_3)(x_3^{-1} x_2 x_4) = x_1 x_4$. More precisely, if $x_1^{\lambda_1} \cdots x_n^{\lambda_n}$ and $y_1^{\delta_1} \cdots y_m^{\delta_m}$ are ~~two~~ nonempty reduced words on X with $n \le m$, let k be the largest integer $(0 \le k \le m)$ such that $x_{n-j}^{\lambda_{n-j}} = y_{j+1}^{-\delta_{j+1}}$ for $j = 0, 1, \ldots, k-1$.

Then define

$$(x_1^{\lambda_1} \cdots x_n^{\lambda_n})(y_1^{\delta_1} \cdots y_m^{\delta_m}) = \begin{cases} x_1^{\lambda_1} \cdots x_{n-k}^{\lambda_{n-k}} y_{k+1}^{\delta_{k+1}} \cdots y_m^{\delta_m} & \text{if } k < n \\ y_{n+1}^{\delta_{n+1}} \cdots y_m^{\delta_m} & \text{if } k = n < m \\ 1 & \text{if } k = m = n \end{cases}$$

(ii) If $n > m$, the product is defined analogously.

Theorem 1.10.4: If X is a nonempty set and $F = F(X)$ is the set of all reduced words on X, then F is a group under the binary operation defined above and $F = \langle X \rangle$.

Defn 1.10.5 The group $F = F(X)$ is called the free group on the set X.

Corollary 1.10.7 Every group G is the homomorphic image of a free group.

Thm 1.10.6: Let F be the free group on a set X and $\iota : X \longrightarrow F$ the inclusion map. If G is a group and $f : X \longrightarrow G$ a map of sets, then there exists a unique homomorphism of groups $\bar{f} : F \longrightarrow G$ such that $\bar{f}\iota = f$. In other words, F is a free object on the set X in the category of groups.

$$\begin{tikzcd} X \arrow[r, "\iota"] \arrow[d, "f"'] \arrow[dr, phantom, "\#"] & F \arrow[dl, "\bar{f}"] \\ G & \end{tikzcd}$$

This diagram commutes: