8. FREE GROUPS

§8.1. Definition

Consider a presentation with no relations or relators such as $\langle x_1, x_2, \ldots, x_n | \rangle$. We call this the free group on the generators. Clearly free groups are infinite (except for the trivial case $\langle \, | \, \rangle$ where there are no generators. This is the trivial group, with one element).

The free group on one generator, such as $\langle A \, | \, \rangle$, is the infinite cyclic group, isomorphic to $\mathbb{Z}$ (under addition). Defining free groups in terms of presentations is good intuitively but it is the wrong way round. Remember that our discussion of group presentations was very informal. To define presentations rigorously we need to do it in terms of free groups. So we need a very precise and rigorous way of defining free groups, which is what we will be doing here.

Let X be a set and let X^{-1} be a set, disjoint from X, which is in 1-1 correspondence with X. Let the element of X^{-1} that corresponds to $x \in X$ be denoted by x^{-1}. And if $y = x^{-1}$ we define y^{-1} to be x.

Although x^{-1} will ultimately become the inverse of x, at this stage I haven't defined a binary operation, so we can't interpret it as an inverse yet.

I'll construct a group, generated by X, in which the inverse of x will be x^{-1} and where no relations hold except

for those of the form $xx^{-1} = x^{-1}x = 1$, for $x \in X$, or consequences of them. This will be called the **free group** on X.

A **word** on X is a string of symbols, each of which is in X or in X^{-1}.

Example 1:

Suppose $X = \{a, b, c\}$ and

$$X^{-1} = \{a^{-1}, b^{-1}, c^{-1}\}.$$

All six of these symbols are purely formal symbols, with no meaning. Then $ab^{-1}aa^{-1}cac^{-1}bb^{-1}cc$ is a word on X. We'd like to be able to cancel this down to $ab^{-1}cac$ but as yet we have no binary operation so the equation $ab^{-1}aa^{-1} = ab^{-1}$ as yet has no meaning.

Counting a^{-1}, b^{-1} and c^{-1} as single symbols we have $ab^{-1}aa^{-1}$ as a string of length 4 and ab^{-1} as a string of length 2, so as strings they're clearly not equal.

I define an **inverse pair** to be a string of the form xx^{-1} or $x^{-1}x$ for some $x \in$ X. I now define two words on X to be **adjacent** if one has the form ab while the other has the form awb where a, b are words on X and w is an inverse pair. I'll write $u \sim v$ if they're adjacent. What we call 'cancellation' is a process of removing inverse pairs from a string.

An **equivalence sequence** is a sequence of words with consecutive elements adjacent. It's **monotonic** if either each term is shorter than the next or if each term is longer than the next.

Example 2: $ab^{-1}aa^{-1}cac^{-1}bb^{-1}cc \to ab^{-1}aa^{-1}cac^{-1}cc$
$\to ab^{-1}cac^{-1}cc$
$\to ab^{-1}cab^{-1}bc^{-1}cc$
$\to ab^{-1}cab^{-1}bc$
$\to ab^{-1}cac$
is an equivalence sequence.
It's not monotonic because the lengths are 11, 9, 7, 9, 7 and 5 respectively.

On the other hand:
$ab^{-1}aa^{-1}cac^{-1}bb^{-1}cc \to ab^{-1}aa^{-1}cac^{-1}cc$
$\to ab^{-1}cac^{-1}cc$
$\to ab^{-1}cac$, and its reversal, are monotonic.

Whenever we cancel we reduce the length by 2 and whenever we insert an inverse pair we increase the length by 2. Normally in cancellation we never insert an inverse pair but it isn't obvious that one needn't do so. Perhaps introducing an inverse pair at some stage will give us additional symbols whereby we can come down a different cancellation path and arrive at a shorter string. In climbing to the highest point of a mountain you often have to go downhill before you can go up higher than before.

Here's an analogy. Suppose you had a matrix in which $A^6 = A^2$ and $A^9 = A^3$. Because A might be singular (ie. have no inverse) you wouldn't be justified in cancelling A's.

Now given the expression A^5 you can write is as a smaller power by the following equivalence sequence using the above relations:
$A^5 = A^2A^3 = A^6A^3 = A^9 = A^3$. Note that we had to increase the power before decreasing it again. There is in fact no monotonic sequence, which can take us from A^5 to A^3 using the above relations.

In the case of inverse pairs it *does* turn out that there's no need to make the string longer before making it shorter again.

A **reduced word** is one that contains no inverse pair. A reduced word is one where no cancellation is

possible. Words that are adjacent to a reduced word must be longer than it.

Theorem 1: Every equivalence sequence can be replaced by one where the deletions of inverse pairs all precede the insertions.

Proof: If a, b, c are adjacent words in an equivalence sequence, with b longer than either a or c, then b is obtained from a by inserting an inverse pair and c is obtained from b by removing an inverse pair (not necessarily the same one).

For example, we might have:
$a = y^{-1}zz^{-1}x$, $b = y^{-1}x^{-1}xzz^{-1}x$ and $c = y^{-1}x^{-1}xx$.

If these pairs are disjoint, as in the above example, the sequence can be modified by carrying out the deletion first.

In the above example we could take $b = y^{-1}x$. The sequence a, b, c would still be an equivalence sequence.

If the deletion simply removes the inserted inverse pair then $a = c$ and we can shorten the equivalence sequence by removing b and c.

The remaining case is where just one symbol in the inserted inverse pair belongs to the deleted pair. For example we might have $a = y^{-1}x^{-1}x$, $b = y^{-1}x^{-1}xx^{-1}x$ and $c = y^{-1}x^{-1}x$.

In going from b to c there are two possible inverse pairs that could have been removed and the x^{-1} that remains in c could be either of the two x^{-1}'s in b.

In this case we must have, for some words u, v, either:

$$a = uxv,\ b = uxx^{-1}xv \text{ and } c = uxv \text{ or}$$
$$a = ux^{-1}v,\ b = ux^{-1}xx^{-1}v = ux^{-1}v.$$

In the first case we inserted an xx^{-1} inverse pair and deleted an $x^{-1}x$ pair and in the second case we inserted an $x^{-1}x$ pair and removed an xx^{-1} pair. Although we didn't remove precisely the same inverse pair that we inserted, the effect is the same as if we did. In both cases $a = c$ and we can shorten the equivalence sequence by removing b and c.

Corollary: Every equivalence sequence between a word and a reduced word can be replaced by a monotonic one.

We say that two words u, v are **equivalent** if there's an equivalence sequence from one to the other. This is clearly an equivalence relation. Let $\mathbf{F(}\boldsymbol{X}\mathbf{)}$ denote the set of equivalence classes and let $\mathbf{[}\boldsymbol{w}\mathbf{]}$ denote the equivalence class containing the word w.

Theorem 2: Every word is equivalent to a unique reduced word.
Proof: The fact that every word is equivalent to a reduced word is obvious. Just remove inverse pairs until there are no more left. The uniqueness follows from the fact that if w is equivalent to two different reduced words they must be equivalent to one another. But there is no monotonic

equivalence sequence between two reduced words. (One of them would have to be adjacent to a shorter word.)

We define the **product** of these equivalence classes by **[*u*][*v*] = [*uv*]**. As usual we must check that this operation is well-defined, since it's defined in terms of class representatives.

Theorem 3: If u is equivalent to u' and v is equivalent to v' then uv is equivalent to $u'v'$.

Proof: We simply convert u to u' and v to v' independently.

Under this operation the set F(X) is a group, with $[\lambda]$ being the identity (here λ is the null string). The inverse of $[x_1 \ldots x_n]$, where each x_i is a generator or the inverse of a generator, is clearly $[x_n^{-1} \ldots x_1^{-1}]$. This is because the strings:

$$x_1 \ldots x_n x_n^{-1} \ldots x_1^{-1} \text{ and}$$
$$x_n^{-1} \ldots x_1^{-1} x_1 \ldots x_n$$

are both equivalent to λ.

The group F(X) so formed is called the **free group** on X. If there are n generators, F/F′ is isomorphic to the direct sum of n copies of $\mathbb{Z}$ and so a free group on a certain number of generators cannot be isomorphic to the free group on any other number of generators. We may therefore unambiguously define the **rank** of the free

group F(X) to be |X|, the cardinal number, or size, of X. We denote the free group on *n* generators by F_n.

Example 3: F_0 is the trivial group and $F_1 \cong \mathbb{Z}$. F_0 is the only *finite* free group. Both F_0 and F_1 are the only *abelian* free groups.

Theorem 4: Every group is a quotient of a free group.
Proof: If G is a group then F(G) is the free group on the set G (ignoring the group structure). Its elements are reduced words on the elements of G as meaningless symbols. If we now interpret the symbols according to the multiplication within G we get an element of G. The map ε that takes a string in the free group to its evaluation in G is clearly a homomorphism whose kernel consists of all those group words that collapse to the identity when evaluated in G. By the First Isomorphism Theorem, $F(G)/\ker(\varepsilon) \cong G$.

So quotients of free groups can be any arbitrary group. By contrast, as we'll show, subgroups of free groups must themselves be free.

Example 4: Let $G = \mathbf{D}_8 = \langle A, B \mid A^4, B^2, (AB)^2 \rangle$, the dihedral group of order 8. The elements are:

$$g_1 = 1, g_2 = A, g_3 = A^2, g_4 = A^3,$$
$$g_5 = B, g_6 = AB, g_7 = A^2B, g_8 = A^3B.$$

Let $X = \{g_1, g_2, g_3, g_4, g_5, g_6, g_7, g_8\}$.

Then F(X) is the free group of rank 8 whose elements are words in $g_1, \ldots, g_8, g_1^{-1}, \ldots, g_8^{-1}$.
Suppose $u = g_3 g_7^{-1} g_2 g_6^{-1} g_8$.
Then $\varepsilon(u) = (A^2)(A^2B)^{-1}(A)(AB)^{-1}(A^3B)$
$= A^2BA^{-1}BA^2B$
$= AB$
$= g_6$.
The kernel of ε will be generated by conjugates of the words: g_1, $g_3 g_2^{-1} g_2^{-1}$, $g_4 g_3^{-1} g_2^{-1}$, $g_6 g_5^{-1} g_2^{-1}$, $g_7 g_5^{-1} g_3^{-1}$, $g_8 g_5^{-1} g_4^{-1}$, $g_4 g_2$, $g_5 g_5$, $g_2 g_5 g_2 g_5$. The first six of these express the g_i in terms of g_2 and g_5 (which we were writing as A, B respectively). The last three correspond to the three defining relations for $\mathbf{D}_8$.

Of course we can represent this dihedral group as a quotient of the free group of rank 2, on the generators A, B. In this case the normal subgroup is generated by the conjugates of A^4, B^2 and ABAB.

§8.2. Presentations of Groups

We've become familiar with the notion of a group presentation but we have been just a little vague as to what it really is. Now that we have introduced free groups we can say precisely what $\langle X \mid R \rangle$ means.

Suppose X is a set and R is a set of words on X (the relators of the presentation). Let $\mathbf{R}^G$ denote the set of all products of conjugates of elements of R, and their inverses, by elements of $\langle X \rangle$.

Example 5: If $X = \{A, B\}$ and $R = \{B^2, ABAB\}$ then an example of an element of R^G is

$(A^2B)^{-1}(ABAB)(A^2B).(ABA^5)^{-1}(B^2)(ABA^5).$

$A^{-1}(ABAB)^{-1}A$

It's clear that in any group where $ABAB = 1$ and $B^2 = 1$ then such elements will be 1 as well. Now R^G is a normal subgroup of F(G) (a product of products is a product and a conjugate of a conjugate is a conjugate). It is in fact the smallest normal subgroup of F(G) that contains R. It's precisely the set of words that are forced to be trivial by the relators in R.

We now define $\langle X \mid R \rangle$ to be $F(X)/R^G$.

§ 8.3. Subgroups of Free Groups

Every group is a quotient of a free group. But subgroups of free groups are not so universal. In fact, every subgroup of a free group is free. I won't prove this in the general case, but only for subgroups of finite index in free groups of finite rank.

It would seem very natural to believe that if F is free and H is a subgroup of F then $\text{rank}(F) \leq \text{rank}(G)$. After all it *is* true for finite-dimensional vector spaces that if U is a subspace of V then $\dim(U) \leq \dim(V)$ and rank is a very similar concept to dimension. However it's certainly not the case here.

Example 6: Let F be the free group on {A, B} and let $H = \langle BAB, BBAABB, BBBAAABBB \rangle$. Then rank(F) = 2 while rank(H) = 3.

To check that indeed rank(H) = 3 we must show that {BAB, BBAABB, BBBAAABBB} is a free set of generators for H. In other words we must show that if we have a word in these three generators we can recover the way it was generated.

In any reduced word in these three generators the B's that will come between the blocks of A's so will never vanish. As a consequence the A's will remain intact and we can recover the original unreduced word.

For example, concentrating on the powers of A we can see that $BAB^3A^2B^{-1}A^{-3}B^{-1}A^2B^2$ can only have come from $(BAB)(BBAABB)^{-1}(BBAABB)$.

Let $K = \langle BAB, BBAABB, BBBAAABBB, \ldots \rangle$. Then, in a similar fashion to the above, we can show that these generators are free and so K is a free group of infinite rank.

So free groups of finite rank can have subgroups of infinite rank. However in such cases the index must also be infinite. A subgroup H of finite index in a free group G of finite rank must be a free group of finite rank, though the rank of H can be larger than that of G.

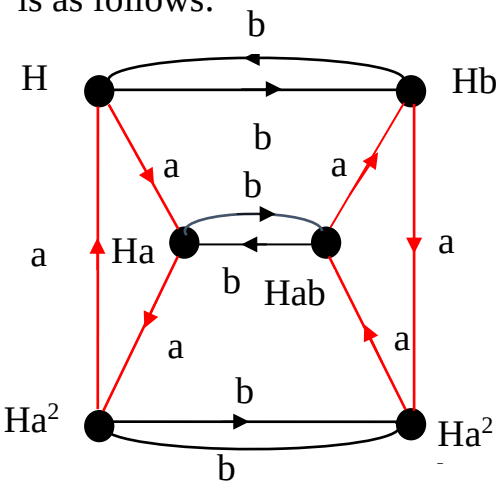
Suppose H is a subgroup of rank h in a free group F of rank r. We form a graph Γ, whose vertices are the right cosets of H in F. For every generator x and for every

vertex Hu we define an edge from H*u* to H*ux*. We label this by the generator *x*.

This graph has *h* vertices and *rh* edges.

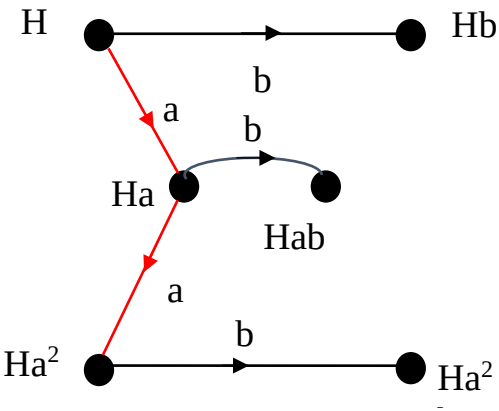
Example 7:
Let F = F(*a*, b) and let H = $\langle aaa, bb, abab\rangle^G$. This is the group generated by all the conjugates of *aaa*, *bb* and *abab*.

Then G/H ≅ $\langle A, B \mid A^3, B^2, (AB)^2\rangle$, the dihedral group of order 6. Thus *r* = 2 and, since we have 6 right cosets, *h* = 6. The graph Γ is as follows:



For the moment consider Γ as an undirected graph. That is, ignore the directions of the arrows. Suppose that T is a spanning tree in Γ. A **tree** is a connected graph that has no loops and a **spanning tree** is one that connects every vertex to every other.

Example 7 (continued): The following is a spanning tree in the above graph Γ.

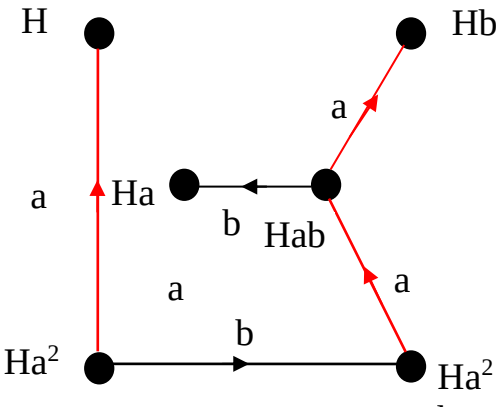


For each coset Hu consider the unique path in T from H to Hu. The fact that there is a unique path is because T has no loops. For each such path write down the generators, or their inverses, which take us along this path. If we follow an arrow we write down the corresponding generator. If we have to go in the opposite direction to an arrow we write down the inverse of the corresponding generator. The word taking us from H to the coset Hu will be in that coset. Note the special case of the path from H to H. This path has length 0 and the corresponding word is 1. The set of words will be a transversal, that is, a set of coset representatives, one from each coset.

Example 7 (continued):
In the above example we have the transversal:

$$\{1, a, ab, aa, aab\}.$$

These just happen to be the representatives we chose when labelling the graph Γ. They happen to be the most convenient ones to use in this example. But we could have chosen some other spanning tree and so produce some other transversal. For example, consider the following alternative spanning tree.
6. The graph Γ is as follows:



In this case our transversal is:

$$\{1, a^{-1}, a^{-1}b, a^{-1}ba, a^{-1}bab, a^{-1}ba^2\}$$

A transversal obtained from a spanning tree has what is called the Schreier property, or is a Schreier transversal. A **Schreier transversal** is a transversal S with the property that every initial segment of a word in

S is also in S. The reason why a transversal obtained from a spanning tree is a Schreier transversal is that every initial segment corresponds to the unique path from H to the corresponding coset.

Example 7 (continued): In the above transversal we could replace a^{-1}, by a^2 because it's in the same coset. The set $\{1, a^2, a^{-1}b, a^{-1}ba, a^{-1}bab, a^{-1}ba^2\}$ is a transversal, but it no longer has the Schreier property.

For each edge E in the graph Γ we define its **slope**, **σ(E)**, as follows. If E is the edge from Hu to Hv, following the generator x then σ(E) is defined to be uxv^{-1}. If we denote by E^{-1} the opposite edge, going from Hv to Hu following the inverse of a generator x^{-1} (this means following the edge in the opposite direction to the arrow) then $\sigma(E^{-1}) = vx^{-1}u^{-1} = (uxv^{-1})^{-1} = \sigma(E)^{-1}$.

Example 7 (continued): In the above example, the slope of the 12 edges is given by the following table. (The slopes of the inverse edges are the inverses of these.)

	E	**u**	**x**	**v**	**σ(E) = uxv^{-1}**
1	H $\rightarrow$ Ha	1	a	a	1
2	H $\rightarrow$ Ha^2	1	b	b	1
3	Ha $\rightarrow$ Ha^2	a	a	a^2	1
4	Ha $\rightarrow$ Hab	a	b	ab	1
5	Ha^2 $\rightarrow$ H	a^2	a	1	a^3

	E	u	x	v	$\sigma(E) = uxv^{-1}$
6	$Ha^2 \to Ha^2b$	a^2	b	a^2b	1
7	$Hb \to Ha^2b$	b	a	a^2b	$bab^{-1}a^2$
8	$Hb \to H$	b	b	1	b^2
9	$Hab \to Hb$	ab	a	b	$abab^{-1}$
10	$Hab \to Ha$	ab	b	a	ab^2a^{-1}
11	$Ha^2b \to Hab$	a^2b	a	ab	$a^2bab^{-1}a^{-1}$
12	$Ha^2b \to Ha^2$	a^2b	b	a^2	$a^2b^2a^{-2}$

Theorem 2: Suppose H is a subgroup of index h of a free group F and Γ is the graph whose edges have the form

$$Hu \to Hux.$$

Let T be a spanning tree and let S be the corresponding Schreier transversal. Let $\sigma(E)$ denote the slope of the edge E.

Then $\sigma(E) = 1$ if and only if $E \in T$.

Proof: Suppose $\sigma(E) = 1$ where E is $Hu \to Hux = Hv$ and $u, v \in S$. The unique path from H to Hv must go via Hu so $E \in T$.

Conversely suppose that $E \in T$. Then the unique path from H to Hv goes via this edge and so $ux \in S$. Since ux and v are in the same coset and they both belong to the transversal S, they are equal. Hence $\sigma(E) = uxv^{-1} = 1$.

Theorem 3: (**SCHREIER-NIELSEN**) Every subgroup of a free group is free. In particular if G is a free group of rank r and $H \leq G$ with $|G:H| = h$ then H is a free group of rank $rh - h + 1$.

Proof: Let F be a free group of rank r on the generators $x_1, x_2, \ldots, x_r$. Let H be a subgroup of finite index, h. Consider the directed graph Γ whose vertices are the right cosets of H in F and whose edges are of the form $Ha \rightarrow Hax$, where x is a generator.

Choose a spanning tree, T, in Γ and let S be the corresponding Schreier transversal.

Let $B = \{\sigma(E) \mid E \in \Gamma - T\}$. Since Γ has rh edges and T has $h - 1$ edges $\Gamma - T$ has $rh - (h - 1)$ edges and so the number of elements of B is $rh - h + 1$. It remains to show that B is a set of free generators for H. We must first show that B generates H. Then we must show that there are no relations between them.

Let $h \in H$. Writing h as a reduced word $y_1 y_2 \ldots y_k$ where each y_i is one of the generators or one of their inverses, consider the path from H by following the y_i. Since $Hh = H$ this path will both start and end with the vertex H.

Suppose this path is:

$$H \xrightarrow{y_1} Hu_1 \xrightarrow{y_2} Hu_2 \xrightarrow{y_3} \ldots. \xrightarrow{y_{n-1}} Hu_{n-1} \xrightarrow{y_n} H$$

The product of the corresponding $\sigma(E)$'s is

$(1y_1u_1^{-1})(u_1y_2u^{-1})\ldots(u_{n-2}y_{n-2}u_{n-1}^{-1})(u_{n-1}y_n1^{-1}) = h.$

Hence B generates H.

Next we show that each $\sigma(E) = uxv^{-1} \in B$ is reduced as written.

Since u, v are reduced the only possibility for cancellation in uxv^{-1} is for x to cancel with the last character of u or the first of v^{-1}.

In the first case $u = u_0x^{-1}$ and so $Hu_0 = Hux = Hv$.
Since u_0 is an initial segment of $u \in S$, $u_0 \in S$.
But $v \in S$, so $u_0 = v$. Hence $uyv^{-1} = 1$, a contradiction.

In the latter case x^{-1} cancels with the last character of v and so $vx^{-1}u^{-1} = 1$ and so its inverse $uxv^{-1} = 1$, again a contradiction.

Suppose $w = (u_1y_1v_1^{-1})(u_2y_2v_2^{-1})$ is a product of elements of B or their inverses, with $u_1, u_2, v_1, v_2 \in S$ and $y_1, y_2 \in X + X^{-1}$ (the disjoint union). By the definition of B, neither factor is 1. Suppose that $w \neq 1$. We will show that when w is reduced the y_1's will not disappear.

Suppose y_1 does cancel with a symbol in the second factor. For the cancellation to reach back to y_1 we must have one of the following cases:

Case 1: y_1 cancels with a symbol in u_2: Then v_1^{-1} has to cancel with an initial segment of u_2 and so $v_1y_1^{-1}$ is an initial segment of u_2. But $Hu_1y_1 = Hv_1$ so $Hu_1 = Hv_1y_1^{-1}$ and since both u_1 and $v_1y_1^{-1}$ are in S they are equal. Hence $u_1y_1 = v_1$, a contradiction as the first factor is not 1.

Case 2: y_1 cancels with y_2: Then $u_2 = v_1$.
Now $Hu_1y_1 = Hv_1$ whence $Hu_1 = Hv_1y_1^{-1} = Hu_2y_2 = Hv_2$. Since u_1, $v_2 \in$ S they are equal and so $w = 1$, a contradiction.

Case 3: y_1 cancels with a symbol in v_2^{-1}: Then y_2 cancels with a symbol in v_1^{-1}. Thus u_2y_2 is an initial segment of v_1. But $Hu_2y_2 = Hv_2$ and since both u_2y_2 and v_2 are in S, $u_2y_2 = v_2$, a contradiction.

Hence any non-trivial word in the elements of B can't cancel down to the identity.

Example 8: Let F = F(a, b) and let H = $\langle a^2, ab, ba, b^2\rangle$. What is the rank of H?
Solution: It might appear that $\{a^2, ab, ba, b^2\}$ is a free set of generators and that therefore rank(H) = 4. However this is not so.

Let $w \in$ F and let $\Lambda(w)$ be the length of w when written out in terms of a's and b's and their inverses. We're counting a^{-1} and b^{-1} as single symbols.
Let $\pi(w)$ be $\Lambda(w)$ modulo 2.

Clearly π is a homomorphism from F to $\mathbb{Z}_2$. I'll show that $\ker(\pi) = H$.

Suppose $w \in \ker(\pi)$.
Then $w = w_1 w_2 \ldots w_k$ for some k where each w_i has length 2. It remains to show that the words of length 2 are all in H. This can be achieved by the following table.

aa	(aa)
ab	(ab)
ab^{-1}	$(ab)(bb)^{-1}$
ba	(ba)
ba^{-1}	$(ba)(aa)^{-1}$
bb	(bb)
$a^{-1}b$	$(aa)^{-1}(ab)$
$a^{-1}\mathrm{a}^{-1}$	$(aa)^{-1}$
$a^{-1}b^{-1}$	$(ba)^{-1}$
$b^{-1}a$	$(bb)^{-1}ba$
$b^{-1}a^{-1}$	$(ab)^{-1}$
$b^{-1}\mathrm{b}^{-1}$	$(bb)^{-1}$

So H = ker(π) and so has index 2. By the Schreier Nielsen theorem: rank(H) = 2.2 – 2 + 1 = 3.

So one of the generators *aa*, *ab*, *ba* and *bb* must be expressible in terms of the other three. In fact this is so:

$$ba = (bb)(ab)^{-1}(aa).$$

§ 8.4. The Todd-Coxeter Algorithm Revisited

We're now in a position to give a proper proof that the Todd-Coxeter algorithm works, that is, if it terminates it gives a group, H, which is isomorphic to the group G being presented.

Suppose the algorithm terminates. The resulting group, H, is a group of permutations on the set of codes and the number of codes is |H|. Since each element of G is represented by at least one code $|G| \leq |H|$ (and so is finite).

Let F be the free group on the set of generators. Then $G \cong F/R$ where R is the normal subgroup of F generated by the relators.

Since H satisfies all the relations of the presentation there's a normal subgroup of F, containing R, such that $H \cong F/S \cong (F/R)/(S/R)$ so $|H| \leq |F/R| = |G|$. Hence $|G| = |H|$ and so S = R, whence $G \cong H$.

§ 8.5. Coset Enumeration

Suppose we're given a presentation $\langle \Gamma \mid R \rangle$ and a subgroup H of G generated by a set of words S. We adapt the algorithm given above (actually this is the version in the original paper) so that the codes are assigned to left cosets of H rather than to individual elements. The integer code 1 represents the coset H and the number of codes, if and when the process terminates, gives the number of cosets of H in G, that is, |G:H|.

If we know |H| (and assuming it to be finite) we can obtain |G| by multiplying |G:H| by |H|. If we simply want the order of G, using a subgroup can drastically reduce the amount of computation. Also this 'coset enumeration' can terminate in cases of a subgroup of finite index in an infinite group.

The only modification comes right at the beginning.

COSET ENUMERATION
Generate chains of the form 1ρ1 for every generator of H. Continue as before.

Example 9: $G = \langle A, B \mid A^3, B^3, (AB)^2 \rangle$, $H = \langle AB \rangle$

Generators for H	Relators for G		
1A2B1	1A2A4A1	1B3B2B1	1A2B1A2B1
	2A4A1A2	2B1B3B2	2A4B6A3B2
	3A5A6A3	3B2B1B3	3A5B4A1B3
	4A1A2A4	4B6B5B4	4A1B3A5B4
	5A6A3A5	5B4B6B5	5A6B5A6B5
	6A3A5A6	6B5B4B6	6A3B2A4B6

	A	**B**	
1	2	3	= H
2	4	1	= HA
3	5	2	= HB

4	1	6	= 2A
5	6	4	= 3A
6	3	5	= 4B

So |G:H| = 6. Since |H| = 2 we have |G| = 12.

Example 10: $G = \langle A, B | A^4, A = B^2 \rangle$, $H = \langle AB \rangle$

Generators for H	Relators for G	
1A2B1	1A2A3A1A1 !!	1A2b3b1
	2A3A1A1A2	2A3b1b2
	3A1A1A2A3	3A1b2b3

	A	**B**	
1	2	3	= H
2	3	1	= HA = 1
3	1	2	= HB = 1

Hence |G:H| = 1 and so H = G.

§ 8.6. Subgroups of Finite Index

We can use the Todd-Coxeter algorithm to find all of the subgroups of a given finite index in a given finitely presented group. Suppose G is given by some presentation and H is a subgroup H of index $\leq n$.

We carry out the Todd-Coxeter algorithm to assign codes to the left cosets of H, but since we don't know H we have to do without the chains that would have come

from its generators. So effectively we're working with H = 1 at this stage.

If the algorithm terminates with n codes or less then $|G| \leq n$ so the trivial subgroup is one of the subgroups we're looking for. Otherwise we'll get to a stage where we have $n + 1$ codes and if these codes refer to the left cosets of a subgroup whose index is less than or equal to n then two of these codes must be equal. Of course we don't know which two are equal, but there's only a finite number of possibilities to consider: 1 = 2, 1 = 3, 2 = 3 and so on.

Now in each case the equality gives rise to a word that must belong to H. So we now repeat the Todd-Coxeter algorithm, this time including this newly found word as one of the generators of H.

If the algorithm terminates with at most n codes we'll have found the generators of a subgroup whose index is at most n. But if the algorithm continues until $n + 1$ codes have been generated then again we must have a pair of equal codes. And again we won't know which two codes are equal so we'll have to split our working into even more cases.

But the number of cases will be finite and in each one we'll have found a new word to add to our generators for H. If we eventually reach a stage where the algorithm terminates with n codes or fewer in each case then we'll have found all the subgroups whose index is at most n.

At each stage our working splits into finitely many cases, depending on which two codes are equal. At the next stage each of these cases splits into a finite number of subcases, and so on. So our computation proceeds along the edges of a tree, with each node representing a separate Todd-Coxeter calculation.

EXERCISES FOR CHAPTER 8

Exercise 1: For each of the following statements determine whether it is true or false.

(1) The pair $x^{-1}x$ is an inverse pair.

(2) The word $a^{-1}baabb^{-1}ab$ is a reduced word.

(3) The null string is a reduced word.

(4) The words $x^{-1}yxz$ and yz are equivalent.

(5) Free groups are non-abelian.

(6) Every group is a subgroup of some free group.

(7) If w is a group word and $[w]$ is the set of all words that are equivalent to w then $[w]$ contains exactly one reduced word.

(8) The rank of the free group $\langle X, Y, Z \mid Z = XY \rangle$ is 2.

(9) If two free groups are isomorphic the ranks are equal.

(10) If $H \leq G$ and both are free groups then rank(H) $\leq$ rank (G).

Exercise 2: Find an equivalence sequence from the word $a^{-1}bb^{-1}acdc^{-1}ccc^{-1}d^{-1}a^{-1}$ to a reduced word.

Exercise 3: Let G be the free group of rank 2 and let H be the subset consisting of those elements where the sum of the powers is even.

(a) Show that H is a subgroup of G;

(b) Find |G:H|;

(c) Use Schreier-Nielsen to find the rank of H;

(d) Find a set of generators for H.

SOLUTIONS FOR CHAPTER 8

Exercise 1:
(1) TRUE
(2) FALSE
(3) TRUE
(4) FALSE
(5) FALSE: The free group of rank 1 is infinite cyclic.
(6) FALSE
(7) TRUE
(8) TRUE
(9) TRUE.
(10) FALSE.

Exercise 2: $a^{-1}bb^{-1}acdc^{-1}ccc^{-1}d^{-1}a^{-1}$
$\to a^{-1}acdc^{-1}ccc^{-1}d^{-1}a^{-1}$
$\to cdc^{-1}ccc^{-1}d^{-1}a^{-1}$
$\to cdcc^{-1}d^{-1}a^{-1}$
$\to cdd^{-1}a^{-1} \to ca^{-1}$.

Exercise 3:
(a) Let $G = \langle A, B \mid \rangle$. If $w \in G$ let $p(w)$ be the sum of the powers in w, mod 2. Since cancelling an inverse pair doesn't change $p(w)$, p is well-defined.
If $u = A^{m_1}B^{n_1} \ldots$ and $v = A^{s_1}B^{t_1} \ldots$ then

$$uv = A^{m_1}B^{n_1} \ldots A^{m_1}B^{n_1} \ldots \text{ and}$$
$$p(uv) = p(u) + p(v).$$

Hence p:G $\to \mathbb{Z}_2$ is a homomorphism and H = ker(p) and so is a normal subgroup of G.
(b) By the first isomorphism theorem G/H $\cong \mathbb{Z}_2$ and so |G:H| = 2.

(c) Using the notation of the Schreier-Nielsen theorem, $r = h = 2$ and so rank(H) = 3.
(d) H = $\langle A^2, B^2, AB \rangle$.