Indian Institute of Science

KVPY Summer Project 2015

Combinatorial Group Theory

Author:
Sayantan Khan

Supervisor:
Dr. Siddhartha Gadgil

July 2015

Acknowledgements

This project would not have been completed without the help of the following people to whom I'm deeply indebted:

- First of all, I'd like to thank Dr. Siddhartha Gadgil, who was kind enough to let me work with him, as well as helping me learn Scala, group theory, and some amount of topology. He was also kind enough to bear with the occasional dumb question of mine, and helped me whenever I was stuck on the proof of some theorem.
- Next, I'd like to thank Vikramaditya Giri, who pointed out several flaws in my proofs, and later helped me fix them. Without his help, the work would have been incomplete and wrong.
- I'd also like to thank Prabaha Gangopadhyay, who helped me proofread this manuscript, fixing the occasional grammatical and spelling mistake I made in the report.
- Finally, I'd like to thank all my friends and family for providing emotional support throughout the summer, without which the report probably wouldn't be finished by now.

Contents

1 Motivation and a little history **3**

2 Some preliminary notions **4**

3 Presentations **4**

4 Free Groups **7**
4.1 On the isomorphisms of free groups[5] 8

5 A digression to quotient groups **9**
5.1 Cosets and quotient groups 9
5.2 Some useful lemmas[3] 10

6 Presentations revisited **10**

7 Transformations **12**

8 An alternative definition for free groups **13**

9 More about free groups **14**

10 More about presentations **17**

11 An application in algebraic topology **18**

References **20**

1 Motivation and a little history

Groups, as an abstract notion worthy of interest, arose just like all other abstractions in mathematics, i.e. when mathematicians pulled back from solving specific problems, and asked themselves, what properties of the problem were the essential properties and could be abstracted out, i.e. what do permutations of a set, isometries[1] of the plane and modular integers have in common. There were three things, in this specific example, that stood out: one, these 'objects' could be combined or composed to create new objects, two, there existed an object, which when combined with any other object resulted in the same object, unchanged, and finally, all these objects were reversible. For example, the composition of two permutations is yet another permutation, composition of any permutation with the permutation which does not move anything gives one the original permutation back, and finally, every permutation can be reversed.

But that's not all that one needs needs to motivate mathematicians to study this abstraction, unless they are studying these for their own sake. As much as mathematicians claim intellectual purity, and the pursuit of knowledge for its own sake, they are motivated to study something outside their sub-discipline only if it has some application in their sub-discipline, and that's usually demonstrated by solving some long standing open problem using the new theory or abstraction.

The study of groups, as these particular abstractions were called, needed to prove its worth in this manner, by solving some long standing open problem, which would give it the push it needed to enter mainstream mathematics. That push came in the form of a problem, which asked whether a polynomial equation in one variable with degree 5 or higher could be solved using radicals. The answer for lower degrees was known, but the collective failure of the mathematical community to find an answer for degree 5 led to the speculation of its possibility. It was commonly believed that it was not possible to do so. The conjecture, however, needed a proof. The proof came about in 1823 and made the extensive use of group theory, and furthermore, in the pursuit of the proof, group theory itself gained more sophistication, much more so than it had possessed before. The new new sophistications made group theory a powerful tool for mathematical use, and the proof of the solvability in radicals of polynomial equations of degree 5 and higher served as a testament to that power and firmly put group theory in mathematical limelight, and set its place in mainstream mathematics for years to come.

In the following years, once group theory was comfortably a part of mainstream mathematics, various specializations emerged. Two specializations, geometric group theory and combinatorial group theory came about by studying the geometric aspects of groups in the first case, and applying techniques from combinatorics in the second case. These two sub-disciplines had an impact in the study of topology and mathematical logic, two widely disparate fields.

[1] Isometries are transformations that preserve distance between any pair of points, like reflections or translations

2 Some preliminary notions

Definition 2.1. A *group* $(G, \circ)$ is a set G along with an associated binary operation $\circ$ called multiplication, such that it satisfies the following axioms:

- If a and b belong to G, then $a \circ b$ also belongs to G. (Closure axiom)
- Multiplication is associative, i.e. if a, b and c belong to G, then $a \circ (b \circ c) = (a \circ b) \circ c$. (Associativity axiom)
- There exists an element e in the group, called identity, such that for all $a \in G$, $a \circ e = e \circ a = a$. (Existence of identity)
- For every element $a \in G$, there exists an element b, called the inverse of a, such that $a \circ b = b \circ a = e$ (Existence of inverse)

Definition 2.2. A *subgroup* $(S, \circ)$ of a group $(G, \circ)$, is a subset S of the set G, which is a group under the operation $\circ$.

It trivially follows from the axioms that the identity element is unique, and an element has a unique inverse. Now for some examples:

Example 2.1. *The set of integers $\mathbb{Z}$ under the operation of addition is a group.*

Example 2.2. *The set of integers $\mathbb{Z}$ under the operation of addition modulo some positive integer n is a group. It is denoted by the symbol $\mathbb{Z}/n\mathbb{Z}$*

Definition 2.3. A *homomorphism* is a mapping ϕ from a group $(G, \circ)$ to another group $(G', *)$ such that it preserves the group structure, or in other words, for any $a, b \in G$, $\phi(a \circ b) = \phi(a) * \phi(b)$.

Example 2.3. *Consider the mapping ϕ from $\mathbb{Z}$ to $\mathbb{Z}/7\mathbb{Z}$, such that $\phi(x) = x \bmod 7$. Clearly, this is a homomorphism.*

Definition 2.4. An *isomorphism* between G and G' is a homomorphism which is one-one and onto. If an isomorphism exists between two groups, they are said to be isomorphic.

For all practical purposes, two isomorphic groups are same in every aspect, so it's common to treat isomorphic groups as equivalent.

3 Presentations

One of the problems one immediately faces is how to represent groups. The groups mentioned in the example were nice, in the sense that they deal with sets that are familiar to most people. However, for any arbitrary group, representing them compactly might be a problem. One way of representing a group, or at least a finite group, is to write out its multiplication table, that is, for every possible ordered pair, write out their product. This method works, but only for finite groups, and even this grows cumbersome after the group exceeds a certain size.

One way to improve upon this is to note that a multiplication table has a lot of redundant information, information that can be deduced by just using the algebraic structure of the group. For example, if an entry in the table is of the form $a^3 \circ a^4 = b$, then one can immediately deduce from the associativity axiom that $a^2 \circ a^5 = b$, $a \circ a^6 = b$ and so on. Before one tries to answer that question, a few definitions are required. [4]

Definition 3.1. A subset S of a group $(G, \circ)$ is said to generate G if every member of G can be written as the product of powers of elements of S.

Notice that in both examples, example 2.1 and example 2.2, the set $S = \{1\}$ generates the whole group. But in the second example, there is an additional condition that $1^n = 0$ which is not present in the first example. Now consider a singleton set $T = \{a\}$ and the group H generated by it. Since H is generated by T, every element of H is of the form a^p for some integer p. Now, if H is finite, we can, by Pigeonhole principle, find a non negative q such that $a^q = e$. Otherwise, H is infinite and isomorphic to $\mathbb{Z}$. Here's a formal proof:

Theorem 3.1. *If H is a group generated by the singleton set $S = \{a\}$, then H is either isomorphic to $\mathbb{Z}$ or $\mathbb{Z}/q\mathbb{Z}$, where q is a non-negative integer.*

Proof. The proof is split into two parts, one when H is finite, and the next when H is not finite.

- **Finite:** If H is finite, there exists a positive integer (it can't be 0, because a group has at least one element) q, which is the size or the order of the group. Consider the sequence $A = \{a^0, a^1, a^2 \ldots, a^q\}$. Since the set A has $q+1$ elements, but the group only has q distinct objects, by the pigeon-hole principle, at least two objects must be identical. Let them be a^m and a^n $(m > n)$. Let $p = m - n$ (it follows that $q \geq p$). Then, $a^p = e$ and consequently $a^l = a^{l \bmod p}$. Since, there can be at most p distinct elements modulo p, the group can have at most p elements. This implies $p \geq q$. And following from the last inequality, one gets $p = q$. From this one concludes that $a^q = e$, and for all positive integer l less than q, $a^l \neq e$. An isomorphism can now be constructed with $\mathbb{Z}/q\mathbb{Z}$. There exists a unique way of writing every element of H in the form a^l, where $0 \leq l < q$ and consider the mapping $f(a^l) = l$ where l varies from 0 to $q - 1$. Since the kernel of f is just $\{e\}$ and the range is all of $\mathbb{Z}/q\mathbb{Z}$, f is an isomorphism. Hence, if H is finite, it is isomorphic to $\mathbb{Z}/q\mathbb{Z}$.

- **Infinite:** If H is infinite, there cannot exist any positive integer q such that $a^q = e$, otherwise the group would have at most q elements. This immediately implies that if $a^m = a^n$, then $n = m$ and there exists a unique way of writing every element of H in the form a^l, where $l \in \mathbb{Z}$. Consider the mapping f such that $f(a^l) = l$. Clearly, this is onto on $\mathbb{Z}$ and it's also one-one. Hence f is an isomorphism with $\mathbb{Z}$.

□

With the above theorem, all the groups generated by singleton sets have been completely classified. The group $\mathbb{Z}/q\mathbb{Z}$ is completely represented by the information that it is generated by a singleton set and it is of the order q. The following notation is sometimes used to represent the above information:

$$\mathbb{Z}/q\mathbb{Z} = \langle a; a^q = e \rangle$$

Usually, the trailing "$= e$" is skipped:

$$\mathbb{Z}/q\mathbb{Z} = \langle a; a^q \rangle$$

$\mathbb{Z}$ in the same notation looks like this:

$$\mathbb{Z} = \langle a; \rangle$$

The notation used above is called a presentation, with the terms to the left of the semi colon called generators, and the terms to the right called relations. The generators, as the name suggests, generate the group, or in other words, every element of the group can be written as the product of powers of the generators. The relators consist of *words* which evaluate to identity in the group.

Definition 3.2. Given a set S called the generating set, a word is a finite (possibly empty) sequence a_i^j, where $a_i \in S$, and $j = \pm 1$. A word is reduced if a_i^j is never followed by a_i^{-j}.

Example 3.2. *Given a generator set $S = \{a, b\}$, $aba^{-1}b^{-1}$ is a reduced word, but $abb^{-1}a^{-1}$ is not a reduced word.*

If a word is not reduced it's possible to reduce it simply by iterating over the 'letters' in the word, and at the first occurrence of a letter being followed by its inverse letter, deleting both the letters from the word, and starting the process all over again until one has a reduced word. This process terminates because a word has a finite length. Two words are considered equivalent if they can be converted from one to the other just by either deleting adjacent inverse letters, or inserting pairs of adjacent inverse letters somewhere in the word. One can define the operation of multiplication on words as well. The product of two words is just concatenation of their sequence of letters together. And similarly, one defines the formal inverse of a word as the sequence of letters of the word taken in reverse, and the exponent on them inverted.

Example 3.3. *Let W_1 be the word ab and W_2 be the word $b^{-1}a$. The product word W_1W_2 is $abb^{-1}a$ and W_1^{-1} is $b^{-1}a^{-1}$.*

Lemma 3.4. *Inserting or deleting adjacent pair of inverse letters does not change the reduced form of the word.*

Proof. The proof consists of two parts: showing the statement is true for insertions, and then showing it is true for deletions:

- **Insertion:** Let the pair of inverse letters aa^{-1} be inserted somewhere in the word. The new word can be broken up in 3 sub-words, the sub-word preceding the insertion point, the sub-word aa^{-1} and the sub-word following the insertion point. The preceding sub-word will get reduced in the same manner as it did in the original word, with two possible cases arising: either the last letter of the sub-word is a^{-1}; in that case, it will get reduced with the first a of the second sub-word, and the a^{-1} of the second sub-word will get concatenated to the first reduced sub-word. Note that it cannot get reduced any further, otherwise the first reduced sub-word would not have had a^{-1} in the trailing position. Finally, the last sub-word will get reduced just like it did in the original word, and we'll get the original reduced word back. In the other case where the first sub-word does not end with a^{-1}, the middle sub-word will get reduced to the empty word and the reduced form of the new word is the same as the reduced form of the original word.

- **Deletion:** Assume that the pair aa^{-1} is deleted from somewhere in the word. Split the shorter word into two sub-words, the one preceding the point of deletion and the one following the point of deletion. Two cases can arise again, either the preceding word has a trailing a^{-1}, or it does not. If it does not, the deleted pair aa^{-1} gets deleted during the reduction, so the reduced word remains the same. If the preceding word does have a trailing a^{-1}, then it gets reduced with the leading a of the deleted sub-word, leaving a trailing a^{-1}, and that leads to the same reduced word.

Hence, inserting or deleting adjacent pairs of inverse letters does not change the reduced form. □

Since there exists an equivalence relation on the set of words W generated from a given set S, one can partition W into equivalence classes. Furthermore, a group structure can be imposed on the partition classes in the manner described in section 4.

4 Free Groups

Before one formalizes the notion of a presentation of a group, one needs to define free groups. There are many ways of defining or constructing free groups, from formal algebraic methods, to more geometric techniques[6]. The technique used here to define free groups is in the vein of the definition of fundamental groups of topological spaces.

Lemma 4.1. *Given words a_1, a_2, b_1, and b_2 from a generating set S such that a_1 and a_2 are equivalent, and b_1 and b_2 are equivalent, then a_1b_1 is equivalent to a_2b_2.*

Proof. Let S be the generating set of a_1, a_2, b_1 and b_2. If c is an element of S, then inserting cc^{-1} or $c^{-1}c$ somewhere in a word does not change its equivalence class. Conversely, deleting a pair of adjacent inverse letters does not change the equivalence class of the word either. Also, these two operations are reversible and are each other's inverse. Saying that a_1 and a_2 are equivalent means that they reduce to the same reduced word, which means there's a sequence of finite moves consisting of all the deletions that lead from a_1 to $a_{reduced}$ and then a finite sequence of insertions, which are the inverses of the deletions that lead from a_2 to $a_{reduced}$. Similarly, there exist a finite sequence of moves that leads from b_1 to b_2. Applying those moves on a_1b_1, one gets the word a_2b_2, which shows $a_1b_1 \equiv a_2b_2$. □

Definition 4.1. A *free group* on the set S is defined to be the set of equivalence classes on the set of words generated by the set S, with identity being the equivalence class of the empty word, and group multiplication of classes A and B being the equivalence class of the product ab, where $a \in A$ and $b \in B$. In other words:

$$A \circ B = [a \cdot b]$$

Inverse of a class A is defined as the equivalence class of the inverse of a, where $a \in A$.

By lemma 4.1, the multiplication and inverse are well defined.

Using just this definition, one can go about proving a few elementary properties of free groups.

Proposition 4.2. *If α is an element of a free group G and $\alpha^2 = e$, where e is the identity, then $\alpha = e$.*

Proof. Let a be the reduced word belonging to the equivalence class α. aa then belongs to the equivalence class α^2. But $\alpha^2 = e$, which means that aa is equivalent to the empty word. Since a is reduced, but aa reduces to the empty word, the only place reduction can happen is between the end of the first a and the beginning of the second a. Now assume that a is non empty. This means $a[m] = a[n-m-1]$, where $a[m]$ represents the m^{th} letter of a (starting from 0) and n is the length of a. Now a could either have an even number of letters in which case $a\left[\frac{n}{2}-1\right]$ letter is the inverse of the adjacent $a\left[\frac{n}{2}\right]$ letter and those two cancel each other out. This contradicts the fact that a is reduced. Ergo, a must be empty. And if a has an odd number of letters, then the middle letter must be its own inverse, which is not true for any letter in the basis. Hence a can only have an even number of letters and in that case, it's the identity. This completes the proof that $\alpha = e$ □

Using this result, one can prove a slightly stronger result, which is that no power of a non trivial element in a free group is ever trivial.

Proposition 4.3. *If α is an element of a free group G and $\alpha^p = e$, where e is the identity and p is a positive integer, then $\alpha = e$.*

Proof. The last proof can be recycled completely in this proof. Let a be the reduced word from α. Then a^p reduces to the empty word, but reduction can only happen where one word is joined to the next, since the word a is reduced. Proceeding by the same arguments as in the last proof, it's shown that a necessarily must be the empty word, and that concludes the proof. □

4.1 On the isomorphisms of free groups[5]

It is rather interesting to note that the free group on some set S does not use any inherent structure of the set, but just depends on the cardinality of the set. One has already seen this for free groups on sets of cardinality 1, all of which are isomorphic to $\mathbb{Z}$, which leads to the conjecture that free group on sets of the same cardinality are isomorphic to each other.

Theorem 4.4. *If the bases of two free groups are isomorphic (i.e. have the same cardinality) then the groups are isomorphic.*

Proof. Consider a bijective mapping f between the bases B_1 and B_2 of groups X and Y. Extend f to a homomorphism in the following manner:

$$f(x_1^{e_1}x_2^{e_2}\dots x_n^{e_n}) = f(x_1)^{e_1}\dots f(x_n)^{e_n}$$

where x_is belong to the basis B_1. This, by definition, is a homomorphism. All one needs to show now is that it is injective and surjective. Since the whole basis B_2 lies in the image of f, and the basis generates the group, the homomorphism certainly is surjective. The last thing one needs to show is that if $f(\alpha) = \text{identity}_Y$, then $\alpha = \text{identity}_X$. Let x be a word in α, then $f(x)$ is a word in $f(\alpha)$. For each reduction made in $f(x)$, the corresponding reduction is made in x, hence if $f(x)$ reduces to the empty word, so does x, which shows the kernel is trivial and f is an isomorphism. □

The converse, although true, is a little trickier to prove. One needs a few more notions before a proof of the converse can be attempted. See theorem 9.9.

By theorem 4.4, all free groups generated by a basis of size n are isomorphic, so it makes sense to talk of all them as one, as the free group of rank n, or $\mathbb{F}_n$.

5 A digression to quotient groups

The following few sections will develop the necessary 'machinery' required further ahead.

5.1 Cosets and quotient groups

Definition 5.1. Given a group G, a subset H, and an element $a \in G$, the *left coset* aH is defined as the set

$$aH = \{ah \mid h \in H\}$$

A right coset Ha is defined in a similar manner.

Definition 5.2. A subgroup H of a group is called *normal* iff for all $a \in G$, $Ha = aH$.

Definition 5.3. A *cartesian product* of two subsets A and B of a group G is the set

$$A \times B = \{ab \mid a \in A,\ b \in B\}$$

This is where the convenient properties of normal subgroups come in. Since the smaller term can commute around the larger subgroup, so to speak, cosets of normal subgroups multiply very nicely. The following example shows that cosets of normal groups multiply nicely and thus lend themselves naturally to a group structure.

Example 5.1. *If H is a normal subgroup of G and a and b belong to G, then*

$$aH \times bH = Ha \times bH = Hab \times H = abH \times H = ab(H \times H)$$

But $H \times H$ is just H again, since H is a group. Hence

$$aH \times bH = abH$$

Definition 5.4. Given a group G and a normal subgroup H, the *quotient group* G/H is defined as the group whose elements are the cosets of H in G, the group multiplication is defined as the cartesian product of cosets. The multiplication is associative, that is a simple consequence of the definition of a normal subgroup. The identity element is the set H itself, and the inverse of aH is $a^{-1}H$.

5.2 Some useful lemmas[3]

Lemma 5.2. *That H is a normal subgroup of G is equivalent to saying that $aHa^{-1} = H$ for all $a \in G$ where the set aHa^{-1} defined as*

$$aHa^{-1} = \{aha^{-1} \mid h \in H\}$$

Proof. If H is normal in G, then for any $a \in G$, $aH = Ha$. Since $aH = Ha$, $(aH)a^{-1}$ is equal to the set $(Ha)a^{-1}$ which reduces to H. This shows that if H is normal in G, $aHa^{-1} = H$.

Now for the converse. If $aHa^{-1} = H$, then $(aHa^{-1})a = Ha$, but $(aHa^{-1})a = aH$, hence $aH = Ha$. □

Lemma 5.3. *The intersection of two normal subgroups A and B of G is normal in G.*

Proof. Let $C = A \cap B$. Clearly aCa^{-1} is a subset of both A and B for all $a \in G$. Hence $aCa^{-1} \subset C$. But if that's true for all $a \in G$, that's true for a^{-1} as well. That means $a^{-1}Ca \subset C$ or $C \subset aCa^{-1}$. Hence $aCa^{-1} = C$ for all $a \in G$ and C is normal. This proof in fact works for any arbitrary number of normal subgroups, even infinitely many. □

Lemma 5.4. *The kernel of a homomorphism f from G to G' is a normal subgroup of G.*

Proof. Let the kernel of f be H. If we show that $aHa^{-1} = H$ for all $a \in G$, we are done. Consider any $k \in aHa^{-1}$. k is of the form aha^{-1} for some $h \in H$. But $f(k) = f(a) \cdot f(h) \cdot f(a^{-1}) = e$. This shows k is in the kernel of f, hence $aHa^{-1} \subset H$. But this is true for any $a \in G$. In particular, take a^{-1}. $a^{-1}Ha \subset H$, but that means $H \subset aHa^{-1}$, which proves $aHa^{-1} = H$. This shows the kernel is a normal subgroup. □

Lemma 5.5 (First Isomorphism Theorem)**.** *If f is a homomorphism from G, then the image of f, I is isomorphic to $G/\mathrm{Ker}(f)$.*

Proof. Let Q represent the quotient group $G/\mathrm{Ker}(f)$ and H the kernel of f. Elements of Q are of the form aH, where a belongs to G. Consider the mapping ϕ which maps from Q to I in the following manner: $\phi(aH) = f(a)$. First of all, one needs to show that ϕ is well defined. Assume that $aH = bH$, a not necessarily distinct from b. Clearly, $ah_1 = bh_2$ for some h_1 and h_2 in H. $f(ah_1) = f(bh_2)$, but h_1 and h_2 lie in the kernel, so $f(a) = f(b)$. This shows that the value of ϕ only depends upon the element of Q one takes, and not the way one represents it as a coset. Also, since H is normal, $aH \times bH = abH$. Hence $\phi(aH \times bH) = \phi(ab) = \phi(aH)\phi(bH)$. This shows ϕ is a homomorphism. Now to show ϕ is surjective, let i be some element of I. There exists then some $a \in G$, such that $f(a) = i$. And therefore, $\phi(aH) = i$, which shows that ϕ is surjective. And if $f(a) = e$, then $a \in H$. But $aH = H$, which is the identity element of Q. This shows ϕ is injective. Ergo, ϕ must be an isomorphism. □

6 Presentations revisited

Canonically, there are two ways two generate smaller groups from a given group. One way is to generate a subgroup of the given group, and the other way is to generate a quotient group. Cayley's theorem states that every group is isomorphic to a subgroup of a symmetric group of some order. There exists an analogous theorem for quotient groups, which states that every group is isomorphic to the subgroup of a free group of a certain rank.

Lemma 6.1. *[6] If G is a group generated by n elements, then G is isomorphic to a quotient group of $\mathbb{F}_n$*

Proof. Let $B = \{b_1, b_2, \ldots, b_n\}$ be the basis of $\mathbb{F}_n$. Let $S = \{a_1, a_2, \ldots, a_n\}$ be the generating set of G. Consider the mapping $f(b_i) = a_i$. Extend this mapping linearly to all of $\mathbb{F}_n$. Since the set S generates G, S is the image of f. f is a homomorphism from $\mathbb{F}_n$ to G, and by the first isomorphism theorem: $G \cong \mathbb{F}_n/\mathrm{Ker}(f)$. □

Lemma 6.2. *[6] If R is a subset of the group G, then there exists a normal subgroup H, called the normal closure of R such that it is the* minimal *normal subgroup, i.e. if two normal subgroups A and B contain R, then they contain H.*

Proof. There exists at least one normal subgroup that contains R, that is the group G itself. Consider the set S of all normal subgroups of G containing R. By the extension of lemma 5.3, they intersection of all members of S must be normal in G, and that subgroup also contains R. Furthermore, it is minimal by definition, hence the normal closure exists. □

Everything that one needed to define presentations has now been covered.

Definition 6.1. A *presentation* P is a tuple of a set S, and a set of reduced words R from $\mathbb{F}_S$, also called relations. A presentation is represented in the following manner: $\langle S; R\rangle$.

Definition 6.2. A presentation $\langle S; R\rangle$, generates a quotient group Q, which is precisely the group $\mathbb{F}_S/N$, where N is the normal closure of R.

Definition 6.3. A group G is said to have a presentation $\langle S; R\rangle$ if it is isomorphic to the quotient group generated by the presentation.

One question still remains, whether a group actually has a presentation; to be more precise, is every group isomorphic to some quotient of a free group, and that is answered by lemma 6.1.

With that, the notion of a presentation is precisely defined. Here are some concrete examples of presentations of groups.

Example 6.3. *The group $\mathbb{Z}$ can be presented in the following manner: $\langle a; \rangle$. If no relations are specified, the relation set is taken to be the empty one. Hence, the smallest normal subgroup containing the empty set is just the trivial subgroup $\{e\}$, and the quotient group is just $\mathbb{F}_1/\{e\}$, which is isomorphic to $\mathbb{F}_1$, which was shown before to be isomorphic to $\mathbb{Z}$.*

Example 6.4. *The group $\mathbb{Z} \times \mathbb{Z}$ is presented in the following manner: $\langle a, b; aba^{-1}b^{-1}\rangle$. Let N be the smallest normal subgroup of $\mathbb{F}_2$ containing $aba^{-1}b^{-1}$. And let Q be the quotient group $\mathbb{F}_2/N$. The elements of Q, or the cosets of N are distinguished by a tuple of integers representing the sum of exponents of a and b respectively. To put it in simpler terms, ab and a^2ba^{-1} both belong to the same coset of N because they both have the sum of coefficients of a and b respectively* 1 *and* 1. *So an element of Q is identified by a tuple of integers, which is the same as $\mathbb{Z} \times \mathbb{Z}$.*

7 Transformations

A very natural question to ask at this point would be, how does the group represented by the presentation $\langle S; R\rangle$ change when R is changed. The following lemmas partially answer the question.

Lemma 7.1. *Given a group G, and an ordered set of elements of G, $\{a_i\}$, then the smallest normal group containing $\{a_i\}$ does not change if a_i is replaced by a_i^{-1}, $a_i a_j$, or $a_j a_i$, where $j \neq i$.*

Proof. To prove the theorem, it's sufficient to show that every normal group containing $\{a_i\}$ also contains the modified $\{a_i\}$ and vice versa. Let N be a normal subgroup containing $\{a_i\}$. Since it's a group, it also contains a_i^{-1} for all i. And the same argument holds true if N is a normal subgroup containing the modified $\{a_i\}$. Thus, the normal subgroups are invariant under the inversion transformation.

Now suppose N is a normal subgroup containing $\{a_i\}$. Since it's a group, it must also contain $a_i a_j$ for every ij pair. Now assume the converse. Assume N is a normal subgroup containing the modified $\{a_i a_j\}$, where a_i is replaced by $a_i a_j$. But N still contains a_j, and by extension a_j^{-1}, so the product of $a_i a_j$ and a_j^{-1}, which is a_i, must also be in the group. Hence, the normal subgroups are invariant under right multiplication. The same proof also holds for left multiplication. □

Lemma 7.2. *Given a group G, and an ordered set of elements of G, $\{a_i\}$, then the normal subgroups of G are invariant under the replacement of a_i by $x a_i x^{-1}$, where $x \in G$.*

Proof. Consider a normal subgroup N containing $\{a_i\}$. Since it's a normal subgroup, $xNx^{-1} = N$, hence N contains $x a_i x^{-1}$ for any i. Now consider a normal subgroup containing the modified $\{a_i\}$, where a_i has been replaced with $x a_i x^{-1}$. Since N is normal $x^{-1}Nx = N$, so N contains a_i. Hence normal subgroups are invariant under conjugation by generators. □

The transformations mentioned in lemma 7.1 are called *elementary Nielsen transformations*, and the transformation mentioned in lemma 7.2 is called the *conjugation transformation.*

Lemma 7.3. *If $\langle S; R\rangle$ presents a group G, then so does $\langle S; R'\rangle$, where R' is R transformed by the elementary Nielsen transformations or the conjugation transformation.*

Proof. Since the smallest normal subgroup containing R and R' is the same, by lemmas 7.1 and 7.2, the quotient group remains the same and so does the group. □

Definition 7.1. A group is said to be *finitely presented* if it can be presented in the form $\langle G; R\rangle$, where both G and R are finite sets.

Definition 7.2. A finite presentation, i.e. G and R are finite, is said to be balanced if $|G| = |R|$.

It is obvious the if one takes the presentation $\langle S; S\rangle$, the presentation generates just the trivial group, because the normal closure of S in $\mathbb{F}_S$ will be the whole group, which means the quotient reduces to $\{e\}$. This kind of presentation is also called the trivial presentation. It's obvious that for a finite S, a trivial presentation is balanced. It's also obvious that the elementary Nielsen transformations and the conjugation transformation does not change the cardinality of the set of relations, i.e. these transformation preserve balance. It's only a natural question to ask now whether one can obtain any finite balanced presentation of the trivial group starting from the trivial presentation. Here's a more formal statement:

Conjecture 7.4 (Andrews-Curtis Conjecture)**.** *A finite balanced presentation of the trivial group can be transformed into the trivial presentation using a finite sequence of elementary Nielsen transformations and the conjugation transformation.*

The Andrew-Curtis conjecture, as of yet, is an open problem. It's been shown to be true under stronger conditions like limiting the size of relations and generators[7], but the most general statement is unproven. It's also known to be false under weaker conditions, i.e. when one just deals with general groups and not trivial groups in particular.

8 An alternative definition for free groups

Since free groups have already been defined, one is forced to use a made up term, "superfree" groups, until the equivalence of the originally defined free groups and superfree groups is shown. Beyond that point, the text will revert to the use of the term free.

Definition 8.1. [5] Let X be a subset of the group F. Then F is said to be a superfree group with the basis X if any function from X to a group G can be uniquely extended to homomorphism from F to G

This definition does not guarantee the existence of a superfree group. One needs to explicitly construct a superfree group to show its existence. Fortunately as it turns out, a free group is also superfree.

Proposition 8.1. *A free group F with a basis B is superfree with the basis B.*

Proof. Let f be a function from B to some group G. Since B generates the free group F, any homomorphism from F is uniquely determined by its action on the generating set, and since the action of the homomorphism is defined by f, the homomorphism from F to G is uniquely defined. This shows that a free group is superfree. □

For a given set B, there exists a single free group with B as the basis. If free and superfree groups are really the same, the fact must also hold for superfree groups. It does hold, as the following proposition shows.

Proposition 8.2. *If two superfree groups have the same basis, they are isomorphic.*

Proof. Let two superfree groups, F_1 and F_2 have the basis B. Consider the inclusion map from B to F_2. Since F_1 is superfree with the basis B, there exists a unique homomorphism f_{12} from F_1 to F_2. Similarly, there exists a unique homomorphism f_{21} from F_2 to F_1. Consider the composition of f_{12} and f_{21}, $g = f_{21} \circ f_{12}$. g is a homomorphism from F_1 to F_1. Also, g acts as the identity map on the basis B. An identity map on B extends uniquely as the identity automorphism on F_1. This means g is the identity automorphism on F_1 and $f_{12} = f_{21}^{-1}$. If f_{12} is invertible, it must be an isomorphism which proves the proposition. □

This concludes the proof of the fact that free groups and superfree groups are the same thing, and the result of this endeavour is that there exists another definition of a free group which is more concise and does not involve unnecessary constructions.

9 More about free groups

Here's another proof of an already proven theorem, this time using the new definition of a free group.

Theorem 9.1. *If F_1 is a free group with basis B_1 and F_2 a free group with basis B_2, and if $|B_1| = |B_2|$, then $F_1 \cong F_2$.*

Proof. Since B_1 has the same cardinality as B_2, consider an invertible map b from B_2. The map b uniquely extends to a homomorphism f_{12} from F_1 to F_2. Similarly, b^{-1} extends to a unique homomorphism f_{21} from F_2 to F_1. The composition of f_{12} and f_{21} is a homomorphism from F_1 to F_1. But this composed homomorphism acts identically on B_1, and the identity map on B_1 extends uniquely to the identity automorphism on F_1. If the composition of f_{12} and f_{21} is the identity automorphism, then they must be invertible, hence they are isomorphisms. □

This proof was a little more elegant than the earlier proof that explicitly constructed an isomorphism. One can now also prove the converse of the previous theorem after proving a few lemmas.

Lemma 9.2. *[2] If a finite dimensional vector space has two bases of cardinality m and n, then $m = n$.*

Proof. Let the two bases be $\{a_1, a_2, \ldots a_n\}$ and $\{b_1, b_2, \ldots b_m\}$. Consider the ordered set formed by appending the first element of a basis to the b basis: $\{a_1, b_1, b_2, \ldots, b_m\}$. This set is not linearly independent, so one can pick out an b_i such that it's a linear combination of all the elements preceding it and i is minimized. Delete that b_i from the set. Deleting the element does not change the span of the set, so it still spans the whole vector space. Clearly, m can't be less than n otherwise one would run out of b_is and still have some a_i left unused. But that couldn't be possible because the a_is are linearly independent. That means $m \geq n$. One now flip the bases and gets $n \geq m$ which shows $m = n$. □

Lemma 9.3. *If a set in a $\mathbb{Z}$-module is linearly dependent in the vector space one gets after extending the ring $\mathbb{Z}$ to the field $\mathbb{Q}$, it's also linearly dependent in the $\mathbb{Z}$-module.*

Proof. If there exist some non zero coefficients such that $\sum c_i a_i$ is 0, and the c_is are all rational and in their reduced form, then let f be the lowest common denominator of all the denominators. Multiplying f by every c_i gives an integer, and these integers can be used as coefficients to show that the set is dependent in the $\mathbb{Z}$-module. □

Lemma 9.4. *If a $\mathbb{Z}$-module has two bases whose cardinality is at most $\aleph_0$, then the two bases have the same cardinality.*

Proof. If the bases have finite cardinality, then one can use the same proof as in lemma 9.2, and that as allowed because of lemma 9.3. If one of the bases has $\aleph_0$ cardinality, we can show using the same technique as in lemma 9.2 to show that the other basis is also at least countable. Also, because it's at most countable, it's exactly countable. And two countable sets have a bijection between them, so they have the same cardinality. □

Definition 9.1. A group F is called a *free abelian group* with a basis B if for a function f from B to an abelian group G, then there exists a unique homomorphism from F to G, whose restriction to B is f.

Definition 9.2. A *commutator* of two elements a and b of a group is the element $a^{-1}b^{-1}ab$.

Definition 9.3. The abelianization of a group G is the group Q obtained by taking the quotient of G with the commutator of every pair of elements in G. The quotient group Q is abelian.

Lemma 9.5. *Consider a word in the commutator subgroup of some free group. Let the word be of w_1abw_2, where a and b are single letters and w_1 and w_2 are sub-words (possibly empty). Then the word w_1baw_2 is also in the commutator subgroup.*

Proof. If one shows that one can reach w_1baw_2 from w_1abw_2 by just using conjugation and product with commutators, the proof will be done, since the commutator subgroup is a normal subgroup. Consider this sequence of operations: first conjugate by w_1, so the word looks like $w_1^{-1}w_1abw_2w_1$, or the reduced form is abw_2w_1. Next multiply by the commutator $bab^{-1}a^{-1}$. This gives the word baw_2w_1. Now conjugate by w_1^{-1}, so one gets w_1baw_2, which is what one wanted. □

This proof shows that transposing two adjacent letters in a word of the commutator subgroup results in a word that is still in the commutator subgroup. Since every permutation is the product of adjacent transposition, a permutation of any element of the commutator subgroup is still in the commutator subgroup. This means that all the words for which the sum of exponent of each letter is zero is part of the commutator subgroup. And for any word in which the sum of exponents of some letter is not zero, it can be shown that it is a coset of the commutator subgroup. Hence, the commutator subgroup is the set of all words in which the sum of exponents of all the letters is zero.

Lemma 9.6. *The abelianization of the free group on a set X is isomorphic to the free abelian group on X.*

Proof. Let F be the free group on X, and let FA be the free abelian group on X. Consider the inclusion map ϕ_1 from X to F and the inclusion map ϕ_2 from FA. And consider the map q which takes F to its quotient Ab by the commutator subgroup h. The map ϕ_2 extends uniquely to a homomorphism a from F to FA. The composite map $q \circ \phi_1$ extends uniquely to a homomorphism from FA to Ab. Clearly, h is a subset of the kernel of a, as a consequence of lemma 9.5. Now one needs to show that any element in the kernel belongs to the commutator subgroup h. Consider some word w that does not belong to the commutator subgroup. Then, collecting all the letters whose exponents do not sum to 0 in the word will give a word of the form $a_1^{n_1}a_2^{n_2}\dots a_k^{n_k}$, where a_is are distinct and none of the exponents are 0. The image of this word in a is clearly not identity, which shows that the commutator subgroup is the kernel of a. By the first isomorphism theorem, $FA \cong Ab$. □

Lemma 9.7. *If two free abelian groups have the same basis, they are isomorphic*

Proof. The proof is identical to that in proposition 8.2. □

Elements of free abelian groups on a basis B are represented as a set of tuples, with the first element being a unique element of B, and the second being an integer, and there being finitely many tuples with a non-zero second entry. Multiplication of two elements adds the integers in the second field together, and the identity element is where every member has the integer field as 0. This looks a lot like a vector space, and treatment of free abelian groups as vector modules.

Lemma 9.8. *A free abelian group is isomorphic to a* $\mathbb{Z}$*-module with dimension being the cardinality of the basis of the group.*

Proof. Consider a mapping f acting from a $\mathbb{Z}$-module to a free group in the manner: the elements of the canonical basis map to a single letter in the free abelian group. Vector addition correspondingly maps to group multiplication and scalar multiplication with a maps to exponentiation a times if a is non negative, or the inverse of scalar multiplication with $-a$ otherwise. This shows that a $\mathbb{Z}$-module has the same structure as a free abelian group. □

Theorem 9.9. *If two free groups are isomorphic, with the cardinality of their bases being at most* $\aleph_0$*, then their bases have the same cardinality.*

Proof. One begins by abelianizing the free groups, so one gets isomorphic free abelian groups on the same basis. This is true due to lemma 9.6. And since free abelian groups are isomorphic to $\mathbb{Z}$-modules, one gets a pair of isomorphic $\mathbb{Z}$-modules. All one needs to do now is show their bases have the same cardinality because abelianization does not change the cardinality of the basis. Let f be the isomorphism between the modules z_1 and z_2. Let b_1 be the basis of z_1 and b_2 of z_2. The image of z_1, $f(z_1)$ is also a basis for z_2. Now we have two bases for z_2, and both their cardinalities are at most $\aleph_0$. Hence, they must have the same cardinality. This shows the isomorphic free groups have bases with same cardinalities. □

Theorem 9.10. *[6]* $\mathbb{F}_3$ *is isomorphic to a subgroup of* $\mathbb{F}_2$.

The converse of the above statement, of course, trivially true. And one doesn't expect statements like this to be true in general. The analogous statement for vector spaces, for example, is false. The reason why this statement turns out to be true is non-abelianness of $\mathbb{F}_2$ (in fact, any free group of rank greater than 1 is non-abelian).

Proof. Let $\{a, b\}$ be the generator set for $\mathbb{F}_2$. Consider the subgroup H generated by the elements of the set $S = \{a, bab^{-1}, b^2ab^{-2}\}$. Let $\{x, y, z\}$ be the basis of $\mathbb{F}_3$ and consider the mapping f such that $f(x) = a$, $f(y) = bab^{-1}$, and $f(c) = b^2ab^{-2}$. This mapping can be linearly extended to a homomorphism. Since S generates the subgroup H, the mapping is surjective, so all one needs to show now now is that the mapping is injective to prove that it's a homomorphism. For that, shows that no non empty word in $\mathbb{F}_3$ maps to the empty word. This is shown by proving that the length of $f(wl)$ is greater than then length of $f(w)$, where w is a reduced word in $\mathbb{F}_3$ and l is a letter in $\mathbb{F}_3$ and l is not the inverse of the last letter in w. Then two cases can arise: either the last letter of w is the same as l, in which case the length of the image increases by 1. In the second case, the word length of the image will increase by at least 1, if $l = a^{\pm 1}$, in the other case, the word length will increase even more. Also, all the single letter words in $\mathbb{F}_3$ have images of length greater than 0. This shows that any word in $\mathbb{F}_3$ will have an image of length greater than 0, hence the kernel of f is trivial and f is an isomorphism. □

Corollary 9.11. *$\mathbb{F}_C$ is isomorphic to a subgroup of $\mathbb{F}_m$ if $m \geq 2$ where C is countably infinite set.*

Proof. Use the set $\{a, bab^{-1}, b^2ab^{-2}, \ldots\}$ as a basis for $\mathbb{F}_C$. □

10 More about presentations

A presentation of the form $\langle G; R \rangle$ generates the quotient group Q of $\mathbb{F}_G$ by the normal closure of R. This means that G acts as the generator set for Q, and all the words in R evaluate to the identity in Q.

A very natural question one could ask is whether finitely presented groups are finite. That is clearly false, since $\mathbb{Z}$ is finitely presented but not finite. What about imposing certain stronger conditions? What about a finitely presented group, all of whose elements are of finite order? What if the group in question is abelian?[1]

With the last two conditions, it's easy to answer the question; finitely presented abelian groups such that the order of every member is finite are finite. For such groups, it's possible to get an upper bound on their size.

Theorem 10.1. *If G is a finitely presented abelian group such that for all $x \in G$, $x^n = e$ for some n, then G is a finite group.*

Proof. Let G have n generators and the order of the ith generator g_i be m_i. Since G is abelian, every word in the group can be rearranged so that the ith generators are all together. Then every word in G can be written as an n-tuple with the ith term representing the exponent of g_i. And since the exponent of g_i has to be less than m_i, the number of such tuples is bounded by $\prod_{i=1}^{n} o_i$. Hence the group G is finite. □

Corollary 10.2. *If G is a finitely presented group such that all elements of G have order less than or equal to 2, the G is finite.*

Proof. By theorem 10.1, it suffices to prove that G is abelian. If the order of every element in G is less than or equal to 2, then for all $g \in G$,

$$g = g^{-1}$$

Then take any two a and b in G:

$$ab = (ab)^{-1} = b^{-1}a^{-1} = ba$$

This shows that the group is abelian, and hence finite. □

The statement when made a little weaker by lifting the condition of commutativity, is in general, false. This problem is known as Burnside's problem, named after William Burnside who first posed it in the early 20th century.

11 An application in algebraic topology

One of the motivations of any discipline of mathematics is to make certain problems in other disciplines easier to handle, as mentioned in section 1. The following theorem will show how group theory makes a problem in topology much simpler, which otherwise would have been impossibly cumbersome to handle. Before the problem is stated, here are a few definitions and lemmas one will need.

Definition 11.1. The topological space one gets by deleting n distinct points from $\mathbb{R}^2$ is called an *n-space*.

Lemma 11.1. *The* fundamental group *of an n-space is the free group of rank n.*

This lemma will be left unproven, as one will need to take a long digression into topology to prove it.

Lemma 11.2 (Nielsen-Schreier Theorem)**.** *A subgroup of a free group is free.*

This lemma will be left unproven as the author has absolutely no idea how to prove it.

Lemma 11.3. *Two elements a and b of a free group commute with each other iff both a and b are perfect powers of some element x.*

Proof. If a and b are perfect powers of some element x, it's obvious that they commute; it follows from the fact that group multiplication is associative. The converse will use the Nielsen-Schreier theorem. Assume that a and b are not perfect powers of some word x in the free group. That means $a^m \neq b^n$ for all pairs of integers (m, n) except $(0, 0)$. Consider the subgroup H generated by a and b. Since a and b commute, any element of H can be uniquely written as $a^{c_a}b^{c_b}$, where c_a and c_b are integers. This means that the subgroup H is isomorphic to the group $\mathbb{Z}^2$. But this means we have a subgroup of a free group which is not free, but that is false by lemma 11.2. Hence, our assumption that a and b are not perfect powers of some word x must be false. Hence, if a and b commute, they must be of the form x^n and x^m for some word x and some integers m and n. □

Definition 11.2. The commutator of a list of elements is analogous to the commutator of two elements, i.e. $[a_1, a_2, \ldots, a_n]$ is defined as $a_1 a_2 \ldots a_n a_1^{-1} a_2^{-2} \ldots a_n^{-1}$.

Lemma 11.4. *The commutator of two elements is identity iff they commute.*

Proof. If they commute, then the commutator $aba^{-1}b^{-1}$ reduces to identity. If $aba^{-1}b^{-1} = e$, then $ab = ba$, which means they commute. □

Lemma 11.5. *In a free group, if the word $[a_1, a_2, \ldots, a_m]$ ($m > 1$) is x^n for some x in the group and some positive integer n and the a_is are members of the basis, then $n = 1$, and x is the word itself.*

Proof. If x was cyclically reduced, so would x^n, and if x were not cyclically reduced, neither would x^n. This means that in this case, x is cyclically reduced. Powers of cyclically reduced words are obtained by just formal concatenation. Which means x^n is just x concatenated n times, and hence every letter of x is repeated n times in x^n. But each letter in the word occurs exactly once, which means $n = 1$. □

Theorem 11.6. *For any n-space, there exists a loop such that filling in any k of the n holes makes it* nullhomotopic*, but filling in any lesser number of holes leaves it non trivial.*

Proof. The fundamental group of an n-space is the free group on n generators. So any loop in the space is an element of the fundamental group and filling in k holes corresponds to the homomorphism that maps k basis elements to identity and the rest to non trivial elements. To be more precise, if the holes $\{h_i\}$ are filled up, it corresponds to the homomorphism which maps the a_i basis element to identity if the hole h_i is filled up, otherwise, it maps the basis element to itself. Our goal is to find the an element in the free group of rank n such that the homomorphism corresponding to filling up k or more holes maps it to the identity, and any homomorphism corresponding to filling up less than k holes does not map it to the identity. If $k = n$, the answer is trivial, just take the word $abc \dots n$. This word satisfies the required properties. For $k < n$, consider the sequence of words, $\{c_i\}$, where c_i is the commutator of the ith collection of $(k+1)$ letters from the n basis letters. There clearly are $\binom{n}{k+1}$ such commutators. The word W as described below satisfies the properties.

$$W = \left[\dots [[[a^{-1}b^{-1}c^{-1} \dots n^{-1}, c_1], c_2], c_3] \dots c_{\binom{n}{k+1}} \right]$$

Here's why W satisfies the required properties. If at least k basis elements get mapped to the identity, at least one of the $\binom{n}{k+1}$ commutators will map to identity, which means the whole compound commutator will collapse to identity. This shows that the first property is satisfied.

To show that W satisfies the second property, one first needs to show that none of the simple commutators c_i map to identity under the homomorphism. This is obvious because the homomorphism sends at most $(k-1)$ basis elements to identity, and the simple commutators have $(k+1)$ elements, which means their image will have at least 2 elements, which does not evaluate to identity. Now one needs to show that the compound commutator does not collapse either. To prove that, start from the deepest nested commutator, which is $[a^{-1}b^{-1}c^{-1} \dots n^{-1}, c_1]$. The image of the this commutator under the homomorphism will leave at least $(n-k+1)$ terms in the left hand term. From lemma 11.3, we know for this commutator to collapse, they elements have to be perfect powers of some element in the free group, and from lemma 11.5, we know that element has to be c_1. This means the left hand term will have to be a perfect power of c_1 for the commutator to collapse. But that's not possible because the first letter in the left hand term has a negative exponent whereas the first letter in any power of c_1 will have a positive exponent. Extending this argument, and reducing the nesting level, we can say the same for the commutator with c_2, c_3 and so on. This shows the word does not collapse if the homomorphism maps at most $(k-1)$ basis elements to identity.

This concludes the proof and shows the existence of such a loop by explicit construction. □

This problem was adapted from a party trick of stringing a picture frame around two nails such that pulling out any one nail ensures that the frame falls. This example just serves to show how powerful abstractions can be when applied correctly.

References

[1] Gilbert Baumslag, *Topics in combinatorial group theory*, 1993.

[2] Paul R. Halmos, *Finite-dimensional vector spaces*, 1958.

[3] I. N. Herstein, *Topics in algebra*, 1975.

[4] D.L. Johnson, *Presentations of groups*, 1990.

[5] Roger C. Lyndon and Paul E. Schupp, *Combinatorial group theory*, 2001.

[6] John Meier, *Groups, graphs and trees: An introduction to the geometry of infinite groups*, 2008.

[7] A. D. Miasnikov, *Genetic algorithms and the andrews-curtis conjecture*, ArXiv Mathematics e-prints (2003).