Math 4720 & 5210 **Abstract Algebra**

Free Groups

Often one first encounters free groups explained in terms of equivalence classes of words over an alphabet being multiplied by concatenation. While this is fine for a surface level understanding and gives one a construction of this type of free object, it is difficult or impossible to use such a description to rigorously prove anything about free groups. For rigorous proofs one needs a good characterization that is independent of any particular construction. Such a characterization (that ~~can~~ should be taken as the definition) of free groups is the so called *universal property* discussed later.

Construction: Words with Friends

First, let's sketch out the standard construction of a free group. Start with any set X. This will be our set of generators. Next, create a new (disjoint) set $X^{-1} = \{x^{-1} \,|\, x \in X\}$. So far these are just symbols/labels. The -1 exponent doesn't (yet) mean that x^{-1} is the inverse of x (but it will later). Now $X \cup X^{-1}$ is our *alphabet.* Next, form all *words* over our alphabet: $(X \cup X^{-1})^* = \{a_1 a_2 \cdots a_m \,|\, m \in \mathbb{Z}_{m \geq 0}$ and for each i either $a_i \in X$ or $a_i \in X^{-1}\}$. So a word over the alphabet $X \cup X^{-1}$ is just a finite string of letters drawn from X and X^{-1}. Notice that we allow $m = 0$ (the empty word). Let us denote the empty word by ε. *Note:* We will use standard exponent abbreviations so that, for example, $aaac^{-1}c^{-1}baa = a^3c^{-2}ba^2$.

Now we introduce an equivalence relation. For any $w_1, w_2 \in (X \cup X^{-1})^*$ and $x \in X$, require that $w_1xx^{-1}w_2 \sim w_1w_2$ and $w_1x^{-1}xw_2 \sim w_1w_2$. Then let $\sim$ be the equivalence relation generated by those requirements (formally one takes all equivalence relations that satisfy the above conditions and intersect to find the *least* such equivalence relation satisfying these requirements). Long story short, we have that for $w, w' \in (X \cup X^{-1})^*$, $w \sim w'$ iff w' can be obtained from w after a finite number of insertions and deletions of xx^{-1} or $x^{-1}x$ where $x \in X$.

As a random example, let $X = \{a, b, c\}$. Then $acc^{-1}ba^{-1}\underline{bb^{-1}}ac \sim a\underline{cc^{-1}}ba^{-1}ac \sim ab\underline{a^{-1}a}c \sim abc \sim \underline{b^{-1}b}abc$. Thus $acc^{-1}ba^{-1}bb^{-1}ac \sim b^{-1}babc$.

Now denote the equivalence class of a word by $[w] = \{w' \in (X \cup X^{-1})^* \,|\, w \sim w'\}$ and write the set of equivalence classes as $F(X) = (X \cup X)^*/\sim$.

Notice that given two words $w_1, w_2 \in (X \cup X^{-1})^*$, we have that $w_1w_2 \in (X \cup X^{-1})^*$ (this is concatenation, that is, putting two words together one right after the other). Now for the sneaky step. Define $[w_1][w_2] = [w_1w_2]$. We just defined the product of equivalence classes of words to be the equivalence class of the representatives put together (concatenated). It is not clear that this operation is well defined: if $w_1 \sim w_1'$ and $w_2 \sim w_2'$ is it the case that $w_1w_2 \sim w_1'w_2'$? The answer is yes, but while this may seem intuitively clear, writing down a rigorous proof is tricky. Many texts either ignore this step or give a less than convincing proof. I recommend Joseph Rotman's "An Introduction to the Theory of Groups" (4th edition) chapter 11 if you would like to see a careful proof of the existence of the group $F(X)$.

Once we know that this operation on $F(X)$ is well defined, everything else necessary to show that $F(X)$ is a group is absolutely trivial to prove. Closure is obvious. Associativity follows because concatenation is associative. The equivalence class of the empty word, $[\varepsilon]$, serves as the identity. Finally take any word $w = x_1x_2 \cdots x_\ell$ and swap out each letter x_i for its "inverse" (i.e. if $x_i \in X$ exchange it for x_i^{-1} and if $x_i = y_i^{-1} \in X^{-1}$ let $x_i^{-1} = y_i$). Now define $w^{-1} = x_\ell^{-1} \cdots x_1^{-1}$ (invert each letter and write backwards). It isn't hard to show that $ww^{-1} \sim \varepsilon \sim w^{-1}w$. Thus $[w]^{-1} = [w^{-1}]$ exists (i.e., we have inverses).

For example, again let $X = \{a, b, c\}$. Then $[ab^{-1}c^3a^{-2}]^{-1} = [a^2c^{-3}ba^{-1}]$ notice that $(ab^{-1}c^3a^{-2})(a^2c^{-3}ba^{-1}) = ab^{-1}ccca^{-1}\underline{a^{-1}a}ac^{-1}c^{-1}c^{-1}ba^{-1} \sim ab^{-1}ccc\underline{a^{-1}a}c^{-1}c^{-1}c^{-1}ba^{-1} \sim ab^{-1}cc\underline{cc^{-1}}c^{-1}c^{-1}ba^{-1} \sim \cdots \sim aa^{-1} \sim \varepsilon$.

We are ready to *define* what a free group *is.*

Characterization: A Universal Property

Definition: Let X be a set. Then the **free group** generated by X is a group $F(X)$ equipped with a map $i : X \to F(X)$ such that given *any* group G and function $\varphi : X \to G$ there exists a *unique* homomorphism $\widehat{\varphi} : F(X) \to G$ such that $\widehat{\varphi} \circ i = \varphi$.
This means that every function from our set of generators, X, into any group G can be uniquely extended to a homomorphism from $F(X)$ to G.

$$\begin{tikzcd}
F(X) \arrow[rd, dashed, "\exists!\,\widehat{\varphi}"] & \\
X \arrow[u, hook, "i"] \arrow[r, "\varphi"] & G
\end{tikzcd}$$

Consider the group $G = \{\pm 1\}$ (under multiplication). Suppose that $x, y \in X$ such that $x \neq y$. Let $\varphi(x) = -1$, $\varphi(y) = 1$, and let all other elements in X map to 1. Then there is a homomorphism $\widehat{\varphi} : F(X) \to G$ such that $\widehat{\varphi}(i(x)) = \varphi(x) = -1 \neq 1 = \varphi(y) = \widehat{\varphi}(i(y))$. Therefore, we must have that $i(x) \neq i(y)$. Therefore, i is an injection (i.e., one-to-one). Thus, it is harmless to assume i is just the inclusion map: $i(x) = x$.

Theorem: $F(X)$ (as constructed above) is free and generated by X.

Proof: (Sketch) Here we let $i : X \to F(X)$ be the inclusion map $i(x) = [x]$ (send the letter x to its equivalence class). Suppose that $\varphi : X \to G$ is a map into a group G.

First, if $x^{-1} \in X^{-1}$, we define $\varphi(x^{-1}) = \varphi(x)^{-1}$, so our map is extended to $X \cup X^{-1}$. Now define $\varphi(x_1 \dots x_\ell) = \varphi(x_1) \cdots \varphi(x_\ell)$, so our map is defined on $(X \cup X^{-1})^*$. Next, notice that for any $w_1, w_2 \in (X \cup X^{-1})^*$ and $x \in X$, $\varphi(w_1 x x^{-1} w_2) = \varphi(w_1)\varphi(x)\varphi(x)^{-1}\varphi(w_2) = \varphi(w_1)\varphi(w_2) = \varphi(w_1 w_2)$. Likewise, $\varphi(w_1 x^{-1} x w_2) = \varphi(w_1 w_2)$. Thus φ is constant on equivalence classes so we induce a mapping on $F(X) = (X \cup X^{-1})^*/\sim$.

Call this map $\widehat{\varphi} : F(X) \to G$. By construction, this map preserves the operation and thus is a homomorphism. Also, again by construction, we have $\widehat{\varphi} \circ i = \varphi$. Finally, suppose $\psi : F(X) \to G$ is any homomorphism such that $\psi \circ i = \varphi$. Then $\psi([x_1 \cdot x_\ell]) = \psi([x_1]) \cdots \psi([x_\ell]) = \psi(i(x_1)) \cdots \psi(i(x_\ell)) = \varphi(x_1) \cdots \varphi(x_\ell) = \widehat{\varphi}([x_1]) \cdots \widehat{\varphi}([x_\ell]) = \widehat{\varphi}([x_1 \cdots x_\ell])$. This establishes uniqueness. ■

Going forward, let's drop the brackets and understand that when we reference a word over a set of generators in a free group, we really mean the equivalence class of that word.

Theorem: The free group on X, $F(X)$ is uniquely determined (up to isomorphism) by the universal property. Specifically, given free groups on X, $i_1 : X \to F_1$ and $i_2 : X \to F_2$, there is a (unique) isomorphism $\widehat{i_2} : F_1 \to F_2$ such that $\widehat{i_2} \circ i_1 = i_2$. Moreover, $\widehat{i_1}^{-1} = \widehat{i_2}$.

Proof: Notice that in the diagram for F_1, if we set $G = F_1$ and $\varphi = i_1$, we get that $\mathrm{id}_{F_1} \circ i_1 = i_1$ so that id_{F_1} is the unique homomorphism extending i_1 here. A similar statement holds for F_2.
Next, consider the diagram for F_1 with $G = F_2$ and $\varphi = i_2$. Then we get a (unique) homomorphism $\widehat{i_2} : F_1 \to F_2$ where $\widehat{i_2} \circ i_1 = i_2$. Interchanging the roles of F_1 and F_2, we get a (unique) homomorphism $\widehat{i_1} : F_2 \to F_1$ where $\widehat{i_1} \circ i_2 = i_1$.

$$\begin{tikzcd}
F_1 \arrow[dr, dashed, "\mathrm{id}_{F_1}"] & \\
X \arrow[u, hook, "i_1"] \arrow[r, hook, "i_1"] & F_1
\end{tikzcd}$$

$$\begin{tikzcd}
F_1 \arrow[loop left, dashed, "\mathrm{id}_{F_1} = \widehat{i_1} \circ \widehat{i_2}"] \arrow[dr, dashed, bend right, "\widehat{i_2}"'] & \\
X \arrow[u, "i_1"] \arrow[r, hook, "i_2"] & F_2 \arrow[ul, dashed, bend right, "\widehat{i_1}"'] \arrow[loop right, dashed, "\widehat{i_2} \circ \widehat{i_1} = \mathrm{id}_{F_2}"]
\end{tikzcd}$$

Notice that $\widehat{i_1} \circ \widehat{i_2} : F_1 \to F_1$ is a homomorphism such that $\widehat{i_1} \circ \widehat{i_2} \circ i_1 = \widehat{i_1} \circ i_2 = i_1$. Thus $\widehat{i_1} \circ \widehat{i_2}$ solves the same problem that id_{F_1} did at the beginning of our proof. Thus by *uniqueness* we must have that $\widehat{i_1} \circ \widehat{i_2} = \mathrm{id}_{F_1}$. Likewise, $\widehat{i_2} \circ \widehat{i_1} = \mathrm{id}_{F_2}$. Therefore, $\widehat{i_1}$ is the desired isomorphism with inverse $\widehat{i_2}$. ■

Thus if we can show that a group satisfies the necessary universal property, it must be *the* free group on that generating set (determined up to isomorphism).

Theorem: Let $X = \varnothing$ (the empty set). Then $F(\varnothing)$ is the trivial group.

Proof: We show that the trivial group $\{1\}$ satisfies the universal property associated with $X = \varnothing$.

We have $i : \varnothing \to \{1\}$ is the empty map (it does nothing). Let $\varphi : \varnothing \to G$ for some group G. Then again φ is the empty map. Next, there is only one homomorphism from the trivial group to any group: $\widehat{\varphi} : \{1\} \to G$ must be $\widehat{\varphi}(1) = 1$ (we must send the identity 1 to the identity in G).

Trivially, $\widehat{\varphi} \circ i = \varphi$ since both sides are empty maps. Thus we have shown that every φ uniquely extends to a homomorphism. Thus $\{1\}$ is the free group on no generators (i.e., the empty set). ■

Quick Theorems: Using the Universal Property

Let's prove a few basic things about free groups. First, let's show that $F(X)$ is non-trivial iff $X \neq \varnothing$. Actually, it would be just as easy to show that $F(X)$ is infinite whenever $X \neq \varnothing$, but I'll save that for a homework problem.

Theorem: $F(X)$ is non-trivial iff $X \neq \varnothing$

Proof: We already know that $F(\varnothing) \cong \{1\}$. Let's take care of the other implication. Suppose that $X \neq \varnothing$. To show that $F(X)$ is non-trivial we select a nontrivial model group. We will use $G = \{\pm 1\}$.

Since X is non-empty, there is some $x_0 \in X$. Let $\varphi(x_0) = -1$ and set $\varphi(x) = 1$ for any $x \in X - \{x_0\}$ (that may be empty but this is doesn't matter). There exists a unique homomorphism $\widehat{\varphi} : F(X) \to \{\pm 1\}$ such that $\widehat{\varphi} \circ i = \varphi$. In particular, $\widehat{\varphi}(x_0) = -1$ so that $\widehat{\varphi}(x_0^2) = (-1)^2 = 1$. Therefore, we have a homomorphism from $F(X)$ onto $\{\pm 1\}$. Thus $F(X)$ cannot be trivial. ■

It turns out that for $X \neq \varnothing$, $F(X)$ is infinite (this would have been just as easy to prove). A free group on a single element is just infinite cyclic (i.e., isomorphic to $\mathbb{Z}$ under addition).

Theorem: $F(\{x_0\}) \cong \mathbb{Z}$

Proof: Let $i : \{x_0\} \to \mathbb{Z}$ be defined by $i(x_0) = 1$. We will show that $\mathbb{Z}$ has the necessary universal property. Let $\varphi : \{x_0\} \to G$ be a function where G is some group. So $\varphi(x_0) = g$ for some fixed $g \in G$.

Define $\widehat{\varphi} : \mathbb{Z} \to G$ by $\widehat{\varphi}(n) = g^n$. Notice that $\widehat{\varphi}(n+m) = g^{n+m} = g^n g^m = \widehat{\varphi}(n)\widehat{\varphi}(m)$. Thus $\widehat{\varphi}$ is a homomorphism. Note that $\widehat{\varphi}(i(x_0)) = \widehat{\varphi}(1) = g^1 = g = \varphi(x_0)$. It is easy to see that $\widehat{\varphi}$ is the only possible homomorphism with $\widehat{\varphi} \circ i = \varphi$.

Thus by the uniqueness of free groups, we have $F(\{x_0\}) \cong \mathbb{Z}$ ■

What if X has more than one element? Well, then $F(X)$ gets much much more complicated. For example, it is no longer Abelian.

Theorem: Let X be a set with at least two elements. Then $F(X)$ is non-abelian.

Proof: To show $F(X)$ is non-abelian we choose a non-abelian model to force this property to appear. In particular, let's consider the symmetric group S_3 (permutations on three elements).

Let $x_1, x_2 \in X$ with $x_1 \neq x_2$ (these exist since X has at least two elements). Define a function $\varphi : X \to S_3$ by $\varphi(x_1) = (12)$, $\varphi(x_2) = (23)$, and $\varphi(x) = (1)$ for all other $x \in X$.

There exists a unique homomorphism $\widehat{\varphi} : F(X) \to S_3$ such that $\widehat{\varphi} \circ i = \varphi$. In particular, $\widehat{\varphi}(x_1x_2) = \widehat{\varphi}(x_1)\widehat{\varphi}(x_2) = \varphi(x_1)\varphi(x_2) = (12)(23) = (123)$. However, $\widehat{\varphi}(x_2x_1) = \widehat{\varphi}(x_2)\widehat{\varphi}(x_1) = \varphi(x_2)\varphi(x_1) = (23)(12) = (132)$. Therefore, $\widehat{\varphi}(x_1x_2) \neq \widehat{\varphi}(x_2x_1)$ so that $x_1x_2 \neq x_2x_1$. In particular, $F(X)$ is not Abelian. ■

It is not hard to show that if $|X_1| = |X_2|$ (X_1 and X_2 have the same cardinality), then $F(X_1) \cong F(X_2)$. The converse is also true, so that $F(X_1) \cong F(X_2)$ iff $|X_1| = |X_2|$. The converse is a little trickier to prove. One usually does this by reducing the problem to free abelian groups and using uniqueness of rank. Uniqueness of rank in free abelian groups is established by reducing to vector spaces.

It is also true that every subgroup of a free group is free. This result is quite difficult to establish. As a consequence, every nonidentity element must have infinite order (such an element generates a cyclic subgroup that must being nontrivial and free must be infinite). Other stranger things are true. Like even though a subgroup of a free group is free, this subgroup may require a larger set of generators!

Generators and Relations: Everything is a Quotient of a Free Group

Definition: Let X be a set and $R \subseteq (X \cup X^{-1})/\sim$ be a collection of words. Let N be the smallest normal subgroup containing R (take all normal subgroups containing R and intersect). The quotient group $F(X)/N$, denoted $\langle X \,|\, R \rangle$, is called the group with **generators**, X, and **relations**, R.

When R is a finite set, we will usually write its elements as a list. If $r \in R \subseteq N$, then we have $rN = N$ in $F(X)/N$ (i.e., r is equivalent to the identity in $F(X)/N$. Thus we will write $r = 1$ (understanding that this holds mod N). Sometimes, instead of listing a relation r, we write $r = 1$. Or we might write $h = k$ when we actually mean hk^{-1} is in the set of relations.

For example, $\langle x \,|\, x^3 = 1 \rangle$ is the group generated by x subject to the relation $x^3 = 1$. It should seem reasonable to conclude that $\langle x \,|\, x^3 = 1 \rangle = \{1, x, x^2\} \cong \mathbb{Z}_3$.

Now we can denote free groups as $F(X) = \langle X \,|\, \rangle$ (i.e., no relations). So for example, $\langle x \,|\, \rangle \cong \mathbb{Z}$ and $\langle \;|\; \rangle \cong \{1\}$.

Another example, $D_n = \langle x, y \,|\, x^n = 1, y^2 = 1, (xy)^2 = 1 \rangle$. This is the *dihedral group* of order $2n$. It turns out that this is isomorphic to the group of symmetries of a regular n-gon. Notice $y^2 = 1$ means that $y = y^{-1}$. Next, $(xy)^2 = 1$ so that $xyxy = 1$ so that $xyxyy^{-1} = y^{-1}$ so $xyx = y$ since $y = y^{-1}$. This then implies that $xy = yx^{-1}$ and $yx = x^{-1}y$.

In particular, any string of powers of x's and y's can be rewritten so that all of the x's are to the left and y's to the right. But $x^n = 1$, so exponents of x can be reduced mod n. Likewise, exponents of y can be reduced mod 2. So we can write each element in D_n as $x^i y^j$ where $i = 1, \ldots, n-1$ and $j = 0, 1$. Therefore, $D_n = \{1, x, \ldots, x^{n-1}, y, xy, \ldots, x^{n-1}y\}$.

Theorem: Every group is isomorphic to a group described by generators and relations.

Proof: Let G be a group, so in particular, G is a set. Consider the free group $F(G)$. Let $\varphi = \mathrm{id}_G : G \to G$ (so $\varphi(g) = g$). There exists a homomorphism $\widehat{\varphi} : F(G) \to G$. Since $\widehat{\varphi} \circ i = \varphi$ and φ is onto, $\widehat{\varphi}$ is onto. Thus we have a homomorphism from $F(G)$ onto G. The first isomorphism then gives us $F(G)/\ker(\widehat{\varphi}) \cong G$. Let $R = \ker(\widehat{\varphi})$. We have $G \cong F(G)/R = \langle G \,|\, R \rangle$. ■

We call the generators X paired with relations R a *presentation* of the group $\langle X \,|\, R \rangle$. If both X and R are finite, we call $\langle X \,|\, R \rangle$ *finitely presented*.

Theorem: Let $\varphi : X \to G$ be a function, $R \subseteq (X \cup X^{-1})^*$ (a set of words over the generators X), and suppose $\varphi(x_1) \cdots \varphi(x_\ell) = 1$ for all $r = x_1 \cdots x_\ell \in R$. Then there exists a unique homomorphism $\widehat{\varphi} : \langle X \,|\, R \rangle \to G$ such that $\widehat{\varphi} \circ i = \varphi$ where $i : X \to \langle X \,|\, R \rangle$ sends x to its coset in $\langle X \,|\, R \rangle$.

$$\begin{tikzcd}
\langle X \,|\, R \rangle \arrow[dr, dashed, "\exists!\, \widehat{\varphi}"] & \\
X \arrow[u, hook, "i"] \arrow[r, "\varphi"] & G
\end{tikzcd}$$

The proof of the above theorem is straightforward, but I will skip it. In fact, we could (?should?) use this as the definition of a group generated by X with relations R. In a nearly identical proof, one can show that any two groups satisfying this kind of universal property are isomorphic. This characterization says is that $\langle X \,|\, R \rangle$ is the free-est possible group satisfying the specified relations.

Computing with Generators and Relations: Word Problems are Too Hard!

Since every group can be described by generators and relations, one might think that this approach is a cure all. However, it turns out that most everything you might want to know about finitely presented groups in general is incomputable.

For example, given a random $G = \langle X \,|\, R \rangle$ and suppose w_1 and w_2 are words over $X \cup X^{-1}$. One might want to know if $w_1 = w_2$. An algorithm determining when w_1 and w_2 are equal in G would solve the *word problem* for G. It turns out that there is a finitely presented group with an incomputable word problem!

More than that, there is no algorithm that can determine if a random finitely presented group is finite or infinite. There is no such algorithm to decide if it's abelian or not. There is no algorithm that can determine if two finitely presented groups are isomorphic. In fact, there is no algorithm to determine if a random finitely presented group is trivial or not!

Not all is hopeless, if we know ahead of time that our finitely presented group is abelian or finite, we can compute everything about it (for finite groups the Todd-Coxeter algorithm will enable us to do this). But for a general finitely presented group, things are bleak. Chapter 12 of Rotman's group theory text covers the word problem in group theory and related issues.

Other Free Things: Same Old, Same Old

We could also ask about other kinds of free objects. Generally we define a free *thing* generated by a set using the same universal property we used for groups. For example, to define a *free abelian group* we just need to slap the word "abelian" in front of every occurrence of "group" in the definition of free group. To define what a free ring is just swap out the word "group" for "ring".

While you can always write down a definition of how your free algebraic object should behave. Such an object does not always exist. For example, there are no free fields (if you Google "free fields" you will run into a bunch of Physics related pages. This use of "field" is related to vector fields not the abstract algebra kind of field). There are such things as free rings, free associative algebras (tensor algebras), free commutative associative algebras (polynomials), free vector spaces (all vector spaces are free), free Lie algebras, etc.

In fact, free objects exists for every "relationally defined" algebraic object. There is even a universal construction of such things that would include our construction as a special case!