A construction of free groups via involutive monoids

Pedro Resende

Abstract

Support notes for the Algebra course of LMAC in the academic year 2022/2023, meant to provide a construction of free groups which is different from the usual ones found in algebra books. In particular it is different from that of Dummit&Foote. The approach via involutive monoids followed in these notes requires some additional notions, as compared to more common approaches, but it gains in conceptual clarity.

Contents

0 Introduction

The notion of subgroup $\langle A \rangle$ generated by a subset A of a group G can be approached in two ways, as we have seen in the lectures. The "top down approach" defines $\langle A \rangle$ to be the intersection of all the subgroups of G that contain A, whereas the "bottom up approach" generates from A all the "words" constructed in G using the "letters" in A and their inverses. For instance, if a and b are distinct letters in A, the subgroup $\langle A \rangle$ will contain the elements 1, a, b, ab, aa, bb, ba, a^{-1}, $a^{-1}b$, etc.

Given a set X, not necessarily contained in any given group, the idea of the free group generated by X is similar to the idea of generating a subgroup using the bottom up approach. Thinking of the elements of X as "letters," the free group $F(X)$ will contain all the "words" generated by the letters in X and their inverses. Now the "product" of x and y will be interpreted simply as concatenation of the symbols x and y, and x^{-1} is just a new copy of x labelled with the symbol "$^{-1}$." Hence, for instance, if $x, y \in X$ we have words such as $xy^{-1}xxy$. And we have the empty word ε, which contains no letters and thus is the identity for the multiplication that is given by concatenation.

The inverse operation on words is easy to define. For instance, we must have

$$(xy^{-1}xxy)^{-1} = y^{-1}x^{-1}x^{-1}yx^{-1}.$$

The multiplication on words is easy to define, too, but there is a glitch. Suppose xyx^{-1} is another word, which we want to multiply by the previous one. Then concatenation gives us

$$(xyx^{-1})(xy^{-1}xxy) = xyx^{-1}xy^{-1}xxy.$$

Then in the new word we find the product $x^{-1}x$, which is not the same as the empty word, so if we replace it by ε we get the different word

$$xyy^{-1}xxy.$$

Note that this is really different, since in particular it contains only six symbols, whereas the previous word contained eight symbols. The conclusion is that the set of all the words which are generated by the elements of X and their inverses is a monoid, and it even has an operation that resembles an inverse operation of a group, but whose key property is missing because $x^{-1}x$ is not the identity.

The common solution to this problem is to consider only the subset of those words where no occurrences of $x^{-1}x$ or xx^{-1} exist for any symbol $x \in X$, and then to redefine the multiplication of words so that after concatenation we remove such occurrences. Then it is necessary to prove that the resulting multiplication is associative, and this involves quite some work. In these notes we follow a different approach that releases us from the burden of proving such things.

The important aspect to be retained is that, whatever the construction, each letter $x \in X$ will give rise to an element of $F(X)$, usually again denoted by x, although technically X may fail to be an actual subset of $F(X)$. This map of letters into $F(X)$ is called the *injection of generators* of $F(X)$, and the elements of X are the *generators*.

1 Free group on one generator

Let us look at a simple example first, namely $X = \{x\}$. The "words" generated by x should be positive powers x^n with $n \in \mathbb{Z}_{>0}$ or their inverses x^{-n}, and the empty word x^0. In other words, $F(X)$ should be isomorphic to the infinite cyclic group $\mathbb{Z}$, with each $a \in \mathbb{Z}$ representing the "word" x^a. With this idea in mind, the injection of generators

$$\iota : \{x\} \to \mathbb{Z}$$

is defined by $\iota(x) = 1$. Suppose that $f : \{x\} \to G$ is another function into a group G. It is easy to see that there is a unique group homomorphism $f^\sharp : \mathbb{Z} \to G$ such that $f^\sharp(1) = f(x)$, namely given for all $a \in \mathbb{Z}$ by

$$f^\sharp(a) = f(x)^a.$$

In other words, there is a unique homomorphism $f^\sharp : \mathbb{Z} \to G$ such that $f^\sharp \circ \iota = f$. We should think of $f^\sharp$ as being the unique way in which f can be extended to the whole of the free group as a homomorphism. Let us state and prove this carefully:

§1. Proposition. *Let $\iota : \{x\} \to \mathbb{Z}$ be the function defined by $\iota(x) = 1$. For all groups G and all functions $f : \{x\} \to G$ there is a unique group homomorphism $f^\sharp : \mathbb{Z} \to G$ such that the following diagram commutes:*

$$\begin{tikzcd}
\{x\} \arrow[r, "\iota"] \arrow[dr, "f"'] & \mathbb{Z} \arrow[d, dotted, "f^\sharp"] \\
& G
\end{tikzcd}$$

Proof. (Existence.) The function $f^\sharp : a \mapsto f(x)^a$ is a homomorphism, for

$$f^\sharp(a+b) = f(x)^{a+b} = f(x)^a f(x)^b = f^\sharp(a) f^\sharp(b).$$

Since $f^\sharp(\iota(x)) = f^\sharp(1) = f(x)^1 = f(x)$, we have $f^\sharp \circ \iota = f$, so we have found a solution $f^\sharp$ to the extension problem as required.

(Uniqueness.) If $g : \mathbb{Z} \to G$ is any other homomorphism and $g \circ \iota = f$ then $g(1) = g(\iota(x)) = f(x)$, and thus $g(a) = g(1)^a = f(x)^a = f^\sharp(a)$, so $g = f^\sharp$. ▮

The previous proposition is very important and, as we shall see below, it can be used as a definition of the (isomorphism class of the) free group on one generator.

Let us look a little more at this. Suppose we replace $\mathbb{Z}$ by $\mathbb{Z}/n\mathbb{Z}$ and use $\iota(x) = \overline{1}$ as injection of generators. Then the existence part of the proof of the previous proposition does not work. For instance, taking $G = \mathbb{Z}$ and $f(x) = 1$, the homomorphism $f^\sharp : \mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}$ would have to be defined by $f^\sharp(\overline{1}) = 1$, which is impossible. Intuitively, this is because $\mathbb{Z}/n\mathbb{Z}$, although it is indeed generated by a single generator (because $\langle \overline{1} \rangle = \mathbb{Z}/n\mathbb{Z}$), is not *freely* generated because there are constraints in $\mathbb{Z}/n\mathbb{Z}$ that do not follow inevitably from the algebraic laws of groups. Namely, we have $\overline{0} = \overline{n}$, whereas in the actual free group $\mathbb{Z}$ we have $0 \neq n$.

Now suppose we replace $\mathbb{Z}$ by $\mathbb{Z}\times\mathbb{Z}$ as our candidate for a free group, using the injection of generators $\iota(x) = (1,0)$. Now we can find a homomorphism $f^\sharp$ by defining

$$f^\sharp(a,b) = f(x)^a,$$

but it is not a unique extension. For instance, another would be given by

$$f^\sharp(a,b) = f(x)^{a+b}.$$

So, in this case there is an extension, but the uniqueness part of the proof of the above proposition fails. This means that $\mathbb{Z} \times \mathbb{Z}$ is not generated by the set $\{x\}$; that is, there are elements in $\mathbb{Z} \times \mathbb{Z}$ which are not obtained from "words" of the form x^a when we define the injection of generators to be $\iota(x) = (1,0)$.

This gives us the correct intuition with which to understand what a free group is all about: it must be a group whose elements can all be obtained by composing words using the generators, and this group should not be subject to any constraints except those that are derived by the general laws of group theory.

2 Universal property

Let X be any set, and let us suppose there is a group $F(X)$ and a function $\iota : X \to F(X)$ with the same property of §1, called the *universal property* of the pair $(F(X), \iota)$; that is, for all other functions $f : X \to G$ to a group G there is a unique homomorphism $f^\sharp : F(X) \to G$ such that the following diagram commutes:

$$\begin{tikzcd}
X \arrow[r, "\iota"] \arrow[dr, "f"'] & F(X) \arrow[d, dotted, "f^\sharp"] \\
& G
\end{tikzcd}$$

Then we say that $F(X)$ is a *free group generated by* X, and that ι is its *injection of generators.*

Of course, we have not provided an actual construction of the group $F(X)$, indeed we do not (yet) know whether such a group exists. To show that it does is the purpose of these notes. But one thing we can already prove: any two different constructions of $F(X)$ that satisfy the same universal property are equivalent because they yield isomorphic groups, as the following theorem illustrates:

§2. Theorem. *Let X be a set, and let $F(X)$ and $F'(X)$ be two free groups generated by X, with injections of generators ι and ι', respectively. Then there is an isomorphism $h : F(X) \to F'(X)$ such that $\iota' = h \circ \iota$. In particular, then, $F(X) \cong F'(X)$.*

Proof. The universal property of $F(X)$ ensures that there is a unique homomorphism of groups $h : F(X) \to F'(X)$ such that $h \circ \iota = \iota'$. Similarly, the universal property of $F'(X)$ implies that there is a unique homomorphism $k : F'(X) \to F(X)$ such that $k \circ \iota' = \iota$. Hence, we have both $k \circ h \circ \iota = \iota = \mathrm{id} \circ \iota$ and $h \circ k \circ \iota' = \iota' = \mathrm{id} \circ \iota'$. So the uniqueness part of the universal property of $F(X)$ implies that $k \circ h = \mathrm{id}$ and the uniqueness part of the universal property of $F'(X)$ implies that $h \circ k = \mathrm{id}$. This shows that h is an isomorphism with inverse k. ∎

3 Free monoids

Let us begin with the much simpler case of monoids, instead of groups. Let X be a set, and let us denote by X^* the set of all the *words* constructed with symbols taken from X: each word is simply a finite list of symbols $x_1 x_2 \ldots x_n$. The length of a word is the number of occurrences of symbols in it, regardless of how many times each symbol is repeated; for instance, $x_1x_2 \ldots x_n$ has length n. The *empty word*, with no symbols and length zero, is denoted by ε.

X^* has a natural monoid structure: the (associative) product is concatenation of words,

$$(x_1 \ldots x_n) \cdot (y_1 \ldots y_m) = x_1 \ldots x_n y_1 \ldots y_m,$$

and the identity element is the empty word ε. There is also a function $\iota : X \to X^*$ which sends each symbol in X to the corresponding word of length one, and the following universal property is easy to prove:

§3. Proposition. *For all monoids M and all functions $f : X \to M$ there is a unique homomorphism of monoids $f^\sharp : X^* \to M$ such that $f^\sharp \circ \iota = f$.*

Proof. (Existence.) Define, for each word $x_1 \ldots x_n$ with $n \in \mathbb{Z}_{\geq 1}$,

$$f^\sharp(x_1 \ldots x_n) = f(x_1) \cdots f(x_n).$$

And define $f^\sharp(\varepsilon) = 1$. Then $f^\sharp$ is a homomorphism of monoids because for each two words $x = x_1 \ldots x_n$ and $y = y_1 \ldots y_m$ we have

$$f^\sharp(xy) = f(x_1) \cdots f(x_n) f(y_1) \cdots f(y_m) = f^\sharp(x) f^\sharp(y).$$

(Uniqueness.) Let $g : X^* \to M$ be another homomorphism of monoids such that $g \circ \iota = f$. Then, $g(\varepsilon) = 1 = f^\sharp(\varepsilon)$ and for all words $x = x_1 \ldots x_n$ we have, since g preserves products,

$$g(x) = g(x_1 \ldots x_n) = g(x_1) \cdots g(x_n) = f(x_1) \cdots f(x_n) = f^\sharp(x). \quad \blacksquare$$

4 Involutive sets

§4. Definition. By an *involutive set* is meant a set S equipped with an operation $(-)^* : S \to S$ such that for all $x \in S$ we have $x^{**} = x$. A function $f : S \to T$ between involutive sets is *involutive*, or a *homomorphism* of involutive sets, if for all $x \in S$ we have $f(x^*) = f(x)^*$.

An involutive set is a very simple type of algebraic structure, and there is an associated universal property, too:

§5. Proposition. *Let X be a set. Define*

$$i(X) = X \times \{1\} \cup X \times \{2\}.$$

Then $i(X)$ is an involutive set whose involution is defined for all $x \in X$ by

$$(x,1)^* = (x,2) \text{ and } (x,2)^* = (x,1).$$

Let $\iota : X \to i(X)$ be defined by $\iota(x) = (x,1)$ for each $x \in X$. If S is another involutive set and $f : X \to S$ is a function, then there is a unique homomorphism of involutive sets $f^\sharp : i(X) \to S$ such that $f^\sharp \circ \iota = f$.

Proof. That $i(X)$ is an involutive set is obvious. Let us prove the universal property only to call attention to the fact that, contrary to the monoid case above, now ι cannot be regarded merely as an inclusion.

(Existence.) Let $f : X \to S$ be a function. Define for all $x \in X$

$$f^\sharp(x,1) = f(x) \text{ and } f^\sharp(x,2) = f(x)^*.$$

Clearly, this function is involutive, and it satisfies $f^\sharp \circ \iota = f$ because for all $x \in X$

$$f^\sharp(\iota(x)) = f^\sharp(x,1) = f(x).$$

(Uniqueness.) This is left as an exercise. ∎

§6. Definition. $i(X)$ is called a *free involutive set* generated by X.

§7. Corollary. *Any other involutive set satisfying the same universal property of $i(X)$ is isomorphic to $i(X)$.*

Proof. Exercise (the proof is similar to that of §2). ∎

5 Involutive monoids

By an *involutive monoid M* is meant a monoid which is also an involutive set such that for all $m, n \in M$ we have

$$(mn)^* = n^* m^*.$$

A *homomorphism* of involutive monoids is a homomorphism of monoids which is also an involutive function.

§8. Exercise. Prove that for any involutive monoid we have $1^* = 1$.

§9. Lemma. *Let S be an involutive set, and let S^* be the free monoid on S, with inclusion function $\iota : S \to S^*$. Then S^* is an involutive monoid if we define for each word $x_1 \dots x_n \in S^*$*

$$(x_1 \dots x_n)^* = x_n^* \dots x_1^*.$$

Moreover, if M is another involutive monoid and $f : S \to M$ is an involutive function, the unique homomorphism of monoids $f^\sharp : S^* \to M$ such that $f^\sharp \circ \iota = f$ is itself involutive.

§10. Corollary. *Let X be a set. Then $i(X)^*$ is an involutive monoid. Letting*

$$\iota : X \to i(X)^*$$

be the function defined for all $x \in X$ by $\iota(x) = (x, 1)$, for any other function to an involutive monoid

$$f : X \to M$$

there is a unique homomorphism of involutive monoids $f^\sharp : i(X)^*$ such that $f^\sharp \circ \iota = f$.

Proof. Exercise. ∎

§11. Definition. Due to the above property, $i(X)^*$ is called the *free involutive monoid* generated by X.

§12. Exercise. Similarly to groups and involutive sets, the universal property defines the free involutive monoid generated by X uniquely up to an isomorphism. State this precisely and prove it.

6 Quotients of involutive monoids

§13. Definition. Let M be an involutive monoid. A *congruence relation* on M is an equivalence relation on M which contains $(1, 1)$ and is closed under products and the involution in the product involutive monoid $M \times M$ (the identity is $(1, 1)$ and the product and the involution are computed componentwise: $(m, n)(m', n') = (mm', nn')$ and $(m, n)^* = (m^*, n^*)$).

§14. LEMMA. *Let M be an involutive monoid, and let $\sim$ be a congruence relation on M. Then the quotient $M/\sim$ is an involutive monoid. The product and the involution applied to equivalence classes is defined by*

$$[m][n] = [mn] \text{ and } [m]^* = [m^*].$$

If $h : M \to N$ is a homomorphism of involutive monoids that is constant on each equivalence class then there is a unique homomorphism of involutive monoids $\overline{h} : M/\sim \to N$ such that $\overline{h}([m]) = h(m)$ for all $m \in M$.

Proof. Exercise. ▮

§15. DEFINITION. Let M be an involutive monoid. A *group congruence* on M is any congruence of involutive monoids $\sim$ such that $mm^* \sim 1$ for all $m \in M$. The intersection of all the group congruences on M (exercise: show that this is a group congruence) is denoted by $\sim_G$.

§16. LEMMA. *Let M be an involutive monoid. For any group congruence $\sim$, the quotient $M/\sim$ is a group such that $[m]^{-1} = [m]^*$ for each $m \in M$. If $h : M \to G$ is a homomorphism of involutive monoids to a group G (regarded as an involutive monoid with involution given by inverse) there is a unique group homomorphism $\overline{h} : M/\sim_G \to G$ such that $\overline{h}([m]) = h(m)$ for all $m \in M$.*

Proof. Exercise. ▮

§17. DEFINITION. $M/\sim_G$ in the above lemma is called the *universal group quotient* of M.

7 Free groups

The free involutive monoid $i(X)^*$ is "almost" the free group generated by X, for its elements can be identified with products of letters x from X and their "inverses" x^*; more precisely, concretely each element of $i(X)^*$ is a word whose letters are "symbols" $(x, 1)$ or $(x, 2)$, standing respectively for x and x^*. The only problem standing between $i(X)^*$ and the envisaged construction of a free group is that this "inverse" x^* is not an actual inverse, since each product $(x, 1)(x, 2)$ is a word of length 2, therefore not the same as the empty word ε, which is the monoid identity. In order to solve this problem we need to contruct a quotient of involutive monoids $i(X)^*$ that identifies ε with all sequences $(x,1)(x,2)$ and $(x,2)(x,1)$. This is now an immediate application of the construction of a quotient on any involutive monoid.

§18. THEOREM. *Let X be a set. Then $i(X)^*/{\sim_G}$ is a free group generated by X.*

Proof. This is a corollary of the previous propositions and lemmas, and a detailed proof is left as an exercise. ∎

§19. REMARK. This particular construction of the free group $F(X)$ is such that each element of $F(X)$ is an equivalence class of words

$$(x_1,b_1)(x_2,b_2)\ldots(x_n,b_n)$$

where $x_i \in X$ and $b_i \in \{1,2\}$. Each word of length one $(x,1)$ corresponds to the "letter" $x \in X$, and $(x,2)$ corresponds to x^{-1}. In practice, we may forget that we are working with equivalence classes and instead just write expressions such as "$x_1x_2^{-1}x_3x_4$" with the understanding that this represents the equivalence class of $(x_1,1)(x_2,2)(x_3,1)(x_4,1)$. In fact, in general we need not worry too much about such details, and we simply work with some free group $F(X)$ without paying too much attention to its particular construction, at least when all that we need is to identify the free group $F(X)$ up to an isomorphism.

8 Generators and relations

In a group G any equation $g = h$ with $g, h \in G$ can be written equivalently as $gh^{-1} = 1$, and thus any set of equations $\{g_i = h_i \mid i \in I\}$ can be identified with a subset $R \subset G$:

$$R = \{g_1h_i^{-1} \mid i \in I\}.$$

In what follows $F(X)$ denotes some free group generated by the set X, and $\iota : X \to F(X)$ is the injection of generators. Given a function $f : X \to G$ to a group G, the unique homomorphism $f^\sharp : F(X) \to G$ such that $f^\sharp \circ \iota = f$ is called the *homomorphic extension* of f.

§20. DEFINITION. A *group presentation by generators and relations* consists of a set X, of *generators*, and a subset $R \subset F(X)$, whose elements are called *relations.* The *group presented by X and R* is denoted by $\langle X \mid R\rangle$ and it is defined as

$$\langle X \mid R\rangle = F(X)/N(R),$$

where $N(R)$ is the normal subgroup of $F(X)$ generated by R. The *injection of generators* of $\langle X \mid R\rangle$ is the map $x \mapsto \iota(x)N(R)$. A function $f : X \to G$ to a group G is said to *respect the relations* in R if the kernel of its homomorphic extension $f^\sharp : F(X) \to G$ contains R.

§21. Theorem. *Let X be a set, $R \subset F(X)$, and G a group. Any function $f : X \to G$ that respects the relations in R extends uniquely to a homomorphism of groups $f^\sharp : \langle X \mid R\rangle \to G$; in other words, there is a unique homomorphism of groups $f^\sharp$ such that $f^\sharp\big(\iota(x)N(R)\big) = f(x)$ for all $x \in X$.*

Proof. Exercise. ∎

§22. Example. $D_{2n} \cong \langle\{r, s\} \mid \{r^n, s^2, rsrs\}\rangle$. A function $f : \{r, s\} \to G$ respects the relations if and only if, writing $f^\sharp : F(X) \to G$ for the homomorphic extension of f to the free group,

$$f^\sharp(r^n) = f^\sharp(s^2) = f^\sharp(rsrs) = 1.$$

This is equivalent to

$$f(r)^n = f(s)^2 = 1 \text{ and } f(r)f(s) = f(s)f(r)^{-1},$$

which explains the usual recipe for defining homomorphisms whose domains are groups presented by generators and relations: a function $f : X \to G$ defined on the generators respects the relations if and only if upon replacing each generator x by $f(x)$ we obtain valid equations in the group G.