Free (as in group)

Mio Alter

July 30, 2018

Introduction

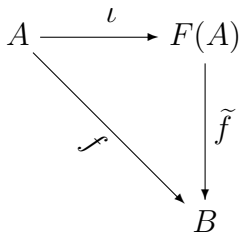
In the FP discussion on free construcions, we looked at the Spire implementation of Free Group. Elements of `FreeGroup[A]` are `Vectors` of `Either[A]` where `Left`s represent the pluses and `Right`s represent the minuses. @abuss asked "what if you flip the pluses and the minuses, is that isomorphic to the original?" The topic of uniqueness came up earlier: mathematically, free groups are unique (up to unique isomorphism) so it makes sense to say "the" free group, whereas different programming implementations have different performance tradeoffs. In the case of flipping the pluses and minuses what we get is isomorphic mathematically and implementation-wise.

Mathematical Construction

Let's go through the mathematical construction of free groups and see why what we get by flipping is isomorphic to what we get by not flipping.

Given a set A, a free group on A consists of two things along with a "universal property":

- a group $F(A)$ along with
- a one-to-one function $\iota : A \to F(A)$, such that
- for any group B and function (of sets) $f : A \to B$, there exists a unique function $\widetilde{f}$ (of groups) which makes this diagram commute



meaning that $f = \widetilde{f} \circ \iota$.

This is a specification with no implementation yet. The univesal property says that: given any group B and $f : A \to B$ of underlying sets, we can extend f to a homomorphism of groups $F(A) \to B$. The equation $f = \widetilde{f} \circ \iota$ says exactly that, on the copy $\iota(A)$ of A inside of $F(A)$, $\widetilde{f}$ is f.

The idea is: we make A into a group $F(A)$ in the dumbest way possible, without actually knowing how to combine things; then, given an actual group B, to map our dumb group $F(A)$ to B where we really *do* know how to combine things, all we have to say is where the original elements of A go, f, and we get the rest, $\widetilde{f}$, for free.

Here's an implementation: start with the set A; for every element $a \in A$ add an element a^{-1}. Form all finite-length strings of these including the empty string ϵ, and cancel out any adjacent aa^{-1} or $a^{-1}a$ pairs. This is the set $F(A)$. It is a group with concatenation of strings as the product, inverses as inverses, and the empty string ϵ as identity element. $\iota : A \to F(A)$ is the function that sends the element $a \in A$ to the string $a \in F(A)$.

But, we're not done: for this to meet the specification of a free group on A, we have to show that it satisfies the universal property. So, suppose that B is a group and $f : A \to B$ is a function. We can define $\widetilde{f} : F(A) \to B$ by: $\widetilde{f}(a) = f(a)$, $\widetilde{f}(a^{-1}) = \widetilde{f}(a)^{-1}$, $\widetilde{f}(\epsilon) = id_B$, the identity element of B, and $\widetilde{f}$ of a string is the product, in B, of $\widetilde{f}$ of its elements. So, $\widetilde{f}$ takes identity to identity, inverses to inverses, and products to products so is a homomorphism of groups and, by definition, $\widetilde{f}(\iota(a)) = f(a)$.

So our $(F(A), \iota)$ implements a free group according to the specification.

Math vs. Spire

Our $\iota : A \to F(A)$ is Spire's `Freegroup.lift` and, given $f : A \to B$, our $\widetilde{f} : F(A) \to B$ is Spire's `FreeGroup.run(f)`. Spire's group operation

`FreeGroup.|+|` eliminates canceling pairs with the `reduce` function.

Examples of Free Groups

If $A = \{a\}$ is a one-element set, then $F(A)$ is isomorphic to the integers $\mathbb{Z}$. For $B = \mathbb{Z}/n\mathbb{Z}$, and $f : A \to B$, $f(a) = 1$, then $\widetilde{f}$ is reduction mod n.

If $A = \{a, b\}$ is a two-element set, then $F(A)$ is the "free group on two generators" which is not abelian/commutative. As @aaronlevin mentioned, it appears in the proof of the Banach-Tarski paradox. The group $\mathbb{Z} \times \mathbb{Z}$ of pairs of integers is an abelian group under component-wise addition. For $B = \mathbb{Z} \times \mathbb{Z}$ and $f : A \to B$ defined by $f(a) = (1, 0)$ and $f(b) = (0, 1)$, $\widetilde{f} : F(A) \to B$ is "the abelianization" function: even though $ab \neq ba$ in $F(A)$, $\widetilde{f}(ab) = \widetilde{f}(ba)$ in $\mathbb{Z} \times \mathbb{Z}$ since

$$\widetilde{f}(ab) = f(a) + f(b) = (1, 0) + (0, 1) = (1, 1)$$

and

$$\widetilde{f}(ba) = f(b) + f(a) = (0, 1) + (1, 0) = (1, 1)$$

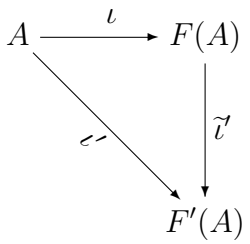
The Original Question

What about the original question: what if we flip the pluses and minuses? We can define a function $flip : F(A) \to F(A)$ by $flip(a) = a^{-1}$ and extend this to a homomorphism of groups (sending the identity to identity and products to products). We can then show that $(F(A), flip \circ \iota)$ is a free group for A and directly show that $flip$ is an isomorphism of groups. It's not hard to show that $flip$ is its own inverse so is an isomorphism, but once we show that free groups are unique, we can also appeal to that.

Programming-implementation-wise as well, if we flipped pluses and minuses in Spire, the performance would not change. If we switched to the case-class encoding where we can represent abc as either `Combine(Combine(a,b),c)` or `Combine(a, Combine(b,c))`, then although we would like these to be equal, they won't be automatically and we are locked into the particular parenthesization we used to construct an element so performance may suffer when we try to `FreeGroup.run` things.

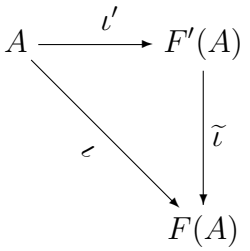
Uniqueness of The (Mathematical) Free Group

While we're here let's go ahead and use the universal property of a free groups to show that there is a unique isomorphism between any two (mathematical) implementations. Suppose that $(F'(A), \iota')$ is another free group on A. Then $F'(A)$ is a group and $\iota' : A \to F'(A)$ is a function and, since $(F(A), \iota)$ is a free group, there exists a unique extension of ι' to $F(A)$ that makes the diagram

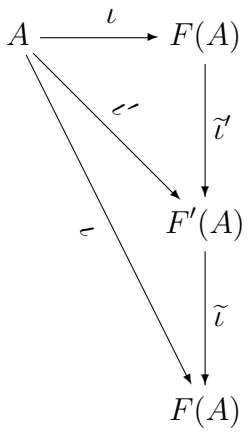


commute.

Similarly, $F(A)$ is a group and $\iota : A \to F(A)$ is a function and, since $(F'(A), \iota')$ is a free group, there exists a unique extension $\widetilde{\iota} : F'(A) \to F(A)$ of ι which makes this diagram



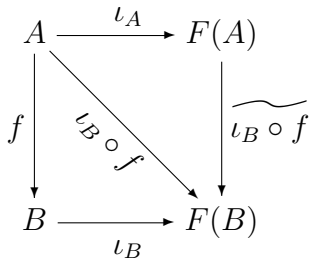
commute. Stacking these, we get the following diagram



We just said that each small triangle commutes so the large triangle does as well. Playing the game one more time on the large triangle: since $(F(A), \iota)$ is a free group, there is a unique group homomorphism $F(A) \to F(A)$ that we can put on the right side to make the diagram commute. Clearly $id : F(A) \to F(A)$ will work and, since it is unique, what we already have there, $\widetilde{\iota} \circ \widetilde{\iota}'$ must be the identity. But this says that $\widetilde{\iota}$ and $\widetilde{\iota}'$ are inverse homomorphisms to each other and thus that each is an isomorphism. Thus $F(A)$ and $F'(A)$ are isomorphic via the unique homomorphisms that we get from knowing that each is a free group. So we can say "the" free group knowing that any two are unique via a unique isomorphism.

Free is a Functor

Given a function $f : A \to B$, we get a function $F(A) \to F(B)$ as follows. First, we compose f with $\iota_B : B \to F(B)$ to get a function $A \to F(B)$. Then, by the universal property of $F(A)$, this extends to a homomorphism $F(A) \to F(B)$.



We have been talking about groups, but this works just as well for any algebraic foo.