use the result of the first part: if c is a solution of the equation, what can you say about $|c|$?) [VII.5.15]

4.13. $\neg$ Prove that $\mathrm{Aut}_{\mathsf{Grp}}(\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}) \cong S_3$. [IV.5.14]

4.14. $\triangleright$ Prove that the order of the group of automorphisms of a cyclic group C_n is the number of positive integers $r < n$ that are *relatively prime* to n. (This is called *Euler's ϕ-function;* cf. Exercise 6.14.) [§IV.1.4, IV.1.22, §IV.2.5]

4.15. $\neg$ Compute the group of automorphisms of $(\mathbb{Z}, +)$. Prove that if p is prime, then $\mathrm{Aut}_{\mathsf{Grp}}(C_p) \cong C_{p-1}$. (Use Exercise 4.11.) [IV.5.12]

4.16. $\neg$ Prove *Wilson's theorem: a positive integer p is prime if and only if*

$$(p-1)! \equiv -1 \mod p.$$

(For one direction, use Exercises 1.8 and 4.11. For the other, assume d is a proper divisor of p, and note that d divides $(p-1)!$; therefore....) [IV.4.11]

4.17. For a few small (but not too small) primes p, find a generator of $(\mathbb{Z}/p\mathbb{Z})^*$.

4.18. Prove the second part of Proposition 4.8.

5. Free groups

5.1. Motivation. Having become more familiar with homomorphisms, we can now contemplate one fancier example of a group. The motivation underlying this new construction may be summarized as follows: given a set A, whose elements have no special 'group-theoretic' property, we want to construct a group $F(A)$ containing A 'in the most efficient way'.

For example, if $A = \emptyset$, then a trivial group will do. If $A = \{a\}$ is a singleton, then a trivial group will *not* do: because although a trivial group $\{a\}$ would itself be a singleton, that one element a in it would have to be the identity, and that is certainly a very special group-theoretic property. Instead, we construct an infinite cyclic group $\langle a\rangle$ whose elements are 'formal powers' a^n, $n \in \mathbb{Z}$, and we identify a with the power a^1:

$$\langle a\rangle := \{\cdots, a^{-2}, a^{-1}, a^0 = e, a^1 = a, a^2, a^3, \cdots\};$$

we take all these powers to be distinct and define multiplication in the evident way—so that the exponential map

$$\epsilon_a : \mathbb{Z} \to \langle a\rangle, \quad \epsilon_a(n) := a^n$$

is an isomorphism. The fact that 'all powers are distinct' is the formal way to implement the fact that there is nothing special about a: in the group $F(\{a\}) = \langle a\rangle$, a obeys no condition other than the inevitable $a^0 = e$.

Summarizing: if A is a singleton, then we may take $F(A)$ to be an infinite cyclic group.

The task is to formalize the heuristic motivation given above and construct a group $F(A)$ for *every* set A. As we often do, we will now ask the reader to put away this book and to try to figure out on his or her own what this may mean and how it may be accomplished.

5.2. Universal property. Hoping that the reader has now acquired an individual viewpoint on the issue, here is the standard answer: the heuristic motivation is formalized by means of a suitable universal property. Given a set A, our group $F(A)$ will have to 'contain' A; therefore it is natural to consider the category $\mathscr{F}^A$ whose objects are pairs (j, G), where G is a group and

$$j : A \to G$$

is a set-function[21] from A to G and morphisms

$$(j_1, G_1) \to (j_2, G_2)$$

are *commutative* diagrams of set-functions

$$\begin{tikzcd} G_1 \arrow[r, "\varphi"] & G_2 \\ A \arrow[u, "j_1"] \arrow[ur, "j_2"'] & \end{tikzcd}$$

in which φ is required to be a *group homomorphism*.

The reader will be reminded of the categories we considered in Example I.3.7: the only difference here is that we are mixing objects and morphisms of one category (that is, Grp) with objects and morphisms of *another* (related) category (that is, Set). The fact that we are considering all possible functions $A \to G$ is a way to implement the fact that we have no *a priori* group-theoretic information about A: we do not want to put any restriction on what may happen to the elements of A once they are mapped to a group G; hence we consider all possibilities at once.

A *free group* $F(A)$ on A will be (the group component of) an *initial* object in $\mathscr{F}^A$. This choice implements the fact that A should map to $F(A)$ in the 'most efficient way': any other way to map A to a group can be reconstructed from this one, by composing with a group homomorphism. In the language of universal properties, we can state this as follows: $F(A)$ is a free group on the set A if there is a set-function $j : A \to F(A)$ such that, for all groups G and set-functions $f : A \to G$, *there exists a unique* group homomorphism $\varphi : F(A) \to G$ such that the diagram

$$\begin{tikzcd} F(A) \arrow[r, "\varphi"] & G \\ A \arrow[u, "j"] \arrow[ur, "f"'] & \end{tikzcd}$$

commutes. By general nonsense (Proposition I.5.4), this universal property defines $F(A)$ up to isomorphism, *if this group exists.* But does $F(A)$ exist?

Before giving a 'concrete' construction of $F(A)$, let's check that if $A = \{a\}$ is a singleton, then $F(A) \cong \mathbb{Z}$, as proposed in §5.1. The function $j : A \to \mathbb{Z}$ will send a to $1 \in \mathbb{Z}$. For any group G, giving a set-function $f : A \to G$ amounts to choosing

[21] We could assume that j is *injective*, identifying A with a subset of G; the construction would be completely analogous, and the resulting group would be the same. However, considering arbitrary functions leads to a stronger, more useful, universal property.

one element $g = f(a) \in G$. Now, if $a \in G$, then *there is a unique* homomorphism $\varphi : \mathbb{Z} \to G$ making the diagram

$$\begin{tikzcd}
\mathbb{Z} \arrow[r, "\varphi"] & G \\
\{a\} \arrow[u, "j"] \arrow[ur, "f"'] &
\end{tikzcd}$$

commute: because this forces $\varphi(1) = \varphi \circ j(a) = f(a) = g$, and then the homomorphism condition forces $\varphi(n) = g^n$. That is, φ is necessarily the exponential map ϵ_g considered in §4.1. Therefore, infinite cyclic groups do satisfy the universal property for free groups over a singleton.

5.3. Concrete construction. As we know, terminal objects of a category need not exist. So we have to convince the reader that free groups $F(A)$ exist, for every set A.

Given any set A, we are going to think of A as an 'alphabet' and construct 'words' whose letters are elements of A or 'inverses' of elements of A. To formalize this, consider a set A' isomorphic to A and disjoint from it; call a^{-1} the element in A' corresponding to $a \in A$. A *word* on the set A is an ordered list

$$(a_1, a_2, \cdots, a_n),$$

which we denote by the juxtaposition

$$w = a_1 a_2 \cdots a_n,$$

where each 'letter' a_i is either an element $a \in A$ or an element $a^{-1} \in A'$. We will denote the set of words on A by $W(A)$; the number n of letters is the 'length' of w; we include in $W(A)$ the 'empty word' $w = (\,)$, consisting of *no* letters.

For example, if $A = \{a\}$ is a singleton, then an element of $W(A)$ may look like

$$a^{-1}a^{-1}aaaa^{-1}aa^{-1}.$$

An element of $W(\{x, y\})$ may look like

$$xxx^{-1}yy^{-1}xxy^{-1}x^{-1}yy^{-1}xy^{-1}x.$$

Now the notation we have chosen hints that elements in $W(A)$ may be redundant: for example,

$$xyy^{-1}x \quad \text{and} \quad xx$$

are distinct words, but they ought to end up being the same element of a group having to do with words. Therefore, we want to have a process of 'reduction' which takes a word and cleans it up by performing all cancellations. Note that we have to do this 'by hand', since we have not come close yet to defining an operation or making formal sense of considering a^{-1} to be the 'inverse' of a.

Describing the reduction process is invariably awkward—it is a completely evident procedure, but writing it down precisely and elegantly is a challenge. We will settle for the following.

- Define an 'elementary' reduction $r : W(A) \to W(A)$: given $w \in W(A)$, search for the first occurrence (from left to right) of a pair aa^{-1} or $a^{-1}a$, and let $r(w)$ be the word obtained by removing such a pair. In the two examples given above,

$$r(a^{-1}\underline{a^{-1}a}aa^{-1}aa^{-1}) = a^{-1}aaa^{-1}aa^{-1},$$

$$r(x\underline{xx^{-1}}yy^{-1}xxy^{-1}x^{-1}yy^{-1}xy^{-1}x) = xyy^{-1}xxy^{-1}x^{-1}yy^{-1}xy^{-1}x.$$

- Note that $r(w) = w$ precisely when 'no cancellation is possible'. We say that w is a 'reduced word' in this case.

Lemma 5.1. *If $w \in W(A)$ has length n, then*[22] $r^{\lfloor \frac{n}{2} \rfloor}(w)$ *is a reduced word.*

Proof. Indeed, either $r(w) = w$ or the length of $r(w)$ is less than the length of w; but one cannot decrease the length of w more than $n/2$ times, since each non-identity application of r decreases the length by two. □

- Now define the 'reduction' $R : W(A) \to W(A)$ by setting $R(w) = r^{\lfloor \frac{n}{2} \rfloor}(w)$, where n is the length of w. By the lemma, $R(w)$ is always a reduced word. For example, $R(a^{-1}a^{-1}aaaa^{-1}aa^{-1})$ is the empty word, since

$$r^4(a^{-1}a^{-1}aaaa^{-1}aa^{-1}) = r^3(a^{-1}aaa^{-1}aa^{-1}) = r^2(aa^{-1}aa^{-1}) = r(aa^{-1}) = (\,);$$

  and $R(xxx^{-1}yy^{-1}xxy^{-1}x^{-1}yy^{-1}xy^{-1}x) = xxxy^{-1}y^{-1}x$, as the reader may check.

Let $F(A)$ be the set of reduced words on A, that is, the image of the reduction map R we have just defined.

We are ready to (finally) define free groups 'concretely'. Define a binary operation on $F(A)$ by *juxtaposition & reduction:* for reduced words w, w', define $w \cdot w'$ as the reduction of the juxtaposition of w and w',

$$w \cdot w' := R(ww').$$

It is essentially evident that $F(A)$ is a group under this operation:

- The operation is associative.
- The empty word $e = (\,)$ is the identity in $F(A)$, since $ew = we = w$ (no reduction is necessary).
- If w is a reduced word, the inverse of w is obtained by reversing the order of the letters of w and replacing each $a \in A$ by $a^{-1} \in A'$ and each a^{-1} by a.

The most cumbersome of these statements to prove formally is associativity; it follows easily from (for example) Exercise 5.4.

There is a function $j : A \to F(A)$, defined by sending the element $a \in A$ to the word consisting of the single 'letter' a.

Proposition 5.2. *The pair $(j, F(A))$ satisfies the universal property for free groups on A.*

[22] $\lfloor q \rfloor$ denotes the largest integer $\leq q$.

Proof. This is also essentially evident, once one has absorbed all the notation. Any function $f : A \to G$ to a group extends uniquely to a map $\varphi : F(A) \to G$, determined by the homomorphism condition and by the requirement that the diagram commutes, which fixes its value on one-letter words $a \in A$ (as well as on $a^{-1} \in A'$).

To check more formally that φ exists as a homomorphism, one can proceed as follows. If $f : A \to G$ is any function, we can extend f to a set-function

$$\tilde{\varphi} : W(A) \to G$$

by insisting that on one-letter words a or a^{-1} (for $a \in A$),

$$\tilde{\varphi}(a) = f(a), \quad \tilde{\varphi}(a^{-1}) = f(a)^{-1},$$

and that $\tilde{\varphi}$ is compatible with juxtaposition:

$$\tilde{\varphi}(ww') = \tilde{\varphi}(w)\tilde{\varphi}(w')$$

for any two words w, w'. The key point now is that reduction is invisible for $\tilde{\varphi}$:

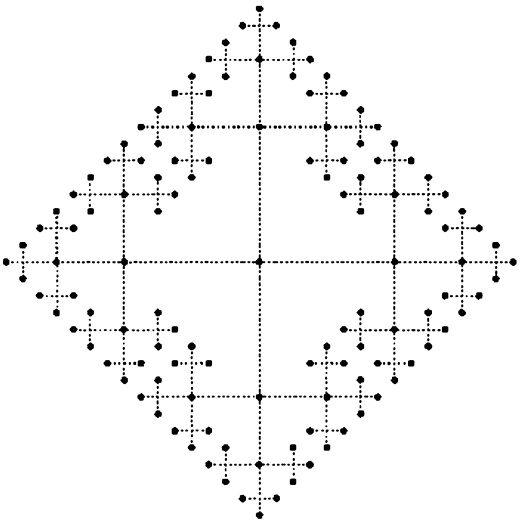
$$\tilde{\varphi}(R(w)) = \tilde{\varphi}(w),$$

since this is clearly the case for *elementary* reductions; therefore, since $\varphi : F(A) \to G$ agrees with $\tilde{\varphi}$ on reduced words, we have for $w, w' \in F(A)$

$$\varphi(w \cdot w') = \tilde{\varphi}(w \cdot w') = \tilde{\varphi}(R(ww')) = \tilde{\varphi}(ww') = \tilde{\varphi}(w)\tilde{\varphi}(w') = \varphi(w)\varphi(w') :$$

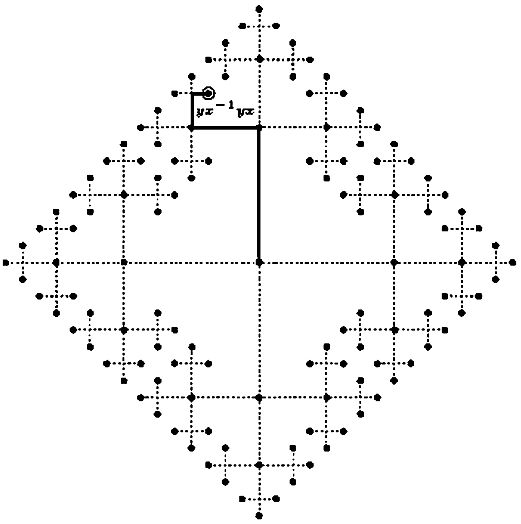
that is, φ is a homomorphism, as needed. □

Example 5.3. It is easy to 'visualize' $F(\{a\}) \cong \mathbb{Z}$; but it is already somewhat challenging for the free group on *two* generators, $F(\{x, y\})$. The best we can do is the following: behold the infinite graph[23]



[23] This is an example of the *Cayley graph* of a group (cf. Exercise 8.6): a graph whose vertices correspond to the elements of the group and whose edges connect vertices according to the action of generators.

obtained by starting at a point (the center of the picture), then branching out in four directions by a length of 1, then branching out similarly by a length of 1/2, then by 1/4, then by 1/8, then... (and we stopped there, to avoid cluttering the picture too much). Then every element of $F(\{x, y\})$ corresponds in a rather natural way to exactly one dot in this diagram. Indeed, we can place the empty word at the center; and we can agree that every x in a word takes us one step to the right, every x^{-1} to the left, every y up, and every y^{-1} down. For example, the word $yx^{-1}yx$ takes us here:



The reader will surely encounter this group elsewhere: it is the *fundamental group* of the 'figure 8'. ⌟

5.4. Free *abelian* groups. We can pose in Ab the same question answered above for Grp: that is, ask for the *abelian* group $F^{ab}(A)$ which most efficiently contains the set A, provided that we do not have any additional information on the elements of A. Of course we *do* know something about the elements of A this time: they will have to commute with each other in $F^{ab}(A)$. This plays no role if $A = \{a\}$ is a singleton, and therefore $F^{ab}(\{a\}) = F(\{a\}) \cong \mathbb{Z}$; but the requirement is different for larger sets, so we should expect a different answer in general.

The formalization of the heuristic requirement is precisely the same universal property that gave us free groups, but (of course) stated in Ab: $F^{ab}(A)$ is a *free abelian group* on the set A if there is a set-function $j : A \to F^{ab}(A)$ such that, for all *abelian* groups G and set-functions $f : A \to G$, *there exists a unique* group homomorphism $\varphi : F^{ab}(A) \to G$ such that the following diagram commutes:

$$\begin{tikzcd}
F^{ab}(A) \arrow[r, "\varphi"] & G \\
A \arrow[u, "j"] \arrow[ur, "f"'] &
\end{tikzcd}$$

Again, Proposition I.5.4 guarantees that $F^{ab}(A)$ is unique up to isomorphism, *if* it exists; but we have to prove it exists! This is in some way simpler than for Grp, in the sense that $F^{ab}(A)$ is easier to understand, at least for finite sets A.

To fix ideas, we will first describe the answer for a finite set, say $A = \{1, \cdots, n\}$. We will denote by $\mathbb{Z}^{\oplus n}$ the direct sum

$$\underbrace{\mathbb{Z} \oplus \cdots \oplus \mathbb{Z}}_{n\text{-times}};$$

recall (§3.5) that this group 'is the same as' the product[24] $\mathbb{Z}^n$ (but we view it as a *co*product). There is a function $j : A \to \mathbb{Z}^{\oplus n}$, defined by

$$j(i) := (0, \cdots, 0, \underset{i\text{-th place}}{1}, 0, \cdots, 0) \in \mathbb{Z}^{\oplus n}.$$

Claim 5.4. *For $A = \{1, \cdots, n\}$, $\mathbb{Z}^{\oplus n}$ is a free abelian group on A.*

Proof. Note that every element of $\mathbb{Z}^{\oplus n}$ can be written uniquely in the form $\sum_{i=1}^n m_i j(i)$: indeed,

$$\begin{aligned}(m_1, \cdots, m_n) &= (m_1, 0, \cdots, 0) + (0, m_2, 0, \cdots, 0) + \cdots + (0, \cdots, 0, m_n)\\ &= m_1(1, 0, \cdots, 0) + m_2(0, 1, 0, \cdots, 0) + \cdots + m_n(0, \cdots, 0, 1)\\ &= m_1 j(1) + \cdots + m_n j(n),\end{aligned}$$

and $(m_1, \cdots, m_n) = (0, \cdots, 0)$ if and only if all m_i are 0.

Now let $f : A \to G$ be any function from $A = \{1, \cdots, n\}$ to an abelian group G. We define $\varphi : \mathbb{Z}^{\oplus n} \to G$ by

$$\varphi\left(\sum_{i=1}^n m_i j(i)\right) := \sum_{i=1}^n m_i f(i) :$$

indeed, we have no choice—this definition is forced by the needed commutativity of the diagram

$$\begin{tikzcd}
\mathbb{Z}^{\oplus n} \arrow[r, "\varphi"] & G \\
A \arrow[u, "j"] \arrow[ru, "f"'] &
\end{tikzcd}$$

and by the homomorphism condition. Thus φ is certainly uniquely determined, and we just have to check that it is a homomorphism. This is where the commutativity of G enters:

$$\varphi\left(\sum_{i=1}^n m_i' j(i)\right) + \varphi\left(\sum_{i=1}^n m_i'' j(i)\right) = \sum_{i=1}^n m_i' f(i) + \sum_{i=1}^n m_i'' f(i) \overset{!}{=} \sum_{i=1}^n (m_i' + m_i'') f(i)$$

because G is commutative,

$$= \varphi\left(\sum_{i=1}^n (m_i' + m_i'')\, j(i)\right) = \varphi\left(\sum_{i=1}^n m_i' j(i) + \sum_{i=1}^n m_i'' j(i)\right)$$

as needed. □

[24] Indeed, it is common to denote this group by $\mathbb{Z}^n$, omitting the $\oplus$. No confusion is likely, but we will try to distinguish the two to emphasize that they play different categorical roles.

Remark 5.5. A less hands-on, more high-brow argument can be given by contemplating the universal property defining free abelian groups vis-à-vis the universal property for coproducts; cf. Exercise 5.7. ⌟

Now for the general case: let A be any set. As we have seen, $H^A = \mathrm{Hom}_{\mathsf{Set}}(A, H)$ has a natural abelian group structure if H is an abelian group (§4.4); elements of H^A are arbitrary set-functions $\alpha : A \to H$. We can define a subset $H^{\oplus A}$ of H^A as follows:

$$H^{\oplus A} := \{\alpha : A \to H \mid \alpha(a) \neq e_H \text{ for only finitely many elements } a \in A\}.$$

The operation in H^A induces an operation in $H^{\oplus A}$, which makes $H^{\oplus A}$ into a group[25].

The reader should note that $H^{\oplus A}$ is the whole of H^A if A is a finite set; and that $\mathbb{Z}^{\oplus A} \cong \mathbb{Z}^{\oplus n}$ if $A = \{1, \cdots, n\}$: indeed, $(m_1, \cdots, m_n) \in \mathbb{Z}^{\oplus n}$ may be identified with the function $\{1, \cdots, n\} \to \mathbb{Z}$ sending i to m_i.

For $H = \mathbb{Z}$ there is a natural function $j : A \to \mathbb{Z}^{\oplus A}$, obtained by sending $a \in A$ to the function $j_a : A \to \mathbb{Z}$ defined by

$$(\forall x \in A) : \quad j_a(x) := \begin{cases} 1 & \text{if } x = a, \\ 0 & \text{if } x \neq a. \end{cases}$$

Note that for $A = \{1, \cdots, n\}$ and identifying $\mathbb{Z}^{\oplus A} \cong \mathbb{Z}^{\oplus n}$, this function j is *the same function* denoted j earlier.

Proposition 5.6. *For every set A, $F^{ab}(A) \cong \mathbb{Z}^{\oplus A}$.*

Proof. The key point is again that every element of $\mathbb{Z}^{\oplus A}$ may be written uniquely as a *finite* sum

$$\sum_{a \in A} m_a\, j(a), \qquad m_a \neq 0 \text{ for only finitely many } a;$$

once this is understood, the argument is precisely the same as for Claim 5.4. □

[25] Thus $H^{\oplus A}$ is a *subgroup* of H^A; cf. §6.

Exercises

5.1. Does the category $\mathscr{F}^A$ defined in §5.2 have final objects? If so, what are they?

5.2. Since trivial groups T are initial in Grp, one may be led to think that (e, T) should be initial in $\mathscr{F}^A$, for every A: e would be defined by sending every element of A to the (only) element in T; and for any other group G, *there is a unique* homomorphism $T \to G$. Explain why (e, T) is *not* initial in $\mathscr{F}^A$ (unless $A = \emptyset$).

5.3. ▷ Use the universal property of free groups to prove that the map $j : A \to F(A)$ is injective, for all sets A. (Hint: It suffices to show that for every two elements a, b of A there is a group G and a set-function $f : A \to G$ such that $f(a) \neq f(b)$. Why? How do you construct f and G?) [§III.6.3]

5.4. ▷ In the 'concrete' construction of free groups, one can try to reduce words by performing cancellations in any order; the process of 'elementary reductions' used in the text (that is, from left to right) is only one possibility. Prove that the result of iterating cancellations on a word is independent of the order in which the cancellations are performed. Deduce the associativity of the product in $F(A)$ from this. [§5.3]

5.5. Verify explicitly that $H^{\oplus A}$ is a group.

5.6. ▷ Prove that the group $F(\{x, y\})$ (visualized in Example 5.3) is a coproduct $\mathbb{Z} * \mathbb{Z}$ of $\mathbb{Z}$ by itself in the category Grp. (Hint: With due care, the universal property for one turns into the universal property for the other.) [§3.4, 3.7, 5.7]

5.7. ▷ Extend the result of Exercise 5.6 to free groups $F(\{x_1, \dots, x_n\})$ and to free *abelian* groups $F^{ab}(\{x_1, \dots, x_n\})$. [§3.4, §5.4]

5.8. Still more generally, prove that $F(A \amalg B) = F(A) * F(B)$ and that $F^{ab}(A \amalg B) = F^{ab}(A) \oplus F^{ab}(B)$ for all sets A, B. (That is, the constructions F, F^{ab} 'preserve coproducts'.)

5.9. Let $G = \mathbb{Z}^{\oplus \mathbb{N}}$. Prove that $G \times G \cong G$.

5.10. ¬ Let $F = F^{ab}(A)$.

- Define an equivalence relation $\sim$ on F by setting $f' \sim f$ if and only if $f - f' = 2g$ for some $g \in F$. Prove that $F/\sim$ is a finite set if and only if A is finite, and in that case $|F/\sim| = 2^{|A|}$.
- Assume $F^{ab}(B) \cong F^{ab}(A)$. If A is finite, prove that B is also, and that $A \cong B$ as sets. (This result holds for free groups as well, and without any finiteness hypothesis. See Exercises 7.13 and VI.1.20.)

[7.4, 7.13]