

**Section 1.4.** This section introduces  $A(S)$ , which is defined to be the set of all **one-to-one** mappings from  $A$  **onto** itself. As soon as this set is introduced, you are given several of its aliases. The elements of  $A(S)$  are called **permutations** of  $S$ . If  $m(S) = n$ , then  $A(S)$ , *with the operation of composition of mappings*, will be denoted  $S_n$ . Warning: the  $S$  in  $S_n$  has nothing to do with the set  $S$ ; that enters only through  $n$ , which is  $m(S)$ . For this to make sense, it will be necessary to show that the names of the elements of  $S$  are irrelevant to the properties of  $A(S)$  that we will be studying. Maybe we should back off before we get too far ahead of what can be done carefully.

The key properties of the composition of elements of  $A(S)$  are collected as **Lemma 1.4.1**.

---

$A(S)$  satisfies the following:

**(a)** For all  $f$  and  $g$  in  $A(S)$ ,  $f \circ g$  is defined and  $f \circ g \in A(S)$ .

**(b)**  $(f \circ g) \circ h = f \circ (g \circ h)$ .

**(c)** There is an **identity**  $i \in A(S)$ . This element satisfies  $f \circ i = f$  and  $i \circ f = f$  for all  $f \in A(S)$ .

**(d)** Given  $f \in A(S)$ , there is  $g \in A(S)$  such that  $f \circ g = i$  and  $g \circ f = i$ . Such a  $g$  is called the inverse of  $f$  and denoted  $f^{-1}$ .

---

The “proof” of this is a claim that you can find it in Section 3. The closest I can find to a proof of (a) is a remark following the definition of composition on page 11. Part (b) is the special case of  $S = T = U = V$  of Lemma 1.3.1 (with all of the sets called  $S$ ). Part (c) is example 10 on page 9 (the *existence* of such an example is part of the properties of sets that are never quite spelled out). Part (d) is part of Lemma 1.3.4. In the proof of that result, a more general object called  $f^{-1}$  is shown to be a mapping if  $f$  is one-to-one and onto.

A familiar counting argument is then given to show that  $S_n$  has  $n!$  elements. In proving this, the elements of a set  $S$  with  $n$  elements are called  $x_1, \dots, x_n$  and every element  $f \in A(S)$  is identified with the set of pairs  $(i, j)$  such that  $f(x_i) = x_j$ .

Finally, on page 18, the author declares that  $f \circ g$  is getting tiresome and will henceforth be denoted  $fg$ . As much as possible the properties of  $A(S)$  will be ex-

pressed in terms of this composition, so the elements of  $S$  will be forced into the background. When they appear, they will continue to be surrounded by parentheses, although I prefer to write the action of  $A(S)$  on  $S$  without parentheses.

As an example, let  $S = \{\alpha, \beta, \gamma\}$ . (This will be the same as the example on page 17, except that different names will be used for the elements of  $S$ .) Since  $S$  has 3 elements,  $A(S)$  will have 6. We know that we have an identity  $i$  defined by

$$i\alpha = \alpha \quad i\beta = \beta \quad i\gamma = \gamma.$$

Then we (not quite arbitrarily) select two other elements  $f$  and  $g$  of  $A(S)$  defined by

$$\begin{array}{lll} f\alpha = \beta & f\beta = \gamma & f\gamma = \alpha \\ g\alpha = \beta & g\beta = \alpha & g\gamma = \gamma \end{array}$$

We can then compose these in all possible ways. Since we will then have seven possible names for some of the six elements of  $A(S)$ , these cannot all be distinct.

Here is the result:

$$\begin{array}{lll} ff\alpha = \gamma & ff\beta = \alpha & ff\gamma = \beta \\ gf\alpha = \alpha & gf\beta = \gamma & gf\gamma = \beta \\ fg\alpha = \gamma & fg\beta = \beta & fg\gamma = \alpha \\ gg\alpha = \alpha & gg\beta = \beta & gg\gamma = \gamma \end{array}$$

Examining the results shows that  $gg = i$  and the remaining expressions are distinct. This gives a name for each element of  $A(S)$ . Before going any further, note that  $fg \neq gf$ . Since commutativity plays an important role in elementary algebra, the lack of such a role here means that we need to base our proofs only on what has been established here, since your intuition may be influenced by properties that hold only on commutative systems. However, the associative law, all by itself, assures us that the repeated products of equal elements commute with one another, so they can be called **powers** of an element and denoted  $a^k$  in the usual way. Note that this tells us that  $A(S)$  must contain an element that is not a power of  $f$ , in fact  $g$  cannot be a power of  $f$ ; because any  $f^k$  must commute with  $f$ , while  $g$  does not commute with  $f$ .

We are thus prepared for accepting the calculation that tells us that  $f^3 = i$ . The other products of three terms (except for those containing  $gg$  which simplify using  $g^2 = i$ ), are  $fgf = g$ ,  $f^2g = gf$ ,  $gf^2 = fg$ , and  $gfg = f^2$ . These rules allow us to shorten any product of three or more terms, so any expression built from  $f$  and  $g$  by repeated operations of composition or taking inverses can be reduced to one of the six product of at most two terms.

Problems for discussion: 1 through 4, 14, 22

The little bit of Number Theory included in the next section is too skimpy to be useful. There is another course devoted to that subject. Mathematical Induction is a standard tool for proving properties of the positive integers. It takes a little practice to see that correct use of induction will not prove false results, but you should have seen this in Math 300 or its equivalent. It would be a mistake to spend too much more time in chapter 1.