

How do we work with mappings? The homework reveals many questions that were not asked in lecture. Several exercises are expressed in terms of mappings, and the statements seem clear enough until one starts to construct a proof. The numerical functions met in other courses were usually given by formulas, but mappings between finite sets may need to be described by giving a complete list of values. Mappings that take the same value at each point are considered equal, so the list of values tells us *everything* about the mapping.

It also shows that the number of mappings from A to B is b^a where b is the number of elements in B and a is the number of elements in A . For each element x of A , there are b possible values of $f(x)$, and the value at one point has no effect on the values at other points, so the number of different mappings is a product of a factors of b .

The case $b = 2$ looks like another formula we have seen: the number of subsets of A . This is not an accident: a function f from A to $\{0, 1\}$ determines the subset

$$X_f = \{x \in A : f(x) = 1\}$$

and a subset $X \subseteq A$ determines the function f_X with

$$f_X(x) = \begin{cases} 1 & \text{if } x \in X \\ 0 & \text{otherwise} \end{cases}.$$

These constructions are seen to be inverses of one another.

Note that the definition of f_X used an extra variable $x \in A$ in order to allow the individual values of the mapping to be described. This answers the question introducing this section: to use a mapping f in a proof, introduce (at least) a variable x representing an element of the domain of f , and express the property of f being studied as a property of the individual $f(x)$.

To say that $f: A \rightarrow B$ is onto, use the formal statement

$$(\forall y \in B)(\exists x \in A) f(x) = y.$$

To say that f is one-to-one, say

$$(\forall x_0 \in A)(\forall x_1 \in A)[f(x_0) = f(x_1) \implies x_0 = x_1].$$

See the “essay” on workshop 1 available on the web page for a discussion of the use of this to solve workshop problem 2.

In addition to these expressions of quantifiers, the individual variables are also used to select elements of a set.

Exercise 1.3#21. A discussion of this was begun in a previous lecture, but not finished. There was also an error written on the blackboard that has made its way into notes taken at the time, and from there to the submitted solution of this exercise. A correction is required.

In this exercise, S denotes the set of rational numbers, and for $a, b \in S$ with $a \neq 0$ we construct $f_{a,b} \in A(S)$ using the formula

$$f_{a,b}s = as + b.$$

Discussion in the text, when expressed using terms introduced in chapter 2, shows that the set of all such $f_{a,b}$ is a subgroup of $A(S)$. Let's call this subgroup G for the rest of the discussion. If $f_{a,b} = f_{a',b'}$, then $f_{a,b}0 = f_{a',b'}0$ and $f_{a,b}1 = f_{a',b'}1$, from which we can conclude that $a = a'$ and $b = b'$. Thus different names $f_{a,b}$ describe different elements of G . A little

algebra shows what the operation in G is:

$$\begin{aligned} f_{a,b}f_{c,d}s &= f_{a,b}(cs + d) = a(cs + d) + b \\ &= (ac)s + (ad + b) = f_{ac,ad+b}s, \end{aligned}$$

so $f_{a,b}f_{c,d} = f_{ac,ad+b}$ and (doing the correct substitution this time) $f_{c,d}f_{a,b} = f_{ca,cb+d}$. (Instead of deriving these formulas for the operation in G , one could work with the formulas for the values at s that were used to derive the formulas, but the exercise introduces quantifiers on a, b, c , and d , so it seems useful to use a statement in which s no longer appears.) Since $A(S)$ is infinite, we also need to identify the identity and inverses of all elements of G before we can claim to have found a subgroup. Since the identity i satisfies $i(s) = s$, we recognize that $f_{1,0} = i$. We can then use our formula for composition to determine the inverse of each element of G . We were asked to give an enumerative or other *simple* description of the set

$$\{ f_{c,d} \in G : (\forall f_{a,b} \in G) f_{a,b}f_{c,d} = f_{c,d}f_{a,b} \}.$$

Using the language introduced in example 11 of Section 2.3, we seek the **center** $Z(G)$ of the group G . It

is claimed that this is a general example of a subgroup of G . In particular, the identity will lie in this set.

Quantifying over G is an abbreviation for quantifying over the rational numbers (with a side condition saying that certain variables must be nonzero). Our formula for composition leads to the equations $ac = ca$ and $ad + b = cb + d$. Note that $c = 1$ and $d = 0$, which corresponds to the identity of G causes these equations to assert only $a = a$ and $b = b$, so the identity is in the set. Conversely, substituting various values for a and b (which is justified because the equations are required to hold for *all* a and b with $a \neq 0$) will give enough equations to force a unique solution for c and d . For example, $a = b = 1$ gives $c = 1$. Then, any other value of a (except the forbidden value of 0) leads to $d = 0$.

Exercise 1.4#12. I won't say anything more about how to prove that each $f \in S_n$ has some power f^k that is the identity, but I will give an example to show that this is false for S^S in spite of the superficial similarity with $A(S)$. Thus, any proof must use the existence of an inverse of f .

The example has $n = 2$, and we can take $S = \{0, 1\}$. The function f has $f0 = f1 = 0$. Then, for all $k > 0$, $f^k = f$.

Exercise 1.4#21. In this exercise, we are given a subset T of S which is used to define a subset of $A(S)$

$$U(T) = \{ f \in A(S) : (\forall t \in T) ft \in T \}.$$

We are asked to show that this is a two properties used in testing it for being a subgroup. The membership test can also be stated: if $t \in T$, then $ft \in T$. First, we show that the identity i of $A(S)$ belongs to $U(T)$. All that is needed is to note that, given $t \in T$, since $T \subseteq S$, $it = t$, and then $it = t \in T$. Then, we show that $U(T)$ is closed under composition. This follows from the transitivity of implication, and will be shown at the blackboard. No proof that $U(T)$ is closed under inverses is requested; indeed, this is a good thing since that is not true if T and $U - T$ are both infinite.

The process of understanding what needs to be proved is often helped by constructing examples. The case

of $S = \{a, b\}$ and $T = \{a\}$ will be shown at the blackboard. Examples are important, even if they stay in your personal notes and appear to contribute nothing to your proofs. Indeed, if you don't plan to show the example to anyone, you can explore it in minute detail, even if these details would be found dull.

Mathematical induction. The principle of mathematical induction is a recipe for writing a finite proof that can be interpreted as a description of a proof that establishes the statements $P(0), P(1), \dots$ one after another. You start the induction proof the same way that the infinite proof it describes starts — by proving an initial case. If you have a uniform way to prove each remaining case from its immediate predecessor, all cases can be obtained by repeating this argument with successive values of the parameter n , so a proof in which n is a free variable is all that is needed to complete the description of the proof.

Factor groups. We have seen that the kernel of a homomorphism $\phi: G \rightarrow G'$ is a normal subgroup of G . The construction of the **factor group** G/N shows

that we don't need to know anything more about N than $N \triangleleft G$ to find a homomorphism whose kernel is exactly N .

We have already noted Theorem 2.5.6 that normal subgroups are characterized by the property that, for all $g \in G$, $gN = Ng$.

If ϕ is a homomorphism with kernel N , then $\phi(gn) = \phi(g)$ for all $n \in N$, so that ϕ is constant on cosets. Moreover, no other element $g' \in G$ can have $\phi(g') = \phi(g)$, since that would give a *new* element $g^{-1}g'$ in the kernel.

We should try to make the set of cosets of N in G into a group, so we need to define a composition. There isn't much choice! If we are to have a homomorphism ϕ with $\phi(g) = gN$, then the requirement that $\phi(g_0g_1) = \phi(g_0)\phi(g_1)$ says that each product $(g_0n_0)(g_1n_1)$ needs to lie in $(g_0g_1)N$. The equation

$$(g_0n_0)(g_1n_1) = (g_0g_1)(g_1^{-1}n_0g_1)n_1$$

shows that the coset of the product depends only on the cosets of the factors, and this gives the operation on cosets.

We now have the operation of G/N , but we do not yet know that this operation defines a group. The details will be supplied at the blackboard, but the verification of each axiom depends mainly on the corresponding statement in G .