

Section 2.3. Consider the group S_4 , of all mappings from $S = \{0, 1, 2, 3\}$ into itself. If we use the elements of S to label the vertices of a square, then the rigid motions taking the square into itself determine elements of S_4 just by seeing how they act on the vertices. The first such rigid motion that you think of is the rotation f defined by

$$f0 = 1 \quad f1 = 2 \quad f2 = 3 \quad f3 = 0,$$

but if you don't live in *Flatland*, you soon realize that you can also turn the square over (in many ways). For example, you can rotate the square about the diagonal joining the vertices 0 and 2 giving the mapping h that satisfies

$$h0 = 0 \quad h1 = 3 \quad h2 = 2 \quad h3 = 1,$$

Look closely, this is different from the mapping g that appeared in Problem 4 of Workshop 1. We have already seen (in that workshop problem) that $f^4 = i$, and the different powers f^k ($k = 0, 1, 2, 3$, i.e., $k \in S$) can be distinguished by $f^k 0 = k$. We also notice

that there are four different flips that leave the vertices of the square in the positions originally occupied by vertices. If you choose where vertex 0 will wind up, then you must rotate about the perpendicular bisector of the line joining 0 to that vertex if the vertex is different from 0, or about the line joining the center of the square to 0 if you want 0 to be fixed (h is the flip that fixes 0). We thus have 8 of the 24 elements of S_4 that describe all rigid motions of the square. There is a similar construction for all n of the $2n$ rigid motions of n sided polygon. This *dihedral group* of order $2n$ was described using motions of rotations and reflections in the plane in Section 2.1. By a quirk of fate, certain elements were designated f and h in that example, but they were opposite to the use here which was chosen to agree with Workshop 1.

Not only can the motions of the square be identified with elements of S_4 , but the rule for composing these functions is the same whether they are thought of as operating on the whole square or just on the vertices. The dihedral group is then viewed as a subset of S_4 that is closed under the multiplication in S_4 .

For any subset S of a group G that is closed under the group operation, one can ask if the subset with this operation forms a group. That is, we should see if it satisfies the other three axioms of a group.

Since a group needs an element to act as identity, the empty set cannot be a group, so we shall restrict to the case in which S is nonempty.

The associative law is no trouble. Given three elements x , y , and z of S , the products $x(yz)$ and $(xy)z$, thought of as elements in S are computed by the same rule that holds for all of G . Since they designate the same element of G , which happens to lie in S , they must designate the same element of S .

We have seen the the identity i of a group is characterized as the only solution of $ax = a$ for any a . If the group operation restricted to S has an identity, it must be the identity of G . In general, if one wants S to be a group, one must require that it contain the identity of G . The positive integers as a subset of the additive group of all integers provides an example of a set that is closed under addition, but does not contain 0.

We have also seen that a^{-1} is characterized as the only solution of $ax = i$ in a group. Since the operation is the same, the only possible inverse of a in S is its inverse in G . Again, there is an example with G being the additive group of integers in which S contains the identity 0, which is its own inverse, but no other inverse of an element of S . This example takes S to be the nonnegative integers.

If G is finite, Lemma 2.3.2 asserts that a subset S closed under the operation of G is automatically a subgroup. To prove this, take $a \in S$ and look at $a^0 = i, a^1 = a, a^2, a^3, \dots$. These all lie in S since S is closed under the operation of G . Since G is finite, this infinite list of names cannot refer to distinct elements of G . Let a^n be the first element that is equal to an earlier element in the list. Then $n > 0$ since there are no elements before a^0 in the list; hence a^{n-1} is in the list. If $a^n = a^j$ with $j > 0$, then multiplication by a^{-1} in G gives $a^{n-1} = a^{j-1}$, contradicting the choice of n . Hence $j = 0$, i.e., $a^n = i$. We also see that $a^{n-1} = a^{-1}$, so we can find the required elements i and a^{-1} among the positive powers of a , all of which

are in S .

Note that this list of powers of a is itself a subgroup of G . In general, if G is allowed to be infinite, all the a^n with $n \geq 0$ may be distinct. If this happens, then a subgroup S containing a must also contain the a^n with $n < 0$, and the collection of *all* a^n is again a subgroup.

Lagrange's Theorem. If H is a subgroup of G , and $a \in G$ consider the set

$$aH = \{ ah : h \in H \}.$$

which is called a **left coset** of H in G . (The text prefers to introduce the analogous *right* coset first, but my preference for left cosets should become clear when we reach theorem 2.5.1.)

Multiplication on the left by a^{-1} shows that $ah_0 = ah_1$ implies that $h_0 = h_1$, so each set aH contains the same number of elements as H .

If $a' \in aH$, so that there is $h_0 \in H$ with $a' = ah_0$, then $a'H$ is the set of things of the form $(ah_0)h = a(h_0h)$. That is, $a'H \subseteq aH$.

We also have $a = a'h_0^{-1}$, so $a \in a'H$, and the above argument shows that $aH \subseteq a'H$. Thus $a'H = aH$.

Now, if $aH \cup cH \neq \emptyset$, we have $b \in aH \cup cH$. Then $aH = bH$ and $bH = cH$, so $aH = cH$. In words, two cosets are either disjoint or identical.

From all of this, one gets that the number of elements in G (called the **order** of G) is the product of the number of elements in H and the number of cosets.

In particular, the order of a subgroup of G divides the order of G .

Since the powers of each element form a subgroup, a corollary of Lagrange's theorem is that the order of every element of a group G divides the order of G . In particular, if the order of a group is a prime number p , an element a has order 1, which means that $a = i$, or order p , which means that a^0, a^1, \dots, a^{p-1} are all distinct, exhausting all elements of G .

We now know exactly what a group looks like if it has order 2, 3 or 5. Properties of subgroups can be used to identify the structure of of a group starting from

a prime factorization of its order, but there are few general theorems when the factorization gets complicated. You might see if you can find two *essentially different* groups of order four and two *essentially different* groups of order six. (The meaning of the italicized phrase will be clarified with the definition of **isomorphism** in Section 2.5. Then we will be able to show that these examples describe all groups of orders 4 or 6.)