

**Apology.** These notes will get a little sketchy towards the end. Details will be filled in somehow.

**Section 2.5.** Homomorphisms and normal subgroups. In general, the word **homomorphism** means structure-preserving mapping. If  $G$  and  $G'$  are groups, a mapping  $\phi$  from  $G$  to  $G'$  is called a homomorphism if

$$\phi(ab) = (\phi(a))(\phi(b)) \quad (h)$$

for all  $a \in G$  and  $b \in G$ . Since  $\phi(a)$  and  $\phi(b)$  belong to  $G'$ , the multiplication on the right side of (h) is done in  $G'$ .

The definition of a group also mentions an identity and inverses with respect to that identity. They are not mentioned here because one can *prove* that a mapping between groups that preserves multiplication also preserves the identity and inverses. This is Lemma 2.5.2 of the text. To prove this, first substitute  $a = e$  and  $b = e$ , where  $e$  is the identity element of  $G$  in (h). This gives  $e^*e^* = e^*$  in  $G'$ , where  $e^* = \phi(e)$ . However, we have already noted that the *only* element of  $G'$  with this property is the identity element  $e'$ . Now take  $a^{-1}$  to be a two-sided inverse of  $a$  in  $G$ . Then

(h) gives that  $\phi(a^{-1})$  is a two-sided inverse of  $\phi(a)$  in  $G'$ .

It is the current fashion to see mappings everywhere. Things that were previously done by special arguments, usually falling back on our understanding of sets, are now considered as special cases of mappings. In particular, subsets are thought of as being defined by an *inclusion mapping* rather than as being the victim of some selection process. In particular this allows us to use a different description of the elements of a subset without jeopardizing its relation to the containing set. From this point of view, a subgroup is characterized by the inclusion mapping being an isomorphism — that is, the multiplication of elements in the subgroup is required to agree with the product in the containing group.

**Groups acting on a set.** A homomorphism  $\phi$  of a group  $G$  into  $A(X)$  for some set  $X$  is treated to an *abuse of notation* in which  $(\phi(g))x$  is abbreviated  $gx$ , which is how the operation would be denoted if  $g$  were actually in  $A(X)$ . As long as there is no other interpretation of  $gx$  lurking around, this is reasonable, and

we can prove the expected rule  $(g_0g_1)x = g_0(g_1x)$ . If  $G$  is any group, and  $X$  is any set for which an operation is defined from  $G \times X$  to  $X$  satisfying this rule, we call it an action of  $G$  on  $X$ . This is really the same as a homomorphism of  $G$  into  $A(X)$ . Among all examples of groups acting on  $X$ ,  $A(X)$  is special because its elements are characterized by their effect on the elements of  $x$ , and any function that can appear in an action is represented in  $A(X)$ .

If  $H$  is a subgroup of  $G$ , we can form the set whose elements are the left cosets  $gH$ . The associative law in  $G$  lead to a statement that can be written

$$g_0(g_1H) = (g_0g_1)H$$

which looks like it is statement about  $G$  acting on the set of left cosets of  $H$  in  $G$ . It is! Details will be given in lecture, though not reproduced here.

**The extreme cases.** There are two constructions that always lead to subgroups: (1)  $G$  is a subgroup of itself; (2) the set  $E = \{e\}$  is a subgroup. In case (1), there is only one coset, and the action of any  $g \in G$

is to take this one coset to itself. In case (2), every coset consists of a single element, so the group action on these cosets looks just like the multiplication in  $G$  (provided one identifies the one-element set that is a coset with its unique element. This is a common *abuse of notation* that should be noticed in case it is not safe to make that identification in a particular case.

**The image of a homomorphism.** Such a set, i.e.,

$$\{ g' \in G' : \exists g \in G, g' = \phi(g) \},$$

is always a subgroup of  $G'$ . The verification will be given orally, but not repeated here. (This result is Lemma 2.5.3, but that won't help you find a proof.) This shows that the general group homomorphism can be written as a homomorphism onto its image, followed by the inclusion of the image into the given codomain.

**The kernel of a homomorphism.** Inclusion mappings are fairly well understood, so a general understanding of group homomorphisms seems to require only an understanding of those that are onto. If such

a mapping were also one-to-one, it would have an inverse and would only serve to use the elements of  $G$  to name those of  $G'$ , so we concentrate on the extent to which the mapping can fail to be one-to-one. That is, we study the equation

$$\phi(g_0) = \phi(g_1). \quad (\Phi)$$

Since  $\phi$  is a homomorphism, and  $G$  is a group, this can be expressed as  $\phi(g_1g_0^{-1}) = e' = \phi(g_0^{-1}g_1)$ , shifting attention to finding

$$K = \{ g \in G : \phi(g) = e' \}.$$

It is easy to see that  $K$ , called the **kernel** of  $\phi$  is a subgroup of  $G$ , but more is true. If  $g \in G$  and  $k \in K$ , then  $\phi(gkg^{-1}) = e'$ , so  $gkg^{-1} \in K$ . Not every subgroup has this property. For a simple example, take your favorite subgroup of order 2 in  $S_3$ . Subgroups with this additional property are called **normal subgroups**.

Returning to our interpretation of  $(\Phi)$ , we see that  $g_1$  must lie in both the left coset  $g_0K$  and the right

coset  $Kg_0$ . Theorem 2.5.6 says that these sets are the same if and only if  $K$  is a normal subgroup. In other words, once you know that  $K$  is a normal subgroup of  $G$ , denote  $K \triangleleft G$ , you know that  $g_1 \in Kg_0$  gives the same information as  $g_1 \in g_0K$ . The mapping  $\phi$  establishes a one-to-one correspondence between the image of  $\phi$  in  $G'$  and the cosets of  $K$  in  $G$ .

**Factor groups.** To complete the picture, we need to show that that the cosets of  $G$  with respect to a normal subgroup  $N$  can be made into a group such that the mapping that sends each element  $g$  of  $G$  into the coset  $gN$  is a homomorphism.

We first note that there is at most one way to define an operation on cosets to have this property. Then, we show that this operation does make the set of cosets into a group.