

Lecture 21. Groups

Reading: Chapter 10.1, Groups.

Kinds of algebras. As noted in Lecture 20, there are different kinds of algebras; each kind is characterized by a certain set of axioms. Some kinds may be closely related to one another, when they vary by just a small change in one axiom. Similarly, some kinds may be subkinds of others, if they vary just by the addition or subtraction of one axiom.

Today we will look at **groups**. Next time we'll look at **semigroups** and **monoids**, which are defined by leaving out certain of the group axioms. In homework 20, you'll get some practice figuring out whether certain things are groups or not, checking whether they do or do not constitute models of the group axioms. In homework 21, you'll get practice applying the notions of isomorphism, homomorphism, and automorphism to groups.

Then on Friday we'll look at a very different kind of algebra, **Boolean algebras**, and we'll see how Boolean algebra captures what logic and set theory have in common – how 'and' and 'or' are structurally parallel to intersection and union, for instance.

Those are the only kinds of algebras we will talk about explicitly, but you will find in the reading that the same axioms we'll use in defining these algebras are also involved in two other interesting kinds of algebras, **integral domains** (related to groups and semigroups) and **lattices** (related to Boolean algebras: Boolean algebras are made up of lattices with some additional structure.) These other kinds of algebras are also described in the textbook.

Groups.

A *group* G is an algebra consisting of a set G and a single binary operation (which we will usually write \bullet , but any other symbol is possible – the textbook uses a small open circle, and mentions that $+$ and \times are also commonly used), which satisfies the following four axioms (called the *group axioms*).

- G1: G is an algebra (i.e. \bullet is completely defined and G is closed under \bullet .)
- G2: The single binary operation \bullet is associative.
- G3: G contains an identity element.
- G4: Each element in G has an inverse element. (two-sided inverse)

The group operation \bullet does not have to be commutative. If it *is* commutative, then the group is called a *commutative group* or an *Abelian group*. (That means that the set of axioms defining commutative (Abelian) groups consists of the group axiom plus a fifth axiom that says that \bullet is commutative.)

Some models of groups.

- a. The positive rational numbers with multiplication forms a group.

To show that that's true, we have to go through the 4 group axioms. Furthermore, it's an Abelian group, because multiplication is commutative.

- b. The set of integers $\{0,1,2,3\}$ with the operation of **addition modulo 4**.

The definition of "modulo arithmetic" is given in Chapter 0, "Preliminaries" of my 1979 math book, which we xeroxed for you at the beginning of the semester. We'll review it now. Here is the "addition table", which constitutes the group operation table, for addition modulo 4.

Convention for operation tables: The result for $a \bullet b$ is shown in the a^{th} row and the b^{th} column. It doesn't matter for commutative operations, but it will for non-commutative ones.

$+$:

	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

Let's verify that this is a group. (We'll do it together in class; we'll see that the most non-obvious property to verify is associativity.)

For contrast: the same set, with the operation of *multiplication modulo 4*, is NOT a group. Here is its table: can you see which axioms are not satisfied? (Note: the operation IS associative, so that's not the problem.)

\times

	0	1	2	3
0	0	0	0	0
1	0	1	2	3
2	0	2	0	2
3	0	3	2	1

- c. The set of *all even integers* with addition forms a group. (Verify)

The set of *all odd integers* with addition does NOT form a group. Why?

- d. The group of "symmetries of the square" is an example of quite a different sort. It's described carefully in the book. We'll study it in class using paper squares. (Keep your square once you've made it; it will be useful for doing the homework, especially the Monday night homework.)

If there is time, we'll look at some theorems that can be proved about groups (see pp. 259-60.)
But this is optional.

Theorem 10.1. In any group, the equation $x \bullet a = b$ has the unique solution $x = b \bullet a^{-1}$, and the equation $a \bullet y = b$ has the unique solution $y = a^{-1} \bullet b$.

(proof p. 259)

Corollary 10.1: A group has only one identity element.

[Digression: what's the difference between a "theorem" and a "corollary"? No formal difference. A corollary is something like an 'add-on' to a theorem: once you have proved the theorem, the corollary follows with very little additional work. So what's called a theorem and what's called a corollary really just depends on the historical order in which things got proved and the methods used to prove them – it could have been different.]

Proof: By the group axioms, there is at least one solution to the equation $e \bullet x = e$, namely $x = e$. By theorem 10.1, this is the only solution.

Corollary 10.2. A group has only one inverse a^{-1} for each element a .

Theorem 10.2. A group with four or fewer elements must be commutative.

(Proof by cases, p.260.)

Note: it's also true for 5-element groups, but it takes quite a lot of tedious work to prove. The smallest non-commutative groups have 6 elements.

General notes related to the homework: It's common in the case of a finite group to specify the operation by drawing a group table, sometimes called a multiplication table. (And we often refer to the operation as "multiplying" even when it has no resemblance to multiplication in arithmetic.) A word of caution when you are checking whether something is a group or not if you have a finite multiplication table for it: it's easy to check for closure, for the existence of an identity element, and (once you know what the identity element is) for inverses. You can also see from the table whether the operation is commutative or not.

But you also have to check for associativity, and that is not something you can simply see by inspection – so be careful to check all the cases, or enough of them to be really sure you haven't missed any possible instance of non-associativity.