

Lecture 2

This week we concentrate on examples of groups and on lattice diagrams of subgroups. Since the book assumes you've seen group theory before, I want to clear up something left tacit that will be made specific in chapter 2.

Definition: A subgroup H of a group $(G, *)$ is a non-empty subset of G that is a group under $*$ as well. In particular, $e \in H$. If $x, y \in H$, then $xy \in H$, and if $x \in H$, then $x^{-1} \in H$. We will see in chapter two that these three conditions are enough to prove that a non-empty subset H is a subgroup of G .

Notice that matrices are closed under addition if they are both $m \times n$ or multiplication if $n \times n$. But all $n \times n$ matrices do not form group under multiplication because lots of matrices don't have inverses. They do form a group under addition, a necessary condition for the the set of $n \times n$ matrices to be a vector space.

Since an $n \times n$ matrix with entries in a field is invertible if and only if its determinant is non-zero, we can take the subset of invertible matrices and call them $GL_n(F)$, which is a group under multiplication.

There are lots of groups of matrices that are subgroups of the two main ones listed. If this is new to you, please take a few minutes and play with some matrices and see which ones form groups.

1.2 Dihedral Groups

The first examples of finite groups in the book come from the symmetries of a regular n -gon. Since we can rotate the n -gon and have to do so n times to get back to where we started, there is a rotation r for which $r^n = e$ and $r^i \neq e$ for $i = 1, 2, \dots, n - 1$, *i.e.*, $|r| = n$. There is also a flip around a vertex, which we will call s . Since flipping twice gets us back to the where we started, $|s| = 2$. It ends up that all symmetries are products of these and that there are $2n$ symmetries. We call this group of symmetries D_{2n} in this book. Spoiler alert: Some books call then D_n , so be careful when looking at other books.

The way I have listed the group is with generators and relations, but I didn't give all the relations. I left out $rs = sr^{-1}$, a third relation which is all we need. We'll be doing a lot with generators and relations over the course, so now is a good time to get used to working with them.

1.2 #4: Suppose $n = 2k$ and that $n \geq 4$. Note that $z = r^k \neq e$ and that $z^2 = (r^k)^2 = r^{2k} = e$. Thus $|z| = 2$. Also, $zr^i = r^{k+i} = r^{i+k} = r^i r^k = r^i z$ and $zs = r^k s = sr^{-k} = sr^k = sz$, so z commutes with every element of D_{2n} . If $b = s^j r^i$ commutes with every element of D_{2n} where $j = 0, 1$, $i = 0, \dots, n-1$, then $br = rb$ and $bs = sb$. If $j = 0$, then $b = r^i$ commutes with any r^j but $r^i s = sr^{-i} = sr^i$ implies that $r^{-i} = r^i$, so $|b| = 2$, whence $i = k$. If $j = 1$, then $b = sr^i$. But $sb = s^2 r^i = r^i$ and $bs = sr^i s = s^2 r^{-i}$ so again $i = k$. But $rb = r s r^i = sr^{i+1}$ and $br = sr^{i+1}$, which requires $r^{i-1} = r^{i+1}$ or that $e = r^2$, contradicting that $|r| \geq 4$. Therefore, $z = r^k$ is the only element other than the identity which commutes with every element of D_{2n} .

1.3 Symmetric Groups

The symmetric groups are a basic building block of finite groups. We will see later that every finite group is isomorphic (essentially the same as up to relabeling) a subgroup of some symmetric group. Being able to work with the cyclic decomposition is very important and will be assumed, so practice if it is new to you.

Since permutations are functions, they compose right to left so $\sigma\tau(1) = \sigma(\tau(1))$, *i.e.*, apply τ first and then σ . For example, if $\sigma = (1\ 2\ 3)$ and $\tau = (1\ 2)$, then $\sigma\tau(1) = \sigma(2) = 3$ but $\tau\sigma(1) = \tau(2) = 1$. So order matters.

1.3 #1: $\sigma = (1\ 3\ 5)(2\ 4)$, $\tau = (1\ 5)(2\ 3)$. Notice that we don't need to put (4) in the cyclic expression for τ . $\sigma^2 = (1\ 5\ 3)$, $\sigma\tau = (2\ 5\ 3\ 4)$, and $\tau\sigma = (1\ 2\ 4\ 3)$. Notice that it is common to put the lowest number first in the cycle, but $(1\ 3) = (3\ 1)$ and so on.

1.3 #3 for question 1 above: The order is the least common multiple of the lengths of the cycles in the disjoint cyclic decomposition, so $|\sigma| = 6$, $|\sigma^2| = 3$, $|\tau| = 2$, $|\sigma\tau| = 4 = |\tau\sigma|$.

Notice that $|D_6| = |S_3|$. We will discover next week that they are isomorphic.

It is not enough, however, for the orders to be the same to force an isomorphism. Remember that last week we showed that there were two different groups of order four.

1.4 Matrix Groups

Since all of you have had linear algebra, I will not write more about matrix groups than I did above.

1.5 Quaternion Group

For those of you who have seen quaternions over the reals in other classes, you may think of the quaternion group as the basis for the quaternions just as $1, i$ is a basis for the complex numbers over the reals. The quaternions over the reals came about because Hamilton wanted to multiply vectors in three space and couldn't. One day he realized he could in four space if he used the basis listed as the Quaternion Group. It is one of the basic groups of order 8 and is not isomorphic to D_8 , as can be seen by counting the number of elements of order 4.