Lecture 3

This week we have a longer section on homomorphisms and isomorphisms and start formally working with subgroups even though we have been using them in Chapter 1. First, let's finish what was claimed in Lecture 2.

Theorem 1: $D_6 \cong S_3$.

Proof: As shown in 1.3, D_6 is generated by r, s where $|r| = 3,\ |s| = |2|, rs = sr^{-1} = sr^2$. So $D_6 = \{e, r, r^2, s, sr, sr^2\}$. In order to define a homomorphism $\phi : D_6 \to S_3$, we need to figure out where to send r and s so that the relations hold. Recall that r stands for a rotation and has order 3. In S_3, a 3-cycle has order 3. So define $\phi(r) = (123)$. Thus $|r| = |\phi(r)| = |(123)| = 3$ and the first relation holds. Since $|s| = 2$, let's try $\phi(s) = (12)$. At least $|s| = |\phi(s)| = |(12)| = 2$ and the second relation holds. Now we need to check the third relation. $\phi(rs) = \phi(r)\phi(s) = (123)(12) = (13)$ and $\phi(sr^{-1}) = \phi(s)\phi(r^2) = (12)(132) = (13)$. So all three relations hold. Thus ϕ is a homomorphism. Since we have not talked about generators for S_3, it is enough to show that (12) and (123) generate all of S_3. Then ϕ would be onto, and, since D_3 is finite, ϕ would also be one-to-one, whence an isomorphism.

So far we have $e = (12)^2, (12), (123), (13) \in \phi(D_3)$. Notice that $(132) = ((123))^{-1} = \phi(r^2)$ and that $(23) = (12)(123) = \phi(sr)$. Therefore, $|\phi(D_6)| = 6$ and ϕ is an isomorphism.

A surjection is a surjective or onto homomorphism. An injection is an injective or one-to-one homomorphism. These fancier words will appear from time to time so please learn them now.

I've been using some results not proved in the book as they are assumed known.

Theorem 2: Let $\phi : G \to H$ be a group homomorphism. Then

1. $\phi(x^n) = \phi(x)^n\ \forall n \in Z^+$.
2. $\phi(e_G) = e_H$.
3. $\phi(x^{-1}) = (\phi(x))^{-1}$.
4. $\phi(x^n) = \phi(x)^n\ \forall n \in Z$.

5. $\phi(G)$ is a group contained in H, i.e., a subgroup of H.

Proof: 1. We proceed by induction on n. If $n = 1$, then $\phi(x) = \phi(x)$ is true since ϕ is well-defined. Assume $\phi(x^{n-1}) = (\phi(x))^{n-1}$. Then $\phi(x^n) = \phi(x^{n-1} * x) = \phi(x^{n-1})\phi(x) = (\phi(x))^{n-1}\phi(x) = (\phi(x))^n$. Therefore by induction, $\phi(x^n) = \phi(x)^n \; \forall n \in Z^+$.

2. $\phi(e_G) = \phi(e_G * e_G) = (\phi(e_G))^2$. By cancellation, $e_H = \phi(e_G)$.

3. $e_H = \phi(e_G) = \phi(x * x^{-1}) = \phi(x)(\phi(x^{-1}))$. Since H is a group, $(\phi(x))^{-1} = (\phi(x^{-1}))$.

4. By 1 and 3, 4 is true.

5. Since H is a group and $\phi(G) \subseteq H$, the operation in $\phi(G)$ is associative. By 2, the identity of H is in $\phi(G)$, so $\phi(G)$ is non-empty and has an identity. By 3, $\phi(G)$ has inverses. Therefore, $\phi(G)$ is a group.

For those to whom homomorphisms and isomorphisms are new, I suggest you look at exercises 2-9 to get yourself more up to speed. To help you get started, I'll do some of them.

1.6 #3 Suppose $\phi : G \to H$ is an isomorphism. Suppose that G is abelian. The $x, y \in H$. Then there exist $a, b \in G$ such that $\phi(a) = x$ and $\phi(b) = y$. Thus, $xy = \phi(a)\phi(b) = \phi(ab) = \phi(ba) = \phi(b)\phi(a) = xy$. Thus, H is abelian. Conversely, suppose H is abelian. Then $\phi(ab) = \phi(a)\phi(b) = \phi(b)\phi(a) = \phi(ab)$. Since ϕ is injective, $ab = ba$ and G is abelian.

Note that we used onto for the first proof and one-to-one for the second. So, by the first proof, it is sufficient for ϕ to be onto for G being abelian to insure H is.

1.6 #8 Suppose $m \neq n$. Then $|S_n = n! \neq m! = |S_m|$. Thus, S_n cannot be isomorphic to S_m.

Now we start Chapter 2 with a discussion of subgroups, a topic alluded to in Chapter 1.

2.1

In order for a non-empty subset H of a group G to be a subgroup, it must be a group under the same operation at G. So the first thing that needs to be checked is that H is closed under the operation of G. If this is true, the best news is that, since $a(bc) = (ab)c\ \forall a, b, c \in G,\ a(bc) = (ab)c\ \forall a, b, c \in H$, *i.e.,* the associative law holds in H. Since the associative law is usually the hardest to check in a set G, it is great not to have to check it. We also get $1_G = 1_H$ for free. The only thing left to check is that H is closed under inverses, *i.e.,* if $x \in H$, then $x^{-1} \in H$. I usually find it easiest to check the three things, non-empty, closed under the operation of G and closed under inverses, instead of the two of **Proposition 1**, but you should do what is easiest for you.

I did not assign problem 6 of this section so want to explain it and do it for you. Note that every element of a group is either of finite or infinite order. Since $1_G = x(x^{-1})$, the set of elements of infinite order is not closed under the group operation. The fun thing is that the elements of finite order are closed in an abelian group, but not necessarily in a non-abelian group. There are invertible matrices of finite order that multiply to a matrix of infinite order. Cool, huh?

Suppose G is an abelian group. Define the torsion subgroup T to be the set of elements of finite order in G, *i.e.,* $T = \{g \in G|\ |g| < \infty\}$. Since $|1_G| = 1$, T is not empty. Suppose $|g| = m,\ |h| = n$. Then $(gh)^{mn} = (g^m)^n(h^n)^m = 1_G(1_G) = 1_G$. Thus T is closed under the group operation. We've already proven that $|x^{-1}| = |x|$, so T is closed under inverses. Thus T is a subgroup of G. Notice that we used that G is abelian when we checked that T is closed under the operation of G.

Another piece that I didn't have you do is Lagrange's Theorem because it was in 1.7 and we didn't do 1.7.

Lagrange's Theorem: Let H be a subgroup of a finite group G. Then $|H|$ divided $|G|$.

We will prove this theorem in chapter 3 using less esoteric tools. You may use the theorem now, if you wish.

It is even easier to prove that something is not a subgroup. For example, 2.1 #2a: (12)(23) = (123) so the set of 2-cycles is not closed for $n \geq 3$.

So let's do a couple of proofs that subsets are subgroups.

2.1 #1a. Let $S = \{a + ai : a \in \mathbb{R}\} \subseteq \mathbb{C}$. Then $(a + ai) + (b + bi) = (a+b) + (a+b)i \in S$. Thus S is closed under addition. Note that $0 + 0i \in S$ so S is not empty. Lastly, $-a - ai \in S$, so S is closed under inverses. Therefore, S is a subset of $\mathbb{C}$.

2.1 #1e. Let S be the set of non-zero real numbers whose square is a rational number. Since $1^2 = 1 \in \mathbb{Q}$, S is non-empty. Let $a, b \in S$. Then $(ab)^2 = a^2b^2 \in \mathbb{Q}$ since $a^2, b^2 \in \mathbb{Q}$. Thus, S is closed under multiplication. Since $(a^{-1})^2 = (a^2)^{-1} \in \mathbb{Q}$, S is closed under inverses. Therefore S is a group.

2.2

We are going to study only half this chapter because we skipped section 1.7, namely, we will learn about centralizers and normalizers of groups and skip stabilizers and kernels of group actions.

The **centralizer** has to do with elements which commute with every element of a given subset, whereas the **normalizer** has to do with elements which fix the entire set under conjugation. Now that I've lost you with jargon, let's go back and decipher what is going on. The big difference is that centralizers have to do with element by element and normalizers have to do with a whole set.

Let A be a non-empty subset of a group G. The **centralizer** of A is the set of all $g \in G$ which commute with each element of A. In notation, $C_G(A) = \{g \in G | ga = ag \ \forall a \in A\}$. So $g \in C_G(A)$ commutes with each $a \in A$ on an element-wise basis. If $A = G$, we call $C_G(G)$ the **center** of G and write $C_G(G) = Z(G)$.

The **normalizer** $N_G(A)$ of A in G is the set of elements $g \in G$ that fix A as a set when one computes gag^{-1}, namely, $N_G(A) = \{g \in G | gAg^{-1} = A\} = \{g \in G | gag^{-1} \in A \ \forall a \in A\}$. The "action" conjugation by g on A is gAg^{-1}. I put action in quotes because we didn't learn about actions in 1.7. Conjugation is probably the most important of the actions so I'm making sure you learn about it as a separate entity. It is also our first time working with an entire set. Notice that conjugation by an element g of the normalizer of A, takes A to A, but it does not necessarily take a to a for each $a \in A$.

For example, let $G = S_3$ and let $A = \{e, (123), (1,3,2)\}$, a subgroup of G of order 3. Since $(12)(123) = (23)$, $(123)(12) = (13)$, $(12) \notin C_G(A)$. Similar computations show that the other transpositions are not in the centralizer. Since the order of A is 3, A is an abelian group (see lecture 2). Therefore, $C_G(A) = A$. We can also conclude from these computations that $Z(G) = \{e\}$.

Since A is a subgroup, it is closed under multiplication so $A \in N_G(A)$. Let's compute conjugation by the other elements. $(12)(123)(12) = (132)$,
$(12)(132)(12) = (123)$, $(13)(123)(13) = (132) = (23)(123)(23)$,
$(13)(132)(13) = (123) = (23)(132)(23)$. So $N_G(A) = G$ but $gag^{-1} \neq a$ for a a transposition and g a three-cycle.

Lastly, let's look at a connection between the centralizer and the normalizer.

2.2 #1 Note that $ag = ga \Leftrightarrow g^{-1}ag = a$, found by multiplying each side of the first equation by g^{-1}. Thus, $C_G(A) = \{g \in G : ag = ga \ \forall a \in A\} = \{g \in G : g^{-1}ag = a \ \forall a \in A\}$.