Lecture 5

3.1

This section and the next are probably the hardest sections in group theory as the concept of quotient group goes against ones intuition. The problem is that an element in the quotient group is actually a set called a coset. We've run into this when young because the rational numbers are really cosets because $1/2 = 2/4 = 3/6 = ...$ and we had to be careful about defining homomorphisms from $\mathbb{Q}$. We've also saw this before in this class with $\mathbb{Z}/n\mathbb{Z}$ where we could pick any element $i + kn$ as a representative of the element $[i]$. Thus $[i] = \{i + kn | k \in \mathbb{Z}\} = i + n\mathbb{Z}$ in the new notation and again had to be careful to see that the operations of addition and multiplication were well-defined, i.e., did not depend on which representative we chose, and ditto for functions.

These observations are true in general: It can be hard working with a set as an element of a group because seeing that an operation or function is well defined takes some doing.

Let's recall some definitions first. Let $\phi : G \to H$ be a group homomorphism. The kernel of ϕ, $\ker(\phi)$, $= \{g \in G | \phi(g) = 1_H\} = \phi^{-1}(1_H)$, i.e., the fiber of 1_H. Recall that a fiber is simply everything that maps to the given element(s) of H and is a set in general. All fibers consist of a single element of G or the empty set if an only if ϕ is one-to-one, a monomorphism. Computing kernels and fibers are important so you have a number of homework exercises this week that ask you to do just that.

3.1.7: Define $\pi : \mathbb{R} \times \mathbb{R} \to \mathbb{R}$ by $\pi(x, y) = x + y$. Then $\pi((a, b) + (c, d)) = \pi((a + c, b + d)) = (a + c) + (b + d) = (a + b) + (c + d) = \pi((a, b)) + \pi((c, d))$. Therefore, π is a homomorphism. Since $\pi((x, 0)) = x + 0 = x$, ϕ is onto and so an epimorphism. $(a, b) \in \ker(\pi) \Leftrightarrow 0 = \pi((a, b)) = a + b \Leftrightarrow b = -a$. This is the line $y = -x$. The fiber over $c = \pi^{-1}(c) = \{(a, b) | c = \pi((a, b)) = a + b\}$ which is the line $x + y = c$.

Now we go on to normality of a subgroup H of a group G. Theorem 6 gives equivalences but the definition is often the easiest to use. In fact theorem 6 is a great example of the fact that for all also means for each. So $ghg^{-1} \in H \ \forall g \in G, h \in H$ is the same as $gHg^{-1} \subseteq H \ \forall g \in G$ because it gathers the for all $h \in H$ into the symbol H.

The book shows that the cosets aH form a group under multiplication $(aH)(bH) = abH$ if and only if H is normal in G. In fact, the subgroup has to be normal (same as $N_G(H) = G$) for multiplication to be well-defined. There is a simple consequence of the definition.

3.1.4: In G/N, $(gN)^n = g^n N \ \forall n \in \mathbb{Z}$.

Proof. We proceed by induction on n. If $n = 1$, $gN = gN$. If $n = 2$, $(gN)^2 = gN(gN) = g^2N$ by definition of multiplication. Assume that $(gN)^{n-1} = g^{n-1}N$. Then $(gN)^n = (gN)(gN)^{n-1} = (gN)(g^{n-1}N) = g^nN$. By induction $(gN)^n = g^nN$ for all positive n. Since $(gN)^0 = eN = g^0N$, the statement is true for $n = 0$. Also, $(gN)^{-n} = ((gN)^n)^{-1} = (g^nN)^{-1} = g^{-n}N$. Therefore the statement is true for every integer.

3.1.3: Of course, for an abelian group, $ghg^{-1} = gg^{-1}h = h$, so every subgroup is normal. Let B be a subgroup of an abelian group A. Then $(xB)(yB) = (xy)B = (yx)B = (yB)(xB)$ and A/B is abelian. It is not true that, if every quotient is abelian, the group is abelian. Consider S_3. Above I showed that $N_{S_3}(< r >) = S_3$, so $< r >$ is normal in S_3. But $|S_3/ < r > | = 2$, so is abelian. As $< r >$ is the only proper, non-trivial normal subgroup ($G/G = 1$, $G/1 = G$ for every group G), all quotients of S_3 are abelian but S_3 is not. We will find later that, if $G/Z(G)$ is cyclic, then G is abelian.

Let S be a nonempty subset of a group G and define a relation on G by $a \sim b$ if and only if $ab^{-1} \in S$. Show that $\sim$ is an equivalence relation if and only if S is a subgroup of G.

Proof: Suppose $\sim$ is an equivalence relation. We are given that S in non-empty, so let $a \in S$. Then $a \sim a$, whence $e = aa^{-1} \in S$. Suppose $b \in S$. Since $b = eb \in S$, we have $e \sim b^{-1}$, so $b^{-1} \sim e$. Therefore, $b^{-1} = b^{-1}e^{-1} = b^{-1} \in S$. Suppose $a, b \in S$. Then $b^{-1} \in S$. Since $a \sim e$ and $e \sim b^{-1}$, $a \sim b^{-1}$ or $ab = a(b^{-1})^{-1} \in S$. Therefore, S is a group.

Conversely, suppose S is a group. For $a \in S$, $e = aa^{-1} \in S$, so $a \sim a$ for all $a \in S$. If $a \sim b$, then $ab^{-1} \in S$, whence $ba^{-1} = (ab^{-1})^{-1} \in S$. Thus, $b \sim a$. Lastly, if $a \sim b$ and $b \sim c$, then $ac^{-1} = ab^{-1}bc^{-1} \in S$, whence $a \sim c$. Therefore $\sim$ is an equivalence relation if and only if S is a group.

Since the equivalence classes of an equivalence relation form a partition of G and vice versa, problem 5 is an alternative proof to Proposition 4.

Proposition 7 is a very important one. It says that normal subgroups correspond to kernels of homomorphisms. In the section 3.3 we are going to extend this idea to an isomorphism, namely, if $\phi : G \to H$ has $\ker(\phi) = N$, then $G/\ker(\phi) \cong \phi(G)$.

Now for some more examples of proofs:

3.1.16: Let G be a group and $N \triangleleft G$. Let $\overline{G} = G/N$. Suppose that $g =< x, y >$. Then, for $aN \in \overline{G}$, $a = \Pi_{k=1}^{N} x^{i_k} y^{j_k}$, so $aN = (\Pi_{k=1}^{N} x^{i_k} y^{j_k})N = \Pi_{k=1}^{N} x^{i_k} y^{j_k} N \in < \overline{x}, \overline{y} >$. In general, is $G =< S >$, then the product with x's and y's is replace by a product of $s_i^{k_i}$ and the proof goes through for a general S.

3.1.22a: Suppose that $H, K \triangleleft G$. We already know that $H \cap K$ is a subgroup. Let $g \in G$. Since $H \cap K \subseteq H$, $g(H \cap K)g^{-1} \subseteq H$. Similarly, $g(H \cap K)g^{-1} \subseteq K$. Therefore, $g(H \cap K)g^{-1} \subseteq H \cap K$. By Proposition 6 (or the proof below), $H \cap K \triangleleft G$.

3.1.25a: Lemma: Let $H < G$ and $g \in G$. Then $gHg^{-1} < G$.

Proof: $1 = g1g^{-1} \in gHg^{-1}$ so gHg^{-1} is not empty. If $gxg^{-1}, gyg^{-1} \in gHg^{-1}$, then $gxg^{-1}gyg^{-1} = gxyg^{-1} \in gHg^{-1}$. Also, $(gxg^{-1})^{-1} = gx^{-1}g^{-1} \in gHg^{-1}$. Therefore, $gHg^{-1} < G$.

Now assume that $gNg^{-1} \subseteq N$, $\forall g \in G$. Let $n \in N$. Then for $g^{-1} \in G$, $g^{-1}ng \in N$ and $n = g(g^{-1}ng)g^{-1}$. Therefore $gNg^{-1} = N$ and $N \triangleleft G$.

3.1.22b: Let N be the subgroup of upper triangular matrices with integer entries, as subgroup of $G = GL_2(\mathbb{A})$. Let $g = \begin{pmatrix} 2 & 0 \\ 0 & 1 \end{pmatrix}$. Then $\begin{pmatrix} 2 & 0 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & n \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1/2 & 0 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 2 & 2n \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1/2 & 0 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 2n \\ 0 & 1 \end{pmatrix} \in N$ Therefore, $gNg^{-1} \subset N$ but they are not equal because gNg^{-1} has only even 1 2 entries.

3.1.30: Suppose $N \leq G$ and let $g \in G$. Then $gN = Ng$ if and only if, for all $n \in N$, $gn = n'g$ for some $n' \in N$ if and only if $gng^{-1} = n' \in N$ $\forall n \in N$ if and only if $g \in N_G(N)$.

3.1.42: Suppose $H, K \lhd G$ and that $H \cap K = \{1\}$. Let $x \in H,\ y \in K$. Then $(xyx^{-1})y^{-1} \in K$ because $K \lhd G$ and $x(yx^{-1}y^{-1}) \in H$ because $H \lhd G$. Thus $xyx^{-1}y^{-1} \in H \cap K$, whence $xyx^{-1}y^{-1} = 1$, so $xy = yx$.

3.2

This section demonstrates the adage "Never underestimate the power of a theorem that counts something." Lagrange's theorem that the order of a subgroup divides the order of the finite group with the consequence that the number of cosets is the order of the group divided by the order of the subgroup - normality not required - is the basis of the entire section. All the results proved in this section are straightforward consequences of Lagrange's theorem and proved by counting. So the best I can do for this section is to keep on counting.

3.2.4: Suppose $|G| = pq$ where p, q are primes, not necessarily distinct. Suppose G is not abelian and $|Z(G)| \neq 1$. Then, without loss of generality, $|Z(G)| = p$. Then $|G/Z(G)| = q$, a prime, so $G/Z(G) \cong \mathbb{Z}/q\mathbb{Z}$ is cyclic. By problem 3.1.36, G is abelian. Contradiction. Therefore $|Z(G)| = 1$.

3.2.6: Suppose $H \leq G$, and let $g \in G$. Suppose $Hg = g'H$. Since $g = 1g,\ g = g'h$ for some $h \in H$. Thus $gH = g'hH = g'H = Hg$. Since $gHg^{-1} = Hgg^{-1} = H,\ g \in N_G(H)$.

3.2.8: Suppose $|H| = a,\ |K| = b$, finite subgroups of a group G such that $(a, b) = 1$. Since $H \cap K$ is a subgroup of both H and K, $|H \cap K|$ divides both a and b, so divides $(a, b) = 1$. Therefore $H \cap K = \{1\}$.

3.2.11: Let $H \leq K \leq G$. Suppose $|G : K| = s$ and $|K : H| = t$ are both finite. Then $G/K = \{g_1K, \ldots, g_sK\}$ for some $g_i \in G$, and $K/H = \{k_1H, \ldots, k_tH\}$ for some $k_j \in K$. Since K is the disjoint union of the k_jH, g_iK is the disjoint union over j of the g_ih_j. So there are st of them and $|G : H| = |G : K||K : H|$. If at least one of s, t is infinite, the product is infinite, so again $|G : H| = |G : K||K : H|$ by the same argument.

3.3

This section has one main theorem from which all others follow, namely, the first isomorphism theorem. It says, in essence, that, if you want to have an isomorphism from G/H, define a homomorphism from G and show that the kernel of that homomorphism is H. Then G/H is isomorphic to the image of the homomorphism. The trick, sometimes, is to figure out which of two quotient groups to use as the domain. If one try doesn't work, try the other. Notice that it is much easier to define a homomorphism from G than from G/H as we don't usually have problems with well-defined from G and do from H.

Since the book didn't prove the Lattice Isomorphism Theorem, I will. It's also exercise 2 in the book.

Let G be a group and let N be a normal subgroup. By Exercise 3.1.1, which was assigned, the preimage of a subgroup $\overline{A} = A/N$ is a subgroup of G which contains N and, if $\overline{A}$ is normal in G/N, then its preimage is normal in G.

Let $S = \{A \leq G|N \leq A\}$and $\overline{S} = \{\overline{A}|\overline{A} \leq G/N$. Let $\phi : S \to \overline{S}$ by $\phi(A) = \overline{A}$. Since $\phi(\phi^{-1}(\overline{A})) = \overline{A}$, ϕ is surjective. Suppose $A \neq B$. Without loss of generality, we may assume there is $b \in B$ such that $b \notin A$. Suppose $\phi(b) = bN = aN \in \phi(A) = A/N$. Then $b = an$ for some $n \in N$. But $N \subseteq A$, so $b = an \in A$. Contradiction. Therefore $\phi(b) \notin \phi(A)$ and $\phi(A) \neq \phi(B)$. Therefore ϕ is bijective.

Property (1): Suppose $A, B \in S$. If $A \subseteq B$, then $\overline{A} = \phi(A) \subseteq \phi(B) = \overline{B}$. Conversely, we just showed that, if $A \not\subseteq B$, then $\overline{A} \not\subseteq \overline{B}$.

Property (2): Suppose $A \subseteq B$ for $A, B \in S$. Let $C = \{bA | b \in B$ and let $D = \{\overline{b}\overline{A} | \overline{b} \in \overline{B}\}$. By definition, ϕ maps C onto D. Suppose $\phi(bA) = \phi(cA)$. Then $\overline{b}\overline{A} = \overline{c}\overline{A}$ so there exists $\overline{a} \in \overline{A}$ so that $\overline{b} = \overline{ca}$, whence there exists $n \in N$ such that $b = (ca)n = c(an)$. Since $N \subseteq A$, $an \in A$ and $bA = cA$. Therefore $\phi : C \to D$ is injective and surjective, so bijective. Thus, $|B : A| = |\overline{B} : \overline{A}|$.

Property (3): $\overline{< A, B >} = \phi(< A, B >) \subseteq < \overline{A}, \overline{B} >$. If $g \in < \overline{A}, \overline{B} >$, then $g = \Pi \overline{a_i}\overline{b_i} = \Pi \phi(a_i)\phi(b_i) = \Pi \phi(a_i b_i) = \phi(\Pi a_i b_i) \in \overline{< A, B >}$. Therefore $< \overline{A}, \overline{B} > = \overline{< A, B >}$.

Property (4): Let $\overline{a} \in \overline{A \cap B}$. Then $\phi(a) \in \phi(A \cap B) \subseteq \phi(A) \cap \phi(B) = \overline{A} \cap \overline{B}$. If $\phi(a) = \overline{a} \in \overline{A} \cap \overline{B}$, then $a \in A$ and $an \in B$ for some $n \in N$. But $N \subseteq A \cap B$, so $an \in A$ and $\overline{a} = \overline{an} \in \overline{A \cap B}$. Therefore, $\overline{A \cap B} = \overline{A} \cap \overline{B}$.

Property (5): $A \lhd G$ iff $gag^{-1} \in A$, $\forall g \in G$, $a \in A$ iff $\overline{gag^{-1}} = \overline{g}\overline{a}\overline{g^{-1}} \in \overline{A}$, $\forall \overline{g} \in \overline{G}$, $\overline{a} \in \overline{A}$. Thus, $A \lhd G$ iff $\overline{A} \lhd \overline{G}$.

3.3.7: Let M and N be normal subgroups of G such that $G = MN$. Define $\phi : G \to (G/M) \times (G/N)$ by $\phi(g) = (gM, gN)$. Then $\phi(gh) = (ghM, ghN) = (gM, gN)(hM, hN) = \phi(g)\phi(h)$, so ϕ is a homomorphism. Let $(gM, hN) \in G/M \times G/N$. Then $g = m_1 n_1 = n_1' m_1$, $h = m_2 n_2$ and $n_1' m_2 = m_2 n_2'$. Thus, $\phi(n_1' m_2) = (n_1' m_2 M, n_1' m_2 N) = (n_1' m_1 M, m_2 n_2' N) = (gM, m_2 n_2 N) = (gM, hN)$. Therefore, ϕ is surjective. $g \in \ker(\phi)$ iff $(1M, 1N) = \phi(g) = (gM, gN)$ iff $g \in M$ and $g \in N$, so $g \in M \cap N$. By the first isomorphism theorem, $G/(M \cap N) \cong (G/M) \times (G/N)$.