M 621 notes: Week of 10.17

Here's a list of the topics we covered. Discussion of those topics follows the list. Below G is a group.

1. Some Chapter 3 topics that were discussed.

   (a) We proved that if $G \geq H$ and $[G : H] = 2$, then H is a normal subgroup of G.

   (b) We reviewed the Fourth Isomorphism Theorem (also known as the *Correspondence Theorem*). For a group G, let $Sub(G)$ denote the lattice of subgroups of G. For a subgroup H of G, let $I[H, G] = \{J \leq G : J \geq H\}$, the interval above H in $Sub(G)$. A statement of most of the Fourth Isomorphism Theorem follows.

   Proposition 0.1 *Let G be a group with normal subgroup N. The map $S : I[N, G] \to Sub(G/N)$ given by $S(K) = K/N$ for all $K \in I[N, G]$ is*

   i. a bijective order-preserving function

   ii. that maps normal subgroups in $I[N, G]$ to normal subgroups of G/N, and

   iii. whenever A is normal in G/N, $S^{-1}(A)$ is normal in G.

   Scott, Christen, and Yuenyen will present a solid sketch of the proof of the above proposition.

   (c) *Maximal subgroups* and *maximal normal subgroups* of G were defined and discussed, and it was observed that if G is a finite group, it contains a maximal normal subgroup (perhaps even several maximal normal subgroups).

   (d) We reviewed the definition of *simple group.* A group G is simple if its only normal subgroups are $\{e\}$ and G. That is, G is simple if it has no proper, non-trivial normal subgroups.

   (e) It follows from the Fourth Isom. Theorem that if G is a group, N is a normal subgroup of G, then G/N is simple if and only if N is a maximal normal subgroup of G.

   (f) We classified the Abelian simple groups, showing that G is a simple Abelian group if and only if there exists a prime p such that $G \cong Z_p$.

(g) We defined the *composition series* of a group G: A composition series an "increasing chain" of subgroups $H_0 = \{e\} \trianglelefteq H_1 \trianglelefteq H_2 \ldots\ H_{n-1} \trianglelefteq H_n = G$ satisfying for all all $i = 1, \ldots, n$,

   i. $H_{i-1} \trianglelefteq H_i$, and

   ii. H_i/H_{i-1} is a simple group.

(h) We provided several examples of composition series. For examples, with $G = Z_2 \times Z_3$, and $H_1 = \{(g, e) : g \in Z_2\}$ and $H_2 = \{(e, h) : h \in Z_3\}$, consider

   i. $\{e\} \trianglelefteq H_1 \trianglelefteq H_1 \times H_2 = G$

   ii. $\{e\} \trianglelefteq H_2 \trianglelefteq H_1 \times H_2 = G$

   These are both composition series for G. (Thus, a group G can have more than one composition series). Let $G = D_8$. Another example:

   i. $\{e\} \trianglelefteq < r^2 > \trianglelefteq < r > \trianglelefteq D_8$.

   ii. $\{e\} \trianglelefteq < s > \trianglelefteq < s, r^2 > \trianglelefteq D_8$.

   Be sure you can explain why both of the above are composition series of D_8—that is, you can show that both properties that comprise the definition of composition series are valid for the above two sequences of subgroups of D_8.

   Here's a short answer question. Complete: A group G has a composition series of length 1 (i.e., $\{e\} \trianglelefteq G$ is a composition series) if and only if G is simple.

(i) We defined the *factors* of a composition series $H_0 = \{e\} \trianglelefteq H_1 \trianglelefteq H_2 \ldots\ H_{n-1} \trianglelefteq H_n = G$ is the multiset of simple groups $\{N_i/N_{i-1} : i = 1, \ldots, n\}$.

   For examples, the factors of the first composition series for $G = Z_2 \times Z_3$ are (up to isomorphism) Z_2, Z_3, and the factors for the second series are Z_3, Z_2.

   For further examples, the factors of the first composition series are (up to isomorphism) Z_2, Z_2, Z_2; the second series for D_8 also has factors Z_2, Z_2, Z_2.

(j) We stated Holder's Theorem.

Theorem 0.2 Holder's Theorem *For any two composition series of a group G, including multiplicities, the factors of each series are the same.*

(k) We defined the notion of a *solvable* group. A group G is solvable if all of its factors are Abelian.

As witnessed by their composition series, both $Z_2 \times Z_3$ and D_8 are solvable groups.

Later, we will show that A_5 is simple. Explain why the following is true: "Since A_5 is simple and non-Abelian, A_5 is not solvable".

(l) **Exercise.** Every finite Abelian group is solvable. Reed, YoYo, and Israel will explain this.

2. The following topics from Chapter 4 were discussed.

(a) The *Orbit-Stabilizer Proposition*: Let G be a group acting on a set A. Then for all $a \in A$ we have $|O_a| = [G : G_a]$. *Proof*: Let $g, h \in G$, and let a, b be in A. We show that there is a bijection between O_a and the left cosets of G_a in G: We have $g \cdot a = b$ and $h \cdot a = b$ if and only if $h^{-1}g \cdot a = a$ if and only if $h^{-1}g \in G_a$ if and only if $hG_a = gG_a$. It is now easy to establish that the map $gG_a \to g \cdot a$ defines a bijection from the left cosets of G_a in G to the elements of O_a. $\square$

(b) Let G act on itself by conjugation. That is, for $g \in G$ and $h \in G$, $g \cdot h = ghg^{-1}$, an action (as you can and should verify). Let $h \in G$. The orbit of h under the action is $\{g \cdot h = ghg^{-1} : h \in G\}$, the set of conjugates of h. We refer to the orbit of h as the *conjugacy class of h*.

Examples: Let's take at the conjugacy classes of S_3. Here they are: $\{e\}, \{(12), (13), (23)\}, \{(123), (132)\}$. In general, for S_n, with the exception of the conjugacy class of e (which is $\{e\}$), each conjugacy class is associated with a "shape". For example, here are the possible shapes of S_4: 2 (the transpositions); $2, 2$ (the elements of the form $(ij)(kl)$, disjoint 2-cycles) 3 (the 3-cycles) and 4 (the 4-cycles).

As we observed in the stabilizer of h is $C_G(h)$, the centralizer of h in G. So the Orbit-Stabilizer formula gives us the size of the conjugacy class of h—it is $[G : C_G(h)]$. Test this: The conjugacy class of (123) in S_4 is the set of all three-cycles in S_4, of which there are 8. On the other hand, $C_{S_4}(123) = \{\alpha \in S_4 : \alpha(123)\alpha^{-1} = (123)\} = \{e, (123), (132)\}$, as you can easily verify. So the conjugacy class of (123) should have $[G : C_{S_4}((123))] = \frac{24}{3} = 8$, which agrees with our original observation.

(c) We reviewed $Aut(G)$, the emphautomorphismsof G, and $Z(G)$, the *center* of G, and connected them.

  i. We observed that $Aut(G)$ is a group—it's operation is function composition. Be sure you can verify that $Aut(G)$ is a group.

  ii. We defined the set of *inner automorphisms* of G: Let $g \in G$. The function $c_g : G \to G$ given by for all $h \in G$, $c_g(h) = ghg^{-1}$, is an automorphism of G, a so-called inner automorphism of G. The set of all inner automorphisms of G, denoted $Inn(G)$, is a subgroup of $Aut(G)$. Suppose c_g is the inner automorphism given by conjugation by g, and that σ is an arbitrary automorphism of G. Determine $\sigma c_g \sigma^{-1}$. Is it an inner automorphism? Is $Inn(G)$ normal in $Aut(G)$?

  iii. We commented that $Inn(G)$ is trivial if and only if G is Abelian.

  iv. Let $n \in \mathbb{N}$, $G = Z_n$. Let $m \in Z_n$. The map $\lambda_m : Z_n \to Z_n$ given by $\lambda_m(k) = mk$, for all $k \in Z_n$, is easily checked to a homomorphism. Conversely, suppose $\phi : Z_n \to Z_n$ is a homomorphism, and that $\phi(1) = m \in Z_n$. Since ϕ is a homomorphism, for any $k \in \mathbb{Z}_n$, $\phi(k) = \phi(1 + \ldots + 1) = \phi(1) + \ldots + \phi(1) = mk = \lambda_m(k)$. That is, all homomorphisms with co-domain Z_n are of the form λ_m, where $m \in Z_n$.
  The image of λ_m is clearly S$< m >$, the cyclic subgroup of Z_n generated by m. So in order for λ_m to be an automorphism, $< m >= Z_n$, and this is the case if and only if $(n, m) = 1$. Notice that $\lambda_m \circ \lambda_j = \lambda_{mj}$, with mj given mod n. It follows now that $Aut(Z_n) \cong Z_n^x$, the group of units of Z_n.

  v. The map $\Gamma : G \to Inn(G)$ given by $g \to c_g$, for all $g \in G$. The map Γ is a homomorphism, as we showed. Its kernel is

$Z(G)$, as you are asked to verify. By the First Isomorphism Theorem, $G/Z(G) \cong Inn(G)$.

vi. We proved the following classic proposition, followed by an important corollary.

Proposition 0.3 *Let G be a group. We have $G/Z(G)$ cyclic implies G Abelian.*

Proof. Since $G/Z(G)$ is cyclic, there exists $hZ(G) \in G/Z(G)$ such that $G/Z(G) =< hZ(G) >$. Let $u, v \in G$. Since the cosets partition G, there exists $i, j \in \mathbb{Z}$ and $z_1, z_2 \in Z(G)$ such that $u = h^i z_1, v = h^j z_2$. So $uv = h^i z_1 h^j z_2 = h^i h^j z_1 z_2 = h^j h^i z_1 z_2 = h^j z_2 h^i z_1 = vu$. □

vii. We discussed the *Class Equation*: Let G be a finite group. We observed that an element $g \in G$ has a singleton conjugacy class if and only if $g \in Z(G)$ if and only if $C_G(g) = G$.

Suppose $A_1, \ldots, A_n$ are the non-singleton conjugacy classes of G. From each non-singleton class A_i, choose a representative $a_i \in A_i$. By the Orbit-Stabilizer result, $|A_i| = [G; C_G(a_i)]$. Note that $|G| = |Z(G| + \sum_{i=1}^{i=n} |A_i = |Z(G)| + \sum_{i=1}^{i=n} [G : A_i]$—this is the Class Equation.

viii. Let p be a prime. We defined *p-group.* A group G is a p-group if there exists $n \in \mathbb{N}$ such that $|G| = p^n$.

Lemma 0.4 *If G is a p-group, then G has a non-trivial center.*

Proof. We refer to the Class Equation. If G is a p-group, A_i is a non-singleton conjugacy class and $a_i \in A_i$, then $[G : C_G(a_i)] = |A_i|$. Since A_i is not a singleton class, $C_G(a_i)$ is a proper subgroup of G. Since G is a p-group, $[G : C_G(a_i)] = |G|/|C_G(a_i)| = p^k$, where $k > 0$. Thus, $p| \sum_{i=1}^{i=n} [G : A_i]$, which implies that $p||Z(G)|$, which means that $Z(G)$ is non-trivial. □

ix. We have classified all groups have a prime number of elements. We do the same for group with p^2 elements, where p is prime.

Corollary 0.5 *Let p be prime. If $|G| = p^2$, then G is Abelian. Moreover, G is either isomorphic to Z_{p^2} or is isomorphic to $Z_p \times Z_p$.*

Proof. Since G is a p-group, it has a non-trivial center $Z(G)$. If $Z(G) = G$, G is Abelian, and there is nothing further to prove. If $Z(G)$ were not G, then $|Z(G)| = p$, and $|G/Z(G)| = p$, so $G/Z(G)$ is cyclic. But then (by an ear If not, $|Z(G)||p^2$, so $|Z(G)| = p$, and $|G/Z(G)| = p$, so $G/Z(G)$ is cyclic, and by Proposition 0.3, G is Abelian after all.

For the second part, if G is cyclic, then $G \cong Z_{p^2}$; if G is not cyclic, for any $a \in G - \{e\}$, $|a| = p$. Since G is not cyclic, there exists $b \in G$ such that $b \notin G- < a >$. Since $|b| = | < b >= p = |a| = | < a > |$. By Lagrange, $< a > \cap < b > -\{e\}$. Since $| < a > || < b > |/| < a > \cap < b > |$, it follows that $< a >< b >= G$. Now apply the homework exercise: $G \cong< a > \times < b >$, and since $< a >\cong Z_p \cong< b >$, $G \cong Z_p \times Z_p$. $\square$