MATH 6121 lecture notes

Transcribed and formatted by John M. Campbell
jmaxwellcampbell@gmail.com

7 September 29 lecture

7.1 Errata

Recall that the normalizer of a subset A of the underlying set of a group G is usually defined as $N_G(A) = \{g \in G : gAg^{-1} = A\}$.

However, the normalizer of a subset $A \subseteq G$ was incorrectly defined in class as $\{g \in G : \forall a \in A \ gag^{-1} \in A\}$. Let sets of this form be denoted as follows:

$$M_G(A) := \left\{g \in G : \forall a \in A \ gag^{-1} \in A\right\}.$$

As indicated in the lecture notes for the previous lecture, $M_G(A)$ may not form a subgroup, as may be verified by letting G denote the group of permutations of $\mathbb{Z}$, and letting $A = \{\sigma \in G : \forall i < 0 \ \sigma(i) = i\}$ and $g(x) = x + 1$, with $g^{-1}(x) = x - 1$. It is thus easily seen that $M_G(A)$ is not closed under inverses.

Consider the classification of infinite non-abelian groups G with a subset A such that $M_G(A)$ is not a subgroup. How can groups of this form be classified?

7.2 Sylow theory

Theorem 7.1. *Letting G be a group of prime power order, with $|G| = p^a$, we have that:*

1. *$Z(G) \neq \{1\}$;*
2. *For $N \trianglelefteq G$, $N \cap Z(G) \neq \{1\}$; and*
3. *For $H \leq G$, where $H \neq G$, $N_G(H) \neq H$.*

Recall that we proved that $Z(G) \neq \{1\}$ if $|G| = p^a$ using a clever counting argument. Theorem 7.1.2. may be proven using a similar enumerative technique.

Sketch of a proof of Theorem 7.1.3.: Find a proper normal subgroup $K \trianglelefteq G$ and $K \triangleleft H$, such that K is maximal and that G/K is not trivial. That is, we take K to be the largest normal subgroup of G which is also contained in H. For example, it is possible that we could take $\{1\}$. Observe that $H/K \leq G/K$. The quotient group G/K is also a p-group, so there exists a non-identity element zK in the center $Z(G/K)$ of G/K, with $z \notin K$ since $zK \neq eK$. For any $h \in H$, we have that $hK \in H/K$, so

$$zhK = zKhK = hKzK = hzK,$$

and we thus have that $hK = z^{-1}hzK$. Therefore, $zhz^{-1} \in hK \subseteq hH = H$. So $zhz^{-1} \in H$ for all $h \in H$. Since $M_G(A) = N_G(A)$ if G is finite, we have that $z \in N_G(H)$, but $z \notin H$. $\square$

Exercise 7.2. Show that $z \notin H$ with respect to the above argument.

Corollary 7.3. *If $H \leq G$, $|H| = p^{\alpha-1}$, and $|G| = p^{\alpha}$, then $H \trianglelefteq G$.*

Sketch of a proof: If $N_G(H) \neq H$, then $|H| \leq |N_G(H)|$ and $|N_G(H)|\big||G| = p^\alpha$, so $|N_G(H)| = p^\alpha$, and $N_G(H) = G$. $\square$

Corollary 7.4. *If $|G| = p^n$, then G is solvable.*

Sketch of a proof: Our strategy is to use induction. Recall that a **subnormal series** of a given group is a sequence of subgroups such that each such subgroup is a (proper) normal subgroup of the next. Consider the following subnormal series:

$$\{1\} \trianglelefteq Z(G) \trianglelefteq G.$$

This subnormal series will have a composition series such that the composition factors are all abelian. Recall that a finite group is said to be **solvable** if it has a subnormal series whose factor groups are all abelian. In particular, abelian groups are solvable. If G is of order p^n, and $Z(G)$ is nontrivial, and is of order p^k, then we have that $G/Z(G)$ is of order p^{n-k}. $\square$

7.2.1 An illustration of a 2-group of order 8

Let the dihedral group D_4 be denoted as follows:

$$D_4 = \left\{1, a, a^2, a^3, b, ba, ba^2, ba^3\right\}.$$

Question 7.5. What is $Z(D_4)$?

We claim that $Z(D_4) = \{1, a^2\}$. It is useful to think about this equality from something of a geometric perspective: one may prove geometrically that the only isometries in D_4 which commute with all the functions in D_4 are the identity isometry, together with the mapping in D_4 given by a half-turn rotation.

Example 7.6. The mapping ba is not in $Z(D_4)$, since $ba = a^3b \neq ab$.

Example 7.7. The mapping ba^2 is not in $Z(D_4)$, because $a(ba^2) = ba^3a^2 = ba$, and since $(ba^2)a = ba^3 \neq ba$.

We thus arrive at the following subnormal series:

$$\{1\} \trianglelefteq \{1, a^2\} \trianglelefteq D_4.$$

What is $D_4/\{1, a^2\}$? It is easily seen that:

$$D_4/\{1, a^2\} = \{\{1, a^2\}, \{a, a^3\}, \{b, ba^2\}, \{ba, ba^3\}\}.$$

Question 7.8. What is the center of $D_4/Z(D_4)$?

It is clear that $Z(D_4/Z(D_4)) = D_4/Z(D_4)$, since $D_4/Z(D_4)$ is of order 4, and therefore must be abelian. Recall that up to isomorphism, there are only two groups of order 4, namely: the cyclic group $\mathbb{Z}/4\mathbb{Z}$, and the Klein four-group $(\mathbb{Z}/2\mathbb{Z}) \times (\mathbb{Z}/2\mathbb{Z})$.

We thus arrive at the following subnormal series:

$$\{\{1, a^2\}\} \trianglelefteq \{\{1, a^2\}, \{a, a^3\}\} \triangleleft D_4/\{1, a^2\}.$$

Also consider the following subnormal series:

$$\{1\} \trianglelefteq \{1, a^2\} \trianglelefteq \{1, a, a^2, a^3\} \trianglelefteq D_4.$$

7.3 Sylow p-subgroups

Recall that a finite group is a p-group iff its order is a power of p.

Similarly, a p-subgroup is a subgroup which is also a p-group.

A **Sylow p-subgroup** of a group $|G| = p^\alpha m$ is a p-subgroup of order p^α with $(p, m) = 1$.

There are many equivalent ways of defining Sylow p-subgroups. In particular, Sylow p-subgroups are defined in the following equivalent ways in John Fraleigh's *A First Course in Abstract Algebra* and Joseph Gallian's *Contemporary Abstract Algebra*, respectively.

Definition 7.9. A **Sylow p-subgroup** P of a group G is a maximal p-subgroup of G, that is, a p-subgroup contained in no larger p-subgroup.

Definition 7.10. Let G be a finite group and let p be a prime. If p^k divides $|G|$ and p^{k+1} does not divide $|G|$, then any subgroup of G of order p^k is called a **Sylow p-subgroup of** G.

Let n_p denote the # of Sylow p-subgroups, and let $\mathrm{Syl}_p(G)$ denote the set of all Sylow p-subgroups.

Theorem 7.11. *Letting G be a finite group, and letting $p \in \mathbb{N}$ be a prime number, we have that:*

1. *Sylow p-subgroups always exist, i.e., $n_p \geq 1$;*
2. *# of Sylow p-subgroups divides $|G|$, i.e., $n_p \big| |G|$;*
3. *# of Sylow p-subgroups $\equiv 1 (\mathrm{mod}\ p)$, i.e., $n_p = kp + 1$ for some $k \geq 0$; and*
4. *All Sylow p-subgroups are conjugate, i.e., if $K, H \in \mathrm{Syl}_p(G)$, then $\exists g \in G\ gHg^{-1} = K$.*

Exercise 7.12. Illustrate the above theorem using the Sylow p-subgroups of $S_3 \cong D_3$. Recall that S_3 denotes the group consisting of permutations on $\{1, 2, 3\}$.

Remark 7.13. This theorem is particularly useful for finding normal subgroups of a group (and thereby showing that G is not simple). List all values of n_p and see if any are forced to be 1 by this theorem.

Proof sketch for Theorem 7.1.1: We inductively assume that the theorem holds for all $n < |G|$. Informally, our strategy is to "get at the center". If $p \big| |Z(G)|$, then we can find an element $c \in Z(G)$ such that $\mathrm{order}(c) = p$, and $|G/\langle c \rangle| = p^{\alpha-1}m$. So it must have a group of order $p^{\alpha-1}$. Let

$$\pi \colon G \to G/\langle c \rangle$$

denote the canonical morphism.

A Sylow p-subgroup of $G/\langle c \rangle$ will have order p^α.

If $p \nmid |Z(G)|$, then:

$$|G| = |Z(G)| = \sum_{\substack{i=1 \\ |c(x_i)|>1}} \frac{|G|}{|N_G(\{x_i\})|}.$$

We know that $p \big| |G|$, but $p \nmid |Z(G)|$, so we know that there exists an index i such that

$$p \nmid \frac{|G|}{|N_G(\{x_i\})|}.$$

This implies that $|N_G(\{x_i\})| = p^\alpha m'$ for some $m' \neq m$. So there exists a nontrivial subgroup of smaller order than G, so $N_G(\{a_i\})$ contains a subgroup of order p^α by induction. $\square$

Question 7.14. Why is it true that if p divides the order of $Z(G)$, then there exists an element $c \in Z(G)$ of order p?

Observe that since $Z(G)$ is abelian, this may be justified using the Fundamental Theorem of Finitely-Generated Abelian Groups. However, we haven't covered this in class.

As indicated on the course webpage, rather than cover the proof of Sylow's theorem in full detail, there is an outline available[1] on the course webpage that includes the proofs with spartan explanations and some details left as exercises.

7.4 Cauchy's Theorem

In class, we tried to prove that if p divides the order of an abelian group, then there exists an element in G of order p.

However, it is actually true in general that if p divides the order of a group G, which may or may not be abelian, then G must have an element of order p.

This important result in group theory is known as **Cauchy's theorem**.

Cauchy's theorem is not especially difficult to prove.

The following proof of Cauchy's theorem is based on a proof of this result given in Fraleigh's *A First Course in Abstract Algebra*.

Theorem 7.15. Cauchy's Theorem*: Let p be a prime, and let G be a finite group such that p divides $|G|$. Then there exists an element in G of order p.*

Proof. Let X denote the following subset of the direct product G^p:

$$X = \{(g_1, g_2, \ldots, g_p) \in G^p \mid g_1 g_2 \cdots g_p = e\}.$$

It is natural to consider the cardinality of X. Given a choice of a first entry g_1 of an element in X, and a choice of a second entry g_2, and a choice of a third entry, and so forth, including a choice for a $(p-1)^{\text{th}}$ entry, we observe that the value of g_p must be uniquely determined: in particular, we have that $g_p = (g_1 g_2 \cdots g_{p-1})^{-1}$. We thus have that $|X| = |G|^{p-1}$. Consequently, p divides the order of X.

Let σ denote the cycle $(1, 2, 3, \ldots, p)$ in the symmetric group S_p. Write:

$$\sigma(g_1, g_2, \ldots, g_p) = \left(g_{\sigma(1)}, g_{\sigma(2)}, \ldots, g_{\sigma(p)}\right) = (g_2, g_3, \ldots, g_p, g_1),$$

letting $(g_1, g_2, \ldots, g_p) \in X$, and observe that since

$$g_1 g_2 \cdots g_p = e,$$

we have that

$$g_2 g_3 \cdots g_p = g_1^{-1},$$

and we thus have that

$$g_2 g_3 \cdots g_p g_1 = e,$$

[1] `http://garsia.math.yorku.ca/~zabrocki/math6121f16/documents/100616sylows.pdf`.

thus proving that

$$\sigma(g_1, g_2, \ldots, g_p) \in X.$$

More generally, we have that

$$\left(g_{\rho(1)}, g_{\rho(2)}, \ldots, g_{\rho(p)}\right) \in X$$

for a cyclic permutation ρ in the cyclic subgroup $\langle \sigma \rangle$ of S_p. We thus have that the cyclic group $\langle \sigma \rangle \leq S_p$ acts on the set X in a natural way, letting

$$*\colon \langle \sigma \rangle \times X \to X$$

denote the group action whereby

$$\rho * (g_1, g_2, \ldots, g_p) = \left(g_{\rho_1}, g_{\rho_2}, \ldots, g_{\rho_p}\right)$$

for $\rho \in \langle \sigma \rangle$ and $(g_1, g_2, \ldots, g_p) \in G$.

But the $\langle \sigma \rangle$-set X must be a disjoint union of orbits, say

$$\left(\mathrm{Orbit}(x_1) \uplus \mathrm{Orbit}(x_2) \uplus \cdots \uplus \mathrm{Orbit}(x_{n_1})\right) \uplus \left(\mathrm{Orbit}(y_1) \uplus \mathrm{Orbit}(y_2) \uplus \cdots \uplus \mathrm{Orbit}(y_{n_2})\right),$$

where $\mathrm{Orbit}(x_i)$ is a singleton set for all indices i and $\mathrm{Orbit}(y_i)$ is not a singleton set for all indices i. But since $|\langle \sigma \rangle| = p$, and since orders of the orbits of the $\langle \sigma \rangle$-set X divide $|\langle \sigma \rangle|$ by the orbit-stabilizer theorem, we may thus deduce that either

$$X = \mathrm{Orbit}(y)$$

for some element y or

$$X = \mathrm{Orbit}(x_1) \uplus \mathrm{Orbit}(x_2) \uplus \cdots \uplus \mathrm{Orbit}(x_p),$$

with $n_1 = p$. But it is clear that

$$\mathrm{Orbit}(e, e, \ldots, e) = \{(e, e, \ldots, e)\},$$

so X must be of the form

$$X = \mathrm{Orbit}(x_1) \uplus \mathrm{Orbit}(x_2) \uplus \cdots \uplus \mathrm{Orbit}(x_p),$$

which shows that there must be an element $a \neq e$ such that $a^p = e$. But then the order of a must be p since p is a prime: it cannot be the case that a^ℓ for some natural number $\ell < p$, because otherwise ℓ and p would be relatively prime, and this would contradict that $a \neq e$. $\square$