ALGEBRA HW 4

CLAY SHONKWILER

1

Let G be a p-group and let Φ be its Frattini subgroup.

(a): Show that if $g \in G$ then $g^p \in \Phi$.

Proof. Suppose $H \subset G$ is a maximal subgroup. Then, as we saw in class, since G is a p-group, H has index p and is normal in G. Then, if $\pi : G \to G/H$ is the standard projection, then

$$\pi(g^p) = \pi(g)^p = 1 \in G/H,$$

since $\#(G/H) = p$. Hence, since $\pi^{-1}(1) = H$, we see that $g^p \in H$. Since our choice of H was arbitary, we see that g^p is in every maximal subgroup, and so we can conclude that $g^p \in \Phi$. □

(b): Deduce that every element of G/Φ has order 1 or p.

Proof. Since π is surjective, every element in G/Φ is of the form $\pi(g)$ for some $g \in G$. Now, since as we showed in (a), $g^p \in \Phi$, we see that

$$\pi(g)^p = \pi(g^p) = 1 \in G/\Phi;$$

since p is prime, this means that the order of $\pi(g)$ is either 1 or p. □

(c): Conclude that G/Φ is isomorphic to $(\mathbb{Z}/p)^n = \mathbb{Z}/p \times \cdots \times \mathbb{Z}/p$ (with n factors) for some $n \geq 0$.

Proof. In problem set 3 question #6, we showed that G/Φ is abelian. Hence, by the fundamental theorem of finite abelian groups,

$$G/\Phi \simeq \mathbb{Z}/p_1^{\alpha_1} \times \cdots \times \mathbb{Z}/p_k^{\alpha_k}.$$

Now, if $a = (0, \ldots, 0, \gamma_i, 0, \ldots, 0) \in \mathbb{Z}/p_1^{\alpha_1} \times \cdots \times \mathbb{Z}/p_k^{\alpha_k}$ such that γ_i is a generator of $\mathbb{Z}/p_i^{\alpha_i}$, then a has order $p_i^{\alpha_i}$. Since every element of G/Φ has order 1 or p, we see that $p_i = p$ for all i and $\alpha_i = 0$ or 1 for all i; hence,

$$G/\Phi \simeq (\mathbb{Z}/p)^n$$

for some $n \geq 0$. □

2

If K is a group and S is a subset of K that generates K, we will call S a *minimal generating set* for K if no proper subset of S also generates K.

(a): Show that every minimal generating set of $(\mathbb{Z}/p)^n$ has exactly n elements.

Proof. Consider $(\mathbb{Z}/p)^n$ as a vector space over $\mathbb{Z}/p$. This is really a vector space, as it is closed under addition and scalar multiplication (multipliction by an element of $\mathbb{Z}/p$). Furthermore, we can define the natural inner product (just the sum of the component-wise products). Then clearly, the set

$$\{(1,0,\dots,0),(0,1,0,\dots,0),\dots,(0,0,\dots,1)\}$$

is linearly independent: if we let e_i be the element of the above set with a 1 in the ith coordinate and zeroes elsewhere, then $e_i \cdot e_j = 0$ for $i \neq j$. Also, this set generates $(\mathbb{Z}/p)^n$, since for all $a \in (\mathbb{Z}/p)^n$, $a = (a_1,\dots,a_n)$ and

$$a = \sum_{i=1}^{n} a_i e_i.$$

Hence, the above set forms a basis for $(\mathbb{Z}/p)^n$, and so any other basis must also consist of exactly n elements. Since a minimal generating set of $(\mathbb{Z}/p)^n$ is simply a basis for $(\mathbb{Z}/p)^n$ as a vector space, we see that any minimal generating set must have exactly n elements. □

(b): Prove or disprove: If G is any finite group, then any two minimal generating sets for G have the same number of elements.

Counter-example: Let $G = \mathbb{Z}/3 \times \mathbb{Z}/4$. Then certainly $\{(1,1)\}$ is a generating set of order 1 (and hence a minimal generating set), since the following shows the results of repeatedly adding $(1,1)$ to itself:

$$(2,2),(0,3),(1,0),(2,1),(0,2),(1,3),(2,0),(0,1),(1,2),(2,3),(0,0)$$

(we could also simply have noted that, since $(3,4) = 1$, $\mathbb{Z}/3 \times \mathbb{Z}/4$ is cyclic). On the other hand, $\{(1,0),(0,1)\}$ also generates $\mathbb{Z}/3 \times \mathbb{Z}/4$, which can be seen most easily by noting that $(1,0)+(0,1) = (1,1)$. However, it's clear that neither $(1,0)$ nor $(0,1)$ generates $\mathbb{Z}/3 \times \mathbb{Z}/4$ by itself, so we see that $\{(1,0),(0,1)\}$ is a minimal generating set of order 2.

♣

(c): Let G be a p-group with Frattini subgroup Φ, so that G/Φ is isomorphic to $(\mathbb{Z}/p)^n$. Show that

(i): Every minimal generating set for G has exactly n elements.

Proof. Suppose S is a minimal generating set with fewer than n elements. Then, if $\pi : G \to G/\Phi$ is the projection map, $\#(\pi(S)) < n$. Then, since we showed in 1(c) that $G/\Phi = (\mathbb{Z}/p)^n$ and in 2(a) that every minimal generating set of $(\mathbb{Z}/p)^n$ has exactly n elements, we see that $\pi(S)$ does not generate G/Φ. However, since π is surjective, this implies that S certainly cannot generate G. So we see that every minimal generating set for G must have at least n elements.

On the other hand, suppose S is a minimal generating set for G containing more than n elements. Then, since S generates G, $\pi(S)$ must generate G/Φ (by the result we proved in HW 2 #6), and so $\pi(S)$ must contain at least n elements. Hence, we can take a minimal generating set S' contained in $\pi(S)$. If $\pi^{-1}(S') \cap S$ contains more than n elements, then there are $s_1, s_2 \in \pi^{-1}(S') \cap S$ such that $\pi(s_1) = \pi(s_2)$. Then, again using the result in PS2#6, we see that

$$(\pi^{-1}(S') \cap S)\backslash\{s_2\}$$

generates G. Since this is a proper subset of S, we see that S is not a minimal generating set. Hence, we conclude that every minimal generating set of G contains exactly n elements. □

(ii): If T is a subset of G with exactly n elements, then T is a minimal generating set for G if and only if its image under $G \twoheadrightarrow G/\Phi$ is a minimal generating set for G/Φ.

Proof. Suppose T is a minimal generating set for G. Then, by (i), T contains exactly n elements. Furthermore, by PS2#6, since T generates G, $\pi(T)$ generates G/Φ. Since $\#(\pi(T)) \leq \#(T)$ and $\pi(T)$ is a generating set, we see that $\pi(T)$ contains exactly n elements and, thus, is a minimal generating set for G/Φ.

On the other hand, suppose $\pi(T)$ is a minimal generating set for G/Φ. Then, by PS2#6, T is a generating set for G. Then, by our work in part (a), T is a minimal generating set for G. □

3

For each n, $9 \leq n \leq 16$, answer the following questions:

(a): Is every group of order n cyclic?

(b): Is every group of order n abelian?

(c): Is every abelian group of order n cyclic?

Answer: Consider $n = 9$. Then, since 3 is not relatively prime to itself, $\mathbb{Z}/3 \times \mathbb{Z}/3$ is not cyclic, so we see that not every group of order 9 is cyclic and not every abelian group of order 9 is cyclic. Since these are the only abelian groups of order 9 and we know that groups of order p^2 for a prime p are abelian, this comprises the entire set of groups of order 9, so we can say that every group of order 9 is abelian.

Consider $n = 10$. Then $\mathbb{Z}/10 \simeq \mathbb{Z}/2 \times \mathbb{Z}/5$ since $(2, 5) = 1$ and, since these are the only abelian groups, we see that every abelian group of order 10 is cyclic. Now,

$$D_5 = \langle x, y | x^5 = y^2 = 1, yxy^{-1} = x^{-1}\rangle$$

is of order 10 but isn't abelian, so we see that every group of order 10 is not abelian and, thus, not all groups of order 10 are cyclic.

Consider $n = 11$. Then every subgroup of a group of order 11 must be of order 1 or 11, so each element except the identity is of order 11, so the only group of order 11 is $\mathbb{Z}/11$.

Consider $n = 12$. Then, since $(3, 4) = 1$, $\mathbb{Z}/12 \simeq \mathbb{Z}/3 \times \mathbb{Z}/4$. However, since $\mathbb{Z}/4$ is not isomorphic to $\mathbb{Z}/2 \times \mathbb{Z}/2$, we see that $\mathbb{Z}/12$ is not isomorphic to $\mathbb{Z}/3 \times \mathbb{Z}/2 \times \mathbb{Z}/2$, which isn't cyclic, so we know that not every group of order 12 is cyclic and not every abelian group of order 12 is cyclic. Furthermore,

$$D_6 = \langle x, y | x^6 = y^2 = 1, yxy^{-1} = x^{-1}\rangle$$

is of order 12 and non-abelian, so we see that not every group of order 12 is abelian.

Consider $n = 13$. By the same reasoning given in the case where $n = 11$, we see that $\mathbb{Z}/13$ is the only group of order 13, so the answer to all the questions is "yes".

Consider $n = 14$. Since $(2, 7) = 1$, $\mathbb{Z}/14 \simeq \mathbb{Z}/2 \times \mathbb{Z}/7$ and, since these are the only abelian groups of order 14, we see that every abelian group of order 14 is cyclic. Now,

$$D_7 = \langle x, y | x^7 = y^2 = 1, yxy^{-1} = x^{-1}\rangle$$

is a non-abelian group of order 14, so not every group of order 14 is abelian or cyclic.

Consider $n = 15$. Since $(3, 5) = 1$, $\mathbb{Z}/15 \simeq \mathbb{Z}/3 \times \mathbb{Z}/5$ and, since these are the only abelian groups of order 15, we see that every abelian group of order 15 is cyclic. Furthermore, since 3 does not divide $(5 - 1) = 4$, we can conclude, using the result proved in PS3#4(b) that any group of order 15 is abelian and, therefore, cyclic.

Consider $n = 16$. Then $\mathbb{Z}/16 \not\simeq \mathbb{Z}/4 \times \mathbb{Z}/4$, so not every (abelian) group of order 16 is cyclic. Furthermore,

$$D_8 = \langle x, y | x^8 = y^2 = 1, yxy^{-1} = x^{-1}\rangle$$

is a non-abelian group of order 16, we see that not every group of order 16 is abelian.

♣

4

(a): Show that every element of A_5 is conjugate (in A_5) to exactly one of the following five elements:

$$1, (123), (12)(24), (12345), (12354).$$

Determine the number of elements conjugate to each.

Proof. First, note that all elements of A_5 can be written in one of the following ways:

$$\begin{gathered} 1 \\ (abc) \\ (ab)(cd) \\ (abcde) \end{gathered}$$

Now, recall that $\#A_5 = 60 = 2^2 \cdot 3 \cdot 5$. Furthermore, note that conjugacy classes must consist entirely of elements of the same order. Then $\langle (123) \rangle$ is a 3-Sylow subgroup, as are all subgroups of the form $\langle (abc) \rangle$; hence, for $(abc) \in A_5$, there exists $\sigma \in A_5$ such that

$$\langle (123) \rangle = \sigma^{-1} \langle (abc) \rangle \sigma.$$

Hence, either

$$(abc) = \sigma(123)\sigma^{-1}$$

or

$$\begin{aligned} (abc) = \sigma(123)^2)\sigma^{-1} = \sigma(132)\sigma^{-1} &= \sigma(23)(45)(123)(23)(45)\sigma^{-1} \\ &= (\sigma(23)(45))(123)(\sigma(23)(45))^{-1}; \end{aligned}$$

in either case, we see that (abc) is conjugate to (123). Since our choice of (abc) was arbitrary, we conclude that all elements of this form are conjugate to (123). There are $12 + 6 + 2 = 20$ elements of this form, so we conclude that the conjugacy class of (123) consists of 20 elements, namely all the 3-cycles.

Now, $\langle (12)(34), (13)(24) \rangle = \{1, (12)(34), (13)(24), (14)(23)\}$ is a 2-Sylow subgroup of A_5; if $(ab)(cd) \in A_5$ then, since $\langle (ab)(cd) \rangle$ is a 2-group and all 2-groups must be contained in a 2-Sylow subgroup, which in turn must be conjugate to all other 2-Sylow subgroups, we see that

$$\langle (12)(34), (13)(24) \rangle \supset \sigma^{-1} \langle (ab)(cd) \rangle \sigma$$

for some $\sigma \in A_5$. Hence, either

$$(ab)(cd) = \sigma(12)(34)\sigma^{-1}$$

or

$$\begin{aligned} (ab)(cd) = \sigma(13)(24)\sigma^{-1} &= \sigma(234)(12)(34)(243)\sigma^{-1} \\ &= (\sigma(234))(12)(34)(\sigma(234))^{-1} \end{aligned}$$

or

$$\begin{aligned} (ab)(cd) = \sigma(14)(23)\sigma^{-1} &= \sigma(123)(12)(34)(132)\sigma^{-1} \\ &= (\sigma(123))(12)(34)(\sigma(123))^{-1}. \end{aligned}$$

In any case, $(ab)(cd)$ is conjugate to $(12)(34)$; since there are 15 elements of this form in A_5, we conclude that the conjugacy class of $(12)(34)$ consists of 15 elements.

Finally, $\langle(12345)\rangle$ is a 5-Sylow subgroup of A_5, and thus, for $(abcde) \in A_5$, there exists $\sigma \in A_5$ such that

$$\langle(12345)\rangle = \sigma^{-1}\langle(abcde)\rangle\sigma.$$

Hence, either

$$(abcde) = \sigma(12345)\sigma^{-1}$$

or

$$\begin{aligned}(abcde) = \sigma(12345)^2\sigma^{-1} &= \sigma(13524)\sigma^{-1}\\ &= (\sigma(235))(12354)(\sigma(235))^{-1}\end{aligned}$$

or

$$\begin{aligned}(abcde) = \sigma(12345)^3\sigma^{-1} &= \sigma(14253)\sigma^{-1}\\ &= (\sigma(243))(12354)(\sigma(243))^{-1}\end{aligned}$$

or

$$\begin{aligned}(abcde) = \sigma(12345)^4\sigma^{-1} &= \sigma(15432)\sigma^{-1}\\ &= (\sigma(25)(34))(12345)(\sigma(25)(34))^{-1}.\end{aligned}$$

In the first and fourth cases, we see that $(abcde)$ is conjugate to (12345); in the second and third that $(abcde)$ is conjugate to (12354). Furthermore, of the 4 elements of $\langle(abcde)\rangle$, exactly two are conjugate to (12345) and exactly two to (12354). Hence, we see that every 5-cycle is conjugate to one of these two and that, furthermore, either the 5-cycles constitute a single conjugacy class of order 24 or two conjugacy classes each of order 12. Now, by PS1#4(a), if C represents the centralizer of (12345), then the order of the conjugacy class of (12345) is equal to $(A_5 : C)$. We've just seen that this order is either 12 or 24; however, it cannot be the case that $(A_5 : C) = 24$, since $60/24 = 2.5$. Thus, we conclude that of the 24 5-cycles, 12 are conjugate to (12345) and the remaining 12 are conjugate to (12354).

Note that, since $1 + 20 + 15 + 12 + 12 = 60$, we've exhausted all elements of A_5. □

(b): Deduce that A_5 is simple.

Proof. First, suppose that $N \lhd A_5$ and that $\sigma \in A_5$. Then, for any $\tau \in A_5$, $\tau N \tau^{-1} = N$, so

$$\tau\sigma\tau^{-1} \in N,$$

so the entire conjugacy class of σ is contained in N. Since this is true for all elements of N, we see that N is the union of conjugacy classes and, hence, that the order of N is the sum of the orders of conjugacy classes, which we computed in part (a) above. Since $1 \in N$, these are the only possibilities for the order of N:

$$\begin{aligned}
&1 \\
&16 &&= 1 + 15 \\
&21 &&= 1 + 20 \\
&25 &&= 1 + 12 + 12 \\
&28 &&= 1 + 12 + 15 \\
&33 &&= 1 + 12 + 20 \\
&36 &&= 1 + 15 + 20 \\
&45 &&= 1 + 12 + 12 + 20 \\
&48 &&= 1 + 12 + 15 + 20 \\
&60 &&= 1 + 12 + 12 + 15 + 20
\end{aligned}$$

Now, the only numbers on this list that divide $60 = \#A_5$ are 1 and 60, so we see that N is either trivial or all of A_5. Hence, we conclude that A_5 is simple. □

5

Suppose that $N \lhd S_5$.

(a): Show that if N contains a transposition (a, b) then $N = S_5$.

Proof. First, note that for $\sigma \in S_5$, $\sigma = (abc)$ or $(abc)(de)$ or $(abcd)$ or $(abcde)$. However,

$$\begin{aligned}
(ac)(ab) &= (abc) \\
(ac)(ab)(de) &= (abc)(de) \\
(ad)(ac)(ab) &= (abcd) \\
(ae)(ad)(ac)(ab) &= (abcde)
\end{aligned}$$

So σ is the product of transpositions, so we see that the transpositions generate S_5. Now, suppose $(ab) \in N$. Let $(cd) \in S_5$. Then

$$(bd)(ac)(ac)(bd) = 1$$

so $((bd)(ac))^{-1} = (ac)(bd)$ and

$$(bd)(ac)(ab)(ac)(bd) = (cd)$$

so $(cd) \in N$. Since our choice of (cd) was arbitrary, we see that N contains all of S_5 and, since the transpositions generate S_5, $N = S_5$. □

(b): Show that if $N \cap A_5 = 1$ and $\sigma \in N$, then either $\sigma = 1$ or else σ is a transposition.

Proof. Consider σ^2. If $\sigma^2 = 1$ then the order of σ is 1 or 2, and, since the only elements of S_5 of order 2 that are not in A_5 are the transpositions (the only other possibilities being elements of the form $(ab)(cd)$), σ is a transposition. If $\sigma^2 \neq 1$ then the order of σ is > 2. Since the order of elements of S_5 are determined by the l.c.m. of the lengths of the cycle in the unique cycle decomposition, the order of σ must be 3, 4, 5 or 6. If 3 then $\sigma = (abc) = (ac)(ab) \in A_5$. If 4, then $\sigma = (abcd)$, and so

$$\sigma^2 = (abcd)(abcd) = (ac)(bd) \in A_5.$$

If 5, then $\sigma = (abcde) = (ae)(ad)(ac)(ab) \in A_5$. If 6 then $\sigma = (abc)(de)$, so

$$\sigma^2 = (abc)(de)(abc)(de) = (acb) \in A_5.$$

Hence, we conclude that $\sigma^2 = 1$ and so σ is either 1 or a transposition. □

(c): Conclude that $N = 1$, A_5, or S_5.

Proof. Suppose $N \cap A_5 = 1$. Then any non-identity element in N must be a transposition (by our work in (b)) and hence (by our work in (a)), it must be the case that $N = S_5$. However, since $S_5 \cap A_5 \neq 1$, it must be the case that $N = 1$.

On the other hand, if $N \cap A_5 \neq 1$, then consider $g \in N \cap A_5$. Let $a \in A_5$. Then, since $N \lhd S_5$, $aga^{-1} \in N$; on the other hand, since $a, g \in A_5$, $aga^{-1} \in A_5$. Thus, we see that $aga^{-1} \in N \cap A_5$, so $N \cap A_5 \lhd A_5$. Hence, by the result proven in 4(b), $N \cap A_5 = A_5$. Then this forces either N to be A_5 or N to be S_5, since A_5 is maximal in S_5. □

6

Show that the three definitions of "solvable" are equivalent: that there is a sequence of subgroups $1 = G_0 \lhd G_1 \lhd \cdots \lhd G_n = G$ with each G_i/G_{i-1} *abelian* (respectively, *cyclic* or *cyclic of prime order*).

Proof. If we label the three definitions as follows:

(i): abelian
(ii): cyclic
(iii): cyclic of prime order

Then it's clear that (iii) ⇒ (ii) ⇒ (i). Hence, it suffices to show that (i) ⇒ (iii). □

DRL 3E3A, University of Pennsylvania
E-mail address: shonkwil@math.upenn.edu