

ALGEBRA HW 5

CLAY SHONKWILER

4.2.11

Let G be a finite group and let $\pi : G \rightarrow S_G$ be the left regular representation. Prove that if x is an element of G of order n and $|G| = mn$, then $\pi(x)$ is a product of m n -cycles. Deduce that $\pi(x)$ is an odd permutation if and only if $|x|$ is even and $\frac{|G|}{|x|}$ is odd.

Proof. Let $g \in G$ where g is not the identity element. Then $x^a g \neq g$ unless $a = n$. To see this, it is clear that $x^n g = eg = g$ and, if $x^a g = g$ for some $a < n$, then $x^a = e$, which contradicts the fact that x has order n . Hence, when we associate g with a number $p_g \in \{1, \dots, n\}$,

$$(p_g x p_g x^2 p_g \dots x^{n-1} p_g)$$

is an n -cycle in $\pi(x)$. To completely construct $\pi(x)$, we need only pick some $h \in G$ where $h \neq x^a g$ for any $a \in \{1, \dots, n\}$. We will be able to iterate this process $\frac{|G|}{n} = \frac{mn}{n} = m$ times, so $\pi(x)$ consists of m n -cycles.

From the previous chapter, we know that $\pi(x)$ is odd if and only if the number of cycles of even length in its cycle decomposition is odd. Since every cycle in its decomposition is of length $n = |x|$ and the number of such cycles is $\frac{|G|}{|x|}$, this means $\pi(x)$ is odd if and only if $|x|$ is even and $\frac{|G|}{|x|}$ is odd. \square

4.3.24

Assume H is a proper subgroup of the finite group G . Prove $G \neq \cup_{g \in G} gHg^{-1}$, i.e., G is not the union of the conjugates of any proper subgroup.

In order to prove this, we will need the following lemma.

Lemma 0.1. *If M is a maximal subgroup of G that is not normal, then the number of nonidentity elements of G contained in conjugates of M is at most $(|M| - 1)|G : M|$.*

Proof. First, we note that if M is a maximal subgroup of G , then either $N_G(M) = M$ or $N_G(M) = G$. This is simply because $M \leq N_G(M) \leq G$ and M is maximal. Since M is not normal in G , this means $N_G(M) = M$. Now, from Proposition 6 in the textbook, we know that the number of conjugates of M in G is

$$|G : N_G(M)| = |G : M|.$$

Furthermore, the number of non-identity elements in any conjugate of M is no greater than $|M| - 1$, the number of non-identity elements of M . Therefore, the number of non-identity elements of G contained in conjugates of M is at most $(|M| - 1)|G : M|$. \square

Now, let M be a maximal subgroup of G containing H . Certainly

$$\bigcup_{g \in G} gHg^{-1} \subseteq \bigcup_{g \in G} gMg^{-1}.$$

Furthermore, we know that the number of non-identity elements of G contained in $|\bigcup_{g \in G} gMg^{-1}|$ is no greater than $(|M| - 1)|G : M|$ by the previous exercise. Since $|G : M| = |G|/|M|$, we know that $(|M| - 1)|G : M| = |G| - 2$, so there is at least one non-identity element of G not contained in $\bigcup_{g \in G} gMg^{-1}$ and, therefore, not contained in $\bigcup_{g \in G} gHg^{-1}$. We conclude that

$$G \neq \bigcup_{g \in G} gHg^{-1}.$$

♣

4.4.18

Fix an integer $n \geq 2$ with $n \neq 6$.

(a) Prove that the automorphism group of a group G permutes the conjugacy classes of G , i.e., for each $\sigma \in \text{Aut}(G)$ and each conjugacy class \mathcal{K} of G the set $\sigma(\mathcal{K})$ is also a conjugacy class of G .

Proof. Let \mathcal{K} be a conjugacy class of G , let σ be an automorphism of G and let $k_i, k_j \in \sigma(\mathcal{K})$. Then $k_i = \sigma(h_i)$ and $k_j = \sigma(h_j)$ for some $h_i, h_j \in \mathcal{K}$. Since \mathcal{K} is a conjugacy class of G ,

$$k_i = \sigma(h_i) = \sigma(gh_jg^{-1}) = \sigma(g)\sigma(h_j)\sigma(g)^{-1} = \sigma(g)k_j\sigma(g)^{-1}$$

for some $g \in G$, so k_i and k_j are conjugate. Since our choice of k_i and k_j was arbitrary, we conclude that $\sigma(\mathcal{K})$ is a conjugacy class. \square

(b) Let \mathcal{K} be the conjugacy class of transpositions in S_n and let \mathcal{K}' be the conjugacy class of any element of order 2 in S_n that is not a transposition. Prove that $|\mathcal{K}| \neq |\mathcal{K}'|$. Deduce that any automorphism of S_n sends transpositions to transpositions.

Proof. Let σ be a transposition in S_n . Then, by 4.3.33, the size of the conjugacy class \mathcal{K} of σ is

$$|\mathcal{K}| = \frac{n!}{(1!2^1)((n-2)!1^{n-2})} = \frac{n!}{2(n-2)!} = \frac{n(n-1)}{2}.$$

Now, let ρ be any element of order 2 in S_n . Then ρ consists of m 2-cycles for some $m \in \mathbb{Z}$ such that $2m \leq n$. Hence, the size of the conjugacy class \mathcal{K}' of ρ is

$$|\mathcal{K}'| = \frac{n!}{(m!2^m)((n-2m)!1^{n-2m})}.$$

So long as $n \neq 6$, we see that $|\mathcal{K}| \neq |\mathcal{K}'|$. Since, by (a), any automorphism of S_n must map \mathcal{K} onto a conjugacy class of elements of order 2, we see that any automorphism of S_n sends transpositions to transpositions. \square

(c) Prove that for each $\sigma \in \text{Aut}(S_n)$

$$\sigma : (12) \mapsto (ab_2), \quad \sigma : (13) \mapsto (ab_3), \quad \dots, \quad \sigma : (1n) \mapsto (ab_n)$$

for some distinct integers $a, b_2, b_3, \dots, b_n \in \{1, 2, \dots, n\}$.

Proof. We showed above that σ maps transpositions to transpositions, so we know that

$$\sigma : (12) \mapsto (ab_2)$$

for some $a, b_2 \in \{1, \dots, n\}$. Now, for $j \in \{3, \dots, n\}$, we know that $(12)(1j) = (1j_2)$, which has order 3, so the image of $(12)(1j)$ has order 3. Since $(1j)$ must map to a transposition, this means that $\sigma : (1j) \mapsto (1b_j)$ or $\sigma : (1j) \mapsto (kb_2)$ for some $k, b_j \neq a, b_2$. \square

(d) Show that $S = (12), (13), \dots, (1n)$ generate S_n and deduce that any automorphism of S_n is uniquely determined by its action on these elements. Use (c) to show that S_n has at most $n!$ automorphisms and conclude that $\text{Aut}(S_n) = \text{Inn}(S_n)$ for $n \neq 6$.

Proof. First, we recall that any element of S_n can be written as a product of transpositions, so it suffices to show that every transposition can be written as a product of transpositions of the form $(1k)$ for $k = 2, \dots, n$. Let (ab) be a transposition. Then

$$(ab) = (1a)(1b)(1a).$$

So we see that any element of S_n can be written as a product of elements of S , so S generates S_n . Hence, any automorphism of S_n is completely determined by its action on the elements of S . If $\sigma \in \text{Aut}(S_n)$, then, in the notation from (c) above, we can let any of the n elements be a , any of the remaining $n - 1$ elements be b_1 , etc. In this way, we see that there are $n(n - 1)$ choices for (ab_1) , $n - 2$ choices for (ab_2) and so on. Therefore, the maximum number of possible automorphisms σ is

$$(n(n - 1))(n - 2)(n - 3) \dots 3 \cdot 2 \cdot 1 = n!$$

Now, since there are $n!$ elements of S_n , there are $n!$ inner automorphisms of S_n , so we conclude that $\text{Aut}(S_n) = \text{Inn}(S_n)$ (remembering that $n \neq 6$). \square

5.5.8

Construct a non-abelian group of order 75. Classify all groups of order 75 (there are three of them).

Let $N = \mathbb{Z}/5\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z}$. Then, by Proposition 4.17(3),

$$A = \text{Aut}(\mathbb{Z}/5\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z}) \simeq GL_2(\mathbb{F}_5).$$

From Chapter 1, we know $|A| = (5^2 - 1)(5^2 - 5) = 480$, so, by Cauchy's theorem, we know there exists $z \in A$ such that $|z| = 3$. Hence, we can

identify the subgroup generated by z with $\mathbb{Z}/3\mathbb{Z}$; call this identified subgroup $\overline{\mathbb{Z}/3\mathbb{Z}}$. Now, let $\phi_0 : \overline{\mathbb{Z}/3\mathbb{Z}} \rightarrow \text{Aut}(N)$ such that ϕ maps $A \in \overline{\mathbb{Z}/3\mathbb{Z}}$ to the automorphism of N obtained by conjugation by A . Then, if $A, B \in \overline{\mathbb{Z}/3\mathbb{Z}}$,

$$\phi_0(AB) = (C \mapsto (AB)C(AB)^{-1} = A(BCB^{-1})A^{-1}) = \phi_0(A) \circ \phi_0(B)$$

so ϕ_0 is a homomorphism and defines the semi-direct product

$$N \rtimes_{\phi_0} \mathbb{Z}/3\mathbb{Z},$$

which has order 75 and is non-abelian, since ϕ_0 is non-trivial.

Certainly $\mathbb{Z}/75\mathbb{Z} = \mathbb{Z}/25\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$ and $\mathbb{Z}/5\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$ are groups of order 75. $\mathbb{Z}/75\mathbb{Z}$ has an element of order 75, whereas $\mathbb{Z}/5\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$ has no elements of order greater than 15, so these groups are not isomorphic. By the Fundamental Theorem of Finitely Generated Abelian Groups, these are the only abelian groups of order 75. Now, let G be a non-abelian group of order 75. Then, by Sylow, G has a normal subgroup N of order 25 and a subgroup P of order 3, which is isomorphic to $\mathbb{Z}/3\mathbb{Z}$. Hence,

$$G = N \rtimes_{\phi} \mathbb{Z}/3\mathbb{Z}$$

where $\phi : \mathbb{Z}/3\mathbb{Z} \rightarrow \text{Aut}(N)$ is a homomorphism. Since $\text{Aut}(\mathbb{Z}/25\mathbb{Z}) \simeq (\mathbb{Z}/25\mathbb{Z})^{\times}$, which has order 20, the only possible such ϕ when $N = \mathbb{Z}/25\mathbb{Z}$ is the trivial homomorphism, so this semi-direct product will simply yield an abelian group. Hence, to get a non-abelian group, it must be the case that $N \simeq \mathbb{Z}/5\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z}$, the only other group of order 25. Now, N contains no elements of order 3, so

$$N \cap P = \{1\}$$

so, by Theorem 12, $G \simeq NP \simeq N \rtimes_{\phi} P$ where ϕ is the homomorphism from P to $\text{Aut}(N)$ that sends $p \in P$ to the automorphism of conjugation by p in N , precisely what we defined above. Therefore, the non-abelian group we constructed above is the only non-abelian group of order 75.

1

Show that if G is a finite group, and $H \neq G$ is a proper subgroup of G , then G is not equal to the union of conjugates of H .

This is problem 4.3.24 above.

2

Let $G = \text{Aut}((\mathbb{Z}/12\mathbb{Z}) \times S_3)$. How many elements does G have? Determine the structure of G .

Answer: G has 24 elements and is isomorphic to $(\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}) \times S_3$. To see this, we note that $N = \mathbb{Z}/12\mathbb{Z} \times \{1\} \simeq \mathbb{Z}/12\mathbb{Z}$ is normal in $\mathbb{Z}/12\mathbb{Z} \times S_3$, so any automorphism must map N to a cyclic normal subgroup N' of order 12. That means $N' = \langle a, \sigma \rangle$ for $a \in (\mathbb{Z}/12\mathbb{Z})^{\times}$, $\sigma \in S_3$. Certainly such a σ must either be the identity permutation or have order 3. If $|\sigma| = 3$, then let $\rho \in S_3$ such that $|\rho| = 2$. Then, if $b \in \mathbb{Z}/12\mathbb{Z}$,

$$(b, \rho) \cdot (a, \sigma) \cdot (-b, \rho) = (a, \rho\sigma\rho).$$

However, $\rho\sigma\rho \neq \sigma$, so $(a, \rho\sigma\rho) \notin N'$, contradicting the fact that N' is normal. Therefore, we see that $N' = N$. Hence, we see that N is a characteristic subgroup of $\mathbb{Z}/12\mathbb{Z} \times S_3$.

Now, $M = \{0\} \times S_3 \simeq S_3$ is normal in $\mathbb{Z}/12\mathbb{Z} \times S_3$, so any automorphism ϕ of $\mathbb{Z}/12\mathbb{Z} \times S_3$ must map M to a normal subgroup isomorphic to S_3 . Now, the elements of order 2 in $\mathbb{Z}/12\mathbb{Z} \times S_3$ are of the form $(0, \gamma)$ or $(6, \gamma)$, where $|\gamma| = 2$. Let ρ_1, ρ_2, ρ_3 denote the elements of order 2 in S_3 . If $\phi : (0, \rho_1) \mapsto (6, \rho_i)$, then it must be true that $\phi : (0, \rho_2) \mapsto (6, \rho_j)$ or $\phi : (0, \rho_3) \mapsto (6, \rho_j)$. Suppose, without loss of generality, that $\phi : (0, \rho_2) \mapsto (6, \rho_j)$. Then, necessarily, $\phi : (0, \rho_3) \mapsto (0, \rho_k)$. Furthermore

$$\phi : (0, \rho_1\rho_3) = (0, \rho_1) \cdot (0, \rho_3) \mapsto (6, \rho_i) \cdot (0, \rho_k) = (6, \rho_i\rho_k)$$

However, $\rho_1\rho_3 = \rho_2\rho_1$ and

$$\phi : (0, \rho_2\rho_1) = (0, \rho_2) \cdot (0, \rho_1) \mapsto (6, \rho_j) \cdot (6, \rho_i) = (0, \rho_j\rho_i).$$

Hence, we see that $(6, \rho_i\rho_k) = (0, \rho_j\rho_i)$, a clear contradiction. Hence, ϕ must map M into itself. Since our choice of automorphism ϕ was arbitrary, we see that M is a characteristic subgroup of $\mathbb{Z}/12\mathbb{Z} \times S_3$.

Therefore, we can distribute as follows:

$$\text{Aut}(\mathbb{Z}/12\mathbb{Z} \times S_3) \simeq \text{Aut}(\mathbb{Z}/12\mathbb{Z}) \times \text{Aut}(S_3).$$

We know that $\text{Aut}(\mathbb{Z}/12\mathbb{Z}) = (\mathbb{Z}/12\mathbb{Z})^\times \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ and that $\text{Aut}(S_3) = \text{Inn}(S_3) \simeq S_3$, so

$$G \simeq (\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}) \times S_3,$$

a group with $4 \cdot 6 = 24$ elements.



3

Let p be a prime number, and let $A = (\mathbb{Z}/p^3\mathbb{Z}) \times (\mathbb{Z}/p^5\mathbb{Z})$, with the group law written additively. Let $[p] : A \rightarrow A$ be the endomorphism of A sending every element x to px . Let $A[p]$ denote the kernel of $[p]$, A/pA denote the quotient of A by the image of $[p]$.

(a) Prove that every nontrivial subgroup $B \neq \{0\}$ of A intersects $A[p]$ nontrivially.

Proof. Since the order of A is p^8 , B must have order p^b for some $b \in \{1, \dots, 7\}$. By Cauchy, B contains an element a of order p . Now,

$$[p](a) = pa = 0$$

since the order of a is p , so

$$A[p] \cap B \ni a.$$

□

(b) Prove that the image in A/pA of any proper subgroup $B \neq A$ of A is a proper subgroup of A/pA .

Proof. □

(c) Show that there is a bijection between $\text{End}(A)$ and the set of all pairs $(x, y), x, y \in A$ such that $p^3x = 0$ in A .

(d) Determine the cardinality of $\text{Aut}(A)$.

4

Let p be a prime number. It is clear that any two elements of $SL_2(\mathbb{F}_p)$ which are conjugate in $SL_2(\mathbb{F}_p)$ are conjugate in $GL_2(\mathbb{F}_p)$. For $p = 3, 5$, decide whether the converse is true. Give a proof if the converse is true; exhibit two elements of $SL_2(\mathbb{F}_p)$ which are conjugate in $GL_2(\mathbb{F}_p)$ but not in $SL_2(\mathbb{F}_p)$ otherwise.

Counter-Example in $GL_2(\mathbb{F}_p)$: Clearly,

$$A = \begin{pmatrix} 1 & 1 \\ 1 & 2 \end{pmatrix}, B = \begin{pmatrix} 0 & 1 \\ 2 & 0 \end{pmatrix} \in SL_2(\mathbb{F}_3)$$

and are conjugate in $GL_2(\mathbb{F}_5)$, since

$$\begin{pmatrix} 2 & 1 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 1 \\ 1 & 2 \end{pmatrix} = \begin{pmatrix} 3 & 4 \\ 1 & 2 \end{pmatrix} = \begin{pmatrix} 4 & 0 \\ 3 & 4 \end{pmatrix} \begin{pmatrix} 2 & 1 \\ 0 & 1 \end{pmatrix}.$$

Now, suppose A and B are conjugate in $SL_2(\mathbb{F}_p)$. Then there exists a matrix

$$C = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(\mathbb{F}_p) \text{ such that}$$

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} 1 & 1 \\ 1 & 2 \end{pmatrix} = \begin{pmatrix} 4 & 0 \\ 3 & 4 \end{pmatrix} \begin{pmatrix} a & b \\ c & d \end{pmatrix},$$

which is to say

$$\begin{pmatrix} a+b & a+2b \\ c+d & c+2d \end{pmatrix} = \begin{pmatrix} 4a & 4b \\ 3a+4c & 3b+4d \end{pmatrix}.$$

From the top-left terms, we see that $a = 2b$, and from the bottom-left terms, that $c + d = 3a + 4c$. Since $3a = 3(2b) = 6b = b$, we can substitute in the above equation and subtract from the equality suggested by the bottom-right terms:

$$\begin{array}{r} c + 2d = 3b + 4d \\ - c + d = b + 4c \\ \hline \end{array}$$

$$d = 2b + 4d - 4c$$

Solving for d , we see that $d = b - 2c$. Now, recalling that

$$1 = \det A = ad - bc$$

and substituting for a and d yields

$$1 = ad - bc = 2b(b - 2c) - bc = 2b^2 - 4bc - bc = 2b^2 + (bc - bc) = 2b^2.$$

Since $2^{-1} = 3$ in \mathbb{F}_5 , this implies that $b^2 = 3$. This, however, is impossible, as

$$0^2 = 0, \quad 1^2 = 1, \quad 2^2 = 4, \quad 3^2 = 4, \quad 4^2 = 1$$

Therefore, A and B are not conjugate in $SL_2(\mathbb{F}_p)$ even though they are in $GL_2(\mathbb{F}_p)$.



(Challenge/Extra credit) The same question, but for an arbitrary prime number p . And if you solve this question, do come to CLC and/or CB to show off!

DRL 3E3A, UNIVERSITY OF PENNSYLVANIA
E-mail address: shonkwil@math.upenn.edu