August 2014 Algebra Prelim

Sarah Arpin

1

Let G be a group. Let $H \trianglelefteq G$ be a normal subgroup of prime index p. Let $a \in H$. Suppose the conjugacy class of a inside G is of size m. Show that the conjugacy class of a inside H is of size either m or m/p,

Solution:
The number of conjugates of an element a in G is equal to the index of the centralizer: $[G : C_G(a)] = m$. The number of conjugates of a in H is the index of the centralizer of a in H: $[H : C_H(a)]$. This is the value we need to find.
Note: $C_G(a) \cap H = C_H(a)$.
Since H is a normal subgroup, we can apply the second isomorphism theorem to get:

$$C_G(a)H/H \cong C_G(a)/C_H(a)$$

This implies that the indices are equal:

$$[C_G(a)H : H] = [C_G(a) : C_H(a)]$$

Then, since we know the index of H in G:

$$\begin{aligned} p &= [G : H] \\ &= [G : C_G(a)H][C_G(a)H : H] \end{aligned}$$

Since p is prime, we have either $[C_G(a)H : H] = 1$ or p. By the equality given in the second isomorphism theorem, this means $[C_G(a) : C_H(a)] = 1$ or p.

Case 1: If $[C_G(a) : C_H(a)] = 1$, then:

$$\begin{aligned} [G : C_H(a)] &= [G : C_H(a)] \\ [G : C_G(a)][C_G(a) : C_H(a)] &= [G : H][H : C_H(a)] \\ m \cdot 1 &= p \cdot [H : C_H(a)] \end{aligned}$$

So in this case $[H : C_H(a)] = m/p$ and this is the size of the conjugacy class of a inside H.

Case 2: If $[C_G(a) : C_H(a)] = p$, then:

$$\begin{aligned} [G : C_H(a)] &= [G : C_H(a)] \\ [G : C_G(a)][C_G(a) : C_H(a)] &= [G : H][H : C_H(a)] \\ m \cdot p &= p \cdot [H : C_H(a)] \\ m &= H : C_H(a)] \end{aligned}$$

So in this case $[H : C_H(a)] = m$ and this is the size of the conjugacy class of a inside H.

□

2

Classify all groups of order 253.

Solution:
Let G be a finite group, $|G| = 253 = 11 \cdot 23$.
Since 11 and 23 are prime, by the Fundamental Theorem of Finitely Generated Abelian Groups there is only one abelian group of order 253, namely $\mathbb{Z}_{253}$, because there is only one invariant factor.
If G is not abelian, investigate the Sylow p-subgroups of G by using Sylow's Theorems:
The number of Sylow 11-subgroups of G is n_{11}, where $n_{11} \equiv 1 \pmod{11}$ and $n_{11} \mid 23$. This means that $n_{11} = 1$ or 23.
The number of Sylow 23-subgroups of G is n_{23}, where $n_{23} \equiv 1 \pmod{23}$ and $n_{23} \mid 11$. This means that $n_{23} = 1$.
Let P_{23} denote the unique Sylow 23-subgroup of G. Since P_{23} is unique, it must be a normal subgroup of G. *(All conjugates of a Sylow p-subgroup must be Sylow p-subgroups, so if there is only one Sylow 23-subgroup P_{23}, all of the conjugates of P_{23} must be equal to P_{23}, and thus $P_{23} \trianglelefteq G$.)*
Let $P_{11} \in \mathrm{Syl}_{11}(G)$.
The non-identity elements of P_{11} are all of order 11, and the non-idenity elements of P_{23} are all of order 23, so $P_{11} \cap P_{23} = \{1\}$.
This means we can construct a semidirect product $G \cong P_{23} \rtimes P_{11}$ with order $|P_{23}| \cdot |P_{11}| = 253$.
Let the action of P_{11} on P_{23} be left multiplication, so that for $p \in P_{11}, q \in P_{23}$:

$$p \cdot q = pq$$

We need to show that this semi-direct product is unique:
For any other choice of action $\varphi : P_{11} \to \mathrm{Aut}(P_{23})$ where φ is a homomorphism, we need to show

$$P_{23} \rtimes_\varphi P_{11} \cong P_{23} \rtimes P_{11}$$

The homomorphisms $\varphi \in \mathrm{Hom}(P_{11}, \mathrm{Aut}(P_{23}))$, so we need to find the size of $\mathrm{Hom}(P_{11}, \mathrm{Aut}(P_{23}))$.

$$\mathrm{Hom}(P_{11}, \mathrm{Aut}(P_{23})) \cong \mathrm{Hom}(\mathbb{Z}_{11}, \mathrm{Aut}(\mathbb{Z}_{23})) \cong \mathrm{Hom}(\mathbb{Z}_{11}, \mathbb{Z}_{23}^\times)$$

Then, $\left|\mathrm{Hom}(\mathbb{Z}_{11}, \mathbb{Z}_{23}^\times)\right| = 11$, since $(11, 22) = 11$.
One of these homomorphisms is the trivial map to the identity, and this one gives us the cyclic direct product we have already mentioned.
It remains to show that the remaining ten homomorphisms in $\mathrm{Hom}(P_{11}, \mathrm{Aut}(P_{23}))$ product isomorphic semidirect products.
Equivalently, we can show that if φ, ψ are two nontrivial homomorphisms in $\mathrm{Hom}(P_{11}, \mathrm{Aut}(P_{23}))$, then $\varphi(P_{11}) = \psi(P_{11})$.
If the images of P_{11} are isomorphic, then the semidirect products are isomorphic:

$$\varphi(P_{11}) = \psi(P_{11}) \Rightarrow P_{23} \rtimes_\varphi P_{11} \cong P_{23} \rtimes_\psi P_{11}$$

Note that $\mathrm{Aut}(P_{23})$ is cyclic, so it has a unique subgroup of order 11, say $\langle\gamma\rangle$ with $|\gamma| = 11$.
For each nontrivial $\varphi_i \in \mathrm{Hom}(P_{11}, \mathrm{Aut}(P_{23}))$, the image of P_{11} under φ_i needs to be a subgroup of $\mathrm{Aut}(P_{23})$ whose order divides 11. Since 11 is prime, our only options are 1 and 11. 1 is already handled in the trivial case where the semidirect product ends up being direct, and for subgroups of order 11 we only have one choice: $\langle\gamma\rangle$.
For each of the ten nontrivial $\varphi_i \in \mathrm{Hom}(P_{11}, \mathrm{Aut}(P_{23}))$, there exists a generator $y_i \in P_{11}$ such that $\varphi_i(y_i) = \gamma$.
Then, $\varphi_i(P_{11}) = \varphi_j(P_{11})$ for each nontrivial $\varphi_i, \varphi_j \in \mathrm{Hom}(P_{11}, \mathrm{Aut}(P_{23}))$, because the images are completely determined by the actions of the homomorphisms on the generators.
Thus, there is only one distinct nontrivial semidirect product, so there are two possibilities for groups of order 253:

$$G \cong \mathbb{Z}_{253} \text{ or } G \cong \mathbb{Z}_{23} \rtimes \mathbb{Z}_{11}$$

□

3

Let R be a commutative ring with identity and I and J two ideals such that $I + J = R$.

(a) Show that $IJ = I \cap J$.

(b) Give an example where $I + J \neq R$ and $IJ \neq I \cap J$.

Solution:

(a) The intersection of two ideals is an ideal, so we have the following equalities:

$$\begin{aligned} I \cap J &= (I \cap J)R \\ &= (I \cap J)(I + J) \\ &= I(I \cap J) + J(I \cap J) \\ &\subseteq IJ + IJ \\ &= IJ \end{aligned}$$

The reverse containment is immediate, since I and J are ideals:

$$IJ \subseteq I \text{ and } IJ \subseteq J$$

So $IJ \subseteq I \cap J$.
Since containment holds in both directions, $IJ = I \cap J$

(b) Let R be the ring of integers and consider the ideals $I = (2)$ and $J = (4)$.
Clearly, $I + J \neq R$, because $3 \in R$ but there is no sum of elements of I and J that will get us an odd integer.
The product $IJ = (2)$, and the intersection $I \cap J = (4)$, so we see $IJ \neq I \cap J$.

□

4

(a) Suppose that A is a complex $n \times n$ matrix with $A^3 = -A$. Show that A is diagonalizable.

(b) Suppose that A is a 2×2 matrix over the field $\mathbb{Q}$ of rational numbers with no non-trivial eigenvectors with entries in $\mathbb{Q}$, and that $A^3 = -A$. Show that A is similar over $\mathbb{Q}$ to $\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$.

Solution:

(a) If $A^3 = -A$, then $A^3 + A = 0$, so the minimal polynomial of A divides $A^3 + A$. If we factor $A^3 + A$ over the complex numbers, we get distinct linear factors: $A(A + iI)(A - iI)$, so the matrix A must be diagonalizable, as its minimal polynomial must be the product of distinct linear factors.

(b) The eigenvalues of A are the roots of the characteristic polynomial, which is a degree 2 polynomial since A is 2×2 and it is the product of the invariant factors of A. The invariant factors must be factors of the minimal polynomial, and the minimal polynomial must divide $x^3 + x = x(x^2 + 1)$. This means that the minimal polynomial must be $x^2 + 1$.
The given matrix is the 2×2 matrix with invariant factor $x^2 + 1$, so this must be the rational canonical form of A in this case.

□

5

Find the number of monic irreducible sextic polynomials in $\mathbb{F}_3[x]$, where $\mathbb{F}_3$ is the field of three elements.

Solution:
The number of monic irreducible polynomials of degree n over the finite field $\mathbb{F}_q$ is given by Gauss's formula:

$$\frac{1}{n}\sum_{d|n}\mu(n/d)q^d$$

where $\mu(1) = 1$, and if r is a product of distinct primes then $\mu(r) = 1$ if there are an even number of distinct primes and $\mu(r) = -1$ if there is an odd number of distinct primes, and $\mu(x) = 0$ for any other composite x. In this particular case, $n = 6, q = 3$:

$$\begin{aligned}\frac{1}{n}\sum_{d|n}\mu(n/d)q^d &= \frac{1}{6}\left(\mu(6)3^1 + \mu(3)3^2 + \mu(2)3^3 + \mu(1)3^6\right)\\ &= \frac{1}{6}(3 - 9 - 27 + 729)\\ &= 116\end{aligned}$$

□

6

Let $\mathbb{Q}$ be the field of rational numbers, and $\mathbb{C}$ the field of complex numbers. Let $\sqrt{2}$ denote the positive square root of 2 in $\mathbb{C}$. Let $\alpha = \sqrt{4+3\sqrt{2}}$ denote the positive square root of $4+3\sqrt{2}$ in $\mathbb{C}$.

(a) Determine the minimal polynomial of α.

(b) Show that $L = \mathbb{Q}(\alpha)$ is not Galois over $\mathbb{Q}$.

(c) Let M be the galois closure of L over $\mathbb{Q}$. What is the order of the galois group G of M over $\mathbb{Q}$?

Solution:

(a) First, show that α^2 is not a perfect square in $\mathbb{Q}(\sqrt{2})$, to show that α is not in $\mathbb{Q}(\sqrt{2})$.
To do this, assume that $\alpha^2 = (a+b\sqrt{2})^2$ for some $a+b\sqrt{2} \in \mathbb{Q}(\sqrt{2})$:

$$\begin{aligned} \alpha^2 &= (a+b\sqrt{2})^2 \\ 4+3\sqrt{2} &= (a^2+2b^2) + 2ab\sqrt{2} \end{aligned}$$

This would imply that $2ab = 3$ and $a^2+2b^2 = 4$. Solving this system of equations:

$$\begin{aligned} a = \frac{3}{2b} &\Rightarrow \left(\frac{3}{2b}\right)^2 + 2b^2 = 4 \\ &\Rightarrow \frac{9}{4b^2} + 2b^2 = 4 \\ &\Rightarrow 9 + 8b^4 = 16b^2 \\ &\Rightarrow 8b^4 - 16b^2 + 9 = 0 \\ &\Rightarrow b^2 = \frac{16 \pm \sqrt{256-288}}{16} \end{aligned}$$

Which would make b imaginary, which is not possible since $i \notin \mathbb{Q}(\sqrt{2})$.
Thus, the conjugates of α are the four elements $\pm\sqrt{4 \pm 3\sqrt{2}}$. These will be the other roots of the minimal polynomial of α. To find this polynomial, multiply:

$$(x - \sqrt{4+3\sqrt{2}})(x + \sqrt{4+3\sqrt{2}})(x - \sqrt{4-3\sqrt{2}})(x + \sqrt{4-3\sqrt{2}}) = x^4 - 8x^2 - 2$$

(b) To show that $L = \mathbb{Q}(\alpha)$ is not Galois, show that one of these roots is not in $\mathbb{Q}(\alpha)$. Consider $\beta = \sqrt{4-3\sqrt{2}}$.
If both α and β are in L, then so must the product $\alpha\beta$:

$$\begin{aligned} \alpha\beta &= (\sqrt{4+3\sqrt{2})(\sqrt{4-3\sqrt{2}}} \\ &= i\sqrt{2} \\ \beta &= i\frac{\sqrt{2}}{\alpha} \end{aligned}$$

But this is not possible, since $i\sqrt{2} \notin \mathbb{Q}(\alpha)$.
This means that the minimal polynomial of α does not split in $\mathbb{Q}(\alpha)$, so this cannot be a Galois extension.

(c) The order of the Galois group is the degree of the extension. We showed that the extension $\mathbb{Q}(\alpha)$ is not Galois, but we do know that $|Gal(M/\mathbb{Q})|$ must divide $4!$.