Pg 1

Abstract Algebra - Hw #7 Solns

Joe Cutrone

1. p. 137-138

#2| Let G be abelian group of order pq, $p \neq q$

Then by Fundamental Thm of Finitely Gen. Abelian Groups, $G \cong \mathbb{Z}_p \times \mathbb{Z}_q \cong \mathbb{Z}_{pq}$

#5| Conjugation by D_{16} gives an injective homomorphism $D_{16}/C_{D_{16}}(D_8) \hookrightarrow Aut(D_8)$

To compute $C_{D_{16}}(D_8)$, $g \in D_{16}$ centralizes $D_8 \longleftrightarrow g$ commutes with both generators r^2, s of D_8,

where r, s generate D_{16}

Since $C_{D_{16}}(r^2)$ contains $\langle r \rangle$ of order 8, but does not contain s, $8 \mid |C_{D_{16}}(r^2)| < 16$

$\therefore C_{D_{16}}(r^2) = \langle r \rangle$

for $r^i \in \langle r \rangle$, $r^i s = s r^i \longleftrightarrow s r^i s = r^i \longleftrightarrow r^{2i} = 1 \longleftrightarrow i = 4k$ $k \in \mathbb{Z}$

$\therefore C_{D_{16}}(D_8) = \{1, r^4\}$ $\therefore \left| D_{16}/C_{D_{16}}(D_8) \right| = 8$

$\therefore D_{16}/C_{D_{16}}(D_8) \cong D_8 \leq Aut(D_8)$. But by #3, $|Aut(D_8)| \leq 8$ $\therefore Aut(D_8) \cong D_8$

#11| Let p prime $P = \mathbb{Z}_p \leq S_p$

by 4.3 #34, $|N_{S_p}(\mathbb{Z}_p)| = p(p-1)$. Since $\mathbb{Z}_p \trianglelefteq N_{S_p}(\mathbb{Z}_p)$,

$N_{S_p}(\mathbb{Z}_p)$ acts on $\mathbb{Z}_p$ by conjugation $\therefore$ induces $\varphi: N_{S_p}(\mathbb{Z}_p) \longrightarrow Aut(\mathbb{Z}_p)$,

where $\ker \varphi = C_{S_p}(\mathbb{Z}_p) = \mathbb{Z}_p$

$\therefore \left| N_{S_p}(\mathbb{Z}_p)/C_{S_p}(\mathbb{Z}_p) \right| = \frac{p(p-1)}{p} = p-1$, and since $|Aut(\mathbb{Z}_p)| = p-1$, φ surjective

$\therefore N_{S_p}(\mathbb{Z}_p)/C_{S_p}(\mathbb{Z}_p) \cong Aut(\mathbb{Z}_p)$

#12| Let $|G| = 3825 = 3^2 \cdot 5^2 \cdot 17$. Let $H \trianglelefteq G$, $|H| = 17$ $\therefore H \cong \mathbb{Z}_{17}$

$G/C_G(H) \cong \_\_ \leq Aut(H)$, with $|Aut(\mathbb{Z}_{17})| = 16$

H is abelian, so $H \leq C_G(H)$

$\therefore 17 \mid |C_G(H)| \mid 3^2 \cdot 5^2 \cdot 17$ and $\frac{3^2 \cdot 5^2 \cdot 17}{|C_G(H)|} \mid 16 \Longrightarrow |C_G(H)| = 3^2 \cdot 5^2 \cdot 17$

$\therefore |G/C_G(H)| = 1$ $\therefore G = C_G(H)$ and $H \leq Z(G)$

Abstract Algebra - Hw #7 Solns

Joe Cutrone

#18 | Fix $n \geq 2$, $n \neq 6$. Let $G = S_n$

a) Let $\sigma \in Aut(G)$, K conjugacy class of G. Let $x \in G$ and fix $g \in G$

Since $\sigma(gxg^{-1}) = \sigma(g)\sigma(x)\sigma(g)^{-1}$, conjugates of x are sent to conjugates of $\sigma(x)$

$\therefore$ σ takes conjugacy classes of x to conjugacy classes of $\sigma(x)$

Similar reasoning with σ^{-1}, so get a bijection b/w classes of x & classes of $\sigma^{-1}(x)$

b) Let K be conjugacy class of transpositions of S_n. Let K' be conjugacy class of any element of order 2 in S_n not transposition

Then $|K| = \#$2-cycles in $S_n = \frac{n(n-1)}{2}$

From 4.3 #33, $|K'| = \frac{n!}{k!2^k} = \frac{(n-(k+1))!}{2^k}$ for $k \geq 4$ $\therefore |K| \neq |K'|$

Since automorphisms preserve order, by a), any automorphism sends transpositions to transpositions

c) Let $\sigma \in Aut(S_n)$. Then σ takes transpositions to transpositions, any any two transpositions in the image of $(1 b_i)$ must have some number in common, else would commute. Since original $(1\, b_i)$, $(1\, b_j)$ for $b_i \neq b_j$ don't commute, images can't commute. Let a be the number that appears most frequently, with frequency $\#a$

If $\#a = 1$, everything commutes $\rightarrow\leftarrow$

If $\#a = 2$, $n \leq 4$

cases for $n = 1, 2, 3$ trivial

if $n = 4$, could have $(12)(23)(13)$, but these don't generate S_4 $\rightarrow\leftarrow$

If $\#a \geq 3$, then have $(a\, b_1) \cdots (a\, b_m)(a_{m+1} b_{m+1}) \cdots (a_n b_n)$

Now, $(a_{m+1}\, b_{m+1})$ must share a number with $(a\, b_1)$, else would commute, so $b_1 = a_{m+1}$ or $b_1 = b_{m+1}$

Similar for $b_2, b_3 \ldots$

$\therefore \{b_i\} \subseteq \{a_{m+1}, b_{m+1}\} \rightarrow\leftarrow$ so a is in every image

Since the map is injective, all b_i's distinct.

note: since every cycle can be written as a product of transpositions, and $(ab) = (1a)(1b)(1a)$, these generate all of S_n

d) by c), any automorphism can be given by the images of $(1\, \cdot)$, so $|Aut(S_n)| \leq n!$

$\therefore$ for $n \neq 6$, any automorphism that sends 2-cycles to 2-cycles is inner

$\therefore$ since $Inn(S_n) \cong S_n/Z(S_n) \cong S_n$, $n! = |Inn(S_n)| \leq |Aut(S_n)| \leq n!$

$\therefore Inn(S_n) = Aut(S_n)$

Abstract Algebra - Hw 7 Solns

Joe Cutrone

2. Let R be a Boolean Ring. $x, y \in R$

Then $2x = x + x = (x+x)^2 = x^2 + 2x + x^2 = 4x \Rightarrow 0 = 2x = x + x$ so $x = -x$

Also, $(x+y) = (x+y)^2 = x^2 + xy + yx + y^2 \Rightarrow 0 = xy + yx \Rightarrow xy = -yx$

$\therefore -xy = -yx \Rightarrow xy = yx$ $\therefore$ commutative

3. Let $a \in A$ s.t. $a^n = 0$ for $n > 0$. Let $x \in A^{\times}$

Then $(x-a)(x^{-1})(1 + ax^{-1} + a^2x^{-2} + \cdots + a^{n-1}x^{n-1}) = (1 - ax^{-1})(1 + ax^{-1} + a^2x^{-2} + \cdots + a^{n-1}x^{n-1})$

$= (1 + ax^{-1} + a^2x^{-2} + \cdots + a^{n-1}x^{n-1}) - ax^{-1} - a^2x^{-2} - \cdots - a^{n-1}x^{n-1} - a^n x^n$

$= 1 - \overset{0}{\cancel{a^n}} x^{-n} = 1$

$\therefore (x-a)^{-1} = (x^{-1})(1 + ax^{-1} + \cdots + a^{n-1}x^{n-1})$

4. Let $R \subseteq \mathbb{Q}$ be smallest subring containing $\frac{1}{5}$

Then $\frac{1}{5} + \frac{1}{5} + \frac{1}{5} + \frac{1}{5} + \frac{1}{5} = 1$ $\therefore \mathbb{Z} \subseteq R$

$\therefore R = \mathbb{Z}[1/5] = \{a + \frac{b}{5} \mid a, b \in \mathbb{Z}\}$

5. See Cor 3, p 228

6. $\mathbb{Z}[\sqrt{2}]$ clearly satisfies axiom of ring (I'll let you work out the details)

7. From linear algebra given matrix $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$, $A^{-1} = \frac{1}{ad-bc}\begin{pmatrix} d & -b \\ -c & a \end{pmatrix} \in M_2(\mathbb{Z})$ iff $ad - bc = \pm 1$

8. Let $A = C([0,1], \mathbb{R})$. Let $I = \{f \in A \mid f(1/2) = 0\}$

I is an ideal since it is the kernel of the ring homomorphism $\varphi: A \to \mathbb{R}$ def by $f(x) \mapsto f(1/2)$

I is prime since for $f(x), g(x) \in A$, if $f(x)g(x) \in I$, then $f(1/2)g(1/2) = 0$ so $f(1/2)$ or $g(1/2) = 0$ since $\mathbb{R}$ is ID

By ex #4, p 225, I is maximal ideal

9. All proper ideals of $\mathbb{Z}/180\mathbb{Z}$ correspond to $d \in \mathbb{N}$ s.t. $d \neq 1$, $d \mid 180$. since $\mathbb{Z}/180\mathbb{Z} \big/ \mathbb{Z}/d\mathbb{Z} \cong \mathbb{Z}/\frac{180}{d}\mathbb{Z}$ is ID iff is field, prime ideals are same as max ideals, which correspond to d s.t. $180/d$ is prime, ie for $d = 90, 60, \& 36$.