HW 4 Solutions

M31 F11

① Let $f = (134)(26)(587)$, & let $g = \begin{pmatrix} 1&2&3&4&5&6&7&8 \\ 1&4&6&5&7&8&2&3 \end{pmatrix}$

Then in 2-line notation, $f = \begin{pmatrix} 1&2&3&4&5&6&7&8 \\ 3&6&4&1&8&2&5&7 \end{pmatrix}$

and in cycle notation, $g = (1)(2457)(368)$.

② $f \circ g = \begin{pmatrix} 1&2&3&4&5&6&7&8 \\ 3&1&2&8&5&7&6&4 \end{pmatrix} = (132)(48)(5)(67)$

$g \circ f = \begin{pmatrix} 1&2&3&4&5&6&7&8 \\ 6&8&5&1&3&4&7&2 \end{pmatrix} = (164)(28)(35)(7)$

HW 4 Solutions M31 F11

(3) a) A cycle $f = (x_1, x_2, \ldots, x_r)$ is an even permutation iff r is odd.

Proof. As in Theorem 8.2, we rewrite

$$(x_1, x_2, \ldots, x_r) = (x_1, x_r)(x_1, x_{r-1}) \cdots (x_1, x_3)(x_1, x_2)$$

There are $r-1$ ~~cycles~~ transpositions on the right-hand-side of this equation, so $(x_1, \ldots, x_r)$ is even iff r is odd.

b) ~~Since~~ Observe that the product of even permutations is even (by Theorem 8.5, which says $A_n \leq S_n$). Also, the product of two odd permutations is even, since the sum of two odd numbers is an even number. This implies that when we write the product of two odd permutations as a product of transpositions, there are an even number of them.

A similar argument shows that the product of an odd & an even permutation is odd.

Hence, to find out whether a permutation is even or odd, write it in disjoint cycle notation. By part (a), the length of the cycles tells you whether each cycle is odd or even. Since the decomposition into [ctd]

8.3 ctd | disjoint cycles is a product of permutations by Theorem 8.1, this tells us whether the original permutation is odd or even:

If there are an odd number of odd permutations (even-length cycles) in the factorization of a permutation f into disjoint cycles, then f is odd.

Otherwise, f is even.

(c) Writing $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 \\ 6 & 7 & 5 & 9 & 8 & 4 & 11 & 3 & 1 & 12 & 2 & 10 \end{pmatrix}$ in disjoint cycle notation, we get

$(1\ 6\ 4\ 9)(2\ 7\ 11)(3\ 5\ 8)(10\ 12)$.

Since there are two cycles of even length, this permutation is the product of two even elements & two odd elements, & hence is even. ⊠

HW 4 Solutions M31 F11

(8.15 c) The center of D_5 is the identity:

$$Z(D_5) = \{e\}.$$

Proof The generators g & f of D_5 are

$$g = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 5 & 4 & 3 & 2 \end{pmatrix}, \quad f = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 3 & 4 & 5 & 1 \end{pmatrix}$$

Since f has order 5, $(f^i)^{-1} = f^{-i} = f^{5-i}$ is never equal to i, for any $1 \le i \le 4$:

$(f^1)^{-1} = f^4$; $(f^2)^{-1} = f^3$.

Since $gf^i = f^{-i}g$ (*) it follows that no nontrivial power of f can be in $Z(D_5)$, since no nontrivial power of f commutes with g.

If $f^i g \in Z(D_5)$ for some $0 \le i \le 4$, that would imply, in particular,

$$f^i g f^i \stackrel{?}{=} f^{2i} g. \quad (☺)$$

But $f^i g f^i = f^i(f^{-i} g)$ by (*)
$= g$

So, if (☺) is true, then $f^{2i} = f^5 = e$ (since f has order 5). But since $(2,5) = 1$, this implies $i = 5 (=0)$ by Theorem 4.4 (iii).

However, as discussed above, g cannot be in $Z(D_5)$, because f^i and f^{-i} are different elements of D_5 for all $i \neq 0$ (or 5);

and $f^i g = g f^{-i}$ for all i.

Therefore, $Z(D_5)$ can't contain any non-identity element, so $Z(D_5) = \{e\}$ as claimed. ☒

d) The group $D_5 \times D_5$ has 100 elements, but every element has order at most 10. Moreover, $D_5 \times D_5$ is non abelian.

Proof Since $|D_5| = 10$, $D_5 \times D_5$ has 100 elements. However, if $d = (d_1, d_2)$, then $o(d) = \operatorname{lcm}(o(d_1), o(d_2))$. Since elements of D_5 can only have orders 1, 2, 5, $\operatorname{lcm}(o(d_1), o(d_2)) \leq 10$, since $o(d_1)$ & $o(d_2)$ must both divide 10.

To see that $D_5 \times D_5$ is non-abelian, it is NOT enough to observe that the direct product of abelian groups is abelian!

However, observe that (for example)

$$(f, g) \cdot (g, f) = (fg, gf) = (fg, f^4 g)$$

whereas $(g, f) \cdot (f, g) = (gf, fg) = (f^4 g, fg)$

which are different elements of $D_5 \times D_5$; since $f \neq f^4$!

Thus $D_5 \times D_5$ is not abelian. ☒

HW 4 Solutions

M31 F11

(8.23) The elements $f, g \in S_{\mathbb{Z}}$ defined by

$$f(n) = -n, \quad g(n) = 2-n$$

both have finite order, but $f \circ g$ has infinite order.

<u>Proof</u> Observe that f, g are actually in $S_{\mathbb{Z}}$ as claimed: $f = f^{-1}$, and

$$g^{-1}(n) = 2 - n = g(n) \quad \text{also.}$$

So in fact f, g have order 2.

However, $f \circ g(n) = n-2$, and $(f \circ g)^k(n)$ is never n, for any $k \in \mathbb{Z}^+$.

To see this, observe that

$$\begin{aligned}(f \circ g)^k(n) &= (f \circ g)^{k-1}(f \circ g(n)) \\ &= (f \circ g)^{k-1}(n-2) \\ &= (f \circ g)^{k-2}(f \circ g(n-2)) \\ &= (f \circ g)^{k-2}(n-4) \\ &= \cdots = n - 2k.\end{aligned}$$

If $n - 2k = n$, then $2k = 0$, and hence $k = 0$.

Thus, $o(f \circ g) = \infty$ as claimed. ☒

M31 F11 Homework 4 Solutions

(12.1) a) The map $\phi: (\mathbb{R}-\{0\},\cdot) \longrightarrow (\mathbb{R}^+,\cdot)$ given by $\phi(x)=|x|$ is an onto homomorphism. It is not a monomorphism.

<u>Proof</u> We must check that $\phi(xy)=\phi(x)\phi(y)$ for any $x, y \in (\mathbb{R}-\{0\},\cdot)$. But,

$$\phi(xy) = |xy| = |x|\,|y| = \phi(x)\phi(y).$$

Thus, ϕ is a homomorphism.

Since any element $x \in (\mathbb{R}^+,\cdot)$ satisfies $=|x|$, and $\mathbb{R}^+ \subseteq \mathbb{R}\setminus\{0\}$, it follows that every element $x \in \mathbb{R}^+$ is the image of some element in $\mathbb{R}\setminus\{0\}$:

If $x \in \mathbb{R}^+ \subseteq \mathbb{R}-\{0\}$, then $x=|x|=\phi(x)$.

Thus ϕ is onto.

However, ϕ is not 1-1 (& hence not an isomorphism): $\phi(1)=1=\phi(-1)$ but $1 \neq -1$.

HW 4 Solutions M31 F11

(12.1) c) Let G be the group of all polynomials with real coefficients, under the operation of addition of polynomials. Let $\phi : G \to (\mathbb{R}, +)$ be given by $\phi(p(x)) = p(1)$: that is, evaluation at 1. Then ϕ is an epimorphism but not an isomorphism.

<u>Proof</u> To show ϕ is a homomorphism, we must check that $\phi(p+q) = \phi(p) + \phi(q)$, for any polynomials p, q. But

$$\phi(p+q) = (p+q)(1) = p(1) + q(1) = \phi(p) + \phi(q),$$

so ϕ is a homomorphism.

Since G contains the constant polynomials, ϕ is onto: every element y in $\mathbb{R}$ gives us a constant polynomial $p(x) = y$, such that $p(1) = y$.

However, ϕ isn't 1-1: for any $y \in \mathbb{R}$, the polynomials $p(x) = y$ and $q(x) = x + y - 1$ satisfy $p(1) = q(1) = y$. Thus, ϕ isn't an isomorphism.

HW 4 Solutions M31 F11

(11.4) b) The groups $(2\mathbb{Z}, +)$ & $(3\mathbb{Z}, +)$ are isomorphic: The map $\phi: 2\mathbb{Z} \to 3\mathbb{Z}$ given by $\phi(2m) = 3m$ is an isomorphism.

Proof First we check that ϕ is a homomorphism:

$$\phi(2m + 2n) = \phi(2(m+n)) = 3(m+n)$$

$$\phi(2m) + \phi(2n) = 3m + 3n = 3(m+n)$$

Thus, for any $x, y \in 2\mathbb{Z}$, we have $\phi(x+y) = \phi(x) + \phi(y)$, $\Leftrightarrow$ ϕ is a homomorphism.

We must check that ϕ is 1-1 and onto. If $\phi(x) = \phi(y)$ for two elements $x, y \in 2\mathbb{Z}$, write $x = 2m$, $y = 2n$, for $m, n \in \mathbb{Z}$. Then $\phi(x) = \phi(y)$ implies $3m = 3n$, and hence $m = n$. But if $m = n$, then $2m = 2n$, so $x = y$ also. Therefore, ϕ is 1-1.

To check that ϕ is onto, let $z = 3k$ be an arbitrary element of $3\mathbb{Z}$. Then, $z = \phi(2k)$ is the image of the element $2k \in 2\mathbb{Z}$, so ϕ is onto. Hence ϕ is an isomorphism. ∎

HW4 Solutions M31 F11

(12.4) c) $(\mathbb{R}-\{0\},\cdot)$ & $(\mathbb{R},+)$ are not isomorphic.

Proof If $\phi: \mathbb{R}-\{0\} \to \mathbb{R}$ were an isomorphism, then by Theorem 12.5(iv), we must have $o(\phi(-1)) = 2$. However, $(\mathbb{R},+)$ has no elements of order 2. If $x \in \mathbb{R}$ satisfies $x + x = e$ (that is, $2x = 0$) then $x = 0$. But we know that the order of the identity element is always 1, not 2: thus $(\mathbb{R},+)$ has no elements of order 2. Since $(\mathbb{R}-\{0\},\cdot)$ does have an element of order 2, the groups can't be isomorphic. ☒

1 4 e) The groups $\mathbb{Z}_3 \times \mathbb{Z}_3$ & $\mathbb{Z}_9$ are not isomorphic.

Proof Suppose $\phi: \mathbb{Z}_9 \to \mathbb{Z}_3 \times \mathbb{Z}_3$ is an isomorphism. Then we must have $o(\phi(1)) = 9$, since $o(1) = 9$ in $\mathbb{Z}_9$.

However, Theorem 6.1 tells us that if $g = (g_1, g_2)$ is an element of $\mathbb{Z}_3 \times \mathbb{Z}_3$, then $o(g) = o((g_1, g_2))$ is given by $o(g) = \operatorname{lcm}(o(g_1), o(g_2))$.
Since elements of $\mathbb{Z}_3$ can have only order 1 or 3, elements of $\mathbb{Z}_3 \times \mathbb{Z}_3$ must have order 1 or 3. Thus, we can't map $1 \in \mathbb{Z}_9$ to an element of order 9 in $\mathbb{Z}_3 \times \mathbb{Z}_3$, so $\mathbb{Z}_3 \times \mathbb{Z}_3$ can't be isomorphic to $\mathbb{Z}_9$.

$\boxtimes$

HW4 Solutions M31 F11

(1.8) The group $(\mathbb{Z}_{14}, \oplus)$ is not isomorphic to a subgroup of $(\mathbb{Z}_{35}, \oplus)$. However, $(\mathbb{Z}_{14}, \oplus)$ is isomorphic to a subgroup of $(\mathbb{Z}_{56}, \oplus)$.

Proof: Theorem 5.5 tells us that, since 14 doesn't divide 35, $\mathbb{Z}_{35}$ has no subgroup of order 14. Since isomorphic groups have the same size, $\mathbb{Z}_{14}$ can't be isomorphic to any subgroup of $\mathbb{Z}_{35}$.

However, since 14 does divide 56 $(14 \cdot 4 = 56)$, Theorem 5.5 tells us that $\mathbb{Z}_{56}$ has a subgroup of order 14. Since $\mathbb{Z}_{56}$ is cyclic, Theorem 5.2 tells us that this subgroup is cyclic, and hence is isomorphic to $\mathbb{Z}_{14}$ by Theorem 12.2.

Alternatively, you could observe that the map $\phi: \mathbb{Z}_{14} \to \mathbb{Z}_{56}$ given by $\phi(m) = 4m$ is a monomorphism, and hence $\mathbb{Z}_{14} \cong \langle 4 \rangle = \mathrm{Im}(\phi)$ in $\mathbb{Z}_{56}$.

M31 F11 HW 4 Solutions

(12.13) Let $\phi: G \to H$ be a homomorphism. Then:

(a) If H is abelian & ϕ is 1-1, then G is abelian.

(b) If G is abelian, and ϕ is onto, then H is abelian

(c) If ϕ is an isomorphism, then G abelian $\Longleftrightarrow$ H abelian.

Proof (a) Let $x, y \in G$ be arbitrary. Since ϕ is a homomorphism, $\phi(xy) = \phi(x)\phi(y)$, which equals $\phi(y)\phi(x)$ since H is abelian. But also, $\phi(y)\phi(x) = \phi(yx)$.

Therefore, $\phi(xy) = \phi(yx)$ for any $x, y \in G$. Since ϕ is 1-1, this implies that $xy = yx$; in other words, since x, y were arbitrary, this tells us that G is abelian. ☒

(b) Let $x, y \in H$ be arbitrary. Since ϕ is onto, there exist $a, b \in G$ such that $\phi(a) = x$, $\phi(b) = y$. But,

$$xy = \phi(a)\phi(b) = \phi(ab) = \phi(ba) = \phi(b)\phi(a) = yx$$

since ϕ is a homomorphism and G is abelian. Since $x, y \in H$ were arbitrary, this tells us that H is abelian. ☒

12.13 continued

Proof of (c). If ϕ is an isomorphism, and G is abelian, then by (b) H is abelian, since ϕ is both 1-1 & onto.

Conversely, if we assume ϕ is an isomorphism & H is abelian, then (a) tells us that G is also abelian.

Thus, If ϕ is an isomorphism,

$$G \text{ abelian} \Leftrightarrow H \text{ abelian}$$

as claimed. $\boxtimes$

HW 4 Solutions M31 F11

(12.21) Let $G = (\mathbb{C}^{\times}, \cdot)$, and let

$$H = \left(\left\{\begin{pmatrix} a & b \\ -b & a \end{pmatrix} : a^2+b^2 \neq 0\right\}, \text{matrix multiplication}\right)$$

Then $G \cong H$.

Proof Observe that any complex number z can be written as $z = x+iy$ for $x, y \in \mathbb{R}$. We define $\phi : G \to H$ by

$$\phi(z) = \phi(x+iy) = \begin{pmatrix} x & +y \\ -y & x \end{pmatrix}$$

Claim ϕ is an isomorphism.

First, we must show that ϕ is a homomorphism.

Observe that

$$\phi(z_1 \cdot z_2) = \phi((x_1+iy_1)(x_2+iy_2))$$
$$= \phi(x_1x_2 - y_1y_2 + i(x_1y_2+y_1x_2))$$
$$= \begin{pmatrix} x_1x_2-y_1y_2 & x_1y_2+y_1x_2 \\ -x_1y_2-y_1x_2 & x_1x_2-y_1y_2 \end{pmatrix}$$

On the other hand,

$$\phi(z_1)\phi(z_2) = \begin{pmatrix} x_1 & y_1 \\ -y_1 & x_1 \end{pmatrix}\begin{pmatrix} x_2 & y_2 \\ -y_2 & x_2 \end{pmatrix}$$
$$= \begin{pmatrix} x_1x_2-y_1y_2 & x_1y_2+y_1x_2 \\ -y_1x_2-x_1y_2 & -y_1y_2+x_1x_2 \end{pmatrix}$$

M31 F11 HW4 Solutions

(12.21) continued.

Since $\phi(z_1 z_2) = \phi(z_1)\phi(z_2)$ for any z_1, z_2 in G, it follows that ϕ is a homomorphism.

To see that ϕ is 1-1, observe that if two matrices $\begin{pmatrix} a & b \\ -b & a \end{pmatrix}$ & $\begin{pmatrix} c & d \\ -d & c \end{pmatrix}$ are equal, then $a=c$ & $b=d$. Since $\begin{pmatrix} a & b \\ -b & a \end{pmatrix} = \phi(a+bi)$ and $\begin{pmatrix} c & d \\ -d & c \end{pmatrix} = \phi(c+di)$, this tells us that if $\phi(a+bi) = \phi(c+di)$ then $a=c$ & $b=d$; hence $a+bi = c+di$. In other words, ϕ is 1-1.

To see that ϕ is onto, observe that any matrix $\begin{pmatrix} a & b \\ -b & a \end{pmatrix}$ is the image of $a+bi$ under ϕ. The only complex number that isn't in G is $0 = 0+0i$, but $\phi(0+0i) = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$, which doesn't satisfy the condition $a^2+b^2 \neq 0$. Thus, ϕ maps every element of G to an element of H, and it doesn't miss any. In other words, ϕ is onto; thus ϕ is an isomorphism. ☒