Homework #7 Solutions

p 132, #4 Since $U(8) = \{1, 3, 5, 7\}$ and $3^2 \bmod 8 = 5^2 \bmod 8 = 7^2 \bmod 8$, every non-identity element of $U(8)$ has order 2. However, $3 \in U(10)$ we have

$$\begin{aligned} 3^2 \bmod 10 &= 9 \\ 3^3 \bmod 10 &= 7 \\ 3^4 \bmod 10 &= 1 \end{aligned}$$

so that $|3| = 4$ in $U(10)$. Since $U(8)$ does not have any elements of order 4, there can be no isomorphism between $U(10)$ and $U(8)$, by Part 5 of Theorem 6.2.

p 132, #6 Let G, H and K be groups and suppose that $G \cong H$ and $H \cong K$. Then there are isomorphisms $\phi : G \to H$ and $\psi : H \to K$. The composite $\psi \circ \phi$ is a function from G to K that is one-to-one and onto since both ϕ and ψ are (this is general nonsense about functions). We will show that it is operation preserving, and hence gives an isomorphism between G and K.

For any $a, b \in G$ we have (since ϕ and ψ are operation preserving)

$$(\psi \circ \phi)(ab) = \psi(\phi(ab)) = \psi(\phi(a)\phi(b)) = \psi(\phi(a))\psi(\phi(b)) = (\psi \circ \phi)(a)(\psi \circ \phi)(b)$$

which proves that $\psi \circ \phi$ is operation preserving. As noted above, this completes the proof that $G \cong K$.

p 133, #18 Since $\phi \in \mathrm{Aut}(\mathbb{Z}_{50})$, we know that $\phi(x) = rx \bmod 50$ for some $r \in U(50)$. Since $\phi(7) = 13$, it must be the case that

$$13 = \phi(7) = 7r \bmod 50.$$

We can remove the 7 and solve for r by multiplying by 7's inverse in $U(50)$. That is, since $43 \cdot 7 \bmod 50 = 1$ we have

$$r = 1 \cdot r \bmod 50 = 43 \cdot 7r \bmod 50 = 43 \cdot 13 \bmod 50 = 9.$$

Hence, $\phi(x) = 9x \bmod 50$ for all $x \in \mathbb{Z}_{50}$.

p 133, #22 It is easy to see that $U(24) = \{1, 5, 7, 11, 13, 17, 19, 23\}$ and

$$\begin{aligned} 5^2 \bmod 24 &= 25 \bmod 24 = 1 \\ 7^2 \bmod 24 &= 49 \bmod 24 = 1 \\ 11^2 \bmod 24 &= 121 \bmod 24 = 1 \\ 13^2 \bmod 24 &= 169 \bmod 24 = 1 \\ 17^2 \bmod 24 &= 289 \bmod 24 = 1 \\ 19^2 \bmod 24 &= 361 \bmod 24 = 1 \\ 23^2 \bmod 24 &= 529 \bmod 24 = 1 \end{aligned}$$

so that every non-identity element of $U(24)$ has order 2. However, since $3 \in U(20)$ and $3^2 \bmod 20 = 9 \neq 1$, $U(20)$ has an element with order greater than 2. As above, Theorem 6.2 (part 5) implies that there cannot be an isomorphism between $U(24)$ and $U(20)$.

p 133, #24 Although we won't prove it here, it is straightforward to verify that G and H are both groups under addition. So it makes sense to ask whether or not G and H are isomorphic.

Since every element in $g \in G$ has the form $g = a + b\sqrt{2}$, $a, b \in \mathbb{Q}$, and this expression is unique[1], the function

$$\begin{aligned} \rho : G &\rightarrow H \\ a + b\sqrt{2} &\mapsto \begin{pmatrix} a & 2b \\ b & a \end{pmatrix} \end{aligned}$$

is well-defined. Our goal is to show that ρ is an isomorphism.

1-1: If $\rho(a_1 + b_1\sqrt{2}) = \rho(a_2 + b_2\sqrt{2})$ then, by the definition of ρ, we must have

$$\begin{pmatrix} a_1 & 2b_1 \\ b_1 & a_1 \end{pmatrix} = \begin{pmatrix} a_1 & 2b_1 \\ b_1 & a_1 \end{pmatrix}$$

which implies that $a_1 = a_2$ and $b_1 = b_2$. Hence, $a_1 + b_1\sqrt{2} = a_2 + b_2\sqrt{2}$, which proves that ρ is one-to-one.

Onto: This is clear, given the definitions of G, H and ρ.

Operation Preservation: Let $x_1 = a_1 + b_1\sqrt{2}, x_2 = a_2 + b_2\sqrt{2} \in G$. Then

$$x_1 + x_2 = (a_1 + b_1\sqrt{2}) + (a_2 + b_2\sqrt{2}) = (a_1 + a_2) + (b_1 + b_2)\sqrt{2}$$

[1] This fact is essential to our construction, so let's quickly prove it. Let $x \in G$ and suppose $x = a_1 + b_1\sqrt{2} = a_2 + b_2\sqrt{2}$ with $a_1, a_2, b_1, b_2 \in \mathbb{Q}$. Then $a_1 - a_2 = (b_2 - b_1)\sqrt{2}$ and if $b_1 \neq b_2$ then we have $\sqrt{2} = (a_1 - a_2)/(b_2 - b_1) \in \mathbb{Q}$, which is impossible. So it must be that $b_1 = b_2$ from which it follows that $a_1 = a_2$ as well.

so that

$$\begin{aligned}\rho(x_1+x_2) &= \rho((a_1+a_2)+(b_1+b_2)\sqrt{2})\\ &= \begin{pmatrix} a_1+a_2 & 2(b_1+b_2)\\ b_1+b_2 & a_1+a_2\end{pmatrix}\\ &= \begin{pmatrix} a_1 & 2b_1\\ b_1 & a_1\end{pmatrix}+\begin{pmatrix} a_2 & 2b_2\\ b_2 & a_2\end{pmatrix}\\ &= \rho(a_1+b_1\sqrt{2})+\rho(a_2+b_2\sqrt{2})\\ &= \rho(x_1)+\rho(x_2)\end{aligned}$$

which proves that ρ is operation preserving.

Since $\rho : G \to H$ is 1-1, onto and preserves the group operations, we conclude that ρ is an isomorphism and hence that $G \cong H$.

It's easy to check that both G and H are closed under multiplication (an exercise left to the reader) and that ρ preserves these operations as well (which we now prove). Let $x_1 = a_1 + b_1\sqrt{2}, x_2 = a_2 + b_2\sqrt{2} \in G$. Then

$$x_1x_2 = (a_1+b_1\sqrt{2})(a_2+b_2\sqrt{2}) = (a_1a_2+2b_1b_2)+(a_1b_2+a_2b_1)\sqrt{2}$$

so that

$$\rho(x_1x_2) = \begin{pmatrix} a_1a_2+2b_1b_2 & 2(a_1b_2+a_2b_1)\\ a_1b_2+a_2b_1 & a_1a_2+2b_1b_2\end{pmatrix}.$$

On the other hand, we have

$$\begin{aligned}\rho(x_1)\rho(x_2) &= \begin{pmatrix} a_1 & 2b_1\\ b_1 & a_1\end{pmatrix}\begin{pmatrix} a_2 & 2b_2\\ b_2 & a_2\end{pmatrix}\\ &= \begin{pmatrix} a_1a_2+2b_1b_2 & 2(a_1b_2+a_2b_1)\\ a_1b_2+a_2b_1 & a_1a_2+2b_1b_2\end{pmatrix}\end{aligned}$$

That is,

$$\rho(x_1x_2) = \begin{pmatrix} a_1a_2+2b_1b_2 & 2(a_1b_2+a_2b_1)\\ a_1b_2+a_2b_1 & a_1a_2+2b_1b_2\end{pmatrix} = \rho(x_1)\rho(x_2)$$

which proves that ρ preserves multiplication.

p 134, #32 Define $f : \mathbb{R}^+ \to \mathbb{R}$ by $f(a) = \log_{10}(a)$. As usual, to prove this is an isomorphism we need to verify that f is one-to-one, onto and preserves the group operations.

One-to-one: If $f(a) = f(b)$ then $\log_{10}(a) = \log_{10}(b)$ so that

$$a = 10^{\log_{10}(a)} = 10^{\log_{10}(b)} = b,$$

proving that f is one-to-one.

Onto: Let $y \in \mathbb{R}$. Then $a = 10^y \in \mathbb{R}^+$ and we see that

$$f(a) = \log_{10}(a) = \log_{10}(10^y) = y,$$

which shows that f is onto.

Operation preservation: Let $a, b \in \mathbb{R}^+$. Then, using a familiar property of logarithms we have

$$f(ab) = \log_{10}(ab) = \log_{10}(a) + \log_{10}(b) = f(a) + f(b).$$

Since the operation in $\mathbb{R}^+$ is multiplication and that in $\mathbb{R}$ is addition, we conclude that f is operation preserving.

Having verified the three defining conditions, we conclude that f is an isomorphism, i.e. $\mathbb{R}^+ \cong \mathbb{R}$.

p 134, #42

Lemma 1. *Let $\phi : \mathbb{Q} \to \mathbb{Q}$ be an operation preserving function*[2]*. Then*

$$\phi(r) = r\phi(1)$$

for all $r \in \mathbb{Q}$.

Proof. Let $n \in \mathbb{Z}^+$, $r \in \mathbb{Q}$. Then

$$\phi(nr) = \phi(\underbrace{r + r + \cdots + r}_{n \text{ times}} = \underbrace{\phi(r) + \phi(r) + \cdots + \phi(r)}_{n \text{ times}} = n\phi(r).$$

If we let $r = 1$ this becomes

$$\phi(n) = n\phi(1)$$

whereas if we let $r = 1/n$ we get

$$\phi(1) = n\phi\left(\frac{1}{n}\right)$$

or

$$\phi\left(\frac{1}{n}\right) = \frac{1}{n}\phi(1).$$

Also, since $\phi(0) = 0$ [3] we have

$$0 = \phi(0) = \phi(r + (-r)) = \phi(r) + \phi(-r)$$

so that

$$\phi(-r) = -\phi(r).$$

With these facts in hand we can now complete the proof. Let $r \in \mathbb{Q}$. If $r > 0$ then $r = m/n$ with $m, n \in \mathbb{Z}^+$ and we have

$$\phi(r) = \phi\left(\frac{m}{n}\right) = \phi\left(m\frac{1}{n}\right) = m\phi\left(\frac{1}{n}\right) = m\frac{1}{n}\phi(1) = r\phi(1).$$

On the other hand, if $r < 0$ then $r = -s$ with $s \in \mathbb{Q}$, $s > 0$ and so by what we have just proven

$$\phi(r) = \phi(-s) = -\phi(s) = -s\phi(1) = r\phi(1).$$

□

[2] Such a function is called a *homomorphism*.

[3] This is proven for homomorphisms the same way it is for isomorphisms.

Proposition 1. *Let $\phi : \mathbb{Q} \to \mathbb{Q}$ be one-to-one and operation preserving*[4]*. Then ϕ is onto.*

Proof. Let $s \in \mathbb{Q}$. Since ϕ is one-to-one and $\phi(0) = 0$, we must have $\phi(1) \neq 0$. Set $r = s/\phi(1)$. Then $r \in \mathbb{Q}$ and so by the Lemma

$$\phi(r) = \phi\left(\frac{s}{\phi(1)}\right) = \frac{s}{\phi(1)}\phi(1) = s$$

which proves that ϕ is onto. □

Finishing the exercise is now almost trivial. Let $H \leq \mathbb{Q}$ and suppose that $\phi : \mathbb{Q} \to H$ is an isomorphism. Since $H \subset \mathbb{Q}$, we can view ϕ as a one-to-one, operation preserving map into $\mathbb{Q}$. The Proposition then tells us that, in fact, ϕ must map onto $\mathbb{Q}$. That is, $\mathbb{Q} = \phi(\mathbb{Q}) = H$, so that H is *not* a proper subgroup of $\mathbb{Q}$. Therefore, $\mathbb{Q}$ cannot be isomorphic to any of its proper subgroups.

Isomorphism Exercise 1: The basic idea here is that given an element $\sigma \in G$, we can simply "forget" that σ acts on the entire set $\{1, 2, \ldots, n\}$. To be specific, let $\sigma \in G$. Since σ is one-to-one and $\sigma(n) = n$, σ must map the complementary set $\{1, 2, \ldots, n-1\}$ onto itself. That is

$$\sigma \in G \;\Rightarrow\; \sigma|_{\{1,2,\ldots,n-1\}} \in S_{n-1}.$$

We can therefore define $\psi : G \to S_{n-1}$ by $\psi(\sigma) = \sigma|_{\{1,2,\ldots,n-1\}}$. We claim that ψ is an isomorphism.

One-to-one: Suppose that $\psi(\sigma) = \psi(\tau)$. Then, by the definition of ψ, it must be that

$$\sigma|_{\{1,2,\ldots,n-1\}} = \tau|_{\{1,2,\ldots,n-1\}}$$

i.e. as functions σ and τ agree on the set $\{1, 2, \ldots, n-1\}$. But since $\sigma, \tau \in G$, we know that $\sigma(n) = \tau(n) = n$. Hence, σ and τ actually agree on all of $\{1, 2, \ldots, n\}$ and so $\sigma = \tau$.

Onto: To build an element $\sigma \in G$, we must specify the values of σ on the set $\{1, 2, \ldots, n-1\}$, since we are forced to set $\sigma(n) = n$. As there are $n-1$ choices for the image of 1, $n-2$ choices for the image of 2, etc., we find that there are $(n-1)!$ elements in G (this is the same argument that was used to count S_n in the first place). That is

$$|G| = (n-1)! = |S_{n-1}|.$$

Therefore ψ is a one-to-one map between two finite sets of the same size. It follows that ψ is onto.

Operation preservation: Let $\sigma, \tau \in G$. For any $i \in \{1, 2, \ldots, n-1\}$ we have

$$\begin{aligned}
(\sigma\tau)\{1, 2, \ldots, n-1\}(i) &= (\sigma\tau)(i) \\
&= \sigma(\tau(i)) \\
&= \sigma|_{\{1,2,\ldots,n-1\}}(\tau|_{\{1,2,\ldots,n-1\}}(i)) \\
&= (\sigma|_{\{1,2,\ldots,n-1\}}\tau|_{\{1,2,\ldots,n-1\}})(i)
\end{aligned}$$

which shows that $\psi(\sigma\tau) = (\sigma\tau)\{1, 2, \ldots, n-1\} = \sigma|_{\{1,2,\ldots,n-1\}}\tau|_{\{1,2,\ldots,n-1\}} = \psi(\sigma)\psi(\tau)$.

[4] Such a function is called a *monomorphism*.

Isomorphism Exercise 2: Let

$$A = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \text{ and } B = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}.$$

We begin by computing:

$$\begin{aligned}
A^2 &= \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix} \\
A^3 &= \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \\
A^4 &= I \\
B^2 &= I \\
AB &= \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \\
A^2B &= \begin{pmatrix} 0 & -1 \\ -1 & 0 \end{pmatrix} \\
A^3B &= \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix} = BA
\end{aligned}$$

Since G is a group containing A and B, then by closure G must contain the matrices $I, A, A^2, A^3, B, AB, A^2B, A^3B$, and we now see that these are all distinct. We claim that in fact, these 8 matrices form a group, i.e. $G = \{I, A, A^2, A^3, B, AB, A^2B, A^3B\}$. This is most easily seen using a Cayley table:

	I	A	A^2	A^3	B	AB	A^2B	A^3B
I	I	A	A^2	A^3	B	AB	A^2B	A^3B
A	A	A^2	A^3	I	AB	A^2B	A^3B	B
A^2	A^2	A^3	I	A	A^2B	A^3B	B	AB
A^3	A^3	I	A	A^2	A^3B	B	AB	A^2B
B	B	A^3B	A^2B	AB	I	A^3	A^2	A
AB	AB	B	A^3B	A^2B	A	I	A^3	A^2
A^2B	A^2B	AB	B	A^3B	A^2	A	I	A^3
A^3B	A^3B	A^2B	AB	B	A^3	A^2	A	I

The entry in the X^{th} row and Y^{th} column is XY, and each was computed using the relations given above: $A^4 = B^2 = I$ and $A^3B = BA$. It is clear from the table that the set $\{I, A, A^2, A^3, B, AB, A^2B, A^3B\}$ is closed under matrix multiplication and so the finite subgroup test implies it is a group. Thus, the smallest group containing A and B is $G = \{I, A, A^2, A^3, B, AB, A^2B, A^3B\}$.

Isomorphism Exercise 3: Let

$$A = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \text{ and } B = \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix}.$$

As in Exercise 2, we begin by computing:

$$\begin{aligned}
A^2 &= \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix} \\
A^3 &= \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \\
A^4 &= I \\
B^2 &= \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix} = A^2 \\
B^3 &= \begin{pmatrix} 0 & -i \\ -i & 0 \end{pmatrix} \\
B^4 &= I \\
AB &= \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix} = B^3A \\
A^2B &= B^3 \\
A^3B &= \begin{pmatrix} -i & 0 \\ 0 & i \end{pmatrix} = AB^3
\end{aligned}$$

Since G is a group containing A and B, then by closure G must contain the matrices $I, A, A^2, A^3, B, B^3, AB, A^3B$, and we now see that these are all distinct. We claim that in fact, these 8 matrices form a group, i.e. $G = \{I, A, A^2, A^3, B, B^3, AB, A^3B\}$. This is most easily seen using a Cayley table:

	I	A	A^2	A^3	B	B^3	AB	A^3B
I	I	A	A^2	A^3	B	B^3	AB	A^3B
A	A	A^2	A^3	I	AB	A^3B	B^3	B
A^2	A^2	A^3	I	A	B^3	A^3B	B	AB
A^3	A^3	I	A	A^2	A^3B	AB	B	B^3
B	B	A^3B	B^3	AB	A^2	I	A	A^3
B^3	B^3	AB	B	A^3B	I	A^2	A^3	A
AB	AB	B	A^3B	B^3	A^3	A	A^2	I
A^3B	A^3B	B^3	AB	B	A	A^3	I	A^2

The entry in the X^{th} row and Y^{th} column is XY, and each was computed using the relations given above. It is clear from the table that the set $\{I, A, A^2, A^3, B, B^3, AB, A^3B\}$ is closed under matrix multiplication and so the finite subgroup test implies it is a group. Thus, the smallest group containing A and B is $G = \{I, A, A^2, A^3, B, B^3, AB, A^3B\}$.

G is not isomorphic to D_4 because D_4 has only 2 elements of order 4 (R_{90} and R_{270}) whereas G has at least 3 elements of order 4 (A, B and AB). And G is not isomorphic to $\mathbb{Z}_8$ because G is not cyclic (every element has order 1, 2 or 4).

Isomorphism Exercise 4: Let $H \leq \mathbb{Z}$, $H \neq \{0\}$. Since $\mathbb{Z}$ is cyclic, we know that H is cyclic as well. Write $H = \langle k \rangle$, $k \in \mathbb{Z}^+$. Define $f : \mathbb{Z} \to H$ by $f(n) = nk$. It is clear that f is onto. If $f(m) = f(n)$ then $mk = nk$ and, since $k \neq 0$, $m = n$. Thus f is one-to-one. Finally, we see that

$$f(m+n) = (m+n)k = mk + nk = f(m) + f(n)$$

proving that f preserves operations. It follows that f is an isomorphism and hence that $\mathbb{Z} \cong H$. Since H was arbitrary, we conclude that $\mathbb{Z}$ is isomorphic to all of its nontrivial subgroups.