DMath_U8_bf

8.3

Let $\langle G, *, \hat{}, e\rangle$ be a group, and let S be a set. Assume that $f: G \to S$ is a bijection, and consider

- the binary operation $\star$ on S given by $s \star s\prime \overset{def}{=} f(f^{-1}(s) * f^{-1}(s\prime))$
- the unary operation $\tilde{}$ on S given by $\tilde{s} \overset{def}{=} f(\widehat{f^{-1}(s)})$.

  Prove the following statement.
  a) Axiom G1 ($\star$ is associative) holds for $\langle S, \star, \tilde{}, f(e)\rangle$

To prove that **G1** holds for $\langle S; \star, \tilde{}, f(e)\rangle$, we will show that the operation $\star$ is associative.

Let $s_1,\ s_2,\ s_3 \in S$
We need to show that $(s_1 \star s_2) \star s_3 = s_1 \star (s_2 \star s_3)$.
Since we have

You should justify (using the fact that $f \circ f^{-1} = id$)

$$(s_1 \star s_2) \star s_3 = f(f^{-1}(f(f^{-1}(s_1) * f^{-1}(s_2))) * f^{-1}(s_3)) = f((f^{-1}(s_1) * f^{-1}(s_2)) * f^{-1}(s_3))$$

and

$$s_1 \star (s_2 \star s_3) = f(f^{-1}(s_1) * f^{-1}(f(f^{-1}(s_2) * f^{-1}(s_3)))) = f(f^{-1}(s_1) * (f^{-1}(s_2) * f^{-1}(s_3)))$$

given by the definition of $\star$ and the operation $*$ is associative in G, we have

$$((f^{-1}(s_1) * f^{-1}(s_2)) * f^{-1}(s_3) = f^{-1}(s_1) * (f^{-1}(s_2) * f^{-1}(s_3))$$
$$f(f^{-1}(s_1) * (f^{-1}(s_2) * f^{-1}(s_3))) = f^{-1}(s_1) * (f^{-1}(s_2) * f^{-1}(s_3))$$

$\frac{4}{4}$

Thus,

$$(s_1 \star s_2) \star s_3 = s_1 \star (s_2 \star s_3)$$

✓

□

8.4

c) Prove that $\langle \mathbb{Z}_{15}^*, \odot_{15}\rangle \simeq \langle \mathbb{Z}_{16}^*, \odot_{16}\rangle$.

For two groups $\langle G; *, \hat{}, e\rangle$ and $\langle H; \star, \tilde{}, e'\rangle$, a function $\psi: G \to H$ is called a group homomorphism if, for all a and b,
$\psi(a * b) = \psi(a) \star \psi(b)$
If ψ is a bijection from G to H, then it is called an isomorphism, and we say that G and H are isomorphic and write $G \simeq H$. (Definition 5.10.)

$\langle \mathbb{Z}_{15}^*, \odot_{15}\rangle$

$\odot_{15}$	**1**	**2**	**4**	**8**	**7**	**11**	**13**	**14**
1	1	2	4	8	7	11	13	14
2	2	4	8	1	14	7	11	13
4	4	8	1	2	13	14	7	11
8	8	1	2	4	11	13	14	7
7	7	14	13	11	4	2	1	8
11	11	7	14	13	2	1	8	4
13	13	11	7	14	1	8	4	2
14	14	13	11	7	8	4	2	1

$\langle \mathbb{Z}_{16}^{*}, \odot_{16} \rangle$

$\odot_{16}$	**1**	**3**	**9**	**11**	**5**	**7**	**13**	**15**
1	1	3	9	11	5	7	13	15
3	3	9	11	1	15	5	7	13
9	9	11	1	3	13	15	5	7
11	11	1	3	9	7	13	15	5
5	5	15	13	7	9	3	1	11
7	7	5	15	13	3	1	11	9
13	13	7	5	15	1	11	9	3
15	15	13	7	5	11	9	3	1

We define a function $\psi : \mathbb{Z}_{15}^{*} \to \mathbb{Z}_{16}^{*}$ as follows:

$\psi(1) = 1$
$\psi(2) = 3$
$\psi(4) = 9$
$\psi(8) = 11$
$\psi(7) = 5$
$\psi(11) = 7$
$\psi(13) = 13$
$\psi(14) = 15$

Obviously the function is bijective, as it maps each element onto one unique element (injective) and each element has an inverse (surjective). ✓

Now we will prove that it is a group homomorphism on $\langle \mathbb{Z}_{15}^{*}, \odot_{15} \rangle$

To do this, we must prove, that for all $a, b \in \mathbb{Z}_{15}^{*}$

$$\psi(a \odot_{15} b) = \psi(a) \odot_{16} \psi(b)$$

We do this by case distinction:

$\psi(1 \odot_{15} 1) = 1 = \psi(1) \odot_{16} \psi(1)$ ✓
$\psi(1 \odot_{15} 2) = 3 = \psi(1) \odot_{16} \psi(2)$
$\psi(1 \odot_{15} 4) = 9 = \psi(1) \odot_{16} \psi(4)$

Oof - sorry you had to this. The more efficient way is to find generators of the groups.

$\frac{4}{4}$

$\psi(1 \odot_{15} 7) = 5 = \psi(1) \odot_{16} \psi(7)$
$\psi(1 \odot_{15} 8) = 11 = \psi(1) \odot_{16} \psi(8)$
$\psi(1 \odot_{15} 11) = 7 = \psi(1) \odot_{16} \psi(11)$
$\psi(1 \odot_{15} 13) = 13 = \psi(1) \odot_{16} \psi(13)$
$\psi(1 \odot_{15} 14) = 15 = \psi(1) \odot_{16} \psi(14)$
$\psi(2 \odot_{15} 1) = 3 = \psi(2) \odot_{16} \psi(1)$
$\psi(2 \odot_{15} 2) = 9 = \psi(2) \odot_{16} \psi(2)$
$\psi(2 \odot_{15} 4) = 11 = \psi(2) \odot_{16} \psi(4)$
$\psi(2 \odot_{15} 7) = 15 = \psi(2) \odot_{16} \psi(7)$
$\psi(2 \odot_{15} 8) = 1 = \psi(2) \odot_{16} \psi(8)$
$\psi(2 \odot_{15} 11) = 5 = \psi(2) \odot_{16} \psi(11)$
$\psi(2 \odot_{15} 13) = 7 = \psi(2) \odot_{16} \psi(13)$
$\psi(2 \odot_{15} 14) = 13 = \psi(2) \odot_{16} \psi(14)$
$\psi(4 \odot_{15} 1) = 9 = \psi(4) \odot_{16} \psi(1)$
$\psi(4 \odot_{15} 2) = 11 = \psi(4) \odot_{16} \psi(2)$
$\psi(4 \odot_{15} 4) = 1 = \psi(4) \odot_{16} \psi(4)$
$\psi(4 \odot_{15} 7) = 13 = \psi(4) \odot_{16} \psi(7)$
$\psi(4 \odot_{15} 8) = 3 = \psi(4) \odot_{16} \psi(8)$
$\psi(4 \odot_{15} 11) = 15 = \psi(4) \odot_{16} \psi(11)$
$\psi(4 \odot_{15} 13) = 5 = \psi(4) \odot_{16} \psi(13)$
$\psi(4 \odot_{15} 14) = 7 = \psi(4) \odot_{16} \psi(14)$
$\psi(7 \odot_{15} 1) = 5 = \psi(7) \odot_{16} \psi(1)$
$\psi(7 \odot_{15} 2) = 15 = \psi(7) \odot_{16} \psi(2)$
$\psi(7 \odot_{15} 4) = 13 = \psi(7) \odot_{16} \psi(4)$
$\psi(7 \odot_{15} 7) = 9 = \psi(7) \odot_{16} \psi(7)$
$\psi(7 \odot_{15} 8) = 7 = \psi(7) \odot_{16} \psi(8)$
$\psi(7 \odot_{15} 11) = 3 = \psi(7) \odot_{16} \psi(11)$
$\psi(7 \odot_{15} 13) = 1 = \psi(7) \odot_{16} \psi(13)$
$\psi(7 \odot_{15} 14) = 11 = \psi(7) \odot_{16} \psi(14)$
$\psi(8 \odot_{15} 1) = 11 = \psi(8) \odot_{16} \psi(1)$
$\psi(8 \odot_{15} 2) = 1 = \psi(8) \odot_{16} \psi(2)$
$\psi(8 \odot_{15} 4) = 3 = \psi(8) \odot_{16} \psi(4)$
$\psi(8 \odot_{15} 7) = 7 = \psi(8) \odot_{16} \psi(7)$
$\psi(8 \odot_{15} 8) = 9 = \psi(8) \odot_{16} \psi(8)$
$\psi(8 \odot_{15} 11) = 13 = \psi(8) \odot_{16} \psi(11)$
$\psi(8 \odot_{15} 13) = 15 = \psi(8) \odot_{16} \psi(13)$
$\psi(8 \odot_{15} 14) = 5 = \psi(8) \odot_{16} \psi(14)$
$\psi(11 \odot_{15} 1) = 7 = \psi(11) \odot_{16} \psi(1)$
$\psi(11 \odot_{15} 2) = 5 = \psi(11) \odot_{16} \psi(2)$
$\psi(11 \odot_{15} 4) = 15 = \psi(11) \odot_{16} \psi(4)$
$\psi(11 \odot_{15} 7) = 3 = \psi(11) \odot_{16} \psi(7)$
$\psi(11 \odot_{15} 8) = 13 = \psi(11) \odot_{16} \psi(8)$
$\psi(11 \odot_{15} 11) = 1 = \psi(11) \odot_{16} \psi(11)$
$\psi(11 \odot_{15} 13) = 11 = \psi(11) \odot_{16} \psi(13)$
$\psi(11 \odot_{15} 14) = 9 = \psi(11) \odot_{16} \psi(14)$
$\psi(13 \odot_{15} 1) = 13 = \psi(13) \odot_{16} \psi(1)$
$\psi(13 \odot_{15} 2) = 7 = \psi(13) \odot_{16} \psi(2)$
$\psi(13 \odot_{15} 4) = 5 = \psi(13) \odot_{16} \psi(4)$
$\psi(13 \odot_{15} 7) = 1 = \psi(13) \odot_{16} \psi(7)$

$\psi(13 \odot_{15} 8) = 15 = \psi(13) \odot_{16} \psi(8)$
$\psi(13 \odot_{15} 11) = 11 = \psi(13) \odot_{16} \psi(11)$
$\psi(13 \odot_{15} 13) = 9 = \psi(13) \odot_{16} \psi(13)$
$\psi(13 \odot_{15} 14) = 3 = \psi(13) \odot_{16} \psi(14)$
$\psi(14 \odot_{15} 1) = 15 = \psi(14) \odot_{16} \psi(1)$
$\psi(14 \odot_{15} 2) = 13 = \psi(14) \odot_{16} \psi(2)$
$\psi(14 \odot_{15} 4) = 7 = \psi(14) \odot_{16} \psi(4)$
$\psi(14 \odot_{15} 7) = 11 = \psi(14) \odot_{16} \psi(7)$
$\psi(14 \odot_{15} 8) = 5 = \psi(14) \odot_{16} \psi(8)$
$\psi(14 \odot_{15} 11) = 9 = \psi(14) \odot_{16} \psi(11)$
$\psi(14 \odot_{15} 13) = 3 = \psi(14) \odot_{16} \psi(13)$
$\psi(14 \odot_{15} 14) = 1 = \psi(14) \odot_{16} \psi(14)$
$\square$