Abstract Algebra I Homework 1

Carson Connard

Section 1.1

Let G be a group.

1 Determine which of the following binary operations are associative:

a) The operation $\star$ on $\mathbb{Z}$ defined by $a \star b = a - b$

Solution. This is associative. We see

$$(a \star b) \star c = (a - b) \star c = a - b - c = a \star (b - c) = a \star (b \star c)$$

b) The operation $\star$ on $\mathbb{R}$ defined by $a \star b = a + b + ab$

Solution. This is associative. We see

$$\begin{aligned}
(a \star b) \star c &= (a + b + ab) \star c \\
&= (a + b + ab) + c + (ac + bc + abc) \\
&= a + b + c + ab + ac + bc + abc \\
&= a + (b + c + bc) + ab + ac + abc \\
&= a \star (b + c + bc) \\
&= a \star (b \star c)
\end{aligned}$$

c) The operation $\star$ on $\mathbb{Q}$ defined by $a \star b = \frac{a+b}{5}$

Solution. This is not associative. We see

$$(a \star b) \star c = \left(\frac{a+b}{5}\right) \star c = \frac{\frac{a+b}{5} + c}{5} \neq \frac{a + \frac{b+c}{5}}{5} = a \star \left(\frac{b+c}{5}\right) = a \star (b \star c)$$

d) The operation $\star$ on $\mathbb{Z} \times \mathbb{Z}$ defined by $(a, b) \star (c, d) = (ad + bc, bd)$

Solution. This is associative. We see

$$\begin{aligned}
((a, b) \star (c, d)) \star (e, f) &= (ad + bc, bd) \star (e, f) \\
&= (adf + bcf + bdc, bdf) \\
&= (a, b) \star (cf + de, df) \\
&= (a, b) \star ((c, d) \star (e, f))
\end{aligned}$$

e) The operation $\star$ on $\mathbb{Q} \setminus \{0\}$ defined by $a \star b = a/b$

Solution. This is not associative. We see

$$(a \star b) \star c = \left(\frac{a}{b}\right) \star c = \frac{a/b}{c} = \frac{a}{bc} \neq \frac{ac}{b} = \frac{a}{b/c} = a \star \left(\frac{b}{c}\right) = a \star (b \star c)$$

8 Let $G = \{z \in \mathbb{C} : z^n = 1, n \in \mathbb{Z}^+\}$.

a) Prove that G is a group under multiplication (called the group of *roots of unity* in $\mathbb{C}$).

Proof. We show the following properties:

(a) Closure under multiplication: Let some $x, y \in G$. Then we know that there exist some $a, b \in \mathbb{Z}_+$ such that $x^a = y^b = 1$ by definition. Then we have that

$$x^a y^b = (xy)^{ab} = (x^a)^b \cdot (y^a)^b = 1^b \cdot 1^b = 1.$$

So we have that $xy \in G$.

(b) Associativity: Since $G \subset \mathbb{C}$, associativity is inherited.

(c) Existence of multiplicative identity: Certainly, we have that the multiplicative identity 1 from $\mathbb{C}$ holds, that is $x \cdot 1 = 1 \cdot x = x$.

(d) Inverses: Take some arbitrary $x \in G$. Then

$$(x^{-1})^n = (x^n)^{-1} = (1)^{-1} = 1.$$

Therefore, $x^{-1} \in G$.

We have shown all necessary conditions for $(G, \cdot)$ to be a group. $\square$

b) Prove that G is not a group under addition.

Proof. We see that $-1^2 = 1$, therefore $-1 \in G$. Certainly, $1 \in G$ as well. But, $-1 + 1 = 0$, and $0^n \neq 1$ for any n. So, $0 \notin G$ and $(G, +)$ is not a group. $\square$

25 Prove that if $x^2 = 1$ for all $x \in G$, then G is abelian.

Proof. Having the condition $x^2 = 1$ implies that $x = x^{-1}$ for all $x \in G$. So, for any $x, y \in G$, we have that

$$xy = (xy)^{-1} = y^{-1}x^{-1} = yx.$$

$\square$

Section 1.2

In these exercises, D_{2n} has the usual presentation $D_{2n} = \{r, s : r^n = s^2 = 1, rs = sr^{-1}\}$.

2 Use the generators and relations above to show that if x is any element if D_{2n} which is not a power of r, then $rx = xr^{-1}$.

Proof. The problem statement states that x is of the form sr^m for $1 \leq m \leq n-1$. So, considering the relations given in the definition of D_{2n} and subsequently the fact that $s = s^{-1}$, we have the following:

$$rx = r\,(sr^m) = (rs)r^m = sr^{m-1} = sr^m r^{-1} = xr^{-1}.$$

$\square$

9 Let G be the group of rigid motions in $\mathbb{R}^3$ of a tetrahedron. Show that $|G| = 12$.

Solution. We notice that a tetrahedron has four vertices. Fix one vertex. We see that there are three rigid rotations that can be made to yield the identity. So, there are 4 choices of vertex, and 3 choices of rotation, giving a total of 12.

Section 1.3

2 Let σ be the permutation

$$\begin{array}{ccccc} 1 \mapsto 13 & 2 \mapsto 2 & 3 \mapsto 15 & 4 \mapsto 14 & 5 \mapsto 10 \\ 6 \mapsto 6 & 7 \mapsto 12 & 8 \mapsto 3 & 9 \mapsto 4 & 10 \mapsto 1 \\ 11 \mapsto 7 & 12 \mapsto 9 & 13 \mapsto 5 & 14 \mapsto 11 & 15 \mapsto 8 \end{array}$$

And let τ be the permutation

$$\begin{array}{ccccc} 1 \mapsto 14 & 2 \mapsto 9 & 3 \mapsto 10 & 4 \mapsto 2 & 5 \mapsto 12 \\ 6 \mapsto 6 & 7 \mapsto 5 & 8 \mapsto 11 & 9 \mapsto 15 & 10 \mapsto 3 \\ 11 \mapsto 8 & 12 \mapsto 7 & 13 \mapsto 4 & 14 \mapsto 1 & 15 \mapsto 13 \end{array}$$

Find the cycle decompositions of the following permutations: $\sigma, \tau, \sigma^2, \sigma\tau, \tau\sigma, \tau^2\sigma$.

Solution. Via the cycle decomposition algorithm given in the book, we have the following:

1. $\sigma = (1\ 13\ 5\ 10)(3\ 15\ 8)(4\ 14\ 11\ 7\ 12\ 9)$
2. $\tau = (1\ 14)(2\ 9\ 15\ 13\ 4)(3\ 10)(5\ 12\ 7)(8\ 11)$
3. $\sigma^2 = (1\ 5)(3\ 8\ 15)(4\ 11\ 12)(7\ 9\ 14)(10\ 13)$
4. $\sigma\tau = (1\ 11\ 3)(2\ 4)(5\ 9\ 8\ 7\ 10\ 15)(13\ 14)$
5. $\tau\sigma = (1\ 4)(2\ 9)(3\ 13\ 12\ 15\ 11\ 5)(8\ 10\ 14)$
6. $\tau^2\sigma = (1\ 2\ 15\ 8\ 3\ 4\ 14\ 11\ 12\ 13\ 7\ 5\ 10)$

Section 1.6

17 Let G be any group. Prove that the map from G to itself defined by $g \mapsto g^2$ is a homomorphism if and only if G is abelian.

Proof. ($\Longrightarrow$) For the sake of contradiction, assume $\phi : G \to G$ ($g \mapsto g^2$) is a homomorphism, and assume G is not abelian. Now taking some $x, y \in G$ such that $xy \neq yx$, we see

$$xyxy = (xy)^2 = \phi(xy) = \phi(x)\phi(y) = x^2y^2 = xxyy$$

Now since G is a group, there exist $x^{-1}, y^{-1} \in G$. Let us left multiply the equation by x^{-1} and right multiply by y^{-1}:

$$\begin{gathered} x^{-1}xyxyy^{-1} = x^{-1}xxyyy^{-1} \\ yx = xy \end{gathered}$$

This yields a contradiction. As such, we must have that G is abelian.

($\Longleftarrow$) Assume G is abelian and consider the map $g \overset{\phi}{\mapsto} g^2$. Let us take two arbitrary elements $x, y \in G$. Then we have the following:

$$\phi(xy) = (xy)^2 = (xy)(xy) = x^2y^2 = \phi(x)\phi(y).$$

Therefore, ϕ is a group homomorphism. $\square$