Homework 2 Solutions

1 (a) By definition, for all \( x \in G \), \( (x^{-1})^{-1}x^{-1} = e = xx^{-1} \). We then right multiply by \( x \), and obtain \( (x^{-1})^{-1}(x^{-1}x) = x(x^{-1}x) \), and so \((x^{-1})^{-1} = x \). We will proceed by induction to show that \((xy)^n = x^n y^n \). Let \( x, y \in G \). For \( n = 1 \), the result is \((xy)^1 = x^1 y^1 \), which is \( xy = xy \), which holds. Now assume that \((xy)^n = x^n y^n \) and look at \((xy)^{n+1} \). We can factor \((xy)^{n+1} = (xy)^n xy \), and then by hypothesis we have \((xy)^{n+1} = x^n y^n xy \). As \( G \) is abelian, we have that \( y^n x = xy^n \), and so \((xy)^{n+1} = x^n(xy^n)y = x^{n+1}y^{n+1} \), and so \( G \) abelian implies that \((xy)^n = x^n y^n \) for all \( n \).

(b) We proceed by induction. Let \( x_1 \in G \). Then \((x_1)^{-1} = x_1^{-1} \). Now let \( x_1, \ldots, x_n \in G \) and assume that \((x_1 \ldots x_{n-1})^{-1} = x_n^{-1} \ldots x_1^{-1} \). Then look at \( x_n^{-1}x_{n-1} \ldots x_1^{-1} \). Multiply this by \( x_1 \ldots x_n \) and we obtain \((x_1 \ldots x_n)(x_n^{-1} \ldots x_1^{-1}) = (x_1 \ldots x_n)(x_n^{-1} \ldots x_1^{-1}) = (x_1 \ldots x_{n-1})(x_{n-1}^{-1} \ldots x_1^{-1}) = (x_1 \ldots x_{n-1})(x_{n-1} \ldots x_1). \) Similarly for left multiplication, and so \((x_1 \ldots x_n)^{-1} = x_n^{-1} \ldots x_1^{-1} \).

(c) Let \( x, y \in G \) arbitrary and assume \((xy)^2 = x^2 y^2 \). Then we expand and obtain \( xxyy = xyxy \). We then left multiply by \( x^{-1} \) and right multiply by \( y^{-1} \) and obtain \( x^{-1}xyxy^{-1} = x^{-1}xyxyy^{-1} \) and so \( xy = yx \), and so \( x, y \) arbitrary, \( G \) is abelian.

(d) Let \( x, y \in G \) arbitrary and let \( i \) be such that \((xy)^i = x^i y^i \), \((xy)^{i+1} = x^{i+1} y^{i+1} \) and \((xy)^{i+2} = x^{i+2} y^{i+2} \). We expand \((xy)^{i+1} = (xy)^i(xy) \), and by the first condition, we have \( x^{i+1} y^{i+1} = (xy)^{i+1} = x^i y^i xy \), we then left multiply by \( x^{-i} \) and \( y^{-1} \) to obtain \( xy^i = y^i x \). Now we look at \((xy)^{i+2} = x^{i+2} y^{i+2} \). The left is \((xy)^{i+2} = (xy)^{i+1}(xy) = x^{i+1} y^{i+1} xy = x^{i+2} y^{i+2} \). We then left multiply by \( x^{-i} \) and right multiply to \( y^{-1} \), and obtain \( y^{i+1} x = xy^{i+1} \). This can be expanded to \( yxy = yx \). We apply \( xy^i = y^i x \) and obtain \( yxy^i = y^i xy \), and then left multiply by \( y^{-1} \), to finally obtain \( gx = xy \), and so \( G \) is abelian.

2 (a) In cycle notation, take \( \sigma = (123) \) and \( \tau = (12) \). Then \( \sigma^2 = (132) \), \( \tau^2 = e \) and \( \sigma \tau = (123)(12) = (13) \), so \( (\sigma \tau)^2 = e \). Thus, \( a^2 \tau^2 = (132) \neq e = (\sigma \tau)^2 \).

(b) Let \( G \) be a finite group. Each element \( g \in G \) defines an integer, \( o(g) \), the order of \( g \). Let \( n_G = \text{LCM}(o(g)|g \in G) \). This is defined, because it is the least common multiple of finitely many numbers.
Additionally, as each $o(g)|n_G$, we have $g^{n_G} = e$ for all $g \in G$, and so the claim is proved.

(c) For $G = \mathbb{Z}/m\mathbb{Z}$, every element has order dividing $m$, and one element has order $m$. Thus, $m$ is the least common multiple. For $G = S_3$, the elements have order $1, 2$ or $3$, and so the least common multiple is $n_G = 6$. The story is slightly more complex in the case of $G = S_7$. The elements of this group all have order $1, 2, 3, 4, 5, 6$ or $7$, and the least common multiple is 420, which is a sufficient $n_G$ for $S_7$.

(d) In general, $n_G$ will always divide $G$, because, as defined, it is the least common multiple of the orders of the elements, but we know that $o(g)|G$ for all $g \in G$, and so $G$ is a common multiple of the $o(g)$.

5 (a) Let $x, y, z \in R^\times$. As $R$ is associative under multiplication, we have $(xy)z = x(yz)$, and so $R^\times$ is as well. Additionally, $1_R \in R^\times$, as $1_R \cdot 1_R = 1_R$, and so $R^\times$ has an identity. As $xx^{-1} = x^{-1}x = 1_R$, whenever $x$ is a unit, $x^{-1}$ is as well, so $R^\times$ has inverses. The only question is whether $R^\times$ is closed under multiplication. So we must show that if $x, y$ are units then $xy$ is. Now, as $x, y$ are units, $y^{-1}, x^{-1}$ are, and so $(xy)(y^{-1}x^{-1}) = 1_R$, and so $xy \in R^\times$.

(b) First, look at $R = \mathbb{Z}$. For this ring, $R^\times = \{1, -1\}$. That 1, -1 are units follows from $1 \cdot 1 = (-1) \cdot (-1) = 1$. To see that they are the only ones, let $n \in \mathbb{Z}$. For $n$ to be a unit, then there must be an integer $m$ such that $nm = 1$. We note that $\mathbb{Z} \subset \mathbb{Q}$, and is in fact a subring, so if $n$ has inverse $m$ in $\mathbb{Z}$, it does in $\mathbb{Q}$. So we can write $m = \frac{1}{n} \in \mathbb{Q}$. Now, for any integer other than $-1, 1$, we have $\frac{1}{n} \not\in \mathbb{Z}$, and so the only invertible elements of $\mathbb{Z}$ are $\{1, -1\}$. For $R = \mathbb{Q}$, we have $R^\times = \mathbb{Q} \setminus \{0\}$, because if $\frac{a}{n} \in \mathbb{Q}$ is nonzero, then $\frac{a}{n} \in \mathbb{Q}$, and $\frac{a}{n} = 1$. For $R = M_{2 \times 2}(\mathbb{R})$, we have $R^\times$ equal to the set of matrices $A$ with $\det A \in \mathbb{R} \setminus \{0\}$. This is because if \( \begin{bmatrix} a & b \\ c & d \end{bmatrix} \), if it exists, is equal to $\frac{1}{ad - bc} \begin{bmatrix} d & -b \\ -c & a \end{bmatrix}$, and the condition is then that $ad - bc = \det A$ is invertible, and over $\mathbb{R}$, every nonzero element is invertible. Similarly, for $R = M_{2 \times 2}(\mathbb{Z})$, we need $ad - bc \in \{1, -1\}$.

(c) If $a, b \in R^\times$, $c \in R$, then the equation $ab = c$ has a unique solution, $x = a^{-1}cb^{-1}$. If either $a$ or $b$ isn’t in $R^\times$, then there may be no solutions, for instance, $1 \cdot x \cdot 2$ in $\mathbb{Z}$ has no solutions.

6 (a) Let $a, b, c \in H_R$. We then write $a = a_0 + a_0i + a_0j + a_0k$, and similarly for $b$ and $c$. So $(a + b) + c = (a_0 + b_0) + (a_1 + b_1)i + (a_2 + b_2)j + (a_3 + b_3)k + (c_0 + c_1 i + c_2 j + c_3 k) = (a_0 + b_0 + c_0) + \ldots + (a_3 + b_3 + c_3)k = a_0 + (b_0 + c_0) + \ldots + a_3 + (b_3 + c_3)k = a + (b + c)$, because $R$ is associative under $+$, Similarly, $a + b = (a_0 + b_0) + \ldots + (a_3 + b_3)k = (b_0 + a_0 + \ldots + (b_3 + a_3)k = b + a$ as $R$ is commutative under $+$. To see that it has an additive identity, we look at $0 = 0 + 0i + 0j + 0k$,
and note that $a + 0 = (a_0 + 0) + \ldots + (a_3 + 0)k = a_0 + \ldots + a_3 k = a$, and to see inverses, let $-a = -a_0 + \ldots + (-a_3)k$, and then $a + (-a) = (a_0 - a_0) + \ldots + (a_3 - a_3)k = 0 + \ldots + 0k = 0$. Now we must show associativity of multiplication. Look at $(ab)c$. This expands to $((a_0 + a_1i + a_2j + a_3k)(b_0 + b_1i + b_2j + b_3k))(c_0 + c_1i + c_2j + c_3k)$, this expands to $(a_0 b_0 - a_1 b_1 - a_2 b_2 - a_3 b_3) + (a_0 b_1 + a_1 b_0 + a_2 b_3 + a_3 b_2) i + (a_0 b_2 + a_1 b_3 - a_1 b_2 + a_2 b_1) j + (a_0 b_3 + a_1 b_2 - a_2 b_1 + a_3 b_0) k (c_0 + c_1 i + c_2 j + c_3 k)$, this, in turn, is equal to $(a_0 b_0 c_0 - a_1 b_1 c_0 - a_2 b_2 c_0 - a_3 b_3 c_0 - a_1 b_0 c_1 - a_0 b_1 c_1 + a_3 b_2 c_1 - a_2 b_3 c_1 - a_3 b_0 c_2 - a_0 b_1 c_2 + a_1 b_3 c_2 + a_2 b_0 c_2 + a_3 b_1 c_2 - a_1 b_2 c_2 - a_2 b_1 c_2 - a_3 b_0 c_3 + a_0 b_1 c_3 - a_1 b_2 c_3 - a_2 b_3 c_3 + (a_1 b_1 c_1 + a_0 b_2 c_1 - a_3 b_3 c_1 + a_2 b_0 c_1 + a_3 b_1 c_1 - a_1 b_3 c_1 - a_2 b_2 c_1 - a_3 b_1 c_2 - a_0 b_3 c_2 + a_1 b_0 c_2 - a_2 b_1 c_2 - a_3 b_2 c_2 - a_1 b_3 c_2 - a_2 b_0 c_3 + a_3 b_1 c_3 - a_1 b_2 c_3 + a_2 b_3 c_3) i + (a_2 b_0 c_0 + a_3 b_1 c_0 + a_0 b_2 c_0 - a_1 b_3 c_0 + a_2 b_2 c_0 - a_3 b_1 c_1 - a_0 b_3 c_1 - a_1 b_0 c_1 + a_2 b_2 c_1 - a_3 b_1 c_2 - a_0 b_3 c_2 + a_1 b_0 c_2 - a_2 b_1 c_2 - a_3 b_2 c_2 - a_1 b_3 c_2 - a_2 b_0 c_3 + a_3 b_1 c_3 - a_1 b_2 c_3 + a_2 b_3 c_3) j + (a_3 b_0 c_0 - a_2 b_1 c_0 + a_1 b_2 c_0 + a_0 b_3 c_0 - a_3 b_1 c_1 - a_2 b_0 c_1 - a_1 b_3 c_1 + a_0 b_2 c_1 + a_1 b_0 c_2 + a_2 b_3 c_2 - a_3 b_1 c_2 - a_2 b_0 c_3 + a_1 b_2 c_3 - a_0 b_3 c_3) k$. A similar multiplication procedure on $a(bc)$ gives the same thing, and so $\mathbb{H}_R$ is associative. As $ij = k$ and $ji = -k$, we can see immediately that $\mathbb{H}_R$ is noncommutative, and now we look at the identity. Let $1 = 1_R + 0i + 0j + 0k$. Then $a1 = (a_0 1_R - a_1 0 + a_0 0 - a_0 3) + (a_0 0 + a_1 1_R + a_0 0 - a_0 3) i + (a_0 0 - a_0 0 + a_1 1_R + a_0 0 - a_0 3) j + (a_0 0 + a_1 1_R + a_0 0 - a_0 3) k = a = 1a$, and so is the identity for $\mathbb{H}_R$.

We must now show that the function $\phi : R \to \mathbb{H}_R$ by $a \mapsto a + 0i + 0j + 0k$ is a homomorphism of rings with identity. We begin by checking $\phi(a + b) = (a + b) + 0i + 0j + 0k = (a + 0i + 0j + 0k) + (b + 0i + 0j + 0k) = \phi(a) + \phi(b)$. We must next work on $\phi(a)\phi(b) = (a + 0i + 0j + 0k)(b + 0i + 0j + 0k) = (ab + 0i - 0j + 0k) + (0i + 0j + 0k + 0i + 0j + 0k + 0i + 0j + 0k) = ab + 0i + 0j + 0k = \phi(ab)$. All that remains now is to check that $\phi(1_R) = 1_{\mathbb{H}_R}$, which holds because $\phi(1_R) = 1_R + 0i + 0j + 0k = 1_{\mathbb{H}_R}$ as determined above.

(b) To see that $\mathbb{H}_R$ is a skew field, the only thing that remains is to check the existence of inverses. Let $a = a_0 + a_1 i + a_2 j + a_3 k$, and define $\bar{a} = a_0 - a_1 i - a_2 j - a_3 k$. Now that $a\bar{a} = a_0^2 + a_1^2 + a_2^2 + a_3^2 + 0i + 0j + 0k$ is invertible if it is nonzero, as it is the image of a real number, and is zero if and only if $a = 0$. So we can look at $a/\bar{a}$ and $a/\bar{a}$, and this will be an inverse for $a$, as $a(a/\bar{a}) = (a\bar{a})(a/\bar{a})^{-1} = 1_{\mathbb{H}_R}$, so $\mathbb{H}_R$ is a skew field. We now solve the equation $(1 + i + j + k)x = xi$ for $x$. Set $x = x_0 + x_1 i + x_2 j + x_3 k$, then we have $(1 + i + j + k)(x_0 + x_1 i + x_2 j + x_3 k) = (x_0 + x_1 i + x_2 j + x_3 k)i$. The right hand side simplifies to $x_0 i - x_1 - x_2 k + x_3 j$, and the left hand side simplifies to $(x_0 - x_3 - x_2 - x_3) + (x_1 + x_0 + x_3 - x_2)i + (x_2 - x_3 + x_0 + x_1)j + (x_3 + x_2 - x_1 + x_0) k$. Setting these equal, we end up with four linear equations over $R$ in the variables $x_0, x_1, x_2, x_3$, which are
\[ x_0 - x_1 - x_2 - x_3 = -x_1 \]
\[ x_1 + x_0 + x_3 - x_2 = x_0 \]
\[ x_2 - x_3 + x_0 + x_1 = x_3 \]
\[ x_3 + x_2 - x_1 + x_0 = -x_2 \]

These give unique solution 0.

(c) Here we must show that the map \( \mathbb{C} \rightarrow \mathbb{H}\mathbb{R} \) given by \((a + bi) \mapsto (a + bi + 0j + 0k)\) is a ring homomorphism. First we check additivity, set \( z, w \in \mathbb{C} \) and write \( z = z_0 + z_1 i, w = w_0 + w_1 i, \phi(z + w) = \phi((z_0 + w_0) + (z_1 + w_1)i) = (z_0 + w_0) + (z_1 + w_1)i + 0j + 0k = (z_0 + z_1i + 0j + 0k) + (w_0 + w_1i + 0j + 0k) = \phi(z) + \phi(w) \). Now we must check that it respects multiplication \( \phi(z)\phi(w) = (z_0w_0 - z_1w_1 - 0 - 0) + (z_0w_1 + z_1w_0 + 0 - 0)i + (0 - 0 + 0)j + (0 + 0 - 0 + 0)k = (z_0w_0 - z_1w_1) + (z_0w_1 + z_1w_0)i + 0j + 0k = \phi(zw) \).

8 We want to show that there are no ideals other than zero and the whole ring for \( R = M_{2 \times 2}(\mathbb{Q}) \). Let \( I \) be an ideal, and assume \( I \neq \emptyset \). Then there exists \( A = \begin{bmatrix} a & b \\ c & d \end{bmatrix} \) such that at least one of \( a, b, c, d \) is nonzero. We note that since \( I \) is an ideal, \( BA + AC \in I \), for matrices \( B, C \), and so if we can find \( B, C \) such that \( BA + AC \) is invertible, then \( I = R \). We break up into four cases.

(a) Assume \( a \neq 0 \). As we have
\[
\begin{bmatrix} 0 & 0 \\ 1 & 0 \end{bmatrix} \begin{bmatrix} a & b \\ c & d \end{bmatrix} = \begin{bmatrix} 0 & 0 \\ a & b \end{bmatrix}
\]
and
\[
\begin{bmatrix} a & b \\ c & d \end{bmatrix} \begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix} = \begin{bmatrix} 0 & a \\ 0 & c \end{bmatrix},
\]
and their sum is \( \begin{bmatrix} 0 & a \\ a & b + c \end{bmatrix} \), which has determinant \( -a^2 \neq 0 \) by assumption.

(b) Assume \( b \neq 0 \). Then we look at
\[
\begin{bmatrix} 0 & 0 \\ 1 & 0 \end{bmatrix} \begin{bmatrix} a & b \\ c & d \end{bmatrix} + \begin{bmatrix} a & b \\ c & d \end{bmatrix} \begin{bmatrix} 0 & 0 \\ 1 & 0 \end{bmatrix} = \begin{bmatrix} b & 0 \\ a + d & b \end{bmatrix}
\]
and so the determinant is \( b^2 \neq 0 \).

(c) Assume \( c \neq 0 \).
\[
\begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix} \begin{bmatrix} a & b \\ c & d \end{bmatrix} + \begin{bmatrix} a & b \\ c & d \end{bmatrix} \begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix} = \begin{bmatrix} c & a + d \\ 0 & c \end{bmatrix}
\]
which has determinant \( c^2 \).
(d) Assume \( d \neq 0 \).

\[
\begin{bmatrix}
0 & 1 \\
0 & 0
\end{bmatrix}
\begin{bmatrix}
a & b \\
c & d
\end{bmatrix} +
\begin{bmatrix}
a & b \\
c & d
\end{bmatrix}
\begin{bmatrix}
0 & 0 \\
1 & 0
\end{bmatrix}
= \begin{bmatrix}
b + c & d \\
d & 0
\end{bmatrix}
\]

which has determinant \(-d^2\).

Thus, if any one component is nonzero, we have a unit in the ideal. Now, if \( R \) is any ring, \( I \) an ideal, and \( u \in I \) a unit, then \( I = R \), as for all \( x \in R \), we have \( xu^{-1} \in R \), and so \( xu^{-1} \cdot u = x \), and as \( u \in I \), this implies that \( x \in I \). Thus, \( \mathcal{M}_{2 \times 2} \) has only two ideals, 0 and itself.