Homework 2 Solutions

1. Let $R$ be a ring with unity. Show that $R^\times$, the set of units of $R$, is a group under multiplication.

   \textbf{Proof.} Let $R$ be a ring with unity 1 and $R^\times$ be the set of units of $R$.

   - Let $a,b \in R^\times$. Then there exist $a^{-1}, b^{-1} \in R$ (so that $aa^{-1} = 1 = a^{-1}a$ and $bb^{-1} = 1 = b^{-1}b$). Take the element $b^{-1}a^{-1}$, which is in $R$ because $R$ is closed under multiplication. Since $(ab)(b^{-1}a^{-1}) = a(b^{-1}b)a^{-1} = a1a^{-1} = 1$ and $(b^{-1}a^{-1})(ab) = b^{-1}(a^{-1}a)b = b^{-1}1b = 1$, $b^{-1}a^{-1}$ is the multiplicative inverse of $ab$ and hence $ab$ is a unit, so $ab \in R^\times$. This shows that $R^\times$ is closed under multiplication.

   - Since $R$ is a ring, multiplication is associative in $R$, and in particular in the subset $R^\times$ of $R$.

   - Since $1(1) = 1$, 1 is a unit and therefore $1 \in R^\times$.

   - Let $a \in R^\times$. Then there exists $a^{-1} \in R$. Since the multiplicative inverse of $a^{-1}$ is $a$, $a^{-1}$ is a unit and hence $a^{-1} \in R^\times$.

   Therefore, $R^\times$ is a group under multiplication. 

2. (§19, #14) Show that the matrix $\begin{bmatrix} 1 & 2 \\ 2 & 4 \end{bmatrix}$ is a zero divisor in $M_2(\mathbb{Z})$.

   Since $\begin{bmatrix} 1 & 2 \\ 2 & 4 \end{bmatrix}$ and $\begin{bmatrix} 4 & -2 \\ -2 & 1 \end{bmatrix}$ are nonzero, and $\begin{bmatrix} 1 & 2 \\ 2 & 4 \end{bmatrix} \begin{bmatrix} 4 & -2 \\ -2 & 1 \end{bmatrix} = \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}$, $\begin{bmatrix} 1 & 2 \\ 2 & 4 \end{bmatrix}$ is a zero divisor of $M_2(\mathbb{Z})$.

3. An element $a$ of a ring $R$ is \textit{idempotent} if $a^2 = a$. Prove that the only idempotent elements in an integral domain $R$ are 0 and 1.

   \textbf{Proof.} Let $R$ be an integral domain. Let $a \in R$ such that $a^2 = a$. Then $a^2 - a = 0$, so $a(a - 1) = 0$ by distributive laws. If $a \neq 0$, then $a - 1 = 0$ and hence $a = 1$ because $R$ does not contain zero divisors. Therefore, $a = 0$ or $a = 1$.

4. (§19, #29) Show that the characteristic of an integral domain $D$ must be either 0 or a prime $p$. [\textit{Hint: If the characteristic of $D$ is $mn$, consider $(m \cdot 1)(n \cdot 1)$ in $D$.}]

   \textbf{Proof.} Let $D$ be an integral domain and $c$ be its characteristic. If $c \neq 0$, then $c$ is a positive integer. Since $D$ is an integral domain, $D$ is not the zero ring, so $c > 1$. For a contradiction, suppose that $c$ is not prime. Then for some integers $1 < m \leq n < c$, $c = mn$. Then $(m \cdot 1)(n \cdot 1) = (mn) \cdot 1 = c \cdot 1 = 0$. Since $R$ does not contain zero divisors, $m \cdot 1 = 0$ or $n \cdot 1 = 0$. This implies that the characteristic of $R$ is at most $n$, but $n < c$, which contradicts the assumption that $c$ is the characteristic of $R$. Therefore, $c$ must be prime. So the characteristic of $R$
5. (§19, #30) This exercise shows that every ring $R$ can be enlarged (if necessary) to a ring $S$ with unity, having the same characteristic as $R$. Let $S = R \times Z$ if $R$ has characteristic 0, and $R \times Z_n$ if $R$ has characteristic $n$. Let addition in $S$ be the usual addition by components, and let multiplication be defined by

$$(r_1, n_1)(r_2, n_2) = (r_1r_2 + n_1 \cdot r_2 + n_2 \cdot r_1, n_1n_2)$$

where $n \cdot r$ has the meaning explained in Section 18.

(a) Show that $S$ is a ring.

\[ \begin{align*}
((r_1, n_1)(r_2, n_2))(r_3, n_3) & = (r_1r_2 + n_1 \cdot r_2 + n_2 \cdot r_1, n_1n_2)(r_3, n_3) \\
& = (((r_1r_2 + n_1 \cdot r_2 + n_2 \cdot r_1)r_3 + (n_1n_2) \cdot r_3 + n_3 \cdot (r_1r_2 + n_1 \cdot r_2 + n_2 \cdot r_1), (n_1n_2)n_3)
\end{align*} \]

\[ \begin{align*}
& = ((r_1r_2)r_3 + (n_1 \cdot r_2)r_3 + (n_2 \cdot r_1)r_3 + (n_1n_2) \cdot r_3 + n_3 \cdot (r_1r_2) + n_3 \cdot (n_1 \cdot r_2) \\
& \quad + n_3 \cdot (n_2 \cdot r_1), (n_1n_2)n_3) \\
& = (r_1(r_2r_3) + n_1 \cdot (r_2r_3) + n_2 \cdot (r_1r_3) + (n_1n_2) \cdot r_3 + n_3 \cdot (r_1r_2) + (n_1n_3) \cdot r_2 \\
& \quad + (n_2n_3) \cdot r_1, n_1(n_2n_3))
\end{align*} \]

\[ \begin{align*}
(r_1, n_1)((r_2, n_2)(r_3, n_3)) & = (r_1, n_1)(r_2r_3 + n_2 \cdot r_3 + n_3 \cdot r_2, n_2n_3) \\
& = (r_1(r_2r_3 + n_2 \cdot r_3 + n_3 \cdot r_2) + n_1 \cdot (r_2r_3 + n_2 \cdot r_3 + n_3 \cdot r_2) + (n_2n_3) \cdot r_1, n_1(n_2n_3)) \\
& = (r_1(r_2r_3) + r_1(n_2 \cdot r_3) + r_1(n_3 \cdot r_2) + n_1 \cdot (r_2r_3) + n_1 \cdot (n_2 \cdot r_3) + n_1 \cdot (n_3 \cdot r_2) \\
& \quad + (n_2n_3) \cdot r_1, n_1(n_2n_3)) \\
& = (r_1(r_2r_3) + n_2 \cdot (r_1r_3) + n_3 \cdot (r_1r_2) + n_1 \cdot (r_2r_3) + (n_1n_2) \cdot r_3 + (n_1n_3) \cdot r_2 \\
& \quad + (n_2n_3) \cdot r_1, n_1(n_2n_3))
\end{align*} \]
• Distributive laws hold: Let \((r_1, n_1), (r_2, n_2), (r_3, n_3) \in S\). Then

\[
(r_1, n_1)((r_2, n_2) + (r_3, n_3)) = (r_1, n_1)(r_2 + r_3, n_2 + n_3) = (r_1(r_2 + r_3) + n_1 \cdot (r_2 + r_3) + (n_2 + n_3) \cdot r_1, n_1(n_2 + n_3)) = (r_1r_2 + r_1r_3 + n_1 \cdot r_2 + n_1 \cdot r_3 + n_2 \cdot r_1 + n_3 \cdot r_1, n_1n_2 + n_1n_3)
\]

\[
(r_1, n_1)(r_2, n_2) + (r_1, n_1)(r_3, n_3) = (r_1r_2 + n_1 \cdot r_2 + n_2 \cdot r_1, n_1n_2) + (r_1r_3 + n_1 \cdot r_3 + n_3 \cdot r_1, n_1n_3)
\]

and

\[
((r_1, n_1) + (r_2, n_2))(r_3, n_3) = (r_1 + r_2, n_1 + n_2)(r_3, n_3) = ((r_1 + r_2)r_3 + (n_1 + n_2) \cdot r_3 + n_3 \cdot (r_1 + r_2), (n_1 + n_2)n_3)
\]

\[
(r_1r_3 + r_2r_3 + n_1 \cdot r_3 + n_2 \cdot r_3 + n_3 \cdot r_1 + n_3 \cdot r_2, n_1n_3 + n_2n_3)
\]

\[
(r_1, n_1)(r_3, n_3) + (r_2, n_2)(r_3, n_3) = (r_1r_3 + n_1 \cdot r_3 + n_3 \cdot r_1, n_1n_3) + (r_2r_3 + n_2 \cdot r_3 + n_3 \cdot r_2, n_2n_3)
\]

\[
= (r_1r_3 + r_2r_3 + n_1 \cdot r_3 + n_2 \cdot r_3 + n_3 \cdot r_1 + n_3 \cdot r_2, n_1n_3 + n_2n_3)
\]

(b) Show that \(S\) has unity.

**Proof.** Let \((r, n) \in S\). Since \((0, 1) \in S\),

\[
(0, 1)(r, n) = (0(r) + 1 \cdot r + n \cdot 0, 1(n)) = (r, n),
\]

and

\[
(r, n)(0, 1) = (r(0) + n \cdot 0 + 1 \cdot r, n(1)) = (r, n),
\]

\((0, 1)\) is the multiplicative identity of \(S\).

(c) Show that \(S\) and \(R\) have the same characteristic.

**Proof.** If \(R\) has characteristic 0, then \(S = R \times \mathbb{Z}\). If \(n \cdot (0, 1) = (0, 0)\) for some \(n \in \mathbb{Z}^+\), then \((0, 0) = n \cdot (0, 1) = (n \cdot 0, n \cdot 1) = (0, n)\), which is a contradiction since \(n \neq 0\). So the characteristic of \(S\) is also 0.

If \(R\) has characteristic \(n\), then \(S = R \times \mathbb{Z}_n\). If \(k \cdot (0, 1) = (0, 0)\) for some \(k \in \mathbb{Z}^+\), then \((0, 0) = k \cdot (0, 1) = (k \cdot 0, k \cdot 1) = (0, k \cdot 1)\), so the smallest such \(k\)
such that \((0, 0) = (0, k \cdot 1)\) is \(n\) since the characteristic of \(\mathbb{Z}_n\) is \(n\). Therefore, \(S\) also has characteristic \(n\). □

(d) Show that the map \(\phi: R \to S\) given by \(\phi(r) = (r, 0)\) for \(r \in R\) maps \(R\) isomorphically onto a subring of \(S\).

Proof. We’ll show that \(\phi\) is an injective ring homomorphism. Let \(r, s \in R\). Then

\[
\phi(r) + \phi(s) = (r, 0) + (s, 0) = (r + s, 0 + 0) = (r + s, 0) = \phi(r + s)
\]

and

\[
\phi(r)\phi(s) = (r, 0)(s, 0) = (rs + 0 \cdot s + 0 \cdot r, 0(0)) = (rs, 0) = \phi(rs),
\]

so \(\phi\) is a ring homomorphism. If \(\phi(r) = \phi(s)\) for some \(r, s \in R\), then \((r, 0) = (s, 0)\), so \(r = s\). Therefore, \(\phi\) is injective. This implies that \(R\) is isomorphic to the subring \(\phi[R]\) of \(S\). □

6. We will see later that the multiplicative group of nonzero elements of a finite field is cyclic. Illustrate this by finding a generator for this group for the given finite field.

(a) (§20, #1) \(\mathbb{Z}_7\)

\[
3, 5
\]

(b) (§20, #2) \(\mathbb{Z}_{11}\)

\[
2, 6, 7, 8
\]

7. (§20, #4) Use Fermat’s theorem to find the remainder of \(3^{47}\) when it is divided by 23.

Since 23 does not divide 3, by Fermat’s theorem, \(3^{22} \equiv 1 \mod 23\). Then

\[
3^{47} \equiv (3^{22})^2 3^3 \equiv 1^2 27 \equiv 4 \mod 23,
\]

so the remainder is 4.

8. (§20, #10) Use Euler’s generalization of Fermat’s theorem to find the remainder of \(7^{1000}\) when divided by 24.

Since 7 and 24 are relatively prime, by Euler’s theorem, \(7^{\varphi(24)} \equiv 1 \mod 24\). Since \(\varphi(24) = \varphi(2^3 \cdot 3) = \varphi(2^3)\varphi(3) = (2^3 - 2^2)(3 - 1) = 8\),

\[
7^{1000} \equiv (7^8)^{125} \equiv 1^{125} \equiv 1 \mod 24,
\]

so the remainder is 1.
9. (a) \((\S20, \#27)\) Show that 1 and \(p-1\) are the only elements of the field \(\mathbb{Z}_p\) that are their own multiplicative inverse.

\[\text{Proof. If } a \in \mathbb{Z}_p \text{ and } a^2 = 1, \text{ then } a^2 - 1 = 0 \text{ so } (a - 1)(a + 1) = 0. \text{ Since } p \text{ is prime, } \mathbb{Z}_p \text{ has no zero divisors, and hence } a - 1 = 0 \text{ or } a + 1 = 0. \text{ Therefore, } a = 1 \text{ or } a = p - 1. \square\]

(b) \((\S20, \#28)\) Using part (a), deduce Wilson’s Theorem: if \(p\) is a prime, then \((p - 1)! \equiv -1 \mod p.\)

By part (a), since 1 and \(p - 1\) are the only elements in \(\mathbb{Z}_p\) that are their own multiplicative inverse,

\[(p - 1)! = 1(2)(3) \cdots (p - 2)(p - 1) = 1(1) \cdots (1)(p - 1) = p - 1 \equiv -1 \mod p.\]