Homework 4 Solutions
MTH 310

• (2.3 Problem 1) We recall that the units in \( \mathbb{Z}_n \) are exactly those \( a \) such that \((a, n) = 1\). So in \( \mathbb{Z}_7 \) the units are 1, 2, 3, 4, 5, 6; in \( \mathbb{Z}_8 \) the units are 1, 3, 5, 7; in \( \mathbb{Z}_9 \) the units are 1, 2, 4, 5, 7, 8; in \( \mathbb{Z}_{10} \) the units are 1, 3, 7, 9.

• (2.3 Problem 2) There are no zero divisors in \( \mathbb{Z}_7 \) because 7 is prime. The zero divisors in \( \mathbb{Z}_8 \) are 2, 4, 6, because \( 2(4) = 8 = 0 \) and \( 6(4) = 24 = 0 \). The zero divisors in \( \mathbb{Z}_9 \) are 3, 6 since \( 3(6) = 18 = 0 \). The zero divisors in \( \mathbb{Z}_{10} \) are 2, 4, 5, 6, 8 because \( 2(5) = 10 = 0 \), \( 4(5) = 20 = 0 \), \( 6(5) = 30 = 0 \), and \( 8(5) = 40 = 0 \).

• (2.3 Problem 9) (a) Let \( a \) be a unit in \( \mathbb{Z}_n \); say \( au = ua = 1 \). Suppose that \( ab = 0 \). But multiplying by \( u \) we see that \( uab = u(0) \), implying that \( b = 0 \). Ergo \( a \) is not a zero divisor.

(b) The above shows that if \( a \) is a zero divisor in \( \mathbb{Z}_n \), it certainly cannot be a unit.

• (2.3 Problem 10) We use bracket notation to distinguish congruence classes from integers. Problem 9 shows that \([a] \neq [0]\) in \( \mathbb{Z}_n \) is at most one of a unit and a zero divisor. Suppose \([a]\) is not a unit, then \((a, n) = d > 1\). Write \( a = dk \) and \( n = ds \) for \( 0 < s < n \). In particular \([s] \neq [0]\) in \( \mathbb{Z}_n \). Then we see \( as = dks = nk \), so in \( \mathbb{Z}_n \), \([a][s] = [0]\). Hence if \([a]\) is not a unit, it is a zero divisor. This implies that a nonzero element of \( \mathbb{Z}_n \) is exactly one of a unit or a zero divisor.

• (Appendix B Problem 13) (a) Consider the functions

- \( f: B \to C \) where \( f(1) = f(2) = a, f(3) = b, f(4) = c. \)
- \( g: B \to C \) where \( g(1) = a, g(2) = g(3) = b, g(4) = c. \)
- \( h: B \to C \) where \( h(1) = a, h(2) = b, h(3) = h(4) = c. \)
- \( j: B \to C \) where \( j(1) = j(4) = a, j(2) = b, j(3) = c. \)

(b) Consider the functions

- \( f: C \to B \) where \( f(a) = 1, f(b) = 2, f(c) = 3. \)
- \( g: C \to B \) where \( g(a) = 1, g(b) = 3, g(c) = 4. \)
- \( h: C \to B \) where \( h(a) = 1, h(b) = 2, h(c) = 4. \)
- \( j: C \to B \) where \( j(a) = 2, j(b) = 3, j(c) = 3. \)

(c) The complete set of bijections from \( C \) to itself is:

- \( f: C \to C \) where \( f(a) = a, f(b) = b, f(c) = c. \)
– $g: C \to C$ where $g(a) = a$, $g(b) = c$, $g(c) = b$.
– $h: C \to C$ where $h(a) = b$, $h(b) = a$, $h(c) = c$.
– $j: C \to C$ where $j(a) = b$, $j(b) = c$, $j(c) = a$.
– $i: C \to C$ where $i(a) = c$, $i(b) = b$, $i(c) = a$.
– $k: C \to C$ where $k(a) = c$, $k(b) = a$, $h(c) = b$.

• (25)(a) Let $f: \mathbb{Z} \to \mathbb{Z}$ be $f(x) = 2x$. We observe that if $f(x_1) = f(x_2)$, then $2x_1 = 2x_2$, implying after dividing by 2 that $x_1 = x_2$, so $f$ is injective. The remaining three are extremely similar instances of solving an equality.

• (26) Let $a \in \mathbb{R}$. Then $f(a^{\frac{1}{2}}) = a$, so $f$ is surjective. Parts (b) and (c) are similar. For (d), we observe that $\mathbb{Q}$ is definitionally the set of numbers that can be written as $a/b$ for some $(a,b) \in \mathbb{Z}$.

• (27) (a) Let $f: B \to C$ and $g: C \to D$ be both injective. Then suppose that $g \circ f(b_1) = g \circ f(b_2)$. We have $g(f(b_1)) = g(f(b_2))$. By injectivity of $g$, $f(b_1) = f(b_2)$; by injectivity of $f$, $b_1 = b_2$. Ergo $g \circ f(b_1) = g \circ f(b_2)$ implies that $b_1 = b_2$, and therefore $g \circ f$ is injective.

(b) Let $f: B \to C$ and $g: C \to D$ be both surjective. Then say $d \in D$. By surjectivity of $g$, there is some $c \in C$ such that $g(c) = d$; by surjectivity of $f$, there is some $b$ such that $f(b) = c$. We conclude that $g \circ f(b) = d$. As $d$ was arbitrary $g \circ f$ is surjective.

• (28) (a) Let $f: B \to C$ and $g: C \to D$ such that $g \circ f: B \to D$ is injective. Let $x_1, x_2$ be any two elements of $B$ such that $f(x_1) = f(x_2)$. Then $g \circ f(x_1) = g \circ f(x_2)$. Since $g \circ f$ is injective, it follows that $x_1 = x_2$. Hence $f$ is injective.

(b) Let $f$ be the function $f: \{0\} \to \{1, 2\}$ such that $f(0) = 1$ and let $g$ be the function $g: \{1, 2\} \to \{3\}$ such that $g(1) = g(2) = 3$. Then $g$ is not injective, since $g(1) = g(2)$, but $g \circ f: \{0\} \to \{3\}$ is the function given by $g \circ f(0) = 3$, hence is injective.