Math 110A Homework 2

Brendan Connelly

Friday, January 31, 2025

Textbook 2.3

Question 8:

(a) Give three examples of equations of the form $ax = b$ in $\mathbb{Z}_{12}$ that have no nonzero solutions.

(b) For each of the equations in part (a), does the equation $ax = 0$ have a nonzero solution?

a. We have $2 \cdot x = 5, 4 \cdot x = 5, 6 \cdot x = 5$. These equations all have no possible solutions. Each of $2, 4, 6$ do not have multiplicative inverses. But, more directly, we can simply check all possible values of x and none of them hold.

b. They all have a non-zero solution, $6, 3, 2$ respectively.

. . . .

Question 14: Let $a, b, n \in \mathbb{Z}$ with $n > 1$. Let $d = (a, n)$ and assume $d \mid b$. Prove that the equation $[a]x = [b]$ has d distinct solutions in $\mathbb{Z}_n$ as follows:

(a) Show that the solutions listed in Exercise 13(b) are all distinct. [Hint: $[r] = [s]$ if and only if $n \mid (r - s)$.]

(b) If $x = [r]$ is any solution of $[a]x = [b]$, show that $[r] = [ub_1 + kn_1]$ for some integer k with $0 \le k \le d - 1$. [Hint: $[ar] - [aub_1] = [0]$ (Why?), so that $n \mid (a(r - ub_1))$. Show that $n_1 \mid (a_1(r - ub_1))$ and use Theorem 1.4 to show that $n_1 \mid (r - ub_1)$.]

a. We want to show that for $[ub_1 + sn_1] \neq [ub_1 + tn_2]$ for $0 \le s < t \le d - 1$. This will show arbitrary solutions from above our distinct. For contradiction, assume $[ub_1 + sn_1] = [ub_1 + sn_2]$

$$\begin{aligned} &\iff n \mid ub_1 + sn_1 - ub_1 - tn_1 \\ &\iff n \mid sn_1 - tn_1 \\ &\iff n \mid n_1(s - t) \\ &\iff d \mid s - t \end{aligned}$$

However, $s - t < d$. Thus, $s - t = 0 \implies s = t$. Therefore, each solution is distinct. □

b. We know that $[ar] - [b] = 0$. We also know $au + nv = d$ and $db_1 = b$. Hence

$$\begin{aligned} &[ar] - [b] = 0 \\ &\implies [ar] - [db_1] = 0 \\ &\implies [ar] - [b_1][au + nv] = 0 \quad \text{by given} \\ &\implies [ar] - [b_1][au] = 0 \quad \text{because multiple of } n \end{aligned}$$

$$\begin{aligned} &\implies [ar] - [b_1 au] = 0 \\ &\implies n \mid ar - aub_1 \\ &\implies n \mid a(r - ub_1) \\ &\implies n_1 \mid a_1(r - ub_1) \quad \text{by dividing out by } d \\ &\implies n_1 \mid r - ub_1 \quad \text{by thm 1.4} \end{aligned}$$

Thus, we have that $[r] = [ub_1]$. Thus, any solutions is of the form $[r] = [ub_1 + kn_1]$ as additions of multiples of n_1 still satisfy our condition.

Textbook 3.1

Question 28: Let p be a positive prime, and let R be the set of all rational numbers that can be written in the form r/p^i with $r, i \in \mathbb{Z}$, and $i \geq 0$. Note that $\mathbb{Z} \subseteq R$ because each $n \in \mathbb{Z}$ can be written as n/p^0. Show that R is a subring of $\mathbb{Q}$.

Suppose that $\frac{n}{p^i}, \frac{m}{p^j} \in R$. Then, $\frac{n}{p^i} + \frac{m}{p^j} = \frac{np^j + mp^i}{p^{i+j}}$. This is clearly in R as the numerator is an integer and denominator is still a power of p. The same is true for $\frac{n}{p^i} \cdot \frac{m}{p^j} = \frac{nm}{p^{i+j}}$. We have shown closure under addition and multiplication.

Thus, all that remains is to check that $0 \in R$ and that all additive inverses are also in R. Clearly, $0 \in \mathbb{Z}$. Thus, $\frac{0}{p} = 0$, which is the same zero as in $\mathbb{Q}$. Hence, we confirmed this existence.

For an $\frac{n}{p^i} \in R$, we know that $-n \in \mathbb{Z}$, thus, $\frac{-n}{p^i} \in R$. And by the definition of addition,

$$\frac{n}{p^i} + \frac{-n}{p^i} = \frac{n-n}{p^i} = 0$$

Hence, R is a subring.

....

Question 32: Let R be a ring, and let $Z(R) = \{a \in R \mid ar = ra \text{ for every } r \in R\}$. In other words, $Z(R)$ consists of all elements of R that commute with every other element of R. Prove that $Z(R)$ is a subring of R. $Z(R)$ is called the center of the ring R. [Exercise 31 shows that the center of $M(R)$ is the subring of scalar matrices.]

Suppose $a, b \in Z(R)$. Then, $ar = ra \quad br = rb$ for all $r \in R$. Then, consider

$$r(a+b) = ra + rb = ar + br = (a+b)r$$

Hence, addition is closed. Consider

$$r(ab) = (ra)b = (ar)b = a(rb) = a(br) = (ab)r$$

Hence, multiplication is closed in $Z(R)$ as well.

We also need to show that $0 \in Z(R)$. We can show that $0r = 0 = r0$. Consider the following

$$\begin{aligned} &0 + 0 = 0 \\ &\implies r(0+0) = r0 \end{aligned}$$

$$\implies r0 + r0 = r0$$
$$\implies r0 = 0 \quad \text{by additive inverse}$$

and similarly,

$$0 + 0 = 0$$
$$\implies (0 + 0)r = 0r$$
$$\implies 0r + 0r = 0r$$
$$\implies 0r = 0 \quad \text{by additive inverse}$$

Thus, we have that $0r = 0 = r0$ and thus $0 \in Z(R)$. This holds true for any ring.

Lastly, suppose $a \in Z(R)$. Then, we want to show $br = rb$ where $a + b = 0$. We know from immediately prior that

$$r(a + b) = 0 = (a + b)r$$

By distributivity, we have

$$ra + rb = ar + br$$

Then

$$ar + rb = ar + br$$

So

$$rb = br$$

□

Textbook 3.2

Question 26: Let S be a subring of a ring R. Prove that $0_S = 0_R$. [Hint: For $a \in S$, consider the equation $a + x = a$.]

For $a \in S$, consider the equation $a + x = a$. By definition, x satisfies the property of 0_S. We can add the additive inverse of a to both sides, produces $x = 0_R$. This relies on the uniquess of the additive identity. Thus, $0_S = 0_R$.

□

Question 32: Let R be a ring without identity. Let T be the set $R \times \mathbb{Z}$. Define addition and multiplication in T by these rules:

$$(r, m) + (s, n) = (r + s, m + n)$$

$$(r, m)(s, n) = (rs + ms + nr, mn).$$

(a) Prove that T is a ring with identity.

(b) Let R consist of all elements of the form $(r, 0)$ in T. Prove that R is a subring of T.

a. We need to show T is a ring and thus need to check a number of axioms. First consider closure of $(r, m) + (s, n) = (r + s, m + n)$. Each of R and $\mathbb{Z}$ are closed so this is still in T. The same is true of $(r, m)(s, n) = (rs+ms+nr, mn)$ as $rs+ms+nr \in R$, just scaled by integers. For addition, associativity and commutativity automatically follows from the associativity in R and $\mathbb{Z}$. The same is true of the existence of the additive identity and inverse, i.e., $(r, m) + (0_R, 0) = (r, m)$ and $(r, m) + (-r, -m) = (0_R, 0)$. Thus, all we have to really check is the multiplication related axioms. Consider

Associativity of Multiplication For any $(r, m), (s, n), (t, d) \in T$,

$$\begin{aligned}[(r, m)(s, n)](t, d) &= (rs + ms + nr, mn)(t, d) \\ &= \big((rs + ms + nr)t + mn \cdot t + d(rs + ms + nr), mn \cdot d\big) \\ &= (rst + mst + nrt + mnt + drs + dms + dnr, mnd)\end{aligned}$$

We also have that

$$\begin{aligned}(r, m)[(s, n)(t, d)] &= (r, m)(st + nt + ds, nd) \\ &= \big(r(st + nt + ds) + m(st + nt + ds) + nd \cdot r, m \cdot nd\big) \\ &= (rst + rnt + rds + mst + mnt + mds + ndr, mnd)\end{aligned}$$

Both expressions simplify to the same result, given that elements in $\mathbb{Z}$ commute. Hence, multiplication is associative in T.

Distributivity: For any $(r, m), (s, n), (t, d) \in T$,

$$\begin{aligned}(r, m)[(s, n) + (t, d)] &= (r, m)(s + t, n + d) \\ &= (r(s + t) + m(s + t) + (n + d)r, m(n + d)) \\ &= (rs + rt + ms + mt + nr + dr, mn + md)\end{aligned}$$

But also,

$$(r, m)(s, n) + (r, m)(t, d) = (rs + ms + nr, mn) + (rt + mt + dr, md) = (rs + rt + ms + mt + nr + dr, mn + md)$$

Thus, we have distributivity from the left hand side. Distributivity from the right hand side follows from essentially the same computation. Therefore, we have distributivity.

Identity Element: I claim that $(0_R, 1)$ satisfies the identity element. We can check

$$(r, m)(0_R, 1) = (r \cdot 0_R + m \cdot 0_R + 1 \cdot r, m \cdot 1) = (0_R + 0_R + r, m) = (r, m)$$

$$(0_R, 1)(r, m) = (0_R \cdot r + 1 \cdot r + m \cdot 0_R, 1 \cdot m) = (0_R + r + 0_R, m) = (r, m)$$

Thus, $(0_R, 1)$ is the identity element in T.

Hence, T is a ring with identity.

. . . .

b. We need to check the four subring axioms

Non-emptiness: $(0_R, 0) \in S$ since $0_R \in R$, which is the same additive identity checked above.

Closure under Addition: For any $(r, 0), (s, 0) \in S$,

$$(r, 0) + (s, 0) = (r + s, 0 + 0) = (r + s, 0) \in S$$

Closure under Multiplication: For any $(r, 0), (s, 0) \in S$,

$$(r, 0)(s, 0) = (rs + 0 \cdot s + 0 \cdot r, 0 \cdot 0) = (rs, 0) \in S$$

Additive Inverses: For any $(r, 0) \in S$, its additive inverse is $(-r, 0)$, which is also in S.
Hence, S is a subring of T.

. . . .

Question 40: An element a of a ring is nilpotent if $a^n = 0_R$ for some positive integer n. Prove that R has no nonzero nilpotent elements if and only if 0_R is the unique solution of the equation $x^2 = 0_R$.

$(\implies)$ This direction is relatively trivial. Assume that R has no nonzero nilpotent elements. This means that $a^n \neq 0_R$ for all $a \in R$. Take $n = 2$. Then, 0_R is the unique solution of the equation $x^2 = 0_R$.

$(\impliedby)$ Assume 0_R is the unique solution of the equation $x^2 = 0_R$. Then, consider $a^n = 0$. We need to show that for all $n \geq 1$, a must be the zero element for this to hold. We can consider our smaller cases $n = 1$ is trivially true and $n = 2$ is true by our given. We will show this is true for higher n by contradiction.

For contradiction, assume there exists an $n \in \mathbb{N}$ such that $a^n = 0$ but $a \neq 0$. By the WOP, we can choose n to be minimal. However, then, we have that $(a^{n-1})^2 = 0$ but $a \neq 0$ necessarily as $2n - 2 \geq n$ for all $n \geq 2$. But, by our given, we have that

$$a^{n-1} \cdot a^{n-1} = 0 \implies a^{n-1} = 0$$

This contradicts the minimality of n. Thus, such an $n \in \mathbb{N}$ such that $a^n = 0$ but $a \neq 0$ does not exist. Hence, R has no nonzero nilpotent elements. We have shown both directions of the proof and are therefore done.

□