MATH 521A: Abstract Algebra

Exam 2 Solutions

1. Determine, with proof, all zero divisors in $\mathbb{Z}_{34}$. How many are there?

For every integer x satisfying $1 \le x \le 16$, we have $[2x][17] = [34x] = [0]$. However none of the $[2x]$ are $[0]$, and neither is $[17]$; hence we have seventeen zero divisors. There are no more, because Theorem 2.10 states that $[x]$ is a unit in $\mathbb{Z}_{34}$ if and only if $\gcd(x, 34) = 1$. Hence all other elements are units (and not zero divisors), or $[0]$ itself.

2. Find all solutions to the modular equation $50x \equiv 20 \pmod{630}$.

We first apply our congruence theorem with $a = 10$; x a solution to our congruence if and only if it is a solution to $5x \equiv 2 \pmod{63}$. We now use the generalized Euclidean algorithm to determine that $(-25)5 + (2)63 = 1$, so $[-25][5] = [1]$ in $\mathbb{Z}_{63}$. Multiplying, we get $x \equiv (-25)5x \equiv (-25)2 = -50 \pmod{63}$. Hence the unique solution mod 63 is $x = -50$, or $x = 13$. However the problem is mod 630, so there are ten solutions: $[13], [76], [139], [202], [265], [328], [391], [454], [517], [580]$.

3. For ring R and element $x \in R$, we say that x is *silver* if $x + x + x = 0_R$. Define $T \subseteq R$ to be the set of silver elements of R. Prove that T is a subring of R.

(1) T is nonempty, since $0 + 0 + 0 = 0 + 0 = 0$, so $0 \in T$.
(2) Suppose $x, y \in T$. We calculate $(x-y)+(x-y)+(x-y) = (x+x+x)-(y+y+y) = 0 - 0 = 0$, so $x - y \in T$, so T is closed under subtraction.
(3) Suppose again $x, y \in T$. We calculate $xy+xy+xy = (x+x)y+xy = (x+x+x)y = 0y = 0$, so $xy \in T$. Hence T is closed under multiplication.

4. Consider the function $f : \mathbb{Z}_{34} \to \mathbb{Z}_2 \times \mathbb{Z}_{17}$ given by $f : [x]_{34} \mapsto ([x]_2, [x]_{17})$. Prove that f is well-defined.

Suppose that $[x]_{34} = [y]_{34}$, i.e. we have two names for the same element of the domain. Then $34|(x-y)$, i.e. there is some $k \in \mathbb{Z}$ with $34k = x - y$. We use this equation twice: First, $x - y = 34k = 2(17k)$, and $17k \in \mathbb{Z}$, so $2|(x-y)$. This means that $x \equiv y \pmod 2$ and so $[x]_2 = [y]_2$. Second, $x - y = 17(2k)$, and $2k \in \mathbb{Z}$, so $17|(x-y)$. This means that $x \equiv y \pmod{17}$ and so $[x]_{17} = [y]_{17}$. Hence $([x]_2, [x]_{17}) = ([y]_2, [y]_{17})$.

5. Let R have ground set $\mathbb{Z}$ and operations given by:

$$\forall x, y \in \mathbb{Z}, \quad x \oplus y = x + y - 2, \quad x \odot y = 2x + 2y - xy - 2.$$

Prove that R, with operations $\oplus, \odot$, is a commutative ring.

We must check all the axioms. (0) Since $x+y-2, 2x+2y-xy-2 \in \mathbb{Z}$, R is closed under both operations. (1) $x \oplus y = x + y - 2 = y + x - 2 = y \oplus x$, so $\oplus$ is commutative. (2) $(x \oplus y) \oplus z = (x+y-2) \oplus z = x+y-2+z-2 = x+y+z-2-2 = x+(y \oplus z)-2 = x \oplus (y \oplus z)$, so $\oplus$ is associative. (3) We have $0_R = 2$, as $2 \oplus y = 2 + y - 2 = y$, for all $y \in R$. (4) Let $y \in R$. Note that $y \oplus (4-y) = y + (4-y) - 2 = 2 = 0_R$, so $-y = 4 - y$. (5) We calculate $(x \odot y) \odot z = (2x+2y-xy-2) \odot z = 4x+4y-2xy-4+2z-2xz-2yz+xyz+2z+2z-2 =$

$2x+4y+4z-2yz-4-2xy-2yz+xyz+2x-2 = x\odot(2y+2z-yz-2) = x\odot(y\odot z)$. (commutative) We have $x\odot y = 2x+2y-xy-2 = 2y+2x-yx-2 = y\odot x$. This lets us just prove one of the two distributive axioms: (6) $x\odot(y\oplus z) = x\odot(y+z-2) = 2x+2y+2z-4-xy-xz+2x-2 = 2x+2y-xy-2+2x+2z-xz-2-2 = (2x+2y-xy-2)\oplus(2x+2z-xz-2) = (x\odot y)\oplus(x\odot z)$.

6. Let R be a (not necessarily commutative) ring with identity and $x, y \in R$. Suppose that neither x nor y is a zero divisor, and that xy is a unit. Prove that x is a unit.

Since xy is a unit, there is some $u \in R$ with $uxy = xyu = 1$. We have $x(yu) = 1$, so yu is a right inverse to x. We multiply $uxy = 1$ on the left by y to get $yuxy = y1 = y = 1y$. Since y is not a zero divisor, we may cancel it on the right (by a theorem proved in class), to get $yux = 1$ or $(yu)x = 1$. Hence yu is also a left inverse to x.

7. Let R be the ring of 2×2 upper triangular matrices with entries from $\mathbb{Q}$, i.e. $R = \{\left(\begin{smallmatrix} a & b \\ 0 & c \end{smallmatrix}\right) : a, b, c \in \mathbb{Q}\}$. Determine, with proof, all units and zero divisors of R.

Claim 1: If $ac \neq 0$ then the matrix is a unit. We have $\left(\begin{smallmatrix} a & b \\ 0 & c \end{smallmatrix}\right)\begin{pmatrix} 1/a & -b/ac \\ 0 & 1/c \end{pmatrix} = \left(\begin{smallmatrix} 1 & 0 \\ 0 & 1 \end{smallmatrix}\right) = 1_R$.

Claim 2: If $ac = 0$ then the matrix is a zero divisor. We have $\left(\begin{smallmatrix} a & b \\ 0 & c \end{smallmatrix}\right)\left(\begin{smallmatrix} c & -b \\ 0 & a \end{smallmatrix}\right) = \left(\begin{smallmatrix} 0 & 0 \\ 0 & 0 \end{smallmatrix}\right) = 0_R$.

No element can be both a unit and a zero divisor (by a homework problem). Since the two claims above cover all cases, no element can be neither.

8. Let R be the ring of 2×2 matrices with entries from $\mathbb{Q}$. Define $f : R \to R$ via $f : \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \mapsto \left(\begin{smallmatrix} a & c \\ b & d \end{smallmatrix}\right)$, a.k.a. the matrix transpose. Prove or disprove that f is a ring isomorphism.

We calculate $f\left(\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)\left(\begin{smallmatrix} a' & b' \\ c' & d' \end{smallmatrix}\right)\right) = f\left(\left(\begin{smallmatrix} aa'+bc' & ab'+bd' \\ ca'+dc' & cb'+dd' \end{smallmatrix}\right)\right) = \left(\begin{smallmatrix} aa'+bc' & ca'+dc' \\ ab'+bd' & cb'+dd' \end{smallmatrix}\right)$.
However $f\left(\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)\right)f\left(\left(\begin{smallmatrix} a' & b' \\ c' & d' \end{smallmatrix}\right)\right) = \left(\begin{smallmatrix} a & c \\ b & d \end{smallmatrix}\right)\left(\begin{smallmatrix} a' & c' \\ b' & d' \end{smallmatrix}\right) = \left(\begin{smallmatrix} aa'+cb' & ac'+cd' \\ ba'+db' & bc'+dd' \end{smallmatrix}\right)$. Since these disagree, f is not a ring homomorphism (and hence not a ring isomorphism). As it happens, f satisfies all other ring isomorphism properties.