Modern Algebra I HW 2 Solutions

Theo Coyne

Problem 1.

1. Reflexivity: $a \leq a$ holds for every $a \in \mathbb{Q}$.

   Symmetry: $a \leq b$ does not imply $b \leq a$. Take any $a < b$ to see this.

   Transitivity: $a \leq b$ and $b \leq c$ does imply $a \leq c$.

   Since symmetry fails, R isn't an equivalence relation.

2. Reflexivity: $a - a = 0 \in \mathbb{Z}$ is true for every $a \in \mathbb{R}$

   Symmetry: If $a - b \in \mathbb{Z}$, then $b - a = -(a - b)$ is an integer too, since integers are closed under negation.

   Transitivity: If $a-b \in \mathbb{Z}$ and $b-c \in \mathbb{Z}$, then $a-c = (a-b)+(b-c) \in \mathbb{Z}$ since the integers are closed under addition.

   So, R is an equivalence relation

3. Reflexivity: $a + a = 2a$ is even for every $a \in \mathbb{Z}$. So $(a, a) \notin R$ for every $a \in \mathbb{Z}$.

   Symmetry: If $a + b$ is odd, then $b + a$ is odd too since $b + a = a + b$ (addition is commutative).

   Transitivity: If $a+b$ is odd and $b+c$ is odd, then $a+c = (a+b)+(b+c) - 2b$ is of the form $odd + odd - even$ and so is even. So, for any choice of $(a, b) \in R$ and $(b, c) \in R$, it is necessarily the case that $(a, c) \notin R$. Since such a, b, c exist, transitivity fails.

   Since reflexivity and transitivity fail, R isn't an equivalence relation. Of course, it's not necessary to check that reflexivity and transitivity fail this strongly; it's enough to give a single example of an a for which $(a, a) \notin R$ (for reflexivity) and a single example of a, b, c for which $(a, b) \in R$ and $(b, c) \in R$ but $(a, c) \notin R$ (for transitivity). For example, note that $(1, 1) \notin R$ because $1 + 1 = 2$ is even and $(0, 1) \in R$, $(1, 0) \in R$, but $(0, 0) \notin R$.

4. There's not much to check here. Equality satisfies reflexivity, symmetry, transitivity. It is an equivalence relation.

5. All of reflexivity, symmetry, and transitivity follow from the same properties of equality on $\mathbb{R}$.

   Reflexivity: For any $a \in \mathbb{C}$, we have $|a| = |a|$ because equality (on $\mathbb{R}$) is reflexive, so $(a, a) \in R$.

   Symmetry: If $a, b \in \mathbb{C}$ satisfy $|a| = |b|$, then we must have $|b| = |a|$, by symmetry of equality on $\mathbb{R}$.

   Transitivity: If $|a| = |b|$ and $|b| = |c|$, then $|a| = |c|$, because, you guessed it, equality is transitive.

6. The condition $n = m$ or $n = -m$ is equivalent to $|n| = |m|$, which defines an equivalence relation on $\mathbb{Q}$ by the above argument.

   Remark 1. *In general, if X is a set and $f : X \to Y$ is a function, we can define an equivalence relation on X by $(x_1, x_2) \in R$ if $f(x_1) = f(x_2)$ since equality (on Y) is an equivalence relation. The last three items are the clearest examples of this in the problem (take $f : X \to X$ the identity, $f : \mathbb{C} \to \mathbb{R}$ absolute value and $f : \mathbb{Q} \to \mathbb{R}$ absolute value, respectively) but in fact every equivalence relation can be realized this way by careful choice of f. To see this, let Y be the set of equivalence classes of X and set $f(x)$ to be the equivalence class of x for each x.*

Problem 2.

1. $\gcd(-100, 16) = \gcd(-100 + 96(6), 16) = \gcd(-4, 16) = 4$
2. $\gcd(468, 528) = \gcd(468, 528-467) = \gcd(468, 60) = \gcd(468-7(60), 60) = \gcd(48, 60) = \gcd(48, 12) = 12$
3. $\gcd(-30, -27) = \gcd(-30 - (-27), -27) = \gcd(-3, -27) = 3$
4. Every factor of -15 is also a factor of 0, so the greatest common divisor of -15 and 0 is just the largest divisor of -15, which is 15.
5. $\gcd(1, -1) = 1$
6. $lcm(100, 16) = \frac{(100)(16)}{\gcd(100,16)} = \frac{(100)(16)}{4} = 400$
7. $lcm(27, -5) = 27(5) = 135$ since $5, 27$ are coprime. Keep in mind that lcm is always defined to be positive.

Problem 3.

First, we verify the fact that a natural number has only even exponents in its prime factorization if and only if it is a perfect square. Let a be a perfect square and write $a = b^2$ for some natural b. Let $b = \prod_{p \in P} p^{e_p}$ be the prime factorization of b with the product taken over the (possibly empty) set P of primes dividing b (the empty product is by convention equal to 1). Then $a = b^2 = \prod_{p \in P} p^{2e_P}$ has all even exponents as required. For the other direction, suppose $c \in \mathbb{N}$ has prime factorization $c = \prod_p p^{e_p}$ with all of the e_p even, say equal to $2f_p$. Then $c = \left(\prod_p p^{f_p}\right)^2$ is a perfect square.

Now, onto the problem: let $x = \prod_{p \in P} p^{e_p}$ be the prime factorization of x and let $y = \prod_{q \in Q} q^{f_q}$ be the prime factorization of y, where P and Q are the sets of primes dividing x and y, respectively. Then, $p \neq q$ for all $p \in P$ and $q \in Q$, i.e. $P \cap Q = \emptyset$, because x and y are coprime. So, the prime factorization of xy is

$$xy = \prod_{p \in P} p^{e_p} \prod_{q \in Q} q^{f_q} = \prod_{p \in P \cup Q} p^{g_p}$$

where g_p is defined to be e_p if $p \in P$ and f_p if $p \in Q$; this is well-defined because every element of $P \cup Q$ is in either P or Q and no such element is in both. Since xy is a perfect square, all of the g_p are even and for all $p \in P$, we have $e_p = g_p$, so x is a perfect square by the first paragraph. Similarly for y. Notice that this argument works even if P or Q is empty, corresponding to $x = 1$ or $y = 1$.

Problem 4.

1. Since $d|m$ and $e|n$, there are integers q, r such that $dq = m$ and $er = n$. So, $mn = (dq)(er) = (de)(qr)$ and we see that de divides mn.

2. Since $d|n$, we may write $n = dq$ for some $q \in \mathbb{Z}$. Since $n \neq 0$ and $d \neq 0$ (because $d \in \mathbb{N}$), we also have $q \neq 0$, which implies $|q| \geq 1$. Now, $|n| = |q| \cdot |d| \geq |d|$.

3. Since $c|m$ and $c|n$, there exist integers q, r such that $m = cq$ and $n = cr$. So, $xm+yn = xcq+ycr = c(xq+yr)$ and it follows that c divides $xm+yn$.

Problem 5.

Suppose $n = dq_1+r_1 = dq_2+r_2$ are as stated in the problem. Then, $d(q_2-q_1) = r_1 - r_2$. Suppose for contradiction $q_1 \neq q_2$. Since r_1 and r_2 are elements of $\{0, \ldots, d-1\}$, we have $-r_2 \leq r_1 - r_2 \leq r_1$ and so $|r_1 - r_2| \leq \max(r_1, r_2) < d$. But by part 2 of the previous problem, we know $d \leq |r_1 - r_2|$ since d divides $r_1 - r_2 = d(q_2 - q_1) \neq 0$. This is a contradiction. So, $q_1 = q_2$ and also $r_1 = r_2$ follows from $d(q_2 - q_1) = r_1 - r_2$.