Solutions to Select Problems of HW #1

Dmytro Yeroshkin

September 20, 2013

Section 1.1 Problem 12

Problem

In Example 1.1.3 of an equivalence relation given in the text, prove that the relation defined is an equivalence relation and that there are exactly n distinct equivalence classes, namely, $cl(0), cl(1), \ldots, cl(n-1)$.

Solution

From Example 1.1.3 we have $a \sim b$ if $a - b$ is divisible by n. So we verify the three properties of an equivalence relation. $a - a = 0$ is divisible by every $n \in \mathbb{Z}$, so $a\tilde{a}$ holds. If $a \sim b$, then $a - b = k \cdot n$, so $b - a = (-k) \cdot n$, and so we conclude that $b \sim a$. Finally, if $a \sim b$ and $b \sim c$, we have $a - b = k \cdot n$, $b - c = l \cdot n$, so $a - c = (a - b) + (b - c) = (k + l) \cdot n$, so $a \sim c$. Therefore, $\sim$ is an equivalence relation on the integers.

Next, we illustrate that $cl(0), cl(1), \ldots, cl(n-1)$ are the equivalence classes of $\sim$. To do this, we first verify that all n of these classes are distinct. Let a, b be two distinct positive integers in the list $0, 1, \ldots, n-1$, then $0 < |a - b| < n$, so $a - b$ is not divisible by n. Therefore, a and b are in different equivalence classes, so the n classes listed above are distinct. Now suppose that $a \in \mathbb{Z}$, we demonstrate that a is in one of these n classes. We use the division algorithm to see that $a = q \cdot n + r$, where $0 \leq r < n$ is an integer, so $a - r = q \cdot n$ is a multiple of n, so $a \sim r$, and $a \in cl(r)$. Therefore, a is in one of these classes.

This means that $cl(0), cl(1), \ldots, cl(n-1)$ are the n distinct equivalence classes of $\sim$.

Section 1.2 Problem 1

Problem

In the following, where $\sigma : S \to T$, determine whether the σ is onto and/or one-to-one and determine the inverse image of any $t \in T$ under σ.

(a) S=set of real numbers, T=set of nonnegative real numbers $s\sigma = s^2$.

(b) S=set of nonnegative real numbers, T=set of nonnegative real numbers, $s\sigma = s^2$.

(c) S=set of integers, T=set of integers, $s\sigma = s^2$.

(d) S=set of integers, T=set of integers, $s\sigma = 2s$.

Solution

We remark, that to show that σ is not one-to-one, it suffices to show that there exist $s_1, s_2 \in S$ such that $s_1\sigma = s_2\sigma$. Similarly, to show that σ is not onto, it suffices to show that there exists $t \in T$ such that there is no $s \in S$ with $s\sigma = t$.

(a) $s\sigma = s^2$ is onto, but not one-to-one. Observe that $1\sigma = 1 = (-1)\sigma$, therefore, σ is not one-to-one. But given $t \in T$, $\left(\sqrt{t}\right)\sigma = t$, and similarly, $\left(-\sqrt{t}\right)\sigma = t$, shows that σ is onto. Furthermore, for any $t \in T$, if $t > 0$, the inverse image of t is $\{-\sqrt{t}, \sqrt{t}\}$; if $t = 0$, the inverse image of t is $\{0\}$.

(b) $s\sigma = s^2$ is one-to-one and onto. Observe that the inverse image of each $t \in T$ is the unique nonnegative real number $\sqrt{t}$. Therefore, for each t we have some s with $s\sigma = t$, and for any s_1 there is no distinct s_2 such that $s_1\sigma = s_2\sigma$.

(c) $s\sigma = s^2$ is neither one-to-one nor onto. Observe that there is no integer s such that $s\sigma = -1$, so σ is not onto. Furthermore, $(-1)\sigma = 1 = (1)\sigma$, so σ is not one-to-one. Finally, if t is in the image of σ, then the inverse image of t is either $\{0\}$ if $t = 0$ or $\{-\sqrt{t}, \sqrt{t}\}$ if $t > 0$.

(d) $s\sigma = 2s$ is one-to-one, but not onto. Observe that there is no integer s such that $s\sigma = 1$, so σ is not onto. Also, if $s_1\sigma = t = s_2\sigma$, then $2s_1 = 2s_2$, so $s_1 = s_2$. Therefore, σ is one-to-one. If t is in the image of σ, then the inverse image of t is $\{t/2\}$.

Section 1.3 Problem 6

Problem

Given a, b, non applying the Euclidean algorithm successively we have

$$\begin{aligned}
a &= q_0 b + r_1, && 0 \le r_1 < |b|, \\
b &= q_1 r_1 + r_2, && 0 \le r_2 < r_1, \\
r_1 &= q_2 r_2 + r_3, && 0 \le r_3 < r_2, \\
&\vdots \\
r_k &= q_{k+1} r_{k+1} + r_{k+2}, && 0 \le r_{k+2} < r_{k+1}.
\end{aligned}$$

Since the integers r_k are decreasing and are all nonnegative, there is a first integer n such that $r_{n+1} = 0$. Prove that $r_n = (a, b)$. (We consider, here, $r_0 = |b|$.)

Solution

We prove that $r_n = (a, b)$ in two steps. We first prove that r_n divides both a and b; then we show that $r_n = a \cdot l_n + b \cdot m_n$, and therefore, if d divides a and b, it must divide r_n.

Observe that $r_{n-1} = q_n r_n$, so r_n divides r_{n-1}. By induction, we assume that r_n divides $r_n, r_{n-1}, \ldots, r_{k+1}$, so r_n must divide $r_k = q_{k+1} r_{k+1} + r_{k+2}$. This shows that r_n divides all r_j, so in particular, r_n must divide r_1 and r_2. Therefore, r_n divides $b = q_1 r_1 + r_2$, and it must divide $a = q_0 b + r_1$. So, r_n divides both a and b.

For the second part, we observe that $r_0 = |b|$ is either b or $-b$ and $r_1 = a - q_0 b$. By induction, we assume that $r_0, r_1, \ldots, r_{k-1}$ are of the form $r_i = a \cdot l_i + b \cdot m_i$, then $r_{k-2} = q_{k-1} r_{k-1} + r_k$, so

$$\begin{aligned}
r_k &= r_{k-2} - q_{k-1} r_{k-1} \\
&= (a l_{k-2} + b m_{k-2}) - q_{k-1}(a l_{k-1} + b m_{k-1}) \\
&= a(l_{k-2} - q_{k-1} l_{k-1}) + b(m_{k-2} - q_{k-1} m_{k-1})
\end{aligned}$$

has the form $a l_k + b m_k$. In particular we have $r_n = a \cdot l_n + b \cdot m_n$, so if d divides a and b, then d must divide r_n.

Therefore, we conclude that $r_n = (a, b)$.