Math 347, Honors h/wk 3 (Solutions)
Due Monday, April 15

**Problem 1.** Let $A$ be a non-empty set and let $R' \subseteq A \times A$ be a binary relation on $A$. Put

$$S = \{ R'' \subseteq A \times A | \text{R'' is an equivalence relation on A such that R' \subseteq R''} \}.$$ 

Finally, put

$$R = \cap_{R'' \in S} R''$$

(1) Prove that $S \neq \emptyset$, that is, that there exists some equivalence relation $R''$ on $A$ such that $R' \subseteq R''$.

(2) Prove that $R$ is an equivalence relation on $A$.

[The relation $R$, defined above, is called the equivalence relation on $A$ generated by $R'$.]

**Solution.**

(1) Take $R'' = A \times A$. Then $R''$ is an equivalence relation on $A$, and thus $S \neq \emptyset$, as required.

(2) For every $x \in A$ and every $R'' \in S$ we have $(x, x) \in R''$ since $R''$ is an equivalence relation on $A$ and thus is reflexive. Since $S \neq \emptyset$ and $(x, x) \in R''$ for every $R'' \in S$, it follows, by definition of the intersection of sets, that $(x, x) \in \cap_{R'' \in S} R''$, that is, $(x, x) \in R$. Thus $R$ is reflexive.

Now let $x, y \in A$ be such that $(x, y) \in R = \cap_{R'' \in S} R''$. This means that $(x, y) \in R''$ for every $R'' \in S$. Since each $R'' \in S$ is an equivalence relation on $A$ and thus is symmetric, it follows that $(y, x) \in R''$ for every $R'' \in S$. Therefore $(y, x) \in \cap_{R'' \in S} R''$, that is, $(y, x) \in R$. Thus $R$ is symmetric.

Suppose now that $x, y, z \in A$ are such that $(x, y) \in R$ and $(y, z) \in R$. Since $R = \cap_{R'' \in S} R''$, this implies that for every $R'' \in S$ we have $(x, y) \in R''$ and $(y, z) \in R''$. Since each $R'' \in S$ is an equivalence relation on $A$ and thus is transitive, it follows that $(x, z) \in R''$ for every $R'' \in S$. Therefore $(x, z) \in \cap_{R'' \in S} R'' = R$, so that $R$ is reflexive.

Thus the relation $R$ on $A$ is reflexive, symmetric and transitive, that is $R$ is an equivalence relation on $A$.

**Problem 2.**

Let $A = \mathbb{Z}$ and consider the relation $R'$ on $\mathbb{Z}$ defined as

$$R' = \{(n, n + 2) | n \in \mathbb{Z} \}.$$ 

Let $R$ be the equivalence relation on $\mathbb{Z}$ generated by $R'$.

Prove that $R$ is exactly the relation $\equiv_2$ of congruence mod 2 on $\mathbb{Z}$.

**Proof.** Recall that $\equiv_2 = \{(m, n) \in \mathbb{Z} \times \mathbb{Z} : 2|(m - n)\}$.

We will show that $\equiv_2 \subseteq R$ and that $R \subseteq \equiv_2$.

Put

$$S = \{ R'' \subseteq \mathbb{Z} \times \mathbb{Z} | \text{R'' is an equivalence relation on Z such that R' \subseteq R''} \}.$$
By definition \( R = \cap_{R' \in S} R'' \).

Since for every \( n \in \mathbb{Z} \) we have \( n \equiv_2 n + 2 \), it follows that \( R' \subseteq \equiv_2 \).

Moreover, \( \equiv_2 \) is an equivalence relation on \( \mathbb{Z} \). Hence, by definition of \( S \), we have \( \equiv_2 \in S \). Since \( R = \cap_{R' \in S} R'' \) and \( \equiv_2 \in S \), it follows that \( R \subseteq \equiv_2 \).

We now need to show that \( \equiv_2 \subseteq R \). Note that \( R \) is an equivalence relation on \( \mathbb{Z} \). Also, since \( R' \subseteq R'' \) for every \( R'' \in S \), it follows that \( R' \subseteq R \).

Let \( m, n \in \mathbb{Z} \) be arbitrary integers such that \((m, n) \in \equiv_2\), that is, such that \( 2|(m - n) \). We claim that \((m, n) \in R\).

If \( m = n \) then \((m, n) \in R\) since \( R \) is an equivalence relation and thus \( R \) is transitive.

If \( m \neq n \) then either \( m < n \) or \( m > n \). We will assume that \( m < n \) as the other case is similar. Since \( 2|(m - n) \) and \( m < n \), there exists \( k \in \mathbb{N} \) such that \( n = m + 2k \).

Then, by definition of \( R' \), we have \((m, m + 2) \in R', (m + 2, m + 4) \in R', \ldots, (m + 2(k - 1), m + 2k) \in R' \). Since \( R' \subseteq R \), this means that

\[
(m, m + 2) \in R, (m + 2, m + 4) \in R, \ldots, (m + 2(k - 1), m + 2k) \in R.
\]

Since \( R \) is an equivalence relation and thus is transitive, it follows that \((m, m + 2k) \in R \), that is \((m, n) \in R \).

Thus we have verified that whenever \((m, n) \in \equiv_2\) then \((m, n) \in R \). Therefore \( \equiv_2 \subseteq R \). Since we have already shown that \( R \subseteq\equiv_2 \), it follows that \( R = \equiv_2 \), as required.

\(\square\)

**Problem 3.** Let \( A = \mathbb{R}[x] \), the set of all polynomials with coefficients in \( \mathbb{R} \), and let \( h = x^2 + 1 \in \mathbb{R}[x] \).

Consider the binary relation \( R \) on \( \mathbb{R}[x] \) where

\[
R = \{(f, g) \in \mathbb{R}[x] \times \mathbb{R}[x] | \text{ there exists } q \in \mathbb{R}[x] \text{ such that } \ f = g + qh \}.
\]

(1) Prove that \( R \) is an equivalence relation on \( \mathbb{R}[x] \).

(2) Prove that \( T = \{a + bx | a, b \in \mathbb{R}\} \) is a transversal for \( R \) on \( \mathbb{R}[x] \). **Hint:** Use division with the remainder for polynomials.

(3) For all \( f, g \in \mathbb{R}[x] \) put \([f]_R + [g]_R := [f + g]_R \) and \([f]_R \cdot [g]_R := [fg]_R \). Prove that these formulas give well-defined binary operations \(+, \cdot\) on \( \mathbb{R}[x]/R \).

(4) Consider the map \( \tau : \mathbb{C} \to \mathbb{R}[x]/R \) given by \( \tau(a + bi) = [a + bx]_R \), where \( a, b \in \mathbb{R} \).

Prove that \( \tau \) is a bijection and that \( \tau \) has the property that for all \( z_1, z_2 \in \mathbb{Z} \) we have \( \tau(z_1 + z_2) = \tau(z_1) + \tau(z_2) \) and \( \tau(z_1z_2) = \tau(z_1)\tau(z_2) \).

(5) Find a polynomial \( f(x) \in \mathbb{R}[x] \) such that \([f]_R \cdot [2x^3 + 3]_R = [1]_R \) in \( \mathbb{R}[x] \). Carefully justify that your \( f(x) \) has the required property. **Hint:** Use the result of part (4).

**Solution.**
(1) For any $f \in \mathbb{R}[x]$ we have $f - f = 0 = 0 \cdot h$, so that $(f, f) \in R$. Thus $R$ is transitive.

Suppose now that $f, g \in \mathbb{R}[x]$ are such that $(f, g) \in R$. Thus there exists $q \in \mathbb{R}[x]$ such that $f - g = qh$. Hence $g - f = -qh = (-q)h$ and so $(g, f) \in R$. Thus $R$ is symmetric.

Suppose now that $f, g, p \in \mathbb{R}[x]$ are such that $(f, g) \in R$ and $(g, p) \in R$. Hence there exist $q_1, q_2 \in \mathbb{R}[x]$ such that $f - g = q_1h$ and $g - p = q_2h$.

Adding these two equalities we get $f - p = q_1h + q_2h = (q_1 + q_2)h$. Therefore $(f, p) \in R$. Thus $R$ is transitive.

We have shown that the relation $R$ on $\mathbb{R}[x]$ is reflexive, symmetric and transitive, so that $R$ is an equivalence relation, as required.

(2) First we claim that if $t_1, t_2 \in T$ are such that $t_1Rt_2$ then $t_1 = t_2$.

Indeed, suppose $t_1 = a_1 + b_1x, t_2 = a_2 + b_2x \in T$ are such that $t_1Rt_2$ (where $a_1, b_1, a_2, b_2 \in \mathbb{R}$.)

Then $t_1 - t_2 = (a_1 - a_2) + (b_1 - b_2)x = q(x^2 + 1)$ for some polynomial $q \in \mathbb{R}[x]$. Note that if $q \neq 0$ then $\deg(q(x^2 + 1)) \geq 2$. Since $\deg((a_1 - a_2) + (b_1 - b_2)x) \leq 1$, it now follows that $q = 0$. Thus $t_1 - t_2 = 0 \cdot (x^2 + 1) = 0$ and hence $t_1 = t_2$ as claimed.

We now claim that for every $f \in \mathbb{R}[x]$ there exists $t \in T$ such that $(f, t) \in R$.

Let $f \in \mathbb{R}[x]$ be arbitrary. Then there exist polynomials $q, r \in \mathbb{R}[x]$ such that $f = q(x^2 + 1) + r$ in $\mathbb{R}[x]$ and such that $\deg(r) < \deg(x^2 + 1) = 2$, i.e. $\deg(r) \leq 1$. Thus $r = a + bx$ for some $a, b \in \mathbb{R}$, so that $r \in T$. Then $f - r = q(x^2 + 1)$ and hence $(f, r) \in R$, establishing the second claim.

Thus we have shown that for every $f \in \mathbb{R}[x]$ there exists $t \in T$ such that $fRt$. We have also shown that if $t_1, t_2 \in T$ are such that $t_1Rt_2$ then $t_1 = t_2$.

It follows that $T$ is a transversal for $R$, as required.

(3) We need to check that if $f, g, f_1, g_1 \in \mathbb{R}[x]$ are such that $[f]_R = [f_1]_R$ and $[g]_R = [g_1]_R$ then $[fg]_R = [f_1g_1]_R$ and $[f + g]_R = [f_1 + g_1]_R$.

Since $[f]_R = [f_1]_R$ and $[g]_R = [g_1]_R$, there are $q, g_1 \in \mathbb{R}[x]$ such that $f - f_1 = qh$ and $g - g_1 = q_1h$.

By adding these two equalities we get

$$(f + g) - (f_1 + g_1) = qh + q_1h = (q + q_1)h$$

and hence $(f + g)R(f_1 + g_1)$, that is $[f + g]_R = [f_1 + g_1]_R$, as required.

By multiplying the equalities $f = f_1 + qh$ and $g = g_1 + q_1h$ we get

$$fg = f_1g_1 + f_1q_1h + qhg_1 + qq_1h^2 = f_1q_1 + (f_1q_1 + gq_1 + qg_1)h$$

and hence

$$fg - f_1g_1 = (f_1q_1 + gq_1 + qg_1)h.$$
have $[a + bx]_R = [a_1 + b_1x]_R$, that is $(a + bx, a_1 + bx) \in R$. Since $T$ is a transversal for $R$ and $a + bx, a_1 + bx \in T$, the fact that $(a + bx, a_1 + bx) \in R$ implies that $a + bx = a_1 + b_1x$, so that $a = a_1$ and $b = b_1$. Hence $z = z_1$ and thus $\tau$ is injective.

Now let $f \in \mathbb{R}[x]$ be arbitrary. Since $T$ is a transversal for $R$, there exists a polynomial $a + bx \in T$ such that $[f]_R = [a + bx]_R$. Then, by definition of $\tau$, we have $\tau(a + bi) = [a + bx]_R = [f]_R$. Therefore $\tau$ is surjective. We have shown that $\tau : \mathbb{C} \to \mathbb{R}[x]/R$ is both injective and surjective, so that $\tau$ is a bijection, as required.

Now let $z_1 = a_1 + b_1i, z_2 = a_2 + b_2i \in \mathbb{C}$ be arbitrary. We have $z_1 + z_2 = (a_1 + a_2) + (b_1 + b_2)i$ and $z_1 z_2 = (a_1a_2 - b_1b_2) + (a_1b_2 + a_2b_1)i$.

We have
\[\tau(z_1 + z_2) = \tau((a_1 + a_2) + (b_1 + b_2)i) = [(a_1 + a_2) + (b_1 + b_2)x]_R = [a_1 + b_1x]_R + [a_2 + b_2x]_R = \tau(z_1) + \tau(z_2),\]
as required.

We also have
\[\tau(z_1 z_2) = [(a_1a_2 - b_1b_2) + (a_1b_2 + a_2b_1)x]_R\]
and
\[\tau(z_1)\tau(z_2) = [a_1 + b_1x]_R + [a_2 + b_2x]_R = [(a_1 + b_1x)(a_2 + b_2x)]_R = [a_1a_2 + (b_1a_2 + a_1b_2)x + b_1b_2x^2]_R\]
Note that $x^2 - (-1) = h = 1 \cdot h$, so that $x^2 R(-1)$, that is $[x^2]_R = [-1]_R$. Therefore
\[\tau(z_1)\tau(z_2) = [a_1a_2 + (b_1a_2 + a_1b_2)x + b_1b_2x^2]_R = [(a_1a_2 - b_1b_2) + (a_1b_2 + a_2b_1)x]_R = \tau(z_1 z_2),\]
as required.

(5) We have $2x^3 + 3 = 2x(x^2 + 1) - 2x + 3$. Therefore
\[[2x^3 + 3]_R = [3 - 2x]_R = \tau(3 - 2i)\]
In $\mathbb{C}$ we have
\[(3 - 2i)^{-1} = \frac{1}{3 - 2i} = \frac{1}{3 - 2i} \cdot \frac{3 + 2i}{3 + 2i} = \frac{3 + 2i}{3^2 + 2^2} = \frac{3 + 2i}{13} = \frac{3}{13} + \frac{2}{13}i.
Thus $(3 - 2i)(\frac{3}{13} + \frac{2}{13}i) = 1$. Note that by definition of $\tau$ we have $\tau(1) = [1]_R$.
By the result of (4) we now have
\[[1]_R = \tau(1) = \tau((3 - 2i)(\frac{3}{13} + \frac{2}{13}i)) = \tau(3 - 2i)\tau(\frac{3}{13} + \frac{2}{13}i) =
[3 - 2x]_R [\frac{3}{13} + \frac{2}{13}x]_R = [2x^3 + 3]_R [\frac{3}{13} + \frac{2}{13}x]_R.
Thus $f = \frac{3}{13} + \frac{2}{13}x$ satisfies the requirement $[f]_R \cdot [2x^3 + 3]_R = [1]_R$.