MATH 273 LAB TEST 5 SOLUTIONS Noon Friday November 19, 2010

Time allowed: 50 minutes. Books, notes and calculators allowed. You may work together, but please write out your answers in your own words.

1. (p. 194 #8.20) A relation R on a nonempty set A is defined to be **circular** if, for all $x, y, z \in A$, whenever xRy and yRz, then zRx. Prove that a relation R on A is an equivalence relation if and only if R is circular and reflexive.

Proof. Let R be an arbitrary relation on A. We must prove that

(i) If R is an equivalence relation on A, then R is circular and reflexive; and

(ii) If R is circular and reflexive, then R is an equivalence relation on A.

Proof of (i). Assume that R is an equivalence relation on A, which means that R is reflexive, symmetric, and transitive. We want to prove that R is circular and reflexive. We already know R is reflexive, so we only need to prove that R is circular. So let $x, y, z \in A$ be arbitrary so that xRy and yRz. We want to prove that zRx. Since R is transitive and xRy and yRz, we know that xRz. Since R is symmetric and xRz, we know that zRx. Thus R is circular.

Proof of (ii). Assume that R is circular and reflexive. We want to prove that R is an equivalence relation. We already know R is reflexive, so we need to prove that R is symmetric and transitive.

For symmetry, assume that $x, y \in A$ so that xRy. We want to prove that yRx. Since R is reflexive and $y \in A$, we know that yRy. Since R is circular and xRy and yRy, we know that yRx. Thus R is symmetric.

For transitivity, assume that $x, y, z \in A$ so that xRy and yRz. We want to prove that xRz. Since R is circular and xRy and yRz, we know that zRx. Since we already proved that R is symmetric, zRx implies that xRz. Thus R is transitive.

Therefore R is an equivalence relation.

2. The relation R on the set $\mathbf{Z}$ of all integers is defined by: for all $a, b \in \mathbf{Z}$, aRb if and only if $a^2 \equiv b^2 \pmod 5$.

(a) Prove that R is an equivalence relation.

Proof. R is reflexive: Let $a \in \mathbf{Z}$ be arbitrary. Then $a^2 - a^2 = 0$ and $5 \mid 0$, so $a^2 \equiv a^2 \pmod 5$, so aRa.

R is symmetric: Let $a, b \in \mathbf{Z}$ be arbitrary so that aRb. This means that $a^2 \equiv b^2 \pmod 5$, which means that $a^2 - b^2 = 5k$ for some integer k. Thus

$$b^2 - a^2 = -(a^2 - b^2) = -5k = 5(-k),$$

where $-k$ is an integer, so $b^2 \equiv a^2 \pmod 5$, so bRa. Therefore R is symmetric.

R is transitive: Let $a, b, c \in \mathbf{Z}$ be arbitrary so that aRb and bRc. We want to prove that aRc. Since aRb, we know that $a^2 \equiv b^2 \pmod 5$, which means that $a^2 - b^2 = 5k$ for some integer k. Since bRc, we know that $b^2 \equiv c^2 \pmod 5$, which means that $b^2 - c^2 = 5\ell$ for some integer ℓ. Thus

$$a^2 - c^2 = (a^2 - b^2) + (b^2 - c^2) = 5k + 5\ell = 5(k + \ell),$$

where $k + \ell$ is an integer, so $a^2 \equiv c^2 \pmod 5$, so aRc. Therefore R is transitive.

Therefore R is an equivalence relation.

Note. This argument may seem familiar, which is because it is just repeating our proof in class that $\equiv \pmod{n}$ (congruence mod n) is an equivalence relation on $\mathbf{Z}$ for every positive integer n (Theorem 8.6 on page 185). In fact here is a shorter proof of this problem using this Theorem.

R is reflexive: Let $a \in \mathbf{Z}$ be arbitrary. Then $a^2 \in \mathbf{Z}$, so $a^2 \equiv a^2 \pmod{5}$ (since $\equiv \pmod{5}$ is reflexive), so aRa.

R is symmetric: Let $a, b \in \mathbf{Z}$ be arbitrary so that aRb. This means that $a^2 \equiv b^2 \pmod{5}$, which means (since a^2 and b^2 are integers and $\equiv \pmod{5}$ is symmetric) that $b^2 \equiv a^2 \pmod{5}$, so bRa. Therefore R is symmetric.

R is transitive: Let $a, b, c \in \mathbf{Z}$ be arbitrary so that aRb and bRc. This means that $a^2 \equiv b^2 \pmod{5}$ and $b^2 \equiv c^2 \pmod{5}$. Since a^2, b^2, c^2 are all integers and $\equiv \pmod{5}$ is transitive, this means that $a^2 \equiv c^2 \pmod{5}$, so aRc. Therefore R is transitive.

Therefore R is an equivalence relation.

Note: As announced in the lab, everything beyond this point will not count in the lab test, but will be for bonus points only.

Note. In this question, the symbol $[a]$ (for $a \in \mathbf{Z}$) will denote an element of $\mathbf{Z}_5$, that is, an equivalence class of the equivalence relation $\equiv \pmod{5}$ on $\mathbf{Z}$. So the elements of $\mathbf{Z}_5$, in standard form, are $[0], [1], [2], [3]$ and $[4]$, though they have other names as well. But we have another equivalence relation on $\mathbf{Z}$ in this question, namely R. So to avoid confusion, write the equivalence classes of R as $[a]_R$ (for $a \in \mathbf{Z}$) rather than as $[a]$. So for instance, $[1]_R$ will denote the equivalence class of R which contains 1, while $[1]$ will denote one of the elements of $\mathbf{Z}_5$. All clear? Then let's continue.

(b) Prove that, for all $a \in \mathbf{Z}$, $[a] \subseteq [a]_R$.

Proof. Let $a \in \mathbf{Z}$ be arbitrary. Note that both $[a]$ and $[a]_R$ are equivalence classes and thus **sets**, so to prove that $[a] \subseteq [a]_R$ we should use the normal "element" method of proving that one set is a subset of another. So let b be an arbitrary element of $[a]$, and we want to prove that $b \in [a]_R$. Since $b \in [a]$ (and $[a]$ is an equivalence class of $\equiv \pmod{5}$), $b \equiv a \pmod{5}$ which means that $b - a = 5k$ for some $k \in \mathbf{Z}$. Thus

$$b^2 - a^2 = (b - a)(b + a) = 5k(b + a),$$

where $k(b + a)$ is an integer. Therefore $b^2 \equiv a^2 \pmod{5}$, so bRa, and thus $b \in [a]_R$ by definition of equivalence class. Therefore $[a] \subseteq [a]_R$.

Note: Once again we could use results from the course to shorten this argument a bit. Let $b \in [a]$ be arbitrary. Since $b \in [b]$, this means that the equivalence classes $[a]$ and $[b]$ are not disjoint, hence they must be identical, so $[b] = [a]$. Therefore, by the definition of multiplication in $\mathbf{Z}_5$, $[a^2] = [a][a] = [b][b] = [b^2]$, so $b^2 \in [a^2]$, which means $b^2 \equiv a^2 \pmod{5}$, so bRa, so $b \in [a]_R$. Therefore $[a] \subseteq [a]_R$.

(c) Disprove the statement: for all $a \in \mathbf{Z}$, $[a] = [a]_R$.

A counterexample is $a = 1$. To show that $[1] \neq [1]_R$, we must find an element in $[1]_R$ which is not in $[1]$ (because $[1] \subseteq [1]_R$ by part (b)). Since $4^2 \equiv 1^2 \pmod{5}$ (because $4^2 - 1^2 = 16 - 1 = 15$

is a multiple of 5), we get that $4R1$, so $4 \in [1]_R$. But clearly $4 - 1$ is not a multiple of 5, so $4 \not\equiv 1 \pmod 5$, so $4 \notin [1]$.

(d) Write all the distinct equivalence classes of R as unions of elements of $\mathbf{Z}_5$.

By part (b), $[0] \subseteq [0]_R$, $[1] \subseteq [1]_R$, $[2] \subseteq [2]_R$, $[3] \subseteq [3]_R$, and $[4] \subseteq [4]_R$, and this accounts for all elements of $\mathbf{Z}_5$. But also note (from part (c)) that $4 \in [1]_R$, and since $4 \in [4]_R$ as well, the equivalence classes $[1]_R$ and $[4]_R$ are not disjoint, so $[1]_R = [4]_R$. Similarly, notice that $3^2 - 2^2 = 9 - 4 = 5$ means that $3^2 \equiv 2^2 \pmod 5$, so $3R2$, so $[3]_R = [2]_R$. So R has exactly three distinct equivalence classes: $[0]_R$, $[1]_R$ and $[2]_R$. These equivalence classes are distinct because:

- since $0^2 \not\equiv 1^2 \pmod 5$, $0 \not R\ 1$, so $[0]_R \neq [1]_R$;
- since $0^2 \not\equiv 2^2 \pmod 5$, $0 \not R\ 2$, so $[0]_R \neq [2]_R$;
- since $1^2 \not\equiv 2^2 \pmod 5$, $1 \not R\ 2$, so $[1]_R \neq [2]_R$.

Thus from part (b) we get that $[1] \cup [4] \subseteq [1]_R$ and $[2] \cup [3] \subseteq [2]_R$. Since $\{[0], [1], [2], [3], [4]\}$ and $\{[0]_R, [1]_R, [2]_R\}$ are both partitions of $\mathbf{Z}$, we get

$$[1] \cup [4] = [1]_R, \qquad [2] \cup [3] = [2]_R, \qquad \text{and} \qquad [0] = [0]_R.$$

Note: problem #2 is an expanded version of problem 8.36 on page 194.