Survey HW 5

nxr8dq Sankalpa Banjade

October 2023

1 Introduction

1.1 Problem List

11.3.1, 11.3.2, 12.4.1, 12.4.2, 12.4.3, 12.4.5, 12.4.7, 12.4.8.

11.3.1 Exercise

Definition 11.1.3 introduced the three subnotions of a reflexive, symmetric, and transitive relation. If a relation satisfies all of these, then it is an equivalence relation; but one can also ask for relations that only satisfy a subset of these. For each of the following, find a set X and relation R on X which satisfies the given conditions.

1. R is not reflexive, symmetric, or transitive.
2. R is reflexive and symmetric, but not transitive.
3. R is reflexive and transitive, but not symmetric.
4. R is transitive and symmetric, but not reflexive.
5. R is reflexive, but not symmetric or transitive.
6. R is symmetric, but not reflexive or transitive.
7. R is transitive, but not symmetric or reflexive.

A relation that satisfies the condition of being neither reflexive, symmetric, nor transitive is the *friendship* relation, represented as R. Let's consider a set of individuals, denoted as $\{a, b, c\}$.

1. **Not Reflexive:** The friendship relation is not necessarily reflexive, as an individual may not consider themselves their own friend. For instance, it is not always true that aRa.

2. **Not Symmetric:** The relation is not inherently symmetric. For instance, if a considers b a friend (i.e., aRb), it does not necessarily imply that b considers a a friend (i.e., bRa). There might be scenarios where one individual dislikes another while still being regarded as a friend by the latter.

3. **Not Transitive:** Friendship is not transitive. Given that a is a friend of b (i.e., aRb) and b is a friend of c (i.e., bRc), it does not necessarily follow that a is a friend of c (i.e., aRc). Individuals a and c may not even know each other or might not have a friendly relationship.

A relation satisfying the conditions of being reflexive and symmetric, but not transitive, is the *is related to* relation within a set of people. Consider a set A consisting of individuals a, b, c, and d.

1. **Reflexive:** The relation is reflexive as every individual is related to themselves. For all $x \in A$, the pair (x, x) belongs to the relation.

2. **Symmetric:** The relation is symmetric. If a is related to b, then b is related to a. Formally, for all $a, b \in A$, if (a, b) belongs to the relation, then (b, a) belongs to the relation as well.

3. **Not Transitive:** The relation is not transitive. For instance, if a is related to b (perhaps as siblings), and b is related to c (maybe as cousins), it does not necessarily mean that a is related to c in the same way (as siblings or cousins). Thus, it does not guarantee that for all $a, b, c \in A$, if (a, b) and (b, c) belong to the relation, then (a, c) must belong to the relation.

A relation that is reflexive and transitive but not symmetric is the $\leq$ (less than or equal to) relation on the set of real numbers, $\mathbb{R}$.

1. **Reflexive:** The relation is reflexive as for any $x \in \mathbb{R}$, it is always true that $x \leq x$.

2. **Not Symmetric:** The $\leq$ relation is not symmetric. For example, if $x \leq y$, it does not necessarily follow that $y \leq x$. Take 2 and 3 as an instance; while $2 \leq 3$ is true, $3 \leq 2$ is not.

3. **Transitive:** The relation is transitive. If $x \leq y$ and $y \leq z$, then it must be that $x \leq z$. This property holds for all $x, y, z \in \mathbb{R}$ such that $x \leq y$ and $y \leq z$.

Consider a set A of lines in a plane with the *"is parallel to"* relation. This relation is transitive and symmetric but not reflexive.

1. **Not Reflexive:** The *"is parallel to"* relation is not reflexive as a line cannot be parallel to itself. For every line $L \in A$, it is not the case that L is parallel to L.

2. **Symmetric:** The relation is symmetric. If line L_1 is parallel to line L_2, then it necessarily follows that L_2 is parallel to L_1.

3. **Transitive:** The relation is transitive. If L_1 is parallel to L_2, and L_2 is parallel to L_3, then it must be that L_1 is parallel to L_3.

Consider a set A of individuals with the "likes" or "has positive feelings towards" relation. This relation is reflexive but neither symmetric nor transitive.

1. **Reflexive:** The "likes" relation is reflexive as individuals generally have positive feelings towards themselves. For all $x \in A$, it can be assumed that x likes x.

2. **Not Symmetric:** The relation is not symmetric. If individual a likes individual b, it does not necessarily imply that b likes a.

3. **Not Transitive:** The "likes" relation is not transitive. For instance, if a likes b and b likes c, it does not necessarily mean that a likes c.

Consider a set $A = \{a, b, c, d\}$ of people with the *"is a sibling of"* relation, which includes half-siblings and step-siblings. This relation is symmetric but neither reflexive nor transitive.

1. **Not Reflexive:** The *"is a sibling of"* relation is not reflexive as a person cannot be a sibling of themselves. For every person $x \in A$, it is not the case that x is a sibling of x.

2. **Symmetric:** The relation is symmetric. If person a is a sibling of person b, it necessarily follows that b is a sibling of a.

3. **Not Transitive:** The *"is a sibling of"* relation is not transitive. For instance, if a is a sibling of b and b is a sibling of c, it does not necessarily mean that a is a sibling of c, especially when considering half-siblings and step-siblings.

Consider a set $\mathcal{P}$ which is a power set of some set $A = \{1, 2, 3\}$, with the *"is a subset of"* relation. This relation is transitive but neither symmetric nor reflexive.

1. **Not Reflexive:** In the general set of all sets, the *"is a subset of"* relation is not reflexive as a set is not necessarily a subset of itself.

2. **Not Symmetric:** The relation is not symmetric. If set A is a subset of set B, it does not necessarily follow that B is a subset of A.

3. **Transitive:** The relation is transitive. If A is a subset of B and B is a subset of C, then it must be that A is a subset of C.

11.3.2

Define a relation $\sim$ on $\mathbb{Z} \times \mathbb{Z}$ by

$$(a, b) \sim (c, d) \iff ad = cb.$$

Is $\sim$ an equivalence relation? In order for to be an equivalence relation the relation must be transitive symmetric and reflexive. Let us fix three relations (a, b), (c, d), and (u, v) in X, and suppose that $(a, b) \sim (c, d)$ and $(c, d) \sim (u, v)$. Then, by the definition of the relation, we have that:

$$ad = bc,$$
$$cv = du.$$

From the equation $ad = bc$, we can multiply both sides by v to obtain:

$$adv = bcv.$$

Then, we can substitute cv for du on the right-hand side of the equation, yielding:

$$adv = bdu.$$

Dividing both sides of the equation by d (assuming $d \neq 0$), we obtain the relation:

$$a = bu \implies (a, b) \sim (u, v).$$

Symmetric: We aim to prove that the relation $\sim$ is symmetric. Suppose that $(a, b) \sim (c, d)$. By the definition of the relation, this means that

$$ad = bc.$$

Since $\mathbb{Z}$ is a commutative ring, multiplication in $\mathbb{Z}$ is commutative. Therefore, we can rewrite the equation as

$$da = cb.$$

Now, invoking the definition of the relation again with the terms reordered, we have by the reflexive property that

$$cb = da.$$

This implies that $(c, d) \sim (a, b)$, proving that the relation is symmetric.

Reflexive: This is reflexive due to the fact that the set Z is a commutative ring.

12.4.1

Find an integer $n \in \mathbb{Z}^+$ for which the equation $x^2 = 1$ has more than two solutions in $\mathbb{Z}/(n)$.

Let's consider the ring of $\mathbb{Z}$ modulo 8, or when $n = 8$. In $\mathbb{Z}/(8)$, the equation $x^2 = 1$ has four solutions, namely $x = 1, 3, 5$, and 7. To verify this, we can check:

$$\begin{aligned}
&1^2 \equiv 1 \pmod 8, \\
&3^2 \equiv 9 \equiv 1 \pmod 8, \\
&5^2 \equiv 25 \equiv 1 \pmod 8, \\
&7^2 \equiv 49 \equiv 1 \pmod 8.
\end{aligned}$$

Thus, when $n = 8$, the equation $x^2 = 1$ has more than two solutions in $\mathbb{Z}/(8)$, specifically four solutions: $x = 1, 3, 5$, and 7.

2 12.4.2

We are given that p is a prime number, and we need to prove that the equation $x^2 = x$ has exactly two solutions in $\mathbb{Z}/(p^2)$. Without loss of generality, consider the ring represented as modulo p^2.

Given that p is a prime number, we need to prove that the equation $x^2 = x$ has exactly two solutions in $\mathbb{Z}/(p^2)$.

Proof: Firstly, observe the given equation:

$$x^2 - x = 0$$

We can factorize the left-hand side of the equation as follows:

$$x(x - 1) = 0 \quad \text{in} \quad \mathbb{Z}/(p^2)$$

Now consider the two factors, x and $(x-1)$. In the ring $\mathbb{Z}/(p^2)$, the equation $x(x - 1) = 0$ has solutions when either $x = 0$ or $x - 1 = 0$.

1. If $x = 0$, we have:
$$0 \cdot (0 - 1) \equiv 0 \pmod{p^2}$$
which is a valid solution in $\mathbb{Z}/(p^2)$.

2. If $x - 1 = 0$, then $x \equiv 1 \pmod{p^2}$, which is another valid solution in $\mathbb{Z}/(p^2)$.

No other element in $\mathbb{Z}/(p^2)$ will satisfy the equation, as these are the only solutions that will make either of the factors zero. Therefore, the equation $x^2 = x$ has exactly two solutions in $\mathbb{Z}/(p^2)$ when p is prime: $x = 0$ and $x = 1$.

3 12.4.3

Proof of Solutions to $x^2 = x$ in $\mathbb{Z}/(pq)$

Proof

Let p and q be distinct prime numbers. We want to show that the equation $x^2 = x$ has exactly four solutions in the ring $\mathbb{Z}/(pq)$, also denoted as $\mathbb{Z}_{pq}$. The given equation can be rewritten and factored as follows:

$$x^2 - x = 0,$$
$$x(x-1) = 0.$$

Now, consider the equation in $\mathbb{Z}_p$ and $\mathbb{Z}_q$ respectively. In both of these rings, the equation $x(x-1) = 0$ has the solutions $x = 0$ and $x = 1$. By the Chinese Remainder Theorem (CRT), since p and q are coprime, we can find the solutions in $\mathbb{Z}_{pq}$ by considering all combinations of solutions in $\mathbb{Z}_p$ and $\mathbb{Z}_q$. Formally, we will consider pairs of solutions (x_p, x_q) where x_p is a solution mod p and x_q is a solution mod q. We have four possible combinations:

1. $(0,0)$, which corresponds to the solution $x = 0 \pmod{pq}$.
2. $(1,0)$, corresponding to the solution with $x \equiv 1 \pmod{p}$ and $x \equiv 0 \pmod{q}$. Applying CRT, we can find a unique solution modulo pq.
3. $(0,1)$, corresponding to the solution with $x \equiv 0 \pmod{p}$ and $x \equiv 1 \pmod{q}$. Again, using CRT, we can find a unique solution modulo pq.
4. $(1,1)$, corresponding to the solution $x = 1 \pmod{pq}$.

Each of the above pairs corresponds to a distinct solution in $\mathbb{Z}_{pq}$ due to the Chinese Remainder Theorem, and these are the only solutions. Thus, there are exactly four solutions to the equation $x^2 = x$ in $\mathbb{Z}_{pq}$.

4 12.4.5

The Ring $\mathbb{Z}/12\mathbb{Z}$

The set $\mathbb{Z}/12\mathbb{Z}$, or $\mathbb{Z}_{12}$, is a ring with the following elements:

$$\mathbb{Z}_{12} = \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11\}.$$

Multiplicative Inverses (Units)

Table of Z mod 12

Multiplication Table

$\cdot$	0	1	2	3	4	5	6	7	8	9	10	11
0	0	0	0	0	0	0	0	0	0	0	0	0
1	0	1	2	3	4	5	6	7	8	9	10	11
2	0	2	4	6	8	10	0	2	4	6	8	10
3	0	3	6	9	0	3	6	9	0	3	6	9
4	0	4	8	0	4	8	0	4	8	0	4	8
5	0	5	10	3	8	1	6	11	4	9	2	7
6	0	6	0	6	0	6	0	6	0	6	0	6
7	0	7	2	9	4	11	6	1	8	3	10	5
8	0	8	4	0	8	4	0	8	4	0	8	4
9	0	9	6	3	0	9	6	3	0	9	6	3
10	0	10	8	6	4	2	0	10	8	6	4	2
11	0	11	10	9	8	7	6	5	4	3	2	1

In the ring $\mathbb{Z}_{12}$, not all elements have a multiplicative inverse. However, the elements that do have inverses (units) and their inverses are listed below:

Element	Inverse
1	1
5	5
7	7
11	11

For example, $5 \cdot 5 = 25 \equiv 1 \pmod{12}$, showing that 5 is indeed its own inverse in this ring.

Part 2: Solving the Congruence Equation $5x \equiv 4 \pmod{12}$

We consider the congruence equation:

$$5x \equiv 4 \pmod{12}.$$

Let's verify some potential solutions for x.

Case 1: $x = 8$

For $x = 8$, we compute:

$$5 \cdot 8 = 40.$$

Since $40 \equiv 4 \pmod{12}$, $x = 8$ is indeed a solution to the given congruence equation.

Case 2: $x = 20$

For $x = 20$, we compute:

$$5 \cdot 20 = 100.$$

Since $100 \equiv 4 \pmod{12}$, $x = 20$ is also a solution to the given congruence equation.

5 12.4.7

Proof: An Element in a Ring Cannot Be Both Invertible and a Zero Divisor

Let R be a ring and let $r \in R$. We aim to show that an element r cannot be both invertible and a zero divisor in R.

Proof. Assume, for the sake of contradiction, that r is both invertible and a zero divisor in R.

Firstly, if r is invertible, there exists some non-zero element $k \in R$ such that

$$r \cdot k = 1.$$

Secondly, if r is a zero divisor, there exists some non-zero element $s \in R$ such that

$$r \cdot s = 0.$$

Assuming both statements are true, consider the congruences modulo n where n represents an ideal in the ring R. Then, we have

$$r \cdot k \equiv 1 \pmod{n} \quad \text{and} \quad r \cdot s \equiv 0 \pmod{n}.$$

From the assumption, it follows that n divides $r \cdot s$, which implies n also divides $1 - r \cdot s$. However, this is impossible: for any ring with characteristic greater than 2, there does not exist an element n that divides both $r \cdot s$ and $1 - r \cdot s$. This leads to a contradiction, hence our original assumption that r is both invertible and a zero divisor must be false. ☐

6 12.4.8

Show that for n 2, the ring Z/(n) has zero divisors if and only if n is not a prime number. Hint. If you are not sure how to proceed, work out some examples: write out the multiplication table for Z/(n) and see if you learn anything about zero divisors. we proveed by contadiciton we assume that n is prime and Z/n has zero divisors so there exists a 0 divisor when ns = 0 mod n

Zero Divisors in $\mathbb{Z}/(n)$

We aim to show that for $n \geq 2$, the ring $\mathbb{Z}/(n)$ has zero divisors if and only if n is not a prime number.

Proof. We will prove the statement by considering both directions of the implication.

Forward Direction: Assume n is not a prime number. Then, n can be expressed as a product of two smaller positive integers a and b where $1 < a, b < n$. Consider the product of the equivalence classes $[a]$ and $[b]$ in $\mathbb{Z}/(n)$. We have:

$$[a] \cdot [b] = [a \cdot b] = [n] = [0],$$

since $a \cdot b = n$. Here, $[a]$ and $[b]$ are non-zero elements in $\mathbb{Z}/(n)$, but their product is zero, showing that $[a]$ and $[b]$ are zero divisors.

Reverse Direction: Assume $\mathbb{Z}/(n)$ has zero divisors. This means there exist non-zero elements $[c]$ and $[d]$ in $\mathbb{Z}/(n)$ such that

$$[c] \cdot [d] = [0].$$

Without loss of generality, suppose $0 < c, d < n$. Then cd is a multiple of n, but neither c nor d are multiples of n (since $c, d < n$). This implies that n cant be prime, as it can be factored into two smaller positive integers, namely c and d.

Therefore, we have shown that $\mathbb{Z}/(n)$ has zero divisors if and only if n is not a prime number. $\square$