Discrete Mathematics
Chapters 8.1,8.2,8.3 & 8.4 Homework

November 25, 2024

Mustafa Rashid

Fall 2024

Exercise Set 8.1

20. Let $A = \{-1, 1, 2, 4\}$ and $B = \{1, 2\}$ and define relations R and S from A to B as follows: For all $(x, y) \in A \times B$,

$$x\ R\ y \Leftrightarrow |x| = |y| \text{ and}$$
$$x\ S\ y \Leftrightarrow x - y \text{ is even}$$

State explicitly which ordered pairs are in $A \times B, R, S, R \cup S$, and $R \cap S$.

Ans:

$$\begin{aligned} A \times B &= \{(-1,1),(-1,2),(1,1),(1,2),(2,1),(2,2),(4,1),(4,2)\} \\ R &= \{(-1,1),(1,1),(2,2)\} \\ S &= \{(-1,1),(1,1),(2,2),(4,2)\} \\ R \cup S &= \{(-1,1),(1,1),(2,2),(4,2)\} \\ R \cap S &= \{(-1,1),(1,1),(2,2)\} \end{aligned}$$

Exercise Set 8.2

14. O is the relation defined on $\mathbb{Z}$ as follows: For all $m, n \in \mathbb{Z}$, $m\ O\ n \Leftrightarrow m - n$ is odd. Determine whether this relation is reflexive, symmetric, transitive, or none of these. Justify your answer.

Ans:
O is not reflexive: Suppose m is a particular but arbitrarily chosen integer. Now $m - m = 0$. But this is not odd. Hence $m - m$ is not odd and O is not reflexive.
O is symmetric: Suppose m and n are particular but arbitrarily chosen integers

that satisfy the condition $m\ O\ n$. By definition of O, since $m\ O\ n$ then $m-n$ is odd. By definition of odd, this means that $m-n=2k+1$ for some integer k. Multiplying both sides by -1 gives $n-m=2(-k-1)+1$ since $-k-1$ is an integer, this equation shows that $n-m$ is odd. Hence, by defintion of O, $n\ O\ m$. **O is not transitive:** Suppose m, n and p are particular but arbitrarily chosen integers that satisfy condtion $m\ O\ n$ and $n\ O\ p$. By definition of O, since $m\ O\ n$ and $n\ O\ p$, then $m-n$ is odd and $n-p$ is also odd. By definition of odd, this means that $m-n=2k+1$ and $n-p=2q+1$ for some integers k and q. Adding the two equations gives $(m-n)+(n-p)=2k+1+2q+1$ and simplifying this gives $m-p=2(k+q+1)$. Since $k+q+1$ this equation shows that $m-p$ is even and not odd. Hence, by defintion of O, $m\ \not{O}\ p$.

36. If R is transitive, then R^{-1} is transitive. (Prove or disprove this statement.)

Ans: Suppose R is any relation on a set A that is transitive. By defintion of transitive, this means that for all x, y, and z in A, if $(x, y) \in R$ and $(y, z) \in R$ then $(x, z) \in R$. Suppose that $x\ R\ y$ and $y\ R\ z$. Because R is transitive, then $x\ R\ z$. The inverse relation by definition would contain the relations $y\ R^{-1}\ x$, $z\ R^{-1}\ y$, and $z\ R^{-1}\ x$. This means that for any x, y, and z in A if $z\ R^{-1}\ y$ and $y\ R^{-1}\ x$ then $z\ R^{-1}\ x$. Hence, R^{-1} is also transitive.

40. If R and S are reflexive, is $R \cup S$ reflexive? Why? (Assume R and S are relations on a set A. Prove or disprove the statement.)

Ans: Suppose not, suppose that R and S are reflexive and that $R \cup S$ is not reflexive. This means that there is an element x in $R \cup S$ such that $(x, x) \notin R$ or $(x, x) \notin S$. But we know that R and S are reflexive so it is not true that that there is an element x in R such that $(x, x) \notin R$ and it is not true that here is an element x in S such that $(x, x) \notin R$. This means that $R \cup S$ also has to be reflexive because all ordered pairs (x, x) in $R \cup S$ come are in R or S and so they are also reflexive.

Exercise Set 8.3

In 9 and 10 the relation R is an equivalence relation on the set A. Find the distinct equivalence classes of R.

9. $X = \{-1, 0, 1\}$ and $A = \mathscr{P}(X)$. R is defined on $\mathscr{P}(X)$ as follows: For all sets s and T in $\mathscr{P}(X)$,

$$s\ R\ T \Leftrightarrow \text{ the sum of elements in } s \text{ equals the sum of the elements in } T$$

Ans:

$$\{\phi\}$$
$$\{\{-1\}, \{-1, 0\}\}$$
$$\{\{0\}, \{-1, 1\}, \{-1, 0, 1\}\}$$
$$\{\{1\}, \{0, 1\}\}$$

10. $A = \{-5, -4, -3, -2, -1, 0, 1, 2, 3, 4, 5\}$. R is defined on A as follows: For all $m, n \in \mathbb{Z}$,

$$m\ R\ n \Leftrightarrow 3 \mid (m^2 - n^2).$$

Ans:

$$[0] = [3] = [-3] = \{-3, 0, 3\}$$
$$[1] = [-1] = [2] = [-2] = [4] = [-4] = [5] = [-5] = \{-5, -4, -2, -1, 1, 2, 4, 5\}$$

39. The following argument claims to prove that the requirement that an equivalence relation be reflexive is redundant. In other words, it claims to show that if a relation is symmetric and transitive, then it is reflexive. Find the mistake in the argument.
"**Proof:** Let R be a relation on a set A and suppose R is symmetric and transitive. For any two elements x and y in A, if $x\ R\ y$ then $y\ R\ x$ since R is symmetric. But then it follows by transitivity that $x\ R\ x$. Hence R is reflexive."

Ans: By definiton, a relation R is symmetric if, and only if, for all $x, y \in A$, if $x\ R\ y$ then $y\ R\ x$. However, this is still vacuously true (that is the relation is still symmetric by definition) in the following cases where:

$$x \not R\, y \vee y\ R\ x$$

$$x \not R\, y \vee y \not R\, x$$

The second case shows that there is an element x in A such that $x \not R\, x$ and so R is not necessarily reflexive.

Exercise Set 8.4

16. What is the units digit of 3^{1789}?

Ans: By looking at $3^0 = 1, 3^1 = 3, 3^2 = 9, 3^3 = 27, 3^4 = 81$ we can see that

$$3^4 \equiv 1 \pmod{10}$$

By Theorem 8.4.3 and exponent laws we get

$$3^{1788} = (3^4)^{447} \equiv 1^{447} \pmod{10}$$
$$3^{1788} \equiv 1 \pmod{10}$$

We know that $3 \equiv 1 \pmod{10}$ and so by Theorem 8.4.3, $3^{1788} \cdot 3 \equiv 1 \cdot 3 \pmod{10}$. Therefore, the units digit of 3^{1789} is 3.

32. Prove that in any commutative ring R, there is only one multiplicative identity. In other words, prove that in any commutative ring R, if $ec = c$ for all elements c in R, then $e = 1$

Ans:

Proof. Suppose $c = 1$,and so because $ec = c$ then $e \cdot 1 = 1$ by the identity for multiplication. Because 1 is the identity for multiplication $e \cdot 1 = e$ and therfore $e = e \cdot 1 = 1$. $\square$

33. Prove that given any element a in any commutative ring R, there is only one additive inverse for a. In other words, prove that if $a + b = 0$ and $a + c = 0$, then $b = c$.

Ans:

Proof. Because $a+b=0$ and $a+c=0$ we can say that $a+b=a+c$. Subtracting a from both sides gives $b=c$. $\square$

Exercise Set 8.5

19. Use the extended Euclidean algorithm to find the greatest common divisor of 2583 and 349. Express the greatest common divisor as a linear combination of the two numbers.

Ans:

1. Applying the Euclidean Algorithm
   (a) gcd(2583,349): $2583 = 348 \cdot 7 + 140$
   (b) gcd(349,140):$349 = 140 \cdot 2 + 69$
   (c) gcd(140,69):$140 = 69 \cdot 2 + 2$
   (d) gcd(69,34):$69 = 34 \cdot 2 + 1$
   (e) gcd(34,1):$34 = 1 \cdot 34 + 0$
   (f) gcd(1,0)$= 1$
2. Substituting back the results

$$\begin{aligned}
1 &= 69 - 34 \cdot 2 && \text{By (d)}\\
&= 69 - (140 - 69 \cdot 2)34 && \text{By (c)}\\
&= 6969 - (2583 - 349 \cdot 7) \cdot 34 && \text{By (a) \& algebra}\\
&= 69(349 - 140 \cdot 2) - 2583 \cdot 34 + 349 \cdot 7 \cdot 34 && \text{By (b)}\\
&= 2583 \cdot (-172) + 349 \cdot 1273 && \text{By algebra}
\end{aligned}$$

41. Use the extended Euclidean algorithm to find a postive integer n so that $2 \leq n \leq 30$ and $[n]$ is an inverse for $[13]$ in $\mathbb{Z}_{31}$

Ans: $\exists x$ such that $[13] \cdot [x]$ if, and only if, $13x \equiv 1 \pmod{31}$. So $13x + 31(-k) = 1$ and applying the euclidean algorithm on 31 and 13 gives:

(a) gcd(31,13): $31 = 13 \cdot 2 + 5$

(b) gcd(13,5):$13 = 5 \cdot 2 + 3$

(c) gcd(5,2):$5 = 3 \cdot 1 + 2$

(d) gcd(3,2):$3 = 2 \cdot 1 + 1$

(e) gcd(2,1):$2 = 1 \cdot 2 + 0$

(f) gcd(1,0)$= 1$

Substituting the results back gives:

$$\begin{aligned}
1 &= 3 - 2 \cdot 1 \\
&= 3 - (5 - 3 \cdot 1) \cdot 1 && \text{By (c)} \\
&= 2(13 - 5 \cdot 2) - (31 - 13 \cdot 2) && \text{(By algebra \& (a))} \\
&= 13 \cdot 4 - 31 - 4(31 - 13 \cdot 2) && \text{By algebra \& (a)} \\
&= 13(12) + 31(-5)
\end{aligned}$$

So $1 = 13(12) + 31(-5)$ or $13 \cdot 12 \equiv 1 \pmod{31}$ and so $n = 12$.

Extra-credit