

For full credit show the complete solution of each problem including steps of calculations. Support answers by citing definitions and theorems. No credit will be given for mere answers unsupported by calculations or reasons.

1. (5 points) Complete the definition: “An *equivalence relation* on a set S is a set R of ordered pairs of elements of S such that”

(1) for every $a \in S$, $(a, a) \in R$ (R is *reflexive*);

(2) for every $a, b \in S$, if $(a, b) \in R$ then $(b, a) \in R$ (R is *symmetric*);

(3) for every $a, b, c \in S$, if $(a, b) \in R$ and $(b, c) \in R$ then $(a, c) \in R$ (R is *transitive*).

2. (25 points) Let A and B be sets, and $f : A \rightarrow B$ a function. For $x, y \in A$ define a relation by $x \sim y$ if $f(x) = f(y)$. Prove that \sim is an equivalence relation on A .

What is the equivalence class of an element $a \in A$?

Solution. First we show that \sim is reflexive. For every $x \in A$ we have $f(x) = f(x)$, so $x \sim x$.

Next, if $x, y \in A$ and $x \sim y$, then $f(x) = f(y)$. Of course then $f(y) = f(x)$ so also $y \sim x$; thus \sim is symmetric.

To verify the transitive property let $x, y, z \in A$ and assume $x \sim y$ and $y \sim z$. This means $f(x) = f(y)$ and $f(y) = f(z)$. It follows that $f(x) = f(z)$ so $x \sim z$.

The equivalence class of an element $a \in A$ is $[a] = \{x \in A : f(x) = f(a)\}$, the set of all elements mapped to the same point as a is.

3. Complete the definitions:

(a) (5 points) A *group* is a set G with a binary operation $(a, b) \mapsto a \cdot b \in G$ defined for all $a, b \in G$ such that

(1) The operation is *associative*: for all $a, b, c \in G$, $(a \cdot b) \cdot c = a \cdot (b \cdot c)$.

(2) There is an *identity* element $e \in G$ such that for every $a \in G$ we have $e \cdot a = a \cdot e = a$.

(3) For every $a \in G$ there is an *inverse* $b \in G$ such that $a \cdot b = b \cdot a = e$.

(b) (5 points) If G is a group and $g \in G$, the *cyclic subgroup generated by g* is

$$\{g^n : n \in \mathbb{Z}\}.$$

4. (30 points) Find the order of the group $U(18)$.

Solution: The group $U(18)$ is the group of natural numbers less than 18 and relatively prime to 18; the group operation is multiplication mod 18. Thus

$$U(18) = \{1, 5, 7, 11, 13, 17\}$$

has 6 elements, so the order of the group is 6.

(a) Find the order of the cyclic subgroup $\langle 5 \rangle$ of $U(18)$.

Solution: Compute the powers of 5 mod 18.

$$\begin{aligned} 5^2 &= 25 &&= 7 \pmod{18} \\ 5^3 &= 5 \cdot 7 = 35 &&= 17 \pmod{18} \\ 5^4 &= 5 \cdot 17 = 85 &&= 13 \pmod{18} \\ 5^5 &= 5 \cdot 13 = 65 &&= 11 \pmod{18} \\ 5^6 &= 5 \cdot 11 = 55 &&= 1 \pmod{18}. \end{aligned}$$

We have found that

$$\langle 5 \rangle = \{5, 7, 17, 13, 11, 1\} = U(18) \quad (!)$$

is a subgroup of order 6.

(b) Is $U(18)$ a cyclic group?

Answer: Yes. It is equal to its cyclic subgroup $\langle 5 \rangle$.

5. (5 points) Complete the definition: Let X and Y be sets, and $f : X \rightarrow Y$ a function. The function f is *one-to-one* if for all $x_1, x_2 \in X$, if $f(x_1) = f(x_2)$ then $x_1 = x_2$.
6. (25 points) Let G be a group, and $a \in G$. Define a function $f : G \rightarrow G$ by $f(g) = ag$. Prove that f is one-to-one.

Solution: We verify that this f satisfies the definition above. Let $g, h \in G$ and suppose that $f(g) = f(h)$. This means

$$ag = ah$$

by the way f is defined. It follows by the cancellation law that $g = h$, so f is one-to-one.