MGF1107 Notes

1 Relations

Definition 1.1. Let A and B be sets. The *cartesian product* of A and B, $A \times B$, is the set of all ordered pairs such that the first coordinate is in A and the second coordinate is in B.

$$A \times B = \{(a, b) \mid a \in A \text{ and } b \in B\}$$

Definition 1.2. Let A and B be sets. Let $R \subseteq A \times B$. Then R is a relation from A to B.

Example 1.1. (a) Let $A = \{1, 2, 3\}$ and $B = \{4, 5, 6\}$. The set

$$R = \{(2, 4), (3, 6)\}$$

is a relation from A to B. R can be written as

$$R = \{(a, b) \in A \times B \mid b = 2a\}$$

(b) $R = \{(x, y) \in \mathbb{R} \times \mathbb{R} \mid x = y\}$ is a relation from the real numbers to the real numbers. The graph of R is a straight line with a slope of 1. R is the identity map on $\mathbb{R}$. It maps every real number to itself.

(c) For the set $P = \{\varnothing, \{1\}, \{2\}, \{3\}, \{1, 2\}, \{1, 3\}, \{2, 3\}\}$,

$$R = \{(A, B) \in P \times P \mid A \subseteq B\}$$

is a relation on P. R is the subset relation that we previously saw is a partial ordering of P.

Definition 1.3. Let A and B be sets. Let R be a relation from A to B.

The *domain* of R is the set of all $a \in A$ such that there exists a $b \in B$ such that $(a, b) \in R$.

The range of R is the set of all $b \in B$ such that there exists an $a \in A$ such that $(a, b) \in R$.

In set notation,

$$\text{Dom}R = \{a \in A \mid \exists b \in B \text{ such that } (a, b) \in R\}$$

and

$$\text{Ran}R = \{b \in B \mid \exists a \in A \text{ such that } (a, b) \in R\}$$

Definition 3 says that for a relation R, the domain of R is the set of all the first coordinates that appear in the ordered pairs contained in R, and the range of R is the set of all the second coordinates that appear in the ordered pairs contained in R.

Definition 1.4. Let A and B be sets, R a relation from A to B. The inverse of R is

$$R^{-1} = \{(b, a) \subseteq A \times B \mid (a, b) \in R\}$$

Example 1.2. Let A, B, and R be as in example 1(a)

(a) The domain of R is $\{2, 3\}$ and the range of R is $\{4, 6\}$.

(b) $R^{-1} = \{(4, 2), (6, 3)\}$

Definition 1.5. Let A, B, and C be sets. Let R be a relation from A to B and let S be a relation from B to C. The *composition* of S and R, $S \circ R$, is a relation from A to C defined as follows.

$$S \circ R = \{(a, c) \in A \times C \mid \exists b \in B \text{ such that } (a, b) \in R \text{ and } (b, c) \in S\}$$

Exercise 1. Let S the set of students at a university, C be the set of courses offered at the university, and T is the set of teachers at the university.

Define the following relations

$$R = \{(s, c) \in S \times C \mid s \text{ is enrolled in } c\}$$

$$V = \{(c, t) \in C \times T \mid c \text{ is taught by } t\}$$

Describe the following relations

(a) $R^{-1} \circ R$

(b) $R \circ R^{-1}$

(c) $T \circ E$

From these definitions, we get some properties of relations that are worth mentioning.

Theorem 1.1. *Let A, B, and C be sets. Let R be a relation from A to B and let S be a relation from B to C. Then*

(i) $(R^{-1})^{-1} = R$

(ii) $\text{Dom}(R^{-1}) = \text{Ran}R$

(iii) $\text{Ran}(R^{-1}) = \text{Dom}R$

(iv) $(S \circ R)^{-1} = R^{-1} \circ S^{-1}$

Proof. (i)

$$(a, b) \in R \Leftrightarrow (b, a) \in R^{-1} \Leftrightarrow (a, b) \in (R^{-1})^{-1}$$

(ii)

$$b \in \text{Ran}R \Leftrightarrow \exists a \in A \text{ such that } (a, b) \in R$$
$$\Leftrightarrow \exists a \in A \text{ such that } (b, a) \in R^{-1} \Leftrightarrow b \in \text{Dom}(R^{-1})$$

(iii)

$$a \in \text{Dom}R \Leftrightarrow \exists b \in B \text{ such that } (a, b) \in R$$
$$\Leftrightarrow \exists b \in B \text{ such that } (b, a) \in R^{-1} \Leftrightarrow a \in \text{Ran}(R^{-1})$$

(iv) Note that both $(S \circ R)^{-1}$ and $R^{-1} \circ S^{-1}$ are both relations from C to A.

$$(c, a) \in (S \circ R)^{-1} \Leftrightarrow (a, c) \in S \circ R$$
$$\Leftrightarrow \exists b \in B \text{ such that } (a, b) \in R \text{ and } (b, c) \in S$$
$$\Leftrightarrow \exists b \in B \text{ such that } (c, b) \in S^{-1} \text{ and } (b, a) \in R^{-1}$$
$$\Leftrightarrow (c, a) \in R^{-1} \circ S^{-1}$$

■

Exercise 2. Find the domain and range of each relation from problem 6 of homework 2.

Definition 1.6. Let X, Y be sets. Let f be a relation from X to Y. f is a function from X to Y, written $f : X \to Y$, if for every $x \in X$, there is exactly one $y \in Y$ such that $(x, y) \in f$.

Since for every $x \in X$, there is a unique $y \in Y$ such that $(x, y) \in f$, we write $f(x) = y$. f is a map from the set X to Y, and for $x \in X$, $f(x)$ is the image of x under f.

If, for the sets X and Y, we have two functions, $f : X \to Y$ and $g : X \to Y$, such that for every $x \in X$, $f(x) = g(x)$, then $f = g$.

Since functions are relations, the same definitions for relations apply to functions as well. However, the inverse of a function may not be a function.

Theorem 1.2. *Let X, Y, Z be sets. Let $f : X \to Y$ and $g : Y \to Z$, then $g \circ f : X \to Z$ and the image of x under $g \circ f$ is*

$$(g \circ f)(x) = g(f(x))$$

Proof. Let $x \in X$. Since f is a function, $f(x)$ exists. Let $y = f(x)$. Also, since g is a function, there is a $z \in Z$ such that $g(y) = z$. So $g(y) = g(f(x))$. Therefore, for every $x \in X$, there is a $z \in Z$ such that $(g \circ f)(x) = z$.

Now we just need to show that there is only one such z. Let $x \in X$, and suppose that $(g \circ f)(x) = z_1$ and $(g \circ f)(x) = z_2$. Then there exists y_1 such that $z_1 = g(y_1)$ and $y_1 = f(x)$, and there exists y_2 such that $z_2 = g(y_2)$ and $y_2 = f(x)$. This means that $f(x) = y_1$ and $f(x) = y_2$. Since f is a function, y_1 must equal y_2. And since g is a function, $g(y_1)$ must equal $g(y_2)$, otherwise we have $(y_1, z_1) = (y_2, z_1) \neq (y_2, z_2)$. Therefore, $z_1 = z_2$.

■

For examples and exercises, refer to homework.

2 Groups

Definition 2.1. A group is a set, G, along with an operation, say $\cdot$, such that

(i) For all $a, b \in G$, $a \cdot b \in G$.

(ii) There exists $e \in G$ such that for every $a \in G$, $e \cdot a = a \cdot e = a$.

(iii) For all $a, b, c \in G$, $(a \cdot b) \cdot c = a \cdot (b \cdot c)$

(iv) For all $a \in G$, there exists $b \in G$ such that $a \cdot b = b \cdot a = e$.

We refer to the operation, $\cdot$, as the product. If $x, y \in G$, then $x \cdot y$ is the product of x and y.

Property (i) says that the set G is closed under the operation $\cdot$. Closure means that whenever you have the product of two group elements, another element of G is produced. In other words, the product of any elements of the group will never give you an element not in G.

Property (ii) gives the existence of an identity element. The product of any $x \in G$ and the identity element, on either the right or the left, will be x. "Multiplying" x by the identity will not change x.

Property (iv) gives the existence of inverses. Each element of a group, G, has an inverse. The product of any element with its inverse yields the identity element.

Definition 2.2. A group, G, is *abelian* if for any $x, y \in G$,

$$x \cdot y = y \cdot x$$

Example 2.1. The rotations of a square, and reflections of a square about its axes of symmetries forms a group, called the dihedral group of order 8, $D_8 = \{R^0, R^1, R^2, R^3, s, sR^1, sR^2, sR^3\}$, where s is a reflection about any axis of symmetry and sR^i means the product of the reflection and rotation. Since rotating then reflecting gives a reflection, each reflection can be represented by the product of a reflection and each rotation.

Example 2.2. The integers with addition form a group. The identity is 0, and the inverse of an integer, n, is $-n$.

Example 2.3. The integers modulo n form a group with addition.

Example 2.4. The set of permutations (rearrangements) of the set

$$\{1, 2, 3, ..., n\}$$

forms a group under function composition.

Exercise 3. Which groups from the previous examples are abelian? Give an example of an abelian group not found in the previous exercises (can be a subgroup of a nonabelian group).

Proposition 2.1. *Let G be a group. The identity element of G is unique.*

Proof. Let e and e' be such that for every $x \in G$, $e \cdot x = x \cdot e = x$ and $e' \cdot x = x \cdot e' = x$. Then $e = e' \cdot e = e'$

■

Proposition 2.2. *Let G be a group. Suppose $a, x, y \in G$ and $a \cdot x = a \cdot y$. Then $x = y$.*

Proof. Since each element of G has an inverse, say b is an inverse of a. Then

$$x = e \cdot x = (b \cdot a) \cdot x = b \cdot (a \cdot x) = b \cdot (a \cdot y) = (b \cdot a) \cdot y = e \cdot y = y$$

■

Similarly, if $x \cdot a = y \cdot a$, then $x = y$. These properties are called left and right cancellation laws. As a consequence of the cancellation laws, we can show that every element of a group has a unique inverse. For a group, G, if an element, x, of G has two inverses, say a and b, then $b \cdot x = e = a \cdot x$, so $b \cdot x = a \cdot x$. Now using the cancellation law, we have $b = a$. So the two inverses are the same element.

Definition 2.3. The order of a group, G, is the number of elements in G, denoted $|G|$.

Definition 2.4. Let G be a group and $g \in G$. The order of g is the smallest positive integer, n, such that $g^n = e$.

Example 2.5. The dihedral group, D_8, is the group of rotations and reflections of a square. D_8 contains 4 rotations and 4 reflections. So $|D_8| = 8$.

The order of any reflection in D_8 is 2, since applying the same reflection twice will return the original arrangement of the square. The order of R^1 is 4. $\left|R^2\right| = 2$, and $\left|R^3\right| = 4$.

Exercise 4. What is the order of the integers mod 5, $\mathbb{Z}/5\mathbb{Z}$, with addition? What is the order of each element of $\mathbb{Z}/5\mathbb{Z}$ with addition?

Definition 2.5. Let G be a group. A subset $H \subseteq G$ is a subgroup if H itself forms a group under the operation of G.

Example 2.6. The subset of D_8 consisting of only rotations, $\{R^0, R^1, R^2, R^3\}$ forms a subgroup. Note that it contains the identity, R^0, and we have shown in class that it has closure, contains inverses, and the operation is associative.

Exercise 5. Show that the subset of $5\mathbb{Z} \subseteq \mathbb{Z}$ is a subgroup with addition, where $5\mathbb{Z} = \{5n \mid n \in \mathbb{Z}\}$ is the subset containing all integers multiples of 5.

Definition 2.6. A group, G, is called cyclic if it can be generated by one element.

Example 2.7. The group of integers with addition is cyclic. $\mathbb{Z} = \{1^n \mid n \in \mathbb{Z}\}$

Exercise 6. Is the subgroup of rotations of D_8 cyclic?