CHAPTER 5: EQUIVALENCE RELATIONS AND EQUIVALENCE CLASSES

Section 5.1: Equivalence Relations

Relations

Examples of relations on the set of real numbers include "=", "<", and "$\leq$". Examples of relations on $P(\mathbf{R})$, the power set of $\mathbf{R}$, include "=" and "$\subseteq$".

Definition 1: A **relation** on a set S is subset of $S \times S$.

Comments: At first glance, there appears to be a disconnect between the examples of relations given above and the definition of a relation. To make the connection, consider the relation "<" on $\mathbf{R}$. Technically, "<" is a subset of $\mathbf{R} \times \mathbf{R}$. For instance, $(1, 2) \in <$. Our practice, however, is to write $1 < 2$, and we will continue that practice, even in the abstract.

If S is a set, we will use the symbol "$\simeq$" to denote either an abstract relation or a specific relation for which there is no standard notation. For a, $b \in S$ we will write $a \simeq b$, not $(a, b) \in \simeq$, to indicate that a and b are related.

Definition 2: Let $\simeq$ be a relation of a set S. We say that $\simeq$ is **reflexive** provided for all $a \in S$, $a \simeq a$.

Definition 3: Let $\simeq$ be a relation of a set S. We say that $\simeq$ is **symmetric** provided for all a, $b \in S$, if $a \simeq b$ then $b \simeq a$.

Definition 4: Let $\simeq$ be a relation of a set S. We say that $\simeq$ is **transitive** provided for all a, b, $c \in S$, if $a \simeq b$ and $b \simeq c$ then $a \simeq c$.

Exercise 1: Let $\simeq$ be a relation of a set S. Complete each of the following definitions:

(a) $\simeq$ is not reflexive provided ....

(b) $\simeq$ is not symmetric provided ....

(c) $\simeq$ is not transitive provided ....

Proof Forms:

Before proceeding with examples, we pause to outline the forms for proving or disproving that a relation $\simeq$ is reflexive, symmetric, or transitive.

Let $\simeq$ be a relation on a set S.

Proving $\simeq$ is reflexive.

To Prove: $(\forall a \in S)\, a \simeq a$.

Form of Proof:
- Let a be an arbitrary (variable) element of S.
- Give an argument which concludes that $a \simeq a$.

Proving $\simeq$ is not reflexive.

To Prove: $(\exists a \in S)\, a \not\simeq a$.

Form of Proof:
- Let a be a specific element of S.
- Verify that $a \not\simeq a$.

Let $\simeq$ be a relation on a set S.

Proving $\simeq$ is symmetric.

To Prove: $(\forall a, b \in S)\, a \simeq b \rightarrow b \simeq a$.

Form of Proof:
- Let a and b be arbitrary (variable) elements of S.
- Assume that $a \simeq b$.
- Expand if its helpful. (It usually is.)
- Give an argument which concludes that $b \simeq a$.

Proving $\simeq$ is not symmetric.

To Prove: $(\exists a, b \in S)\, (a \simeq b) \wedge (b \not\simeq a)$.

Form of Proof:
- Let a and b be specific elements of S.
- Verify that $a \simeq b$.
- Verify that $b \not\simeq a$.

Let $\simeq$ be a relation on a set S.

Proving $\simeq$ is transitive.

To Prove: $(\forall a, b, c \in S)\,(a \simeq b) \wedge (b \simeq c) \rightarrow (a \simeq c)$.

Form of Proof:
- Let a, b and c be arbitrary (variable) elements of S.
- Assume that $a \simeq b$ and $b \simeq c$.
- Expand if its helpful. (It usually is.)
- Give an argument which concludes that $a \simeq c$.

Proving $\simeq$ is not transitive.

To Prove: $(\exists a, b, c \in S)\,(a \simeq b) \wedge (b \simeq c) \wedge (a \not\simeq c)$.

Form of Proof:
- Let a, b, and c be specific elements of S.
- Verify that $a \simeq b$.
- Verify that $b \simeq c$.
- Verify that $a \not\simeq c$.

Example 1: For a, $b \in \mathbf{Z}$ define $a \simeq b$ to mean that a divides b.

(a) Prove or disprove that $\simeq$ is reflexive.

(b) Prove or disprove that $\simeq$ is symmetric.

(c) Prove or disprove that $\simeq$ is transitive.

Solution: (a) Since 0 does not divide 0, $0 \not\simeq 0$ and $\simeq$ is not reflexive.

(b) 2 divides 4 so $2 \simeq 4$. But 4 does not divide 2, so $4 \not\simeq 2$. Thus, $\simeq$ is not symmetric.

(c) To see that $\simeq$ is transitive, let a, b, c be integers. Suppose that $a \simeq b$ and $b \simeq c$. Thus, a divides b and b divides c so there exist integers k and l such that $b = ak$ and $c = bl$. This gives $c = bl = (ak)l = a(kl)$. Therefore, a divides c so $a \simeq c$.

Exercise 2: For A, $B \in P(\mathbf{Z})$ define $A \simeq B$ to mean that $A \bigcap B = \emptyset$. (Recall that $P(\mathbf{Z})$ is the power set of $\mathbf{Z}$.)

(a) Prove or disprove that $\simeq$ is reflexive.

(b) Prove or disprove that $\simeq$ is symmetric.

(c) Prove or disprove that $\simeq$ is transitive.

Equivalence Relations

Definition 5: A relation $\simeq$ on a set S is called an **equivalence relation** provided $\simeq$ is reflexive, symmetric, and transitive.

Example 2: For $x, y \in \mathbf{R}$ define $x \simeq y$ to mean that $x - y \in \mathbf{Z}$. Prove that $\simeq$ is an equivalence relation on $\mathbf{R}$.

Proof: To see that $\simeq$ is reflexive, let $x \in \mathbf{R}$. Then $x - x = 0$ and $0 \in \mathbf{Z}$, so $x \simeq x$.

To see that $\simeq$ is symmetric, let $a, b \in \mathbf{R}$. Suppose $a \simeq b$. Then $a - b \in \mathbf{Z}$ – say $a - b = m$, where $m \in \mathbf{Z}$. Then $b - a = -(a - b) = -m$ and $-m \in \mathbf{Z}$. Thus, $b \simeq a$.

To see that $\simeq$ is transitive, let $a, b, c \in \mathbf{R}$. Suppose that $a \simeq b$ and $b \simeq c$. Thus, $a - b \in \mathbf{Z}$, and $b - c \in \mathbf{Z}$. Suppose $a - b = m$ and $b - c = n$, where $m, n \in \mathbf{Z}$. Then $a - c = (a - b) + (b - c) = m + n$. Now $m + n \in \mathbf{Z}$; that is, $a - c \in \mathbf{Z}$. Therefore $a \simeq c$.

It now follows from Definition 5 that $\simeq$ is an equivalence relation on the set $\mathbf{R}$.

Exercise 3: For $(a, b), (c, d) \in \mathbf{R}^2$ define $(a, b) \simeq (c, d)$ to mean that $2a - b = 2c - d$. Prove that $\simeq$ is an equivalence relation on $\mathbf{R}^2$.

Congruence Modulo n

Definition 6: Let n be a positive integer. For integers a and b we say that a **is congruent to** b **modulo** n, and write $a \equiv b \pmod{n}$, provided $a - b$ is divisible by n.

Comment: The following statements are various ways to say $a \equiv b \pmod{n}$; that is, the statements are equivalent.

(a) $a \equiv b \pmod{n}$

(b) $a - b = kn$ for some integer k.

(c) $a = kn + b$ for some integer k.

Theorem 1: Congruence modulo n is an equivalence relation on $\mathbf{Z}$.

Proof: To see that congruence modulo n is reflexive, let a be an integer. Then $a - a = 0$ and 0 is divisible by n (since $0 = 0n$). Therefore, $a \equiv a \pmod{n}$ for every integer a.

To prove symmetry, let a and b be integers. Suppose that $a \equiv b \pmod{n}$ – say $a - b = kn$, where k is an integer. Then $b - a = -(a - b) = -(kn) = (-k)n$. Thus, n divides $b - a$ and $b \equiv a \pmod{n}$.

The proof that congruence mod n is transitive is Exercise 4 below.

Exercise 4: Complete the proof of Theorem 1 by proving that congruence modulo n is transitive.

Example 3: Describe the set of all integers x such that $x \equiv 4 \pmod{9}$ and use the description to list all integers x such that $-36 \leq x \leq 36$ and $x \equiv 4 \pmod{9}$.

Solution: By (c) of the comment following Definition 6, for an integer x we have $x \equiv 4 \pmod{9}$ if and only if $x = 9k + 4$. Thus, we simply calculate multiples of 9 then add 4 and restrict x so that $-36 \leq x \leq 36$. The possibilities for x are -32 (which equals $(-4)9 + 4$), -23, -14, -5, 4, 13, 22, and 31.

Exercise 5: Find all integers x such that $7x \equiv 2x \pmod{8}$.

Section 5.1. EXERCISES

5.1.1. For $a, b \in \mathbf{R}$ define $a \simeq b$ to mean that $ab = 0$. Prove or disprove each of the following:

(a) The relation $\simeq$ is reflexive.

(b) The relation $\simeq$ is symmetric.

(c) The relation $\simeq$ is transitive.

5.1.2. For $a, b \in \mathbf{R}$ define $a \simeq b$ to mean that $ab \neq 0$. Prove or disprove each of the following:

(a) The relation $\simeq$ is reflexive.

(b) The relation $\simeq$ is symmetric.

(c) The relation $\simeq$ is transitive.

5.1.3. For $a, b \in \mathbf{R}$ define $a \simeq b$ to mean that $|\, a - b \,| < 5$. Prove or disprove each of the following:

(a) The relation $\simeq$ is reflexive.

(b) The relation $\simeq$ is symmetric.

(c) The relation $\simeq$ is transitive.

5.1.4. Define a function $f : \mathbf{R} \to \mathbf{R}$ by $f(x) = x^2 + 1$. For $a, b \in \mathbf{R}$ define $a \simeq b$ to mean that $f(a) = f(b)$.

(a) Prove that $\simeq$ is an equivalence relation on $\mathbf{R}$.

(b) List all elements in the set $\{\, x \in \mathbf{R} \,|\, x \simeq 3 \,\}$.

5.1.5. For points $(a, b), (c, d) \in \mathbf{R}^2$ define $(a, b) \simeq (c, d)$ to mean that $a^2 + b^2 = c^2 + d^2$.

(a) Prove that $\simeq$ is an equivalence relation on $\mathbf{R}^2$.

(b) List all elements in the set $\{\, (x, y) \in \mathbf{R}^2 \,|\, (x, y) \simeq (0, 0) \,\}$.

(c) List five distinct elements in the set $\{\, (x, y) \in \mathbf{R}^2 \,|\, (x, y) \simeq (1, 0) \,\}$.

5.1.6. Recall that for $a, b \in \mathbf{Z}$, $a \equiv b \,(\mathrm{mod}\ 8)$ means that $a - b$ is divisible by 8.

(a) Find all integers x such that $0 \leq x < 8$ and $2x \equiv 6 \ (\mathrm{mod}\, 8)$.

(b) Use the Division Algorithm to prove that for every integer m there exists an integer r such that $m \equiv r \ (\mathrm{mod}\ 8)$ and $0 \leq r < 8$.

(c) Use the Division Algorithm (as in (a)) to find integers r_1 and r_2 such $0 \leq r_1 < 8$, $0 \leq r_2 < 8$, $1038 \equiv r_1 \ (\mathrm{mod}\ 8)$, and $-1038 \equiv r_2 \ (\mathrm{mod}\ 8)$.

5.1.7. For what positive integers $n > 1$ is:

(a) $30 \equiv 6 \ (\mathrm{mod}\, n)$ (b) $30 \equiv 7 \ (\mathrm{mod}\, n)$

5.1.8. Let m and n be positive integers such that m divides n. Prove that for all integers a and b, if $a \equiv b \pmod{n}$ then $a \equiv b \pmod{m}$.

5.1.9. (a) Prove or disprove: For all positive integers n and for all integers a and b, if $a \equiv b \pmod{n}$ then $a^2 \equiv b^2 \pmod{n}$.

(b) Prove or disprove: For all positive integers n and for all integers a and b, if $a^2 \equiv b^2 \pmod{n}$ then $a \equiv b \pmod{n}$.

Section 5.2: EQUIVALENCE CLASSES

Example 1: For $x, y \in \mathbf{R}$ define $x \simeq y$ to mean that $x - y \in \mathbf{Z}$. We have seen (cf Example 2 of Section 5.1.) that $\simeq$ is an equivalence relation on $\mathbf{R}$.

(a) List three real numbers x such that $x \simeq \sqrt{2}$.

(b) Give (without proof) a useful description of all real numbers x such that $x \simeq \sqrt{2}$; that is, give a statement $P(x)$ such that

$$\{\, x \in \mathbf{R} \,|\, x \simeq \sqrt{2} \,\} = \{\, x \in \mathbf{R} \,|\, P(x) \,\}.$$

Solution:(a) It is easily verified that $\sqrt{2} \simeq \sqrt{2} + 1$, $\sqrt{2} \simeq \sqrt{2} + 2$, and $\sqrt{2} \simeq \sqrt{2} - 1$.

(b) $\{\, x \in \mathbf{R} \,|\, x \simeq \sqrt{2} \,\} = \{\, x \in \mathbf{R} \,|\, x - \sqrt{2} \in \mathbf{Z} \,\} = \{\, x \in \mathbf{R} \,|\, x - \sqrt{2} = m \text{ for some } m \in \mathbf{Z} \,\} = \{\, x \in \mathbf{R} \,|\, x = \sqrt{2} + m \text{ for some } m \in \mathbf{Z} \,\}$.

Definition 1: Let $\simeq$ be an equivalence relation on a set S. For each $a \in S$, we define the **equivalence class** of a, denoted by $[a]$, to be the set

$$[a] = \{\, x \in S \,|\, x \simeq a \,\}.$$

Example 2: For $x, y \in \mathbf{R}$ define $x \simeq y$ to mean that $|x| = |y|$. You are given that $\simeq$ is an equivalence relation in $\mathbf{R}$. Describe $[0]$, $[5]$, and $[-5]$.

Solution: $[0] = \{\, x \in \mathbf{R} \,|\, x \simeq 0 \,\} = \{\, x \in \mathbf{R} \,|\, |x| = |0| \,\} = \{\, 0 \,\}$.

$[5] = \{\, x \in \mathbf{R} \,|\, x \simeq 5 \,\} = \{\, x \in \mathbf{R} \,|\, |x| = |5| \,\} = \{\, -5, 5 \,\}$.

$[-5] = \{\, x \in \mathbf{R} \,|\, x \simeq -5 \,\} = \{\, x \in \mathbf{R} \,|\, |x| = |-5| \,\} = \{\, -5, 5 \,\}$.

Comment: Later we will begin to treat an equivalence class as a single mathematical object (rather than view it as a set). For example, in certain circumstances we will add and multiply equivalence classes.

The difficulty that arises in working with equivalence classes is illustrated by Example 2 above. In that example we have a single object, $[5]$, that has two different labels; that is, $[5]$ and $[-5]$ are very distinct labels for the same object. We are already accustomed to this with the rational numbers. For instance, $\frac{1}{2}$ and $\frac{2}{4}$ are very distinct labels for one object.

Exercise 1: For (a, b), $(c, d) \in \mathbf{R}^2$ define $(a, b) \simeq (c, d)$ to mean that $2a - b = 2c - d$. We have seen in Exercise 3 of Section 5.1 that $\simeq$ is an equivalence relation on $\mathbf{R}^2$.

(a) Give a set-theoretic description of $[(1, 1)]$; that is, find a statement $P(x, y)$ such that $[(1, 1)] = \{ (x, y) \in \mathbf{R}^2 \mid P(x, y) \}$.

(b) Graph $[(1, 1)]$.

(c) Give a set-theoretic description of the equivalence class $[(0, -1)]$. How are the equivalence classes $[(1, 1)]$ and $[(0, -1)]$ related?

(d) Give a set-theoretic description of the equivalence class $[(2, 0)]$. How are the equivalence classes $[(1, 1)]$ and $[(2, 0)]$ related?

Comment: In Exercise 1 we once again encounter a single equivalence class with distinct labels. For instance, $[(1, 1)]$ and $[(0, -1)]$ are different labels for the same equivalence class. In contrast with Example 2, it is not at all obvious at a glance that $[(1, 1)] = [(0, -1)]$.

Equal Equivalence Classes

The next theorem is basic for working with equivalence classes as mathematical objects. The theorem permits us to quickly determine whether or not two equivalence classes are equal.

Theorem 1: Let $\simeq$ be an equivalence relation on the set S. For a, b in S the following statements are equivalent:

(a) $[a] = [b]$.
(b) $a \simeq b$.
(c) $a \in [b]$.
(d) $[a] \bigcap [b] \neq \emptyset$.

Since the statements (a) – (d) of Theorem 1 are equivalent, either all are true or all are false. Thus, the negations of (a) – (d) are also equivalent; that is,

for all a, $b \in S$, the following statements are equivalent:

(a) $[a] \neq [b]$.
(b) $a \not\simeq b$.
(c) $a \notin [b]$.
(d) $[a] \bigcap [b] = \emptyset$.

Proof of Theorem 1: Let a, $b \in S$.

(a) → (b): Assume that $[a] = [b]$. Now $\simeq$ is an equivalence relation, so is reflexive. In particular, $a \simeq a$. Thus $a \in [a]$. Since $[a] = [b]$, it follows that $a \in [b]$. Therefore $a \simeq b$.

(b) → (c): Assume that $a \simeq b$. Clearly, then, $a \in [b]$.

(c) → (d): Assume that $a \in [b]$. Since $a \simeq a$ we also have $a \in [a]$. Thus $a \in [a] \bigcap [b]$, so $[a] \bigcap [b] \neq \emptyset$.

(d) → (a): See Exercise 2 below.

Exercise 2: Complete the proof of Theorem 1 by proving that (d) → (a). [HINT: First prove that $a \simeq b$ then use that to prove that $[a] = [b]$.]

Exercise 3: Let $\mathbf{R}^{\#}$ denote the set of all nonzero real numbers and let $\mathbf{Q}^{\#}$ denote the set of all nonzero rational numbers. For a, $b \in \mathbf{R}^{\#}$ define $a \simeq b$ to mean that $a/b \in \mathbf{Q}^{\#}$. Given that $\simeq$ is an equivalence relation, use Theorem 1 to prove each of the following.

(a) $[\sqrt{3}] = [\sqrt{12}]$.

(b) $[\sqrt{3}] \bigcap [\sqrt{6}] = \emptyset$.

(c) $[\sqrt{8}] \neq [\sqrt{12}]$.

(d) $x = 3$ is a solution to the equation $[x\sqrt{2}] = [2\sqrt{2}]$.

Congruence Classes and the Set $\mathbf{Z}_n$

Comment: Equivalence classes for congruence mod n are also called **congruence classes**. Let a be an integer. By the definition of an equivalence class we have

$$[a] = \{\, x \in \mathbf{Z} \,|\, x \equiv a \pmod{n} \,\} = \{\, x \in \mathbf{Z} \,|\, x = a + kn \text{ for some integer } k \,\}.$$

Example 3: (a) For $n = 3$ describe the congruence class [0]. How are [3] and [−6] related to [0]?

(b) For $n = 3$ describe the congruence class [1]. Compare [4] and [−2] to [1].

Solution: (a) $[0] = \{\, x \in \mathbf{Z} \,|\, x \equiv 0 \pmod{3} \,\} = \{\, x \in \mathbf{Z} \,|\, x = 0 + 3k \text{ for some integer } k \,\} = \{\, x \in \mathbf{Z} \,|\, x = 3k \text{ for some integer } k \,\}$. Thus, [0] consists of all integer multiples of 3. Written informally, $[0] = \{\ldots, -6, -3, 0, 3, 6, \ldots\}$.

Similarly, $[3] = \{\, x \in \mathbf{Z} \,|\, x \equiv 3 \pmod{3} \,\} = \{\, x \in \mathbf{Z} \,|\, x = 3 + 3k \text{ for some integer } k \,\} = \{\, x \in \mathbf{Z} \,|\, x = 3(k+1) \text{ for some integer } k \,\}$. Thus, [3] also consists of all integer multiples of 3; that is $[0] = [3]$. Note that $0 \equiv 3 \pmod{3}$ and recall Theorem 1, parts (a) and (b), from Section 5.2.

In a similar fashion, we can see that $[-6] = [0] = [3]$.

(b) $[1] = \{\, x \in \mathbf{Z} \,|\, x \equiv 1 \pmod 3 \,\} = \{\, x \in \mathbf{Z} \,|\, x = 1 + 3k \text{ for some integer } k \,\}$. Thus, [1] consists of all integer multiples of 3 with one added. Written informally, $[1] = \{\ldots, -5, -2, 1, 4, 7, \ldots\}$.

By similar analysis, or by applying Theorem 1, we get $[1] = [4] = [-2]$.

Notation: Let n be a positive integer. We denote by $\mathbf{Z}_n$ the set of all congruence classes of $\mathbf{Z}$ for the relation congruence mod n. Thus, $\mathbf{Z}_n = \{\, [a] \,|\, a \in \mathbf{Z}\}$.

Example 4: List the elements of $\mathbf{Z}_3$.

Solution: We have seen in Example 3 that $[0] = \{\ldots, -6, -3, 0, 3, 6, \ldots\}$ and $[1] = \{\ldots, -5, -2, 1, 4, 7, \ldots\}$. Similarly, one can show that $[2] = \{\ldots, -4, -1, 2, 5, 8, \ldots\}$. Intuitively, it appears that every integer is included in one of these equivalence classes so all equivalence classes are accounted for. For example, $7 \in [1]$ so $[7] = [1]$ and $8 \in [2]$ so $[8] = [2]$.

Exercise 4: In $\mathbf{Z}_3$ determine which of [0], [1] or [2] equals the congruence class [4192].

Theorem 2: For every positive integer n, $\mathbf{Z}_n = \{\, [0], [1], \ldots, [n-1] \,\}$.

NOTE: We need to be clear about what Theorem 2 says. To illustrate with a specific example, although Theorem 2 implies that $\mathbf{Z}_4 = \{\, [0], [1], [2], [3] \,\}$, the definition of $\mathbf{Z}_4$ still includes, for instance, [413]. What the theorem tells us then, is that [413] equals one of the listed congruence classes. Indeed, $[413] = [1]$.

Proof: Let a be an integer. By the Division Algorithm, there exists integers q and r such that $a = qn + r$ and $0 \leq r < n$. Thus, $a - r = qn$; that is, n divides $a - r$. This means that $a \equiv r \pmod n$. By Theorem 1 (parts (a) and (b)), $[a] = [r]$.

Example 5: List the elements of $\mathbf{Z}_6$ and find integers r_1 and r_2 such that $0 \leq r_1 < 6$, $0 \leq r_2 < 6$, $[917] = [r_1]$, and $[-917] = [r_2]$.

Solution: By Theorem 2, $\mathbf{Z}_6 = \{\, [0], [1], [2], [3], [4], [5] \,\}$. If we divide 917 by 6, the remainder is 5; specifically, $917 = (152)6 + 5$. Therefore, $917 \equiv 5 \pmod 6$, so $[917] = [5]$.

Question: Is $\mathbf{Z}_2 \subseteq \mathbf{Z}_3 \subseteq \mathbf{Z}_4 \subseteq \cdots$?

The following theorem is a restatement of Theorem 1 for congruence classes.

Theorem 3: Let n be a positive integer. For a, $b \in \mathbf{Z}$ the following statements are equivalent.

(a) In $\mathbf{Z}_n$, $[a] = [b]$.

(b) $a \equiv b \pmod{n}$; that is, n divides $a - b$.

(c) $a \in [b]$.

(d) $[a] \bigcap [b] \neq \emptyset$.

Exercise 5: In $\mathbf{Z}_9$ use Theorem 3 to argue that:

(a) $[32] = [50]$.

(b) $[-33] = [75]$.

(c) $[5278] = [3082]$.

(d) $[16] \neq [37]$

Section 5.2. EXERCISES

In Exercises 5.2.1 – 5.2.4, $\simeq$ denotes the following equivalence relation (cf. Exercise 5.1.5):

$(**)$ For points (a, b), $(c, d) \in \mathbf{R}^2$ define $(a, b) \simeq (c, d)$ to mean that $a^2 + b^2 = c^2 + d^2$.

5.2.1. Let $\simeq$ be the equivalence relation defined in $(**)$ above.

(a) Give a set-theoretic description of $[(3, 4)]$; that is, $[(3, 4)] = \{\, (x, y) \in \mathbf{R}^2 \mid ?????? \,\}$.

(b) Graph $[(3, 4)]$.

5.2.2. Let $\simeq$ be the equivalence relation defined in $(**)$ above. Use Theorem 1 of Section 5.2 to prove each of the following:

(a) $[(0, 2)] = [(1, \sqrt{3})]$.

(b) $[(0, 2)] \neq [(1, 1)]$.

(c) $(2, 0) \in [(0, 2)]$.

(d) $[(1, 1)] \bigcap [(2, 1)] = \emptyset$.

(e) $(1, 0) \notin [(1, 1)]$.

Comments for 5.2.3 and 5.2.4: If $[(a, b)]$ is an equivalence class (other than $[(0, 0)]$) for the relation $\simeq$ defined in $(**)$ above, there are infinitely many different labels for the class. Specifically, if $r^2 = a^2 + b^2$ then for any point (x, y) on the circle $x^2 + y^2 = r^2$ we have $(x, y) \simeq (a, b)$ so $[(x, y)] = [(a, b)]$

The objective in Exercises 5.2.3 and 5.2.4 is to exhibit a "standard" set of labels for the equivalence classes so that we can immediately distinguish one equivalence class from another by its label. We will choose labels of the form $[(c, 0)]$, where $c \geq 0$.

Exercise 5.2.3 shows that every equivalence class has such a label and Exercise 5.2.4 shows that different labels represent different equivalence classes.

5.2.3. Let $\simeq$ be the equivalence relation defined in $(**)$ above. Prove that for all $(a, b) \in \mathbf{R}^2$ there exists $c \in \mathbf{R}$ such that $c \geq 0$ and $[(a, b)] = [(c, 0)]$.

5.2.4. Let $\simeq$ be the equivalence relation defined in $(**)$ above. Prove that for all nonnegative real numbers c and d, $[(c, 0)] = [(d, 0)]$ if and only if $c = d$.

NOTE: 5.2.4 is an equivalence, so two proofs are required.

5.2.5. In each of the following, prove that there exists (that is, exhibit) an integer x such that $0 \leq x < 9$ and the given equation is satisfied in $\mathbf{Z}_9$.

(a) $[3156] = [x]$ (b) $[-3156] = [x]$

(c) $[7 + x] = [3]$ (d) $[7x] = [1]$.

5.2.6. For a positive integer n set

$$\mathbf{Z}_{(n)} = \{\, [a] \in \mathbf{Z}_n \mid 1 = \gcd(a, n) \,\}.$$

Thus, for example, $\mathbf{Z}_{(10)} = \{\, [1], [3], [7], [9] \,\}$.

(a) Prove that the set $\mathbf{Z}_{(n)}$ is well-defined; that is, prove that for all integers a_1 and a_2, if $[a_1] = [a_2]$ in $\mathbf{Z}_n$ and if $[a_1] \in \mathbf{Z}_{(n)}$ then $[a_2] \in \mathbf{Z}_{(n)}$.

(b) Prove that for all integers a and b, if $[a], [b] \in \mathbf{Z}_{(n)}$, then $[ab] \in Z_{(n)}$.

Section 5.3: MAPPINGS

Definition 1: A **mapping** (or function) from a set A to a set B is a correspondence that assigns

- to **each element** of A
- a **uniquely determined** element of B.

Notation and Terminology:

- We will denote mappings with Greek letters. If α is a mapping of the set A to the set B we write $\alpha : A \to B$.
- With notation as above, the set A is called the **domain** of α and B is called the **codomain** of α.
- For each element $a \in A$, we denote by $\alpha(a)$ the image of a under the mapping α. [NOTE: It follows that the symbols α and $\alpha(a)$ are not interchangeable. α is the name of the mapping, whereas $\alpha(a) \in B$.]
- The set $\{\, \alpha(a) \,|\, a \in A \,\}$ is called the **range** of α.

Example 1: Let $A = \{a, b\}$ and $B = \{1, 2, 3\}$. If we define $\alpha_1 : A \to B$ by $\alpha_1(a) = 1$ and $\alpha_1(b) = 2$ then $\alpha_1 : A \to B$ is a mapping.

Exercise 1: Let $A = \{a, b\}$ and $B = \{1, 2, 3\}$.

(a) How many mapping are there from A to B?

(b) List all the mappings from A to B. (Call them α_1, α_2, etc.)

(c) How many mappings are there from B to A?

(d) Let A and B be finite sets with $|A| = m$ and $|B| = n$. How many mappings are there from A to B?

A Mapping Must be Defined

Let $\alpha : A \to B$ be a mapping. Note that by Definition 1, α **assigns to <u>each</u> element of** A a uniquely determined element of B. Thus, for α to be a mapping α **must be defined** on its entire domain.

Example 2:

(a) The correspondence $\alpha : \mathbf{R} \to \mathbf{R}$ defined by $\alpha(x) = \ln(x^2 - 1)$ is not a mapping since, for example, $\alpha(0)$ is not defined.

(b) If we use the same formula for α as in (a) but change the domain to the interval $(1, \infty)$ then α is a mapping.

(c) The correspondence $\beta : \mathbf{R}^2 \to \mathbf{R}$ defined by $\beta(x, y) = x/y$ is not a mapping since β is not defined at any point of the form $(x, 0)$.

(d) Let $A = \{ 1, 2 \}$ and $B = \{ a, b \}$. The correspondence $\gamma : A \to B$ defined by $\gamma(1) = a$ is not a mapping until we also define $\gamma(2)$.

A Mapping Must be Well-Defined

Let $\alpha : A \to B$ be a mapping. Note that by Definition 1, α assigns to each element of A **a uniquely determined element of** B. This means, for example, that we cannot have both $\alpha(1) = 3$ and $\alpha(1) = 4$.

A correspondence $\alpha : A \to B$ is **well-defined** provided for all a_1, $a_2 \in A$, if $a_1 = a_2$ then $\alpha(a_1) = \alpha(a_2)$.

Thus, to say a correspondence is well-defined is equivalent to saying that **equals can be substituted for equals**.

By Definition 1, a mapping must be well-defined.

Exercise 2: Complete the following:
A correspondence $\alpha : A \to B$ is not well-defined provided ....

To prove that a correspondence $\alpha : A \to B$ is not well-defined, we must prove, in symbolic form:

$$(\exists a_1, a_2 \in A) \Big(a_1 = a_2 \ \wedge \ \alpha(a_1) \neq \alpha(a_2) \Big)$$

Thus, a proof that a correspondence α is not well-defined has the following form:

To Prove: $\alpha : A \to B$ is not well-defined.

Form of Proof:

- Exhibit a_1, $a_2 \in A$ such that $a_1 = a_2$. (If it is not evident, verify that $a_1 = a_2$.)
- Verify that $\alpha(a_1) \neq \alpha(a_2)$.

Example 3: Define a correspondence $\alpha : \mathbf{Q} \to \mathbf{Z}$ as follows: For $x \in \mathbf{Q}$ write $x = \dfrac{a}{b}$ where a and b are integers. Let $\alpha(x) = \alpha(\dfrac{a}{b}) = a + b$. Note that α is not well-defined since $\dfrac{1}{2} = \dfrac{2}{4}$, but $\alpha(\dfrac{1}{2}) = 1 + 2 = 3$, whereas $\alpha(\dfrac{2}{4}) = 2 + 4 = 6$. Thus, $\dfrac{1}{2} = \dfrac{2}{4}$ but $\alpha(\dfrac{1}{2}) \neq \alpha(\dfrac{2}{4})$.

Exercise 3: In each of (a) and (b), demonstrate that the given correspondence is not well-defined.

(a) Define $\alpha : \mathbf{Q}^2 \to \mathbf{Q}$ as follows: For $(x, y) \in \mathbf{Q}^2$ write $(x, y) = (\frac{a}{b}, \frac{c}{d})$ where a and c are integers and b and d are positive integers. Then $\alpha(x, y) = \alpha(\frac{a}{b}, \frac{c}{d}) = \frac{a+c}{b+d}$.

(b) Define $\beta : \mathbf{Z}_4 \to \mathbf{Z}_{12}$ by $\beta([a]_4) = [a]_{12}$ (where the $[a]_4$ on the left is the congruence class of a mod 4 and the $[a]_{12}$ on the right is the congruence class of a mod 12).

NOTE: We will need to check whether a mapping is well-defined when the following two conditions hold:

(i) Elements of the domain have multiple representations, and

(ii) the mapping is defined in terms of a particular representation.

To prove that a correspondence $\alpha : A \to B$ is well-defined, we must prove, in symbolic form:

$$(\forall a_1, a_2 \in A) \Big(a_1 = a_2 \ \to \ \alpha(a_1) = \alpha(a_2) \Big)$$

Thus, a proof that a correspondence α is well-defined has the following form:

To Prove: $\alpha : A \to B$ is well-defined.

Form of Proof:

- Let a_1, a_2 be arbitrary (variable) elements in A.
- Assume that $a_1 = a_2$. Expand if it helps.
- Give a logical argument which concludes that $\alpha(a_1) = \alpha(a_2)$.

Example 4: Define $\alpha : \mathbf{Q} \to \mathbf{Q}$ by $\alpha(\frac{a}{b}) = \frac{a+3b}{2b}$, where a and b are integers and $b \neq 0$. Prove that α is well-defined.

Solution: Let $\frac{a}{b}, \ \frac{c}{d} \in \mathbf{Q}$ with $\frac{a}{b} = \frac{c}{d}$. Then $ad = bc$ so it follows that $2ad + 6bd = 2bc + 6bd$. Factoring both sides gives $(a + 3b)(2d) = (2b)(c + 3d)$. It now follows that $\frac{a+3b}{2b} = \frac{c+3d}{2d}$; that is, $\alpha(\frac{a}{b}) = \alpha(\frac{c}{d})$. Therefore, α is well-defined.

Exercise 4: Define $\beta : \mathbf{Z}_{12} \to \mathbf{Z}_3 \times \mathbf{Z}_4$ by $\beta([a]_{12}) = \Big([a]_3, [a]_4\Big)$, where $[a]_n$ denotes the congruence class of a in $\mathbf{Z}_n$. Prove that β is well-defined.

One – to – One Mappings

Definition 2: Let A and B be sets. A mapping $\alpha : A \to B$ is **one – to – one**, written $1 - 1$, provided for all a_1, $a_2 \in A$, if $a_1 \neq a_2$ then $\alpha(a_1) \neq \alpha(a_2)$.

Exercise 5: Complete the following definition, with the notation as in Definition 2.

A mapping $\alpha : A \to B$ is not $1-1$ provided ....

Exercise 6: In each of (a) – (d) prove that the given mapping is not $1-1$.

(a) $\alpha : \mathbf{R} \to \mathbf{R}$ defined by $\alpha(x) = x^2 - x - 6$ for all $x \in \mathbf{R}$.

(b) $\beta : \mathbf{R} \to \mathbf{R}$ defined by $\beta(x) = \cos(2x)$ for all $x \in \mathbf{R}$.

(c) $\gamma : \mathbf{R}^2 \to \mathbf{R}$ defined by $\gamma(x, y) = x + y$ for all $(x, y) \in \mathbf{R}^2$.

(d) Let M_2 denote the set of all 2×2 matrices with real number entries. Define $\lambda : M_2 \to \mathbf{R}$ by $\lambda(A) = \det(A)$ for all $A \in M_2$.

Comment: To use the definition of $1-1$ as stated, to prove that a mapping $\alpha : A \to B$ is $1-1$ we must prove

$$(*) \qquad (\forall a_1,\, a_2 \in A)\, a_1 \neq a_2 \to \alpha(a_1) \neq \alpha(a_2).$$

Since we are usually more comfortable and competent working with equality, we will typically prove that α is $1-1$ by proving the contrapositive of $(*)$; that is, to prove that a mapping $\alpha : A \to B$ is $1-1$ we prove

$$(**) \qquad (\forall a_1,\, a_2 \in A)\ \alpha(a_1) = \alpha(a_2) \to a_1 = a_2.$$

Example 5: Let $\alpha : \mathbf{R} \to \mathbf{R}$ be defined by $\alpha(x) = 3x + 2$. Prove that α is $1-1$.

Proof: Let x_1, x_2 be real numbers. Suppose that $\alpha(x_1) = \alpha(x_2)$. Thus, $3x_1 + 2 = 3x_2 + 2$. Subtracting 2 from both sides gives $3x_1 = 3x_2$. Dividing by 3 now gives $x_1 = x_2$, so α is $1-1$.

Exercise 7: Define $\alpha : \mathbf{R} \to \mathbf{R}$ by $\alpha(x) = 3e^{2x} + 5$ for all $x \in \mathbf{R}$. Prove that α is $1-1$.

Onto Mappings

Definition 3: Let A and B be sets. A mapping $\alpha : A \to B$ maps A **onto** B provided for every $b \in B$ there exists $a \in A$ such that $\alpha(a) = b$.

Exercise 8: Complete the following definition, with the notation as in Definition 3.

A mapping $\alpha : A \to B$ does not map A onto B provided ....

Exercise 9: In each of (a) – (c), verify that the given mapping is not onto.

(a) $\alpha : \mathbf{R} \to \mathbf{R}$ defined by $\alpha(x) = x^2 - x - 6$ for all $x \in \mathbf{R}$.

(b) $\beta : \mathbf{R} \to \mathbf{R}$ defined by

$$\beta(x) = \frac{2x^2 + 1}{x^2 + 5}$$

for all $x \in \mathbf{R}$.

(c) $\gamma : \mathbf{R}^2 \to \mathbf{R}^2$ defined by $\gamma(x, y) = (x + y, x + y)$ for all $(x, y) \in \mathbf{R}^2$.

Example 6: Define $\alpha : \mathbf{R}^2 \to \mathbf{R}$ by

$$\alpha(x, y) = \frac{2x + 1}{y^2 + 3}$$

for all $(x, y) \in \mathbf{R}^2$. Prove that α maps $\mathbf{R}^2$ onto $\mathbf{R}$.

Proof: Let $z \in \mathbf{R}$. Set $x = \frac{3z-1}{2}$ and $y = 0$. Then

$$\alpha(x, y) = \alpha(\frac{3z - 1}{2}, 0) = \frac{2\frac{3z-1}{2} + 1}{0^2 + 3} = \frac{3z}{3} = z.$$

Therefore, α maps $\mathbf{R}^2$ onto $\mathbf{R}$.

Exercise 10: Let M_2 denote the set of all 2×2 matrices with real number entries. Define $\alpha : M_2 \to M_2$ by

$$\alpha\Big(\begin{bmatrix} a & b \\ c & d \end{bmatrix} \Big) = \begin{bmatrix} a & a - b \\ 2c & 3c + d \end{bmatrix}.$$

Prove that α maps M_2 onto M_2.

Section 5.3 EXERCISES

5.3.1. Let $A = \{ a, b, c \}$ and $B = \{ 1, 2 \}$.

(a) How many $1-1$ mappings are there from A to A? List them.

(b) How many mappings are there from A onto A?

(c) How many $1-1$ mappings are there from A to B?

(d) How many mappings are there from A onto B? (HINT: It may be easier to count the mappings that are not onto.)

(e) How many $1-1$ mappings are there from B to A?

(f) How many mappings are there from B onto A?

5.3.2. Explain why each of the following is not a function.

(a) $\alpha : \mathbf{R} \to \mathbf{R}$ defined by

$$\alpha(x) = \frac{x}{x^2 - 4}$$

for every $x \in \mathbf{R}$.

(b) $\beta : \mathbf{R} \to \mathbf{R}$ defined by $\beta(x) = x \ln |x|$ for every $x \in \mathbf{R}$.

(c) $\gamma : \mathbf{Q} \to \mathbf{Q}$ defined as follows: For a rational number r, write $r = a/b$, where a and b are integers and $b \neq 0$. Set

$$\gamma(r) = \gamma(\frac{a}{b}) = \frac{a+b}{a^2+b^2}.$$

(d) $\lambda : \mathbf{Z}_8 \times \mathbf{Z}_8 \to \mathbf{Z}_6$ defined by $\lambda([a],[b]) = [ab]$ for all $([a],[b]) \in \mathbf{Z}_8 \times \mathbf{Z}_8$.
(NOTE: On the left, $[a]$ and $[b]$ are congruence classes mod 8, whereas on the right, $[ab]$ is a congruence class mod 6.)

5.3.3. Let m and n be positive integers such that m divides n. Prove that $\alpha : \mathbf{Z}_n \to \mathbf{Z}_m$ defined by $\alpha([a]_n) = [a]_m$ is well-defined.

5.3.4. Define $\alpha : \mathbf{R} \to \mathbf{R}$ by $\alpha(x) = 3x + 5$ for all $x \in \mathbf{R}$.

(a) Prove that α is $1-1$.

(b) Prove that α maps $\mathbf{R}$ onto $\mathbf{R}$.

5.3.5. Define $\beta : \mathbf{R} \to \mathbf{R}$ by $\beta(x) = 3x^2 + 5$ for every $x \in \mathbf{R}$. Prove that β is neither $1-1$ nor onto.

5.3.6. Let $A = \mathbf{R} - \{ 3 \}$ and $B = \mathbf{R} - \{ 2 \}$ and define $\gamma : A \to B$ by $\gamma(x) = \dfrac{2x+1}{x-3}$.

(a) Verify that γ maps A to B; that is, show that for all $a \in A$, $\gamma(a) \neq 2$. [HINT: Use contradiction.]

(b) Prove that γ is $1-1$.

(c) Prove that γ maps A onto B.

5.3.7. Let M_2 denote the set of all 2×2 matrices with real number entries. Define $\lambda : M_2 \to \mathbf{R}$ by $\lambda(A) = \det(A)$. Prove that λ maps M_2 onto $\mathbf{R}$.

5.3.8. Let m and n be relatively prime positive integers. Define $\alpha : \mathbf{Z}_{mn} \to \mathbf{Z}_m \times \mathbf{Z}_n$ by $\alpha([a]_{mn}) = \Big([a]_m, [a]_n\Big)$.

(a) Prove that α is well-defined.

(b) Prove that if k is an integer divisible by both m and n then k is divisible by mn.

(c) Prove that α is $1-1$. (Part (a) will be helpful.)

(d) Use (c) to conclude that α is onto.

Section 5.4: BINARY OPERATIONS

In this section we will consider binary operations defined on a set. Addition and multiplication of integers are examples of binary operations. We will use the symbol "$*$" to denote a binary operation.

Definition 1: A **binary operation** $*$ on a set S is a mapping $* : S \times S \to S$. For a, b, $c \in S$ we write $a * b = c$ rather than using the functional notation $*(a, b) = c$.

Thus, for instance, we can think of addition as a mapping $+ : \mathbf{Z} \times \mathbf{Z} \to \mathbf{Z}$ but we write $2 + 3 = 5$, not $+(2, 3) = 5$.

Let S be a set and suppose the correspondence $*$ is a candidate for a binary operation on S. Since $*$ must be a mapping from $S \times S$ to S it follows that:

- $*$ must be **defined** on $S \times S$; that is, for all a, $b \in S$, $a * b$ must be defined.
- $*$ must be well-defined; that is for a_1, a_2, b_1, $b_2 \in S$, if $a_1 = a_2$ and $b_1 = b_2$ then $a_1 * b_1 = a_2 * b_2$.
- The set S must be **closed** with respect to "$*$"; that is, for all a, $b \in S$, $a * b \in S$.

Example 1: In each of the following "$*$" is not a binary operation. Explain why.

(a) For x, $y \in \mathbf{R}$, $x * y = x/y$.

(b) For nonzero integers m and n, $m * n = m/n$.

(c) For $\dfrac{a}{b}$, $\dfrac{c}{d} \in \mathbf{Q}$, where a, b, c, $d \in \mathbf{Z}$ and $b \neq 0$ and $d \neq 0$, set $\dfrac{a}{b} * \dfrac{c}{d} = \dfrac{a + c}{bd}$.

Solution: (a) "$*$" is not defined if $y = 0$.

(b) The set of nonzero integers is not closed under division. For instance, $2 * 3 = 2/3$ and $2/3 \notin \mathbf{Z}$.

(c) "$*$" is not well-defined. For example, $\dfrac{1}{2} = \dfrac{2}{4}$ but $\dfrac{1}{2} * \dfrac{1}{3} = \dfrac{1+1}{(2)(3)} = \dfrac{2}{6} = \dfrac{1}{3}$ whereas, $\dfrac{2}{4} * \dfrac{1}{3} = \dfrac{2+1}{(4)(3)} = \dfrac{3}{12} = \dfrac{1}{4}$.

Exercise 1 Determine whether each of the following is a binary operation.

(a) For x, $y \in \mathbf{R}$ define $x * y = \dfrac{x - y}{x^2 + y}$.

(b) For m, $n \in \mathbf{Z}$ define $m * n = (m + n)/2$.

(c) For m, $n \in \mathbf{Z}$ define $m * n = 1$.

(d) For $\dfrac{a}{b}$, $\dfrac{c}{d} \in \mathbf{Q}$, where a, b, c, $d \in \mathbf{Z}$ and $b \neq 0$ and $d \neq 0$, set $\dfrac{a}{b} * \dfrac{c}{d} = \dfrac{2ad + 3bc}{bd}$.

Binary Operations on Equivalence Classes

Let S denote a set on which there is defined a binary operation $*$. Suppose $\simeq$ is an equivalence relation on S and let E denote the set of all equivalence classes of S corresponding to $\simeq$; that is, $E = \{\, [a] \mid a \in S \,\}$.

On occasion, we wish to "extend" the operation $*$ on S to an operation $\circledast$ on the set E, defined by $[a] \circledast [b] = [a * b]$.

We note that the operation $\circledast$ is defined on E since $*$ is already defined on S. Also, S is closed with respect to $*$ so it follows that E is closed with respect to $\circledast$ A single equivalence class, however, may have many labels. It is essential that we verify that a change of labels does not change the answer. The following example illustrates a case when $\circledast$ is not well-defined.

Example 2: For $x, y \in \mathbf{R}$ define $x \simeq y$ to mean that $|x| = |y|$. You are given that $\simeq$ is an equivalence relation on $\mathbf{R}$. Note that if $x \in \mathbf{R}$ with $x \neq 0$ then $[x] = \{\, x, -x \,\}$ and $[0] = \{\, 0 \,\}$.

Let E be the set of all equivalence classes of $\mathbf{R}$ for the relation $\simeq$. Extend addition and multiplication on $\mathbf{R}$ to operations $\oplus$ and $\odot$ on the set E defined by

$$[a] \oplus [b] = [a + b] \qquad \text{and} \qquad [a] \odot [b] = [ab].$$

(a) Show that $\oplus$ is not well-defined.

(b) Show that $\odot$ is well-defined.

Solution: (a) Note that in E we have $[2] = [-2]$ since $2 \simeq -2$. But $[2] \oplus [1] = [2 + 1] = [3]$, whereas $[-2] \oplus [1] = [-2 + 1] = [-1]$. Now $3 \not\simeq -1$ since $|3| \neq |-1|$, so $[3] \neq [-1]$. Therefore, $[2] \oplus [1] \neq [-2] \oplus [1]$. Since we cannot substitute equals for equals, the operation $\oplus$ is not well-defined.

(b) Let $[a_1]$, $[a_2]$, $[b_1]$, and $[b_2]$ be elements in E such that $[a_1] = [a_2]$ and $[b_1] = [b_2]$. Then $a_1 \simeq a_2$ and $b_1 \simeq b_2$; that is, $|a_1| = |a_2|$ and $|b_1| = |b_2|$. It follows that $|a_1 b_1| = |a_1|\,|b_1| = |a_2|\,|b_2| = |a_2 b_2|$. Consequently, $a_1 b_1 \simeq a_2 b_2$, so $[a_1 b_1] = [a_2 b_2]$. Thus, we can conclude that $[a_1] \odot [b_1] = [a_1 b_1] = [a_2 b_2] = [a_2] \odot [b_2]$ and $\odot$ is well-defined.

Exercise 2: For $x, y \in \mathbf{R}$ define $x \simeq y$ to mean that $x - y \in \mathbf{Z}$. Given that "$\simeq$" is an equivalence relation on $\mathbf{R}$, let E be the corresponding set of equivalence classes.

For $[a]$ and $[b]$ in E define $[a] \odot [b] = [ab]$ and define $[a] \oplus [b] = [a + b]$.

(a) Prove that in E, $[0] = [1]$.

(b) Use the equality in (a) to verify that $\odot$ is not well-defined.

(c) Prove that $\oplus$ is well-defined.

Definition 2: Let n be a positive integer. Extend addition and multiplication on $\mathbf{Z}$ to binary operations $\oplus$ and $\odot$ on $\mathbf{Z}_n$ defined as follows:

(a) For $[a]$, $[b]$ in $\mathbf{Z}_n$, $[a] \oplus [b] = [a + b]$.

(b) For $[a]$, $[b]$ in $\mathbf{Z}_n$, $[a] \odot [b] = [ab]$.

Example 3: To illustrate Definition 2, in $\mathbf{Z}_6$ we have $[3] \oplus [4] = [3 + 4] = [7] = [1]$ and $[3] \odot [4] = [(3)(4)] = [12] = [0]$.

Exercise 3: In $\mathbf{Z}_6$ verify that $[3] = [9]$ and $[4] = [16]$, then verify that $[3] \oplus [4] = [9] \oplus [16]$ and $[3] \odot [4] = [9] \odot [16]$.

Theorem 1: For every positive integer n the operations $\oplus$ and $\odot$ in $\mathbf{Z}_n$ are well-defined. That is, if $[a_1]$, $[a_2]$, $[b_1]$, $[b_2]$ are elements of $\mathbf{Z}_n$ such that $[a_1] = [a_2]$ and $[b_1] = [b_2]$ then

(a) $[a_1] \oplus [b_1] = [a_2] \oplus [b_2]$, and

(b) $[a_1] \odot [b_1] = [a_2] \odot [b_2]$.

Proof of (a): Let $[a_1]$, $[a_2]$, $[b_1]$, $[b_2]$ be elements of $\mathbf{Z}_n$ such that $[a_1] = [a_2]$ and $[b_1] = [b_2]$. Then $a_1 \equiv a_2 \pmod{n}$ and $b_1 \equiv b_2 \pmod{n}$. Thus, n divides both $a_1 - a_2$ and $b_1 - b_2$, so there exist integers k and l such that $a_1 - a_2 = kn$ and $b_1 - b_2 = ln$. Consequently, $(a_1 + b_1) - (a_2 + b_2) = (a_1 - a_2) + (b_1 - b_2) = kn + ln = (k + l)n$ so n divides $(a_1 + b_1) - (a_2 + b_2)$. Therefore, $a_1 + b_1 \equiv a_2 + b_2 \pmod{n}$. It now follows that $[a_1] \oplus [b_1] = [a_1 + b_1] = [a_2 + b_2] = [a_2] \oplus [b_2]$. This proves that $\oplus$ is well-defined.

The proof of (b) is an exercise.

Example 4: For $[a]$ and $[b]$ in $\mathbf{Z}_n$ we say that $[b] = [a]^{-1}$ provided $[a] \odot [b] = [1]$.

(a) Which elements of $\mathbf{Z}_9$ have inverses?

(b) In $\mathbf{Z}_9$ solve the equation $[4] \odot [x] \oplus [3] = [8]$.

Solution: (a) $[1]^{-1} = [1]$, $[2]^{-1} = [5]$ and $[5]^{-1} = [2]$, $[4]^{-1} = [7]$ and $[7]^{-1} = [4]$. The elements $[0]$, $[3]$, and $[6]$ have no inverse.

(b) To solve $[4] \odot [x] \oplus [3] = [8]$, first add $[-3]$ to both sides to get $[4] \odot [x] = [5]$. Now multiply both sides by $[4]^{-1} = [7]$ to obtain $[x] = [7] \odot [5] = [35] = [8]$.

Properties of Binary Operations

Definition 3: Let "$*$" be a binary operation on a set S.

(a) The operation $*$ is **associative** provided for all a, b, $c \in S$, $a * (b * c) = (a * b) * c$.

(b) The operation $*$ is **commutative** provided for all a, $b \in S$, $a * b = b * a$.

(c) An element e in S is an **identity** for the operation * provided for all $a \in S$, $a * e = a$ and $e * a = a$.

(d) Suppose S contains an identity e for the operation $*$. An element $b \in S$ is an **inverse** for an element $a \in S$ provided $a * b = e$ and $b * a = e$.

Exercise 4: Let "$*$" be a binary operation on a set S. Complete each of the following:

(a) The operation $*$ is not associative provided ....

(b) The operation $*$ is not commutative provided ....

(c) An element $f \in S$ is not an identity for $*$ provided ....

(d) The set S contains no identity for $*$ provided ....

(e) If S has identity e then an element $b \in S$ is not an inverse for the element $a \in S$ provided ....

(f) If S has identity e then an element $a \in S$ has no inverse in S provided ....

To say that an operation is binary means that we perform the operation on two elements. The **associativity** of an operation $*$ permits one to easily perform the operation on three or more elements. For example, the instructions to add or multiply the numbers 2, 4, 7 and 10 make sense since both additon and multiplication of real numbers is associative. On the other hand, the instructions to subtract or divide the list of numbers makes no sense since neither subtraction on $\mathbf{R}$ nor division on $\mathbf{R}^{\#}$ is associative. For instance $(3 - 2) - 1 = 0$ whereas $3 - (2 - 1) = 2$. Similarly, $(16 \div 4) \div 2 = 2$ but $16 \div (4 \div 2) = 8$.

Addition and multiplication of real numbers are commutative operations. Likewise, the addition of matrices is a commutative operation. Matrix multiplication is an example of a noncommutative operation.

Theorem 2: Let $*$ be a binary operation on a set S and let T be a nonempty subset of S. Then $*$ restricted to T is also a binary operation on T if and only if T is closed with respect to $*$.

Comment: Note that $*$ is automatically defined and well-defined on T since it is already defined and well-defined on the larger set S. On the other hand, for t_1, $t_2 \in T$ we only know that $t_1 * t_2 \in S$. Thus, T need not be closed with respect to $*$. When it is, $*$ restricted to T is a binary operation on T.

Example 5: On which of the following subsets of **Z** are addition and/or multiplication binary operations.

(a) E, the set of all even integers.

(b) O, the set of all odd integers.

(c) $T = \{ -1, 0, 1 \}$.

Solution: (a) Both addition and multiplication are binary operations on E. To give a proof, let m, $n \in E$. Then there exists integers k and l such that $m = 2k$ and $n = 2l$. Therefore, $m + n = 2k + 2l = 2(k + l)$ and $mn = (2k)(2l) = 2(2kl)$. In particular, both $m + n$ and mn are even.

(b) Addition is not a binary operation on O since, for instance, $1, 3 \in O$, but $1 + 3 = 4$ and $4 \notin O$. In a proof similar to that given in (a) it can be shown that O is closed with respect to multiplication, so multiplication is a binary operation on O.

(c) T is not closed under addition since, for instance, $1 + 1 = 2$ and $2 \notin T$.

Constructing a Cayley table for multiplication on T gives:

$\cdot$	-1	0	1
-1	1	0	-1
0	0	0	0
1	-1	0	1

We conclude that T is closed with respect to multiplication, so multiplication is a binary operation on T.

Exercise 5: Let $*$ be an operation on a set S, let T be a subset of S, and suppose that $*$ restricted to T is a binary operation on T. Prove or disprove each of the following.

(a) If $*$ is associative in S then $*$ is also associative in T.

(b) If $*$ is commutative in S then $*$ is also commutative in T.

(c) If S contains an identity for $*$ then T contains an identity for $*$.

Section 5.4. EXERCISES

5.4.1. **Background**: For x, $y \in \mathbf{R}$ define $x \simeq y$ to mean that $x^2 - 2x = y^2 - 2y$. You are given that $\simeq$ is an equivalence relation on $\mathbf{R}$.
Let E be the set of all equivalence classes of $\mathbf{R}$ for the relation $\simeq$; that is,
$E = \{\, [x] \mid x \in \mathbf{R} \,\}$.
Extend addition on $\mathbf{R}$ to a binary operation "$\oplus$" on E defined by $[x] \oplus [y] = [x + y]$. For example $[3] \oplus [4] = [3 + 4] = [7]$.

(a) Display one other label for each of the equivalence classes [3] and [4].

(b) Use the equivalence classes [3] and [4] to demonstrate that "$\oplus$" is not a well-defined operation.

5.4.2. In $\mathbf{Z}_8$ solve each of the following for $[x]$. In each case choose x so that $0 \leq x \leq 7$.

(a) $[6] \oplus [x] = [3]$.

(b) $[5] \odot [x] = [4]$.

(c) $[5] \odot [x] = [1]$.

(d) $[5] \odot [x] \ \oplus \ [7] = [5]$.

5.4.3. Let n be a positive integer, $n \geq 2$. For the operation $\oplus$ in Z_n prove:

(a) The operation is associative and commutative.

(b) $\mathbf{Z}_n$ contains an identity.

(c) Every element $[a]$ in $\mathbf{Z}_n$ has an inverse in $\mathbf{Z}_n$.

5.4.4. Let n be a positive integer, $n \geq 2$. For the operation $\odot$ in Z_n prove:

(a) The operation is associative and commutative.

(b) $\mathbf{Z}_n$ contains an identity.

5.4.5. Disprove each of the following:

(a) For every positive integer $n \geq 2$ and for all integers a and b, if $[a] \odot [b] = [0]$ in $\mathbf{Z}_n$ then either $[a] = [0]$ or $[b] = [0]$.

(b) For every positive integer $n \geq 2$ and for all integers a, b and c, if $[a] \neq [0]$ and $[a] \odot [b] = [a] \odot [c]$ in $\mathbf{Z}_n$ then $[b] = [c]$.

5.4.6. Let n be a positive integer. This exercise is concerned with the existence of inverses for the operation $\odot$ in $\mathbf{Z}_n$.

(a) Prove that for all $[a] \in \mathbf{Z}_n$, $[a]$ has an inverse in $\mathbf{Z}_n$ if and only if $\gcd(a, n) = 1$.

HINT: First note that the statement is an equivalence so two proofs are required.

In each direction, Theorem 2 of Section 4.3 will be useful.

In one direction, suppose $1 = \gcd(a, n)$. Then there exist integers s and t such that $1 = as + nt$. Argue that $[s] = [a]^{-1}$.

(b) Use the algorithms of Section 4.2 to show that $1 = \gcd(809, 5124)$ and find integers s and t such that $1 = 809s + 5124t$. Now find an integer b such that $0 \leq b < 5124$ and $[b] = [809]^{-1}$ in $\mathbf{Z}_{5124}$.

(c) Use $[809]^{-1}$ found in (b) to solve the equation $[809] \odot [x] = [214]$ in Z_{5124}. Reduce your final answer so that $0 \leq x < 5124$.

5.4.7. Let n be a positive integer. Prove that $\odot$ is a well-defined operation in $\mathbf{Z}_n$; that is, prove that if $[a_1]$, $[a_2]$, $[b_1]$, $[b_2]$ are elements in $\mathbf{Z}_n$ such that $[a_1] = [a_2]$ and $[b_1] = [b_2]$, then $[a_1] \odot [b_1] = [a_2] \odot [b_2]$.

5.4.8. Let $\mathbf{R}^{\#}$ and $\mathbf{Q}^{\#}$ denote, respectively, the set of nonzero real numbers and the set of nonzero rational numbers. For x, $y \in \mathbf{R}^{\#}$ define $x \simeq y$ to mean that $x/y \in \mathbf{Q}^{\#}$. You are given that "$\simeq$" is an equivalence relation on $\mathbf{R}^{\#}$.
Let E be the set of all equivalence classes of $\mathbf{R}^{\#}$ for the relation $\simeq$; that is, $E = \{\, [x] \mid x \in \mathbf{R}^{\#} \,\}$. Extend the operation of multiplication from $\mathbf{R}^{\#}$ to E by defining $[x] \odot [y] = [xy]$.
Prove that the operation $\odot$ is well-defined.

5.4.9. In each of the following, prove or disprove that:

(i) $*$ is associative;

(ii) $*$ is commutative;

(iii) the given set contains an identity for $*$; and

(iv) if the set contains an identity for $*$, then each element in the set has an inverse in the set.

(a) For x, $y \in \mathbf{R}$, $x * y = y$.

(b) For m, $n \in \mathbf{N}$ (where $\mathbf{N}$ is the set of natural numbers), $m * n = 3^{mn}$.

(c) For x, $y \in \mathbf{R} - \{2\}$, $x * y = xy - 2x - 2y + 6$.

5.4.10. Let $M_2(\mathbf{R})$ denote the set of all 2×2 real matrices. Then matrix multiplication is a binary operation on $M_2(\mathbf{R})$. Let $T = \{ A \in M_2(\mathbf{R}) \mid A = \begin{bmatrix} a & 0 \\ 0 & 0 \end{bmatrix}$ for some $a \in \mathbf{R} \}$.

(a) Verify that matrix multiplication is a binary operation on T.

(b) Show that matrix multiplication is noncommutative in $M_2(\mathbf{R})$ but is commutative in T.

(c) Show that both $M_2(\mathbf{R})$ and T contain identities for matrix multiplication, but the identities are not the same.

5.4.11. Let $*$ be an associative binary operation on a set S and let $e \in S$ be an identity for $*$.

(a) Prove that e is the unique identity of S for $*$.

(b) Suppose a, $b \in S$ are such that b is an inverse for a. Show that b is the unique inverse for a.

(c) Suppose that x, y, $z \in S$ are such that $x * y = e$ and $y * z = e$. Prove that $x = z$; hence x is the inverse of y.

Section 5.5: COMPOSITION AND INVERTIBLE MAPPINGS

Composition

Definition 1: Let A, B, and C be sets and let $\alpha : A \to B$ and $\beta : B \to C$ be mappings. The **composition** of α and β is the mapping $\beta \circ \alpha : A \to C$ defined by $(\beta \circ \alpha)(a) = \beta(\alpha(a))$ for every $a \in A$.

Example 1: Let $M_2(\mathbf{R})$ denote the set of all 2×2 matrices with real entries. Define $\alpha : M_2(\mathbf{R}) \to \mathbf{R}^2$ by $\alpha\Big(\begin{bmatrix} a & b \\ c & d \end{bmatrix}\Big) = (ad, bc)$ and define $\beta : \mathbf{R}^2 \to \mathbf{R}$ by $\beta(x, y) = x - y$. Give a formula for $\beta \circ \alpha$.

Solution:

$$(\beta \circ \alpha)\Big(\begin{bmatrix} a & b \\ c & d \end{bmatrix}\Big) = \beta\Big(\alpha\Big(\begin{bmatrix} a & b \\ c & d \end{bmatrix}\Big)\Big) = \beta(ad, bc) = ad - bc.$$

It follows that for $A \in M_2(\mathbf{R})$, $(\beta \circ \alpha)(A) = \det A$.

Exercise 1: Recall that $\mathbf{R}^+$ denotes the set of all positive real numbers. Define $\alpha : \mathbf{R}^3 \to \mathbf{R}$ by $\alpha(a, b, c) = 3a - 2b + c$ and define $\beta : \mathbf{R} \to \mathbf{R}^+$ by $\beta(x) = 3e^{2x}$. Give a formula for $\beta \circ \alpha$ and find $(\beta \circ \alpha)(1, 1, 1)$.

Theorem 1: Let $\alpha : A \to B$ and $\beta : B \to C$ be mappings. If α and β are both $1 - 1$ then $\beta \circ \alpha$ is also $1 - 1$.

Proof: Let $\alpha : A \to B$ and $\beta : B \to C$ be mappings. Assume that α and β are both $1 - 1$. To see that $\beta \circ \alpha$ is $1 - 1$ let a_1, $a_2 \in A$ be such that $(\beta \circ \alpha)(a_1) = (\beta \circ \alpha)(a_2)$. Thus, $\beta(\alpha(a_1)) = \beta(\alpha(a_2))$. But β is $1 - 1$ so it follows that $\alpha(a_1) = \alpha(a_1)$. But α is also $1 - 1$ so $a_1 = a_2$. We conclude that $\beta \circ \alpha$ is $1 - 1$.

Theorem 2: Let $\alpha : A \to B$ and $\beta : B \to C$ be mappings. If $\beta \circ \alpha$ is $1 - 1$ then α is also $1 - 1$.

Exercise 2: Complete the following proof of Theorem 2.

Proof: Let $\alpha : A \to B$ and $\beta : B \to C$ be mappings. Suppose $\beta \circ \alpha$ is $1 - 1$. To see that α is $1 - 1$ let a_1, $a_2 \in A$ and assume ....

Theorem 3: Let $\alpha : A \to B$ and $\beta : B \to C$ be mappings. If α and β are both onto then $\beta \circ \alpha$ is also onto.

Proof: Let $\alpha : A \to B$ and $\beta : B \to C$ be mappings. Assume that α and β are both onto. To see that $\beta \circ \alpha$ is onto let $c \in C$. Now $\beta : B \to C$ is onto by assumption, so there exists

$b \in B$ such that $\beta(b) = c$. We are also assuming that $\alpha : A \to B$ is onto, so there exists $a \in A$ such that $\alpha(a) = b$. It now follows that $(\beta \circ \alpha)(a) = \beta(\alpha(a)) = \beta(b) = c$. This proves that $\beta \circ \alpha$ is onto.

Theorem 4: Let $\alpha : A \to B$ and $\beta : B \to C$ be mappings. If $\beta \circ \alpha$ is onto then β is also onto.

Exercise 3: Complete the following proof of Theorem 4.

Proof: Let $\alpha : A \to B$ and $\beta : B \to C$ be mappings. Suppose $\beta \circ \alpha$ is onto. To see that β is onto let $c \in C$.

Invertible Mappings

Definition 2: Let S be a set. The **identity mapping** on S is the mapping $i : S \to S$ defined by $i(s) = s$ for every $s \in S$.

When it is not clear for which set i is the identity map, we use the notation i_S to specify the identity mapping on S. For example:

$i_{\mathbf{R}}$ is the identity mapping on the reals; for every $x \in \mathbf{R}$ we have $i_{\mathbf{R}}(x) = x$.

If $M_2(\mathbf{R})$ denotes the set of all 2×2 real matrices then $i_{M_2(\mathbf{R})}$ is the identity mapping on $M_2(\mathbf{R})$; for every matrix $A \in M_2(\mathbf{R})$ we have $i_{M_2(\mathbf{R})}(A) = A$.

Comment: Clearly the identity mapping is both $1-1$ and onto.

Exercise 4: Let $\alpha : A \to B$ be a mapping. Prove that

$$\alpha \circ i_A = \alpha \quad \text{and} \quad i_B \circ \alpha = \alpha.$$

Definition 3: A mapping $\beta : B \to A$ is the **inverse** of the mapping $\alpha : A \to B$, and we write $\beta = \alpha^{-1}$, provided $\alpha \circ \beta = i_B$ and $\beta \circ \alpha = i_A$. The mapping α is said to be **invertible** provided it has an inverse.

Caution: When we write α^{-1} to designate the inverse of the mapping α we are borrowing multiplicative notation. The operation involved, however, is composition, not multiplication. In particular, $\alpha^{-1} \neq 1/\alpha$; indeed, the symbol $1/\alpha$ is nonsense.

Example 2: Define $\alpha : \mathbf{Z} \to \mathbf{E}$ by $\alpha(n) = 2n$. ($\mathbf{E}$ denotes the set of all even integers.) Prove that α is invertible.

Proof: Define $\beta : \mathbf{E} \to \mathbf{Z}$ by $\beta(m) = m/2$. For every $n \in \mathbf{Z}$ we have $(\beta \circ \alpha)(n) = \beta\Big(\alpha(n)\Big) = \beta(2n) = 2n/2 = n = i_{\mathbf{Z}}(n)$. Therefore, $\beta \circ \alpha = i_{\mathbf{Z}}$. Similarly, for

$m \in E$ we have $(\alpha \circ \beta)(m) = \alpha\Big(\beta(m)\Big) = \alpha(m/2) = 2(m/2) = m = i_{\mathbf{E}}(m)$. Hence $\alpha \circ \beta = i_{\mathbf{E}}$. We conclude that $\beta = \alpha^{-1}$.

Exercise 5: Set $Y = \{\, y \in \mathbf{R} \,|\, y > -1 \,\}$. Define $\gamma : \mathbf{R} \to Y$ by $\gamma(x) = 3e^x - 1$ for every $x \in \mathbf{R}$. Prove that γ is invertible.

Example 3: Define $\alpha : \mathbf{R} \to \mathbf{R}$ by $\alpha(x) = x^2$. Prove that α is not invertible.

Proof: The proof is by contradiction, and to make a point we will arrive at two contradictions. Thus, assume that α is invertible and that $\beta = \alpha^{-1}$. Thus, β is a mapping and $\beta \circ \alpha = \alpha \circ \beta = i_{\mathbf{R}}$.
It follows that $\beta(4) = \beta\Big(\alpha(2)\Big) = (\beta \circ \alpha)(2) = i_{\mathbf{R}}(2) = 2$. Likewise,
$\beta(4) = \beta\Big(\alpha(-2)\Big) = (\beta \circ \alpha)(-2) = i_{\mathbf{R}}(-2) = -2$. Therefore, $\beta(4) = 2$ and $\beta(4) = -2$ so β is not well-defined, contrary to the assumption that β is a mapping.
Commencing once again with the assumption that $\beta = \alpha^{-1}$, set $\beta(-1) = x$. Then $-1 = i_{\mathbf{R}}(-1) = (\alpha \circ \beta)(-1) = \alpha\Big(\beta(-1)\Big) = \alpha(x) = x^2$. Thus, we have $x \in \mathbf{R}$ and $x^2 = -1$. Thus $\beta(-1)$ is not defined, a contradiction to the assumption that β is a mapping.

Comment: Note that in the proof above, β failed to be well-defined since $\alpha(2) = 4 = \alpha(-2)$; that is, α is not $1-1$. Further, $\beta(-1)$ was not defined because there exists no real number x such that $\alpha(x) = -1$; that is, α is not onto.

Theorem 5: A mapping $\alpha : A \to B$ is invertible if and only if α is both $1-1$ and onto.

Proof: Suppose α is $1-1$ and onto. We will define a mapping $\beta : B \to A$ and show that $\beta = \alpha^{-1}$. Thus, for $b \in B$ define $\beta(b) = a$ provided $\alpha(a) = b$. Since β is onto, for every $b \in B$ there exists $a \in A$ such that $\alpha(a) = b$. Thus β is defined for every $b \in B$. Further, since α is $1-1$, the choice of a is unique and β is well-defined. By definition of β, $\alpha \circ \beta = i_B$ and $\beta \circ \alpha = i_A$. Therefore, $\beta = \alpha^{-1}$ and α is invertible.

Exercise 6: Complete the proof of Theorem 5 by proving that if $\alpha : A \to B$ is invertible, the α is both $1-1$ and onto. (HINT: Use Theorems 2 and 4)

5.5 EXERCISES

5.5.1. Let $A = \{ 1, 2 \}$, $B = \{ x, y, z \}$, and $C = \{ a, b \}$. Define mappings $\alpha : A \to B$ and $\beta : B \to C$ so that $\beta \circ \alpha$ is both $1-1$ and onto but β is not $1-1$ and α is not onto.

5.5.2. Let $\alpha : A \to B$, $\beta : B \to C$, and $\gamma : B \to C$ be such that α is onto and $\beta \circ \alpha = \gamma \circ \alpha$. Prove that $\beta = \gamma$; that is, prove that for every $b \in B$, $\beta(b) = \gamma(b)$.

5.5.3. Let $\alpha : A \to B$, $\beta : A \to B$, and $\gamma : B \to C$ be such that γ is 1-1 and $\gamma \circ \alpha = \gamma \circ \beta$. Prove that $\alpha = \beta$; that is, prove that for every $a \in A$, $\alpha(a) = \beta(a)$.

5.5.4. Set $Y = \{ y \in \mathbf{R} \mid y \geq 0 \}$, define $f : \mathbf{R} \to Y$ by $f(x) = x^2$ and define $g : Y \to \mathbf{R}$ by $g(y) = \sqrt{y}$. Verify that $f \circ g = i_Y$ but that $g \circ f \neq i_{\mathbf{R}}$.

5.5.5. In each of the following:

- If the given mapping is invertible, exhibit an inverse mapping and verify that your mapping is the inverse.
- If the given mapping is not invertible, prove that it isn't by demonstrating that the mapping is either not $1-1$ or is not onto.

(a) $f : \mathbf{R} \to \mathbf{R}$ defined by $f(x) = 2x + 5$.

(b) $\alpha : M_2(\mathbf{R}) \to M_2(\mathbf{R})$ defined by $\alpha(A) = BA$ for every $A \in M_2(\mathbf{R})$, where $B = \begin{bmatrix} -1 & 2 \\ 0 & 2 \end{bmatrix}$ and where $M_2(\mathbf{R})$ denotes the set of all 2×2 real matrices.

(c) $\gamma : M_2(\mathbf{R}) \to M_2(\mathbf{R})$ defined by $\alpha(A) = CA$ for every $A \in M_2(\mathbf{R})$, where $C = \begin{bmatrix} -1 & 2 \\ -2 & 4 \end{bmatrix}$ and where $M_2(\mathbf{R})$ denotes the set of all 2×2 real matrices.

(d) $\delta : \mathbf{Z} \times \mathbf{Z}^{\#} \to \mathbf{Q}$ defined by $\delta(m, n) = m/n$ for all $(m, n) \in \mathbf{Z} \times \mathbf{Z}^{\#}$. (Recall that $\mathbf{Z}^{\#}$ denotes the set of all nonzero integers.)

5.5.6. Let $\alpha\, A \to B$ and $\beta : B \to C$ and $\gamma\, C \to D$ be mappings. Prove that $\alpha \circ (\beta \circ \gamma) = (\alpha \circ \beta) \circ \gamma$. (Thus, composition is associative.)

5.5.7. Let $\alpha\, A \to B$ and $\beta : B \to C$ be invertible mappings.

(a) Prove that $\beta \circ \alpha : A \to C$ is invertible.

(b) Express $(\beta \circ \alpha)^{-1}$ in terms of α^{-1} and β^{-1}.