Algebra I
Chapter 1. Basic Facts from Set Theory

1.1 Glossary of abbreviations.

Below we list some standard math symbols that will be used as shorthand abbreviations throughout this course.

- $\forall$ means "for all; for every"
- $\exists$ means "there exists (at least one)"
- $\exists!$ means "there exists exactly one"
- s.t. means "such that"
- $\Longrightarrow$ means "implies"
- $\Longleftrightarrow$ means "if and only if"
- $x \in A$ means "the point x belongs to a set A;" $x \notin A$ means "x is not in A"
- $\mathbb{N}$ denotes the set of natural numbers (counting numbers) $1, 2, 3, \cdots$
- $\mathbb{Z}$ denotes the set of all integers (positive, negative or zero)
- $\mathbb{Q}$ denotes the set of rational numbers
- $\mathbb{R}$ denotes the set of real numbers
- $\mathbb{C}$ denotes the set of complex numbers
- $\{x \in A : P(x)\}$ If A is a set, this denotes the subset of elements x in A such that statement $P(x)$ is true.

As examples of the last notation for specifying subsets:

$$\begin{aligned}
&\{x \in \mathbb{R} : x^2 + 1 \geq 2\} = (-\infty, -1] \cup [1, \infty) \\
&\{x \in \mathbb{R} : x^2 + 1 = 0\} = \emptyset \\
&\{z \in \mathbb{C} : z^2 + 1 = 0\} = \{+i, -i\} \quad \text{where } i = \sqrt{-1}
\end{aligned}$$

1.2 Basic facts from set theory.

Next we review the basic definitions and notations of set theory, which will be used throughout our discussions of algebra.

- $\emptyset$ denotes the **empty set**, the set with nothing in it
- $x \in A$ means that the point x **belongs to** a set A, or that x is an element of A.
- $A \subseteq B$ means A is a **subset** of B – i.e. any element of A also belongs to B (in symbolic notation: $x \in A \Rightarrow x \in B$). The symbols $A \subseteq B$ and $B \supseteq A$ are used interchangeably.
- $A = B$ means the sets A and B contain exactly the same points. This statement is equivalent to saying: $A \subseteq B$ AND $B \subseteq A$.

- If a set consists of just one point p it is called a **singleton set**, denoted $\{p\}$. (Logically speaking, the "point p" is not the same thing as "the set $\{p\}$ whose only element is p," which is why we need a distinctive notation for singletons.)

- $A \cap B$ indicates the **intersection** of two sets. An element x is in $A \cap B \Leftrightarrow x \in A$ AND $x \in B$. Notice that $A \cap B = B \cap A$.

- $A \cup B$ indicates the **union** of two sets. An element x lies in $A \cup B \Leftrightarrow$ EITHER $x \in A$ OR $x \in B$ (OR BOTH). Notice that $A \cup B = B \cup A$.

see Figure 1.1. Intersections and unions of several sets $A_1, \ldots, A_n$ are indicated by writing

$$\bigcap_{i=1}^{n} A_i = A_1 \cap \ldots \cap A_n \quad \text{This is the set } \{x : x \in A_i \text{ for every } i\}$$

$$\bigcup_{i=1}^{n} A_i = A_1 \cup \ldots \cup A_n \quad \text{This is the set } \{x : \exists \text{ some } i \text{ such that } x \in A_i\}$$

However, this notation is not practical when we wish to discuss unions or intersections of *huge* collections of sets. To handle those we use the following notation: Let I be a set of indices and suppose that we have assigned a set A_α to each index $\alpha \in I$. Then the intersection and union of the sets in this collection are denoted

$\bigcap_{\alpha \in I} A_\alpha$ a point x is in this intersection if and only if x lies in A_α for *every* index $\alpha \in I$.

$\bigcup_{\alpha \in I} A_\alpha$ a point x is in this union of sets if and only if there is *at least one* index $\alpha \in I$ such that x lies in A_α.

In the following exercises we ask you to prove some basic facts governing unions, intersections, and complements. Drawing pictures will help.

Proofs in set theory often ask you to verify that two sets A and B, which might be defined in very different ways, are in fact the same. To prove $A = B$ you need to show BOTH $A \subseteq B$ AND $B \subseteq A$. This is equivalent to showing that both of the following statements are true:

1. $x \in A \implies x \in B \quad (\text{so } A \subseteq B)$
2. $x \in B \implies x \in A \quad (\text{so } B \subseteq A)$

This breaks the task into two simpler pieces, which is to your advantage. Beware: statements 1. and 2. may sound the same, but in practice their proofs may be quite different! □

∗**1.2.1 Exercise.** Consider the subsets of $\mathbb{R}$ defined as follows: A_n is the interval $(0, \frac{1}{n})$ for all $n \in \mathbb{N}$. Show that

$$\text{(a)} \quad \bigcap_{n=1}^{\infty} A_n = \emptyset \qquad\qquad \text{(b)} \quad \bigcup_{n=1}^{\infty} A_n = (0,1) \quad \square$$

Hint: In (a), use the *Archimedean Property* of the integers in the real number system: For every $x \in \mathbb{R}$ there exists an integer $n \in \mathbb{N}$ such that $n > x$.

1.2.2 Exercise. Verify the following laws governing unions and intersections.

$$\begin{aligned}
(A \cap B) \cap C &= A \cap (B \cap C), && \text{(associative law)} \\
(A \cup B) \cup C &= A \cup (B \cup C), && \text{(associative law)} \\
A \cap (B \cup C) &= (A \cap B) \cup (A \cap C) && \text{(distributive law)} \\
A \cup (B \cap C) &= (A \cup B) \cap (A \cup C) && \text{(distributive law)} \\
A \cup B &= B \cup A && \text{(commutative law)} \\
A \cap B &= B \cap A && \text{(commutative law)} \quad \square
\end{aligned}$$

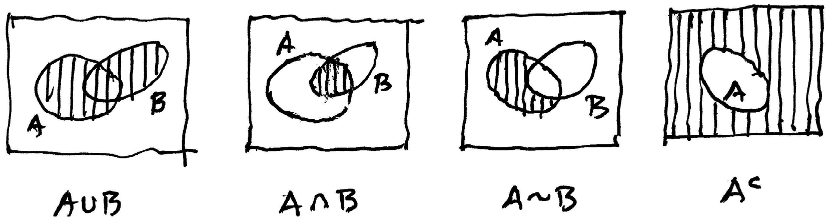

Figure 1.1 The shaded regions represent the basic set operations $A \cup B, A \cap B, A \sim B$, and A^{c} Arguments based on such pictures (*Venn Diagrams*) are not valid proofs, but they can be very helpful in guiding your intution toward a correct proof.

Continuing with our list of set theory notations, we define

- $A \sim B$ is the **difference set** $\{x : x \in A \text{ and } x \notin B\}$. Note carefully that $A \sim B$ need not be the same as $B \sim A$. (Think up an example!)
- A^{c} is the **complement** of a set A. Here A is a subset of some larger space X and its complement is the set $A^{\mathrm{c}} = \{x \in X : x \notin A\} = X \sim A$.

Notice that $A \sim B = A \cap B^{\mathrm{c}}$.

The geometric meaning of the basic set theory operations $A \cup B, A \cap B, A \sim B, A^{\mathrm{c}}$ is shown in the diagrams of Figure 1.1.

$*$**1.2.3 Exercise.** In the space $X = \mathbb{R}$ consider the intervals $A = [2, 5)$ and $B = (1, +\infty)$. Describe the sets (a) A^{c}, (b) B^{c}, (c) $A \sim B$, (d) $B \sim A$. □

$*$**1.2.4 Exercise.** Prove the following statements from the definitions:

(a) $A \sim B = A \sim (A \cap B)$ (b) $A \sim B = A \cap B^{\mathrm{c}}$

Give an example involving subsets in $\mathbb{R}$ such that $A \sim B \neq B \sim A$. (Draw pictures.) □

1.2.5 Exercise. Prove the **DeMorgan Laws** that govern the interaction between complements and unions or intersections. Assume that all sets are subsets of some fixed space X.

$$\begin{array}{rcll}
(A^{\mathrm{c}})^{\mathrm{c}} & = & A & \\
X^{\mathrm{c}} & = & \emptyset \quad \text{and} & \emptyset^{\mathrm{c}} = X \\
\Big(\bigcup_{\alpha \in I} A_\alpha\Big)^{\mathrm{c}} & = & \bigcap_{\alpha \in I} (A_\alpha)^{\mathrm{c}} & \text{(DeMorgan Law)} \\
\Big(\bigcap_{\alpha \in I} A_\alpha\Big)^{\mathrm{c}} & = & \bigcup_{\alpha \in I} (A_\alpha)^{\mathrm{c}} & \text{(DeMorgan Law)} \quad \square
\end{array}$$

The main point in 1.2.5 is easily remembered: taking the complement converts unions to intersections (and vice-versa) and replaces the sets A_α with their complements $(A_\alpha)^{\mathrm{c}}$. Note too that $A \sim B = A \cap B^{\mathrm{c}}$, which means that the DeMorgan laws can be used to good effect in computations that involve difference sets.

$*$**1.2.6 Exercise.** If A, B, C are subsets of a space X, prove the following facts about difference sets

(a) $A \sim (B \cup C) = (A \sim B) \sim C$

(b) $A \sim (B \cap C) = (A \sim B) \cup (A \sim C)$

Hint: The DeMorgan Laws might help. □

1.3 Cartesian product of sets.

We begin with the familiar Cartesian product of *two* sets. Things get more interesting when we try to define the Cartesian product of several, or infinitely many, sets.

1.3.1 Definition. The **Cartesian product** $A \times B$ of two sets A and B is the set consisting of all *ordered pairs* (a, b) with $a \in A$, $b \in B$. □

You have certainly seen this construction before.

1.3.2 Example. For $A = B = \mathbb{R}$, we write $\mathbb{R}^2 = \mathbb{R} \times \mathbb{R}$. Obviously $\mathbb{R}^2$ is the set of the coordinates for points in a plane. Note carefully: even if the sets A and B are the same, as happens here, the pairs (a, b) and (b, a) can be different points in the product space. □.

1.3.3 Exercise. If $A = \emptyset$, or $B = \emptyset$, explain why $A \times B = \emptyset$.

The definition of the product $A_1 \times \ldots \times A_n = \prod_{i=1}^n A_i$ of a finite number of sets is almost the same: its elements are simply the *ordered n-tuples* $\mathbf{a} = (a_1, \ldots, a_n)$ with $a_i \in A_i$. You could even handle the Cartesian product $\prod_{i=1}^\infty A_i$ of countably many sets $A_i, i = 1, 2, \ldots$ in much the same way; its elements are the infinite sequences $\mathbf{a} = (a_1, a_2, \ldots)$ with i^{th} entry $a_i \in A_i$. The notation becomes more subtle when we try to define the Cartesian product for a collection of sets $\{A_\alpha : \alpha \in I\}$ associated with a huge index set I. (For example, we might have a set A_α assigned to every real number $\alpha > 0$.)

1.3.4 Definition. If I is any index set and there exists a set A_α assigned to each index $\alpha \in I$, the **Cartesian product** $\prod_{\alpha \in I} A_\alpha$ is the set consisting of all **indexed words** $(a_\alpha)_{\alpha \in I}$, where $a_\alpha \in A_\alpha$ These are the maps $\phi : I \to \bigcup_{\alpha \in I} A_\alpha$ such that $\phi(\alpha) \in A_\alpha$ for every index $\alpha \in I$. □

1.4 Mappings.

A map ϕ from a set X to another set Y is an operation that associates each element in X to a *single* element in Y. We indicate the map by writing

$$\phi : X \to Y \qquad \text{or} \qquad \phi : x \mapsto \phi(x) \quad \text{(if the sets } X \text{ and } Y \text{ are understood)}$$

Unless stated otherwise, mappings $\phi(x)$ are assumed to be defined for *every* $x \in X$.

Not every $y \in Y$ will be the image of some $x \in X$ under a map $\phi : X \to Y$. The **range** of a map ϕ is the set of image points

$$\text{range}\,\phi = \phi(X) = \{b \in Y : \exists\, a \in X \text{ such that } b = \phi(a)\} \tag{1}$$

More generally, for any subset $S \subseteq X$ we define its **forward image** to be the following subset of Y :

$$\phi(S) = \{b \in Y : \exists\, a \in S \;\text{ such that } b = \phi(a)\} = \{\phi(a) : a \in A\}$$

1.4.1 Definition. *Given a map $\phi : X \to Y$ we say that ϕ is*

(a) ***injective****, or "one-to-one," if $a_1 \neq a_2 \implies \phi(a_1) \neq \phi(a_2)$;*

(b) ***surjective****, or "onto," if $\phi(X) = Y$;*

(c) ***bijective*** *if ϕ is both one-to-one and onto – i.e. $\forall b \in Y, \exists!\, a \in X$ such that $\phi(a) = b$.*

We say that two maps $\phi, \psi : X \to Y$ are **equal***, written $\phi = \psi$, if they have the same action: $\phi(a) = \psi(a)$ for all $a \in X$.*

1.4.2 Example. It is essential to be clear about what "equality of maps" means. The same map can have quite different descriptions, and it is not always obvious whether two maps are in fact

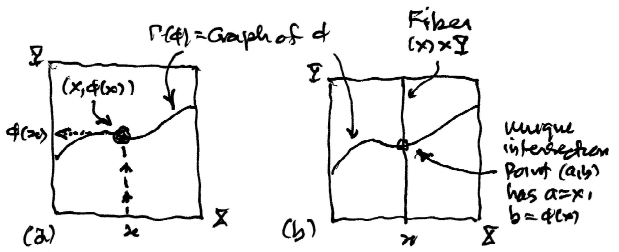

Figure 1.2 Graph of a map $\phi : X \to Y$.

the same. For example, taking $X = Y = \mathbb{R}$, the maps $\phi(x) = x^2$ and $\psi(x) = (x^2 + x^4)/(1 + x^2)$ are equal *as maps* because

$$\frac{x^2 + x^4}{1 + x^2} = \frac{x^2(1 + x^2)}{(1 + x^2)} = x^2$$

for all real x, even though different instructions are followed to compute the image points $\phi(x)$ and $\psi(x)$. Equality of maps $\phi, \psi : X \to Y$ means they yield the same output y for every input x. □

A map $\phi : X \to Y$ can also be described by its **graph** $\Gamma(\phi)$, which is a subset of the Cartesian product set $X \times Y$:

$$\Gamma(\phi) = \{(x, y) \in X \times Y : y = \phi(x)\} = \{(x, \phi(x)) : x \in X\} \tag{2}$$

As shown in Figure 1.1, each $x \in X$ determines a "vertical fiber"

$$(x) \times Y = \{(x, y) : y \in Y\} = \{\text{ all points } (a, b) \in X \times Y \text{ such that } a = x\}$$

in the Cartesian product. This fiber intersects the graph in exactly one point: $\Gamma(\phi) \cap ((x) \times Y) = \{(x, b)\}$. Reading off the second coordinate b of this intersection point we get the value $b = \phi(x)$ when ϕ is applied to the base point x. Hence the output of ϕ for any input x can be determined geometrically from the graph, as in Figure 1.2(b). Thus the map can be reconstructed if we know the graph, and vice versa; the map ϕ and its graph $\Gamma(\phi)$ encode the same information.

1.4.3 Exercise (Projection Maps). A Cartesian product $X = A_1 \times \ldots \times A_n$ is associated with various natural **projection maps** $\pi_j : X \to A_j$, defined by

$$\pi_j(a_1, \ldots, a_n) = a_j \quad j^{\text{th}} \text{ component of the } n\text{-tuple } \mathbf{a} = (a_1, \ldots, a_n) \tag{3}$$

These projections play a major role in several-variable Calculus.

(a) If S is a subset of a Cartesian product set $X \times Y$, what properties must S have relative to the projections π_X, π_Y for S to be the graph of some map $\phi : X \to Y$?

(b) What properties must S have to be the graph of a *surjective* map? Of an *injective* map? Of a *bijective* map? □

∗**1.4.4 Exercise.** Consider a composite $\phi \circ \psi(x) = \phi(\psi(x))$ of two maps $X \xrightarrow{\psi} Y \xrightarrow{\phi} Z$. If the maps ϕ and ψ are injective/surjective/bijective, what can you say about $\phi \circ \psi$? Write $I =$(injective), $S =$(surjective), $B =$(bijective) in the appropriate boxes of the following diagram if the property is always true; write $\boxed{\text{X}}$ if $\phi \circ \psi$ does not always have one of these properties.

		map ϕ		
		I	S	B
	I			
map ψ	S			
	B			

$*$**1.4.5 Exercise.** The standard model for the 2-dimensional sphere S^2 is the subset

$$S^2 = \{\mathbf{x} = (x_1, x_2, x_3) \in \mathbb{R}^3 : x_1^2 + x_2^2 + x_3^2 = 1\}$$

in the Cartesian product space $\mathbb{R}^3 = \mathbb{R} \times \mathbb{R} \times \mathbb{R}$.

(a) Let $J : S^2 \to S^2$ be the *inversion map* $J(x_1, x_2, x_3) = (-x_1, -x_2, -x_3)$. Is this map one-to-one? Onto? A bijection? If J is invertible is there an explicit formula for the inverse J^{-1}?

(b) Consider the projection map $p(x_1, x_2, x_3) = (x_1, x_2)$ from $\mathbb{R}^3$ into $\mathbb{R}^2$ and its restriction $q = p|S^2$ to the unit sphere. What is the range of the map $q : S^2 \to \mathbb{R}^2$? Is this map one-to-one? □

1.4.6 Exercise. Consider the map

$$\phi(t) = (\cos(t), \sin(t)) \qquad \text{for } t \in \mathbb{R}$$

from $\mathbb{R}$ into the unit circle $S^1 = \{(x, y) : x^2 + y^2 = 1\}$ in $\mathbb{R}^2$. Show that $\phi : \mathbb{R} \to S^1$ is surjective, and that $\phi(t_1) = \phi(t_2) \Leftrightarrow t_2 - t_1$ is an integer multiple of 2π.
Note: The map is periodic, with $\phi(t + 2\pi k) = \phi(t)$ for all integers k. □

Inverse Maps.

The **identity map** $\mathrm{id}_X : X \to X$ on a space sends each point $p \in X$ to itself. When a map $\phi : X \to Y$ is a bijection we may reverse its direction to get the **inverse map** $\phi^{-1} : Y \to X$, which has the properties $\phi^{-1} \circ \phi = \mathrm{id}_X$ and $\phi \circ \phi^{-1} = \mathrm{id}_Y$, so that

$$\phi^{-1}(\phi(a)) = a \text{ for all } a \in X \qquad \phi(\phi^{-1}(b)) = b, \text{ for all } b \in Y \quad .$$

In other words, each map ϕ and ϕ^{-1} undoes the action of the other. In an abstract setting, the inverse is given by the following recipe

$$\phi^{-1}(b) = \text{the unique element } a \in X \text{ such that } \phi(a) = b \quad ,$$

which makes sense precisely because ϕ is a bijection. Of course, when ϕ is given by some formula or algorithm, one would like to find a similar formula for the action of ϕ^{-1}. That is not always an easy task.

$*$**1.4.7 Exercise.** Consider the map $f : \mathbb{R} \to \mathbb{R}$ given by the formula $y = f(x) = x^3 + x + 1$. Use Calculus methods to verify that: (a) $\mathrm{range}\, f = \mathbb{R}$, (b) f is an injective map. Can you find an explicit formula for the inverse map $x = f^{-1}(y)$? □

$*$**1.4.7A Exercise.** If $f : X \to Y$ is an arbitrary map, is it always true that

$$f\big(A^{\mathrm{c}}\big) = \big(f(A)\big)^{\mathrm{c}}$$

I.e. is the forward image of the complement in X always equal to the complement of the image $f(A)$ in Y? Prove or provide a counterexample. □

$*$**1.4.8 Exercise.** For $\phi : X \to Y$ and $A, B \subseteq X$, show that the forward map has the properties:

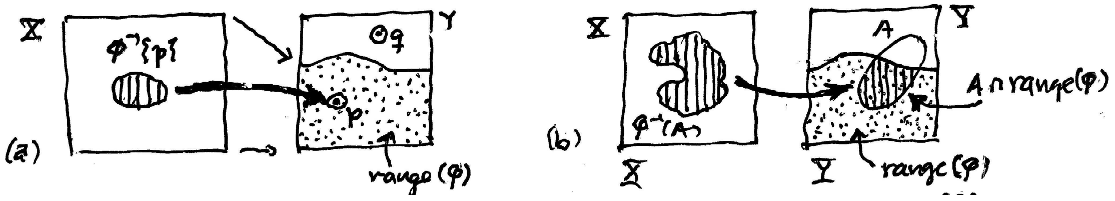

Figure 1.3 In (a), several points in X can map to the same point $p \in Y$ under a map $\phi : X \to Y$, so the pullback $\phi^{-1}\{p\}$ of a single point may contain several points. This pullback is empty $\phi^{-1}\{p\} = \emptyset$ if p lies outside the range of ϕ. In (b) we show the pullback $\phi^{-1}(A)$ of a set $A \subseteq Y$. Only the part of A in range(ϕ) contributes to the pullback; $\phi^{-1}(A) = \emptyset$ if A lies entirely outside the range of ϕ.

(a) $\phi(A \cup B) = \phi(A) \cup \phi(B)$ – i.e. the forward map *preserves unions of sets.*

(b) Produce a counterexample showing that $\phi(A \cap B) = \phi(A) \cap \phi(B)$ is not always true. The forward map *does not* always preserve intersections of sets.

(c) Show that the forward map *does* have the property $\phi(A \cap B) = \phi(A) \cap \phi(B)$ if we further assume that ϕ is one-to-one.

Hint: In (b) take a look at the map $f : \mathbb{R} \to \mathbb{R}$ given by $f(x) = x^2$. □

If $\phi : X \to Y$ is not a bijection, there is no inverse map $\phi^{-1} : Y \to X$. Nevertheless it is possible – and useful – to define the *inverse image* or *pullback* $\phi^{-1}(S)$ of a set $S \subseteq Y$.

1.4.9 Definition. *Given any map* $\phi : X \to Y$ *the* **inverse image** (*or* **pullback**) $\phi^{-1}(A)$ *of a set* $A \subseteq Y$ *is defined to be*

$$\phi^{-1}(A) = \{x \in X : \phi(x) \in A\} \tag{4}$$

Put another way, $\phi^{-1}(A)$ *consists of all* PRE-IMAGES *in* X *of points lying in* A. □

Note that $\phi^{-1}(\emptyset) = \emptyset$ since no $x \in X$ can satisfy $\phi(x) \in \emptyset$; we also have $\phi^{-1}(Y) = X$. Next observe that $\phi^{-1}(S)$ can be empty even if S is not. In fact,

$$\phi^{-1}(S) = \emptyset \Leftrightarrow S \text{ is disjoint from the range of } \phi.$$

Furthermore if S is a singleton, consisting of the single point $p \in Y$, then $\phi^{-1}(S) = \phi^{-1}(p)$ need not be a single point in X. In fact $\phi^{-1}(p)$ is the set of all preimages of p in X, and there may be several if ϕ is not one-to-one.

The geometric meaning of "pullback" $\phi^{-1}(A)$ of a set is illustrated in Figure 1.3.

***1.4.10 Exercise.** Taking $X = Y = \mathbb{R}$ let $f : \mathbb{R} \to \mathbb{R}$ be the map $f(x) = x^2$. Compute the following inverse image sets $\phi^{-1}(S)$ for:

(a) $S = [-1, 1]$ (b) $S = [1, +\infty)$

(c) $S =$ the singleton $\{4\}$ (d) $S = [-10, -4]$ □

1.4.11 Exercise. Show that the process of taking inverse images *preserves all the basic operations on sets.* For a map $\phi : X \to Y$ and $A, B, C, \dots$ subsets of Y, show that:

(a) $\phi^{-1}(\emptyset) = \emptyset$

(b) $\phi^{-1}(A \cap B) = \phi^{-1}(A) \cap \phi^{-1}(B)$

(c) $\phi^{-1}(A \cup B) = \phi^{-1}(A) \cup \phi^{-1}(B)$

(d) $\phi^{-1}(Y \sim A) = X \sim \phi^{-1}(A) \quad$ for $A \subseteq Y$

(e) $\phi^{-1}(A \sim B) = \phi^{-1}(A) \sim \phi^{-1}(B) \quad$ for $A, B \subseteq Y$. □

To illustrate how to put together a proof involving pullbacks of sets we prove part (b) of 1.4.11 below as a guide. You should attempt the other parts.

Proof (1.4.11(b)): We shall prove (⊇) and (⊆) separately (usually a good idea).

Proof (⊆): Consider a typical $x \in \phi^{-1}(A \cap B)$, which means the forward image $\phi(x)$ lies in $A \cap B$. Then

$$\phi(x) \in A \cap B \Rightarrow \begin{cases} \phi(x) \in A \\ \text{AND} \\ \phi(x) \in B \end{cases} \Rightarrow \begin{cases} x \in \phi^{-1}(A) \\ \text{AND} \\ x \in \phi^{-1}(B) \end{cases} \Rightarrow x \in \phi^{-1}(A) \cap \phi^{-1}(B)$$

so that $\phi^{-1}(A \cap B) \subseteq \phi^{-1}(A) \cap \phi^{-1}(B)$

Proof (⊇): Now we have $x \in \phi^{-1}(A) \cap \phi^{-1}(B)$, which implies that

$$\begin{cases} x \in \phi^{-1}(A) \\ \text{AND} \\ x \in \phi^{-1}(B) \end{cases} \Rightarrow \begin{cases} \phi(x) \in A \\ \text{AND} \\ \phi(x) \in B \end{cases} \Rightarrow \phi(x) \in A \cap B \Rightarrow x \in \phi^{-1}(A \cap B)$$

so that $\phi^{-1}(A) \cap \phi^{-1}(B) \subseteq \phi^{-1}(A \cap B)$

Putting the two parts together we get $\phi^{-1}(A \cap B) = \phi^{-1}(A) \cap \phi^{-1}(B)$. □

*__1.4.12 Exercise.__ For $X = \mathbb{N} \times \mathbb{N}$, $Y = \mathbb{N}$, define $\phi : X \to Y$ as $\phi(x, y) = x + y$. Find the inverse image of $\phi^{-1}(5)$ of the singleton set $\{5\}$. If $\eta : X \to Y$ is the product operation $\eta(x, y) = xy$, find $\eta^{-1}(4)$. □

1.5 Equivalence Relations in a Set.

If X is a set, a **relation** between points in X is defined by specifying some subset R in the Cartesian product $X \times X$. Once R is given we say that "a is related to b," indicated by writing $a \underset{R}{\sim} b$ (or simply $a \sim b$), if the pair (a, b) lies in R. This is an extremely general concept and there many kinds of relations, most of them uninteresting. We will be concerned with just one special kind: *equivalence relations*, also known as *RST relations*.

1.5.1 Definition. *A relation R in a set X is called an* **RST relation***, or* **equivalence relation***, if it has the following properties*

(i) $x \sim x$ *for all* $x \in X$ $\quad$ (*the relation is* reflexive)

(ii) $x \sim y \Rightarrow y \sim x$ *for all* $x, y \in X$ $\quad$ (*the relation is* symmetric)

(iii) $x \sim y$ *and* $y \sim z \Rightarrow x \sim z$ $\quad$ (*the relation is* transitive)

We say that "x is equivalent to y" if $x \underset{R}{\sim} y$. The **equivalence class** *of a point $p \in X$ is the set $[p]_R = \{x \in X : x \underset{R}{\sim} p\}$.*

1.5.2 Exercise. Show that the following relations are all rst relations.

(a) X arbitrary and $x \sim y \Leftrightarrow x = y$. The corresponding subset $R \subseteq X \times X$ is the *diagonal*, $R = \{(x, x) : x \in X\}$. This is the *trivial relation* in X.

(b) X arbitrary and $x \sim y$ for *all* pairs (x, y). Here the subset R is the entire Cartesian product $X \times X$, and every point in X is related to every other point. This is not a very interesting relation, but it does satisfy the definition of rst relation.

(c) $X = \mathbb{Z}$ and $x \sim y \Leftrightarrow y - x$ is a multiple of 5. This relation is described by saying "x *is congruent to* y (*mod* 5)".

(d) $X = \mathbb{R}^2$ and $\mathbf{x} \sim \mathbf{y} \Leftrightarrow \mathbf{x}$ and $\mathbf{y}$ lie on the same horizontal line in the plane. If $\mathbf{x} = (x_1, x_2)$ and $\mathbf{y} = (y_1, y_2)$ this means $x_2 = y_2$.

(e) $X = \mathbb{R}^2$ and $\mathbf{x} \sim \mathbf{y} \Leftrightarrow$ there exists a rotation R_θ, around the origin by some angle θ, such that $\mathbf{y} = R_\theta(\mathbf{x})$. Obviously, $\mathbf{x}$ is equivalent to $\mathbf{y}$ under this relation if and only if they have the same radial distance from the origin $\mathbf{0} = (0, 0)$.

There are many other examples. □

$*$**1.5.2A Example (Level Sets for Functions).** If $f : X \to \mathbb{R}$ is a scalar valued function on a space X the **level set**

$$L_c(f) = \{x \in X : f(x) = c\} \qquad (c \in \mathbb{R} \text{ fixed})$$

is the set of points where f takes on some particular value c. The level sets are the equivalence classes for the relation

$$x \underset{R}{\sim} x' \;\Leftrightarrow\; f(x') = f(x)$$

which is easily see to be an RST equivalence relation. For example if $f : \mathbb{R}^2 \to \mathbb{R}$ the level curves L_c are the places where the surface $z = f(x, y)$ has constant height above or below the x, y-plane. The resulting pattern of curves should be familiar to you if you have ever read a "contour map" while hiking cross-country.

Other examples of level sets can be more abstract. For instance if $X = \mathrm{M}(3, \mathbb{R})$ is the space of 3×3 matrices with real entries, it is well known that a matrix A acts linearly on $\mathbb{R}^3$ transforming any rectangular block R to a region $A(R)$, a *paralellopiped*, whose volume is

$$\mathrm{Vol}(A(R)) = |\det(A)| \cdot \mathrm{Vol}(R)$$

where $\det(A)$ is the determinant of the matrix. A level set $L_c(f)$ for the function $f(A) = |\det(A)|$ is the set of matrices that scale volumes by the same factor c. The particular set with $c = 0$ is the set $L_0(f) = \{A : \det A = 0\}$ of *singular* (noninvertible) matrices, which all squash rectangular blocks $B \subseteq \mathbb{R}^3$ into image sets $A(R)$ having *zero volume*. As above, these level sets are the equivalence classes $[A]$ for the RST relation between matrices $A \underset{R}{\sim} B \Leftrightarrow \det(A) = \det(B)$. □

$*$**1.5.3 Exercise.** Verify that the examples above are all RST relations. Explain why the relation

$$x \sim y \Leftrightarrow x < y$$

is *not* an RST relation on $X = \mathbb{R}$. What subset $R \subseteq \mathbb{R} \times \mathbb{R}$ corresponds to this relation? □

Every RST relation corresponds to a *partition* of the underlying set X into disjoint subsets that fill X.

1.5.4 Definition (Equivalence Classes). *Let R be an equivalence relation on X. Given a point a point p in X we define its* **equivalence class** *to be the set*

$$[p] = \{y \in X : y \underset{R}{\sim} p\} \tag{5}$$

Since $p \in [p]$, the equivalence classes fill X. The main properties of these classes are listed next.

1.5.5 Lemma *Let R be an equivalence relation on X. Its equivalence classes have the following properties.*

(a) *If $C = [p]$ is an equivalence class and $p' \in [p]$ then $[p'] = [p]$.*

(6) (b) *If $C_1 = [p_1]$ and $C_2 = [p_2]$ are two equivalence classes in X, then either $C_1 = C_2$ (the sets are identical) or $C_1 \cap C_2 = \emptyset$ (the sets are disjoint).*

Consequently the distinct equivalence classes partition X as a union of disjoint sets, in which two points are equivalent if and only if they lie in the same subset of the partition.

Proof: For (a): If $p' \in [p]$ we must prove that $[p] \subseteq [p']$ and $[p] \supseteq [p']$. If $p' \in [p]$ then $p' \sim p$ (and $p \sim p'$), therefore for every $x \in [p]$ we have $x \sim p \sim p'$, and by transitivity we get $x \sim p'$. Thus

$$x \in [p] \Rightarrow x \in [p'] \qquad \text{so that} \qquad [p] \subseteq [p']$$

For the reverse inclusion suppose $p' \in [p]$ and consider any point $y \in [p']$. Then $p' \sim p$ and $y \sim p'$ by definition of equivalence class, hence $y \sim p' \sim p$ and then $y \sim p$ by transitivity. Thus

$$y \in [p'] \Rightarrow y \in [p] \qquad \text{so that} \qquad [p'] \subseteq [p]$$

We conclude that $[p'] = [p]$ for any point $p' \in [p]$.

For (b), suppose C_1 and C_2 have a common point, say q. Then $p_1 \sim q, p_2 \sim q$ and hence $p_1 \sim p_2$ by symmetry and transitivity. Thus $p_2 \in [p_1]$ and $[p_2] = [p_1]$ by (a). If there is no common point, C_1 and C_2 are disjoint. □

In Example 1.5.2(d) above, the equivalence class of a point $\mathbf{p} \in \mathbb{R}^2$ is the entire horizontal line L passing through $\mathbf{p}$. Obviously, the plane is a disjoint union of the distinct horizontal lines it contains. In 1.5.2(e) not all equivalence classes look the same. If we write $\|\mathbf{x}\| = (x_1^2 + x_2^2)^{1/2}$ for the radial distance from $\mathbf{x} = (x_1, x_2)$ to the origin $\mathbf{0} = (0, 0)$, there is one equivalence class for each value $r \geq 0$. The classes are of two types:

$$\begin{array}{lll} \text{For } r > 0 & C_r = \{\mathbf{x} : \|\mathbf{x}\| = r\} & \text{(circle of radius } r) \\ \text{For } r = 0 & C_0 = \{\mathbf{x} : \|\mathbf{x}\| = 0\} = \{\mathbf{0}\} & \text{(the single point } \mathbf{0}) \end{array} \qquad \square$$

Given an equivalence class $C = [p]$ we refer to p as a **representative** of the class. Of course, according to (6a) every other point in C is also a representative.

We have seen how to go from an RST relation R to a partition $\mathcal{P}_R$ of X into disjoint sets (the equivalence classes for R). One can also go in the reverse direction. Suppose X is a set and $\mathcal{P} = \{X_\alpha : \alpha \in I\}$ is a collection of nonempty subsets (indexed by a set of labels I) that partition X, so that

$$X = \bigcup_{\alpha \in I} X_\alpha \qquad \text{and} \qquad X_\alpha \cap X_\beta = \emptyset \text{ if } \alpha \neq \beta \text{ in } I.$$

Then we can define a relation R on X such that the partition $\mathcal{P}_R$ is the same as the partition $\mathcal{P}$ we started with. In fact, this is what happens if we define

(7) $\qquad x \underset{R}{\sim} y \Leftrightarrow x$ and y lie in the same subset X_α of the partition $\mathcal{P}$

1.5.6 Exercise. Verify the above remarks. In particular, verify that (7) does define an RST relation on X, and that $\mathcal{P}_R = \mathcal{P}$. □

***1.5.7 Exercise.** Determine the sets in the partition $\mathcal{P}_R$ for each of the RST relation in Example 1.5.2. □

1.5.8 Definition (The Quotient Space X/R). *Given a set X and an* RST *relation R on it, the associated* **quotient space** *X/R is defined to be the set whose elements are the equivalence classes $[x]_R$ in X.*

Note carefully: *points* in the quotient space X/R are *subsets* of the original space X. This is clearly illustrated by example 1.5.2(d) where X/R was the collection of all horizontal lines in $\mathbb{R}^2$, each line $L \subseteq \mathbb{R}^2$ being regarded as a single point in the quotient space X/R. Having defined X/R, there is a natural **quotient map** $\pi : X \to X/R$ defined by taking

(8) $\qquad \pi(x) = [x]_R =$ the equivalence class of x.

Quotient spaces, and their associated quotient maps, will pop up frequently in algebra, analysis, and geometry. We now examine some fundamental examples of the interplay between algebraic structure and quotient spaces. We begin with the simplest possible example of a congruence relation in $\mathbb{Z}$, but will go on to show that a similar relation can be defined for each $n \in \mathbb{N}$.

1.5.9 Example: Congruence (mod 2). In $X = \mathbb{Z}$ we define the *parity relation* – also known as "congruence of integers (mod 2)" – as follows

$$\begin{aligned} x \sim y \quad &\Leftrightarrow \quad y - x \text{ is a multiple of } 2 \\ &\Leftrightarrow \quad \text{there is some } m \in \mathbb{Z} \text{ such that } y = x + 2m \\ &\Leftrightarrow \quad y \in x + 2\mathbb{Z} \end{aligned}$$

where $2\mathbb{Z} = \{2k : k \in \mathbb{Z}\}$ and $x + 2\mathbb{Z} = \{x + 2k : k \in \mathbb{Z}\}$. Obviously, $x \sim y \Leftrightarrow x$ and y have the same parity – either both even or both odd. Officially, **parity** of an integer $n \in \mathbb{Z}$ is defined to be $(-1)^n$, which can only take on the values $+1$ (even parity) or -1 (odd parity). Notice that $x \sim y \Leftrightarrow (-1)^x = (-1)^y \Leftrightarrow x$ and y have the same parity. Also note that by this definition 0 is even and 1 is odd. The equivalence class of a point $x \in \mathbb{Z}$ is the subset $[x] = x + 2\mathbb{Z}$ in $\mathbb{Z}$. There are just two equivalence classes because every x is equivalent either to 0 (x even) or to 1 (x odd). The quotient space is denoted by $X/R = \mathbb{Z}/(2\mathbb{Z}) = \mathbb{Z}_2$, and consists of the classes $[0] = 2\mathbb{Z}$ and $[1] = 1 + 2\mathbb{Z}$. Points in $\mathbb{Z}_2$ correspond to the possible parities of elements in $\mathbb{Z}$. □

The remarkable thing about the quotient space $\mathbb{Z}_2$ is that it inherits a natural algebraic structure from $\mathbb{Z}$. The appropriate $(+)$ and $(\cdot)$ operations are defined as follows:

$$\begin{array}{lll} [0] + [0] = [0] & [0] + [1] = [1] + [0] = [1] & [1] + [1] = [2] = [0] \\ [0] \cdot [0] = [0] & [0] \cdot [1] = [1] \cdot [0] = [0] & [1] \cdot [1] = [1] \end{array}$$

The resulting "algebraic quotient structure" $(\mathbb{Z}_2, +, \cdot\,)$ is a miniature number system in its own right, satisfying many of the familiar rules of arithmetic.

1.5.10 Definition (Congruence mod n). *Fix an integer $n > 1$ and define the following* RST *relation in $X = \mathbb{Z}$:*

$$\begin{aligned} a \equiv b \ (mod\ n) \quad &\Leftrightarrow \quad b - a \text{ is a multiple of } n \\ &\Leftrightarrow \quad b = a + nk \text{ for some } k \in \mathbb{Z} \\ &\Leftrightarrow \quad b \in a + n\mathbb{Z} = \{a + nk : k \in \mathbb{Z}\} \\ &\Leftrightarrow \quad b + n\mathbb{Z} = a + n\mathbb{Z} \end{aligned} \tag{9}$$

It is easily seen that this defines a relation that is reflexive, symmetric, and transitive. In plain English, the relation $a \equiv b$ (mod n) is read as: "a is **congruent to** *b* **modulo the integer** *n," and for this reason the equivalence classes*

$$[a] = \{b \in \mathbb{Z} : b \equiv a\} = \{a + kn : k \in \mathbb{Z}\} = a + n\mathbb{Z}$$

are referred to as the (mod n) **congruence classes** *in $\mathbb{Z}$. The class $[a]$ is an evenly spaced lattice of points in $\mathbb{Z}$, centered at a with distance n between successive points.*

The quotient space X/R is denoted by $\mathbb{Z}_n$; it consists of the distinct congruence classes in $\mathbb{Z}$. The associated quotient map $\pi = \pi_n : \mathbb{Z} \to \mathbb{Z}_n$ is given by $\pi : a \to [a] = a + n\mathbb{Z}$.

***1.5.11 Exercise.** For $n > 1$ define $a \equiv b$ (mod n) to mean

$$b - a \text{ is an integer multiple of } n$$

Verify that this is an RST relation on $X = \mathbb{Z}$. □

***1.5.12 Exercise.** Give a careful self-contained proof that

$$a \equiv b \pmod{n} \Leftrightarrow a + n\mathbb{Z} = b + n\mathbb{Z} \text{ as sets in } \mathbb{Z}. \quad \square$$

Obviously there are exactly n distinct equivalence classes in $\mathbb{Z}_n$, namely

$$[0] = 0 + n\mathbb{Z} = n\mathbb{Z} \qquad [1] = 1 + n\mathbb{Z} \qquad \ldots \qquad [n-1] = (n-1) + n\mathbb{Z} \ ,$$

because if we start with some $k \in \mathbb{Z}$ we can add or subtract whole multiples of n to arrive at a unique "normalized" class representative k' such that $0 \leq k' < n$. Here we have described the classes in $\mathbb{Z}_n$ by choosing particular class representatives. Of course we could also write $[n-1] = [-1]$, $[n-2] = [-2]$, etc., and sometimes it is useful to do so.

***1.5.13 Exercise.** If $0 \leq k < \ell < n$, explain why the (mod n) congruence classes $[k]$ and $[\ell]$ are disjoint sets in $\mathbb{Z}$, and are distinct points $[k] \neq [\ell]$ in the quotient space $\mathbb{Z}_n$. $\square$

We now show that the operations $(+)$ and $(\cdot)$ in $\mathbb{Z}$ induce corresponding operations in the quotient space $\mathbb{Z}_n$ of congruence classes, and that the induced operations inherit many properties from $\mathbb{Z}$. For the moment we will denote these operations in $\mathbb{Z}_n$ by $\oplus$ and $\odot$, but will soon revert to writing them as $(+)$ and $(\cdot)$ when there is no chance of confusing them with the original operations in $\mathbb{Z}$.

1.5.14 Theorem (Algebraic Structure in the Quotient Space $\mathbb{Z}_n$). *Fix an integer $n > 1$ Let $\mathbb{Z}_n$ be the quotient space of* (*mod n*) *congruence classes and let $\pi : \mathbb{Z} \rightarrow \mathbb{Z}_n$ be the quotient map. In $\mathbb{Z}_n$ define operations*

$$(10) \qquad [a] \oplus [b] = [a+b] \qquad \text{and} \qquad [a] \odot [b] = [ab]$$

for $a, b \in \mathbb{Z}$. These operations are well-defined despite the fact that class representatives are used to define them. Furthermore,

(a) *The element* $[0]$ *is the zero element with respect to the $\oplus$ operation:* $[0] \oplus x = x$ *for all $x \in \mathbb{Z}_n$.*

(b) *The element* $[1]$ *is the multiplicative identity element with respect to the $\odot$ operation:* $[1] \odot x = x$ *for all $x \in \mathbb{Z}_n$.*

Proof: In (10) we defined the operation $\oplus$ by picking class representatives and applying the following procedure

- Given classes A, B pick representatives a, b such that $A = [a]$ and $B = [b]$.
- Add the representatives to get $a + b$ in $\mathbb{Z}$
- Form the equivalence class $[a+b] = (a+b) + n\mathbb{Z}$ of $a + b$ in $\mathbb{Z}_n$.

The result is, by definition, the sum of classes $A \oplus B$. Similarly for products $A \odot B$.

We must show that this definition makes sense – i.e. if we take different representatives a', b' in place of a, b the class $[a'] \oplus [b'] = [a' + b']$ is the same as $[a] \oplus [b] = [a+b]$. Since elements x, y determine the same equivalence class $\Leftrightarrow x \sim y$, our goal is achieved if we can prove:

Claim: If $a' \sim a$ and $b' \sim b$ then $a' + b' \sim a + b$ and $a'b' \sim ab$

So, suppose $a' \equiv a$ and $b' \equiv b$ (mod n). By definition of congruence, there must be integers k, ℓ such that $a' = a + kn$ and $b' = b + \ell n$. Hence we have

$$\begin{aligned} a' + b' &= (a+b) + (k+\ell)n \\ &\equiv a + b \pmod{n} \\ a' \cdot b' &= a \cdot b + bkn + a\ell n + k\ell n^2 \\ &= a \cdot b + (\text{integer}) \cdot n \\ &\equiv a \cdot b \pmod{n} \end{aligned}$$

Consistency of the definition (10) is proved. The other identities

$$[a] \oplus [0] = [0] \oplus [a] = [a] \qquad \text{and} \qquad [a] \odot [1] = [1] \odot [a] = [a]$$

follow immediately from (10). □

These operations in $\mathbb{Z}_n$ generalize the familiar notion of "clock arithmetic." When $n = 12$, adding m hours and n on a clock is exactly like adding m and n (mod 12): a result like $6 + 8 \equiv 2$ makes perfect sense on a clock, even though $6 + 8 = 14$ in the system of integers $\mathbb{Z}$. Remember that the next time someone asks you why to explain why $2 + 2 = 4$. It *isn't* in some number systems, and if we lived on a planet with a 6-hour day (3 hours from midnight to noon) we might respond by saying "That's silly! Everyone knows $2 + 2 = 1$."

***1.5.15 Exercise.** In the system $\mathbb{Z}_n$ verify that

(a) If $0 \leq a < n$, the element $[a]$ has the property $[a] + [k] = [k]$ for all $[k] \in \mathbb{Z}_n$ if and only if $a = 0$.

(b) If $0 \leq a < n$, the element $[a]$ has the property $[a] \cdot [k] = [k]$ for all $[k] \in \mathbb{Z}_n$ if and only if $a = 1$. □

We say that $[a] \in \mathbb{Z}_n$ has a **multiplicative inverse** if there exists some $[k] \in \mathbb{Z}_n$ such that $[k] \cdot [a] = [a] \cdot [k] = [1]$. If it exists this inverse, or "reciprocal," is denoted by $[a]^{-1}$. The invertible elements in $\mathbb{Z}_n$ are called the **units** of this system, and the set of units is indicated by the symbol U_n. The zero element $[0]$ cannot be a unit, and the set of units always contains the elements $[1]$ and $-[1] = [-1] = [n-1]$; it is possible that these are the only units, as happens in $(\mathbb{Z}_4, +, \cdot\,)$. Notice that when $n = 2$ the multiplicative identity element is its own negative, $[1] = -[1] = [-1]$ because $[1] + [1] = [0]$; thus $[1]$ is the only unit in $\mathbb{Z}_2$ (as well being as the only nonzero element in this system). In Chapter 2 we will see that the nature of the invertible elements in the system $(\mathbb{Z}_n, +, \cdot\,)$ depends largely on the prime divisors of the modulus n.

$*$1.5.16 Exercise. Do all nonzero elements $[a] \neq [0]$ in $\mathbb{Z}_n$ have multiplicative inverses in $\mathbb{Z}_n$? Make multiplication tables for the systems $\mathbb{Z}_4$ and $\mathbb{Z}_7$ and find out. □

$*$1.5.17 Exercise. In $\mathbb{Z}_n$ is it possible to have two *nonzero* elements $[a], [b] \neq [0]$ such that $[a] \cdot [b] = [0]$? Investigate, trying $n = 4$ and $n = 5$. □

1.5.18 Proposition. If $n > 1$ is an integer prove that *every* nonzero element $[a] \neq [0]$ in $\mathbb{Z}_n$ has a multiplicative inverse if and only if n is a prime. □

1.5.19 Example (The Rational Numbers $\mathbb{Q}$). Let $\mathcal{F}$ be the set of all "fraction symbols" $\frac{p}{q}$, with $p, q \in \mathbb{Z}$ and $q \neq 0$. Into this system we introduce a relation ($\sim$) by declaring that

$$(11) \qquad \frac{p'}{q'} \sim \frac{p}{q} \quad \Leftrightarrow \quad p'q = pq' \text{ in } \mathbb{Z}$$

We leave it as an exercise to check that this is an RST relation on the set of symbols $\mathcal{F}$. This equivalence relation should look familiar. For instance, it says that $\frac{1}{2} \sim \frac{2}{4} \sim \ldots \sim \frac{24}{48} \sim \ldots$ or $\frac{5}{8} \sim \frac{15}{24} \sim \frac{10}{16}$. In fact one familiar rule for "reducing fractions"

$$\frac{mp}{mq} \sim \frac{p}{q} \qquad \text{for all } m \neq 0 \text{ in } \mathbb{Z}$$

is an immediate consequence of (11). However, there is more to equivalence than this because there are equivalent symbols $\frac{p'}{q'} \sim \frac{p}{q}$ such that

$$\frac{p'}{q'} \text{ is not of the form } \frac{mp}{mq} \qquad \text{for any integer } m \neq 0$$

and vice-versa. See Exercise 1.5.21.

Generations of grade-school children have been dismayed by the fact that many different symbols correspond to the same rational number. The following geometric interpretation is one way to understand equivalence of fraction symbols. When $p, q > 0$ the symbol p/q encodes instructions for locating a unique point on the number line $\mathbb{R}$.

> Geometric Interpretation of Fractions p/q. *Take the unit interval* $[0, 1] = \{x \in \mathbb{R} : 0 \leq x \leq 1\}$, *subdivide it into q segments of equal length, then join together p such pieces moving to the right of the origin at $x = 0$.*

There are similar interpretations for arbitrary fractions, except that the fraction $0/q$ is always assigned to the origin, and we might have to move to the left of the origin instead of to the right if p and q have opposite signs.

> Geometric Interpretation of Equivalence. *Two fractions $p'/q', p/q$ are equivalent in the sense that $\frac{p'}{q'} \sim \frac{p}{q}$ as defined in* (11) *if they determine the same point on the number line.*

It is also evident from this geometric criterion that equivalence is an RST relation on the set of fraction symbols $\mathcal{F} = \{p/q : p, q \in \mathbb{Z}, q \neq 0\}$. Consequently $\mathcal{F}$ splits into disjoint *equivalence classes*

$$\Big[\frac{p}{q}\Big] = \Big\{\frac{p'}{q'} : \frac{p'}{q'} \sim \frac{p}{q}\Big\} = \Big\{\frac{p'}{q'} : pq' = p'q\Big\}$$

It is these equivalence classes, and not the fraction symbols p/q themselves, that correspond to points on the number line; the resulting set of points in $\mathbb{R}$ is the system of rational numbers $\mathbb{Q}$.

You are all used to thinking of the rational numbers as an algebraic system, equipped with operations of addition $(+)$ and multiplication $(\cdot)$. But most of you have been trained to think of these as operations on fraction symbols, taking

$$\frac{p}{q} + \frac{r}{s} = \frac{ps + qr}{qs} \qquad \text{and} \qquad \frac{p}{q} \cdot \frac{r}{s} = \frac{pr}{qs} \tag{12}$$

You have also been trained to sweep under the rug all thoughts about the distinction between a rational number and the (many) symbols $\frac{p}{q}$ that represent it. This sort of sloppiness is what causes confusion for grade school students learning arithmetic, and is not acceptable in higher level mathematics. Having defined rational numbers as equivalence classes, we must describe the algebraic operations in $\mathbb{Q}$ as *operations on equivalence classes.* The preceding example $\mathbb{Z}_n$ suggests how this is to be done: given two classes, take any representatives $\frac{p}{q}$ and $\frac{r}{s}$ and define

$$\Big[\frac{p}{q}\Big] + \Big[\frac{r}{s}\Big] = \Big[\frac{ps + qr}{qs}\Big] \qquad \text{and} \qquad \Big[\frac{p}{q}\Big] \cdot \Big[\frac{r}{s}\Big] = \Big[\frac{pr}{qs}\Big] \tag{13}$$

Using the definition of fraction equivalence (11) one can verify that the resulting equivalence classes on the right don't depend on which representatives $\frac{p}{q}$ and $\frac{r}{s}$ of the original classes we chose, so the operations (13) on classes are well-defined in spite of the fact that we used class representatives to determine the outcome. (Details are outlined in Exercise 1.5.22 below.) □

***1.5.20 Exercise.** Prove that the relation $\frac{p}{q} \sim \frac{p'}{q'}$ between fraction symbols is an RST relation.

$*$**1.5.21 Exercise.** It is immediate from (11) that a fraction $\frac{p}{q}$ is equivalent to any fraction of the form $\frac{mp}{mq}$ for $m \neq 0$ in $\mathbb{Z}$. Find an example of two fraction symbols such that

$$\frac{p'}{q'} \sim \frac{p}{q} \quad \text{but} \quad \frac{p'}{q'} \text{ is not of the form } \frac{mp}{mq} \text{ for any integer } m \neq 0$$

Hint: What fraction symbols are equivalent to $\frac{p}{q} = \frac{1}{3}$? Are they all related to each other in the above manner? □

$*$**1.5.22 Exercise.** To prove that the operations on equivalence classes are well defined (independent of the choice of representatives used to determine the outcome) we need to verify the following statements: If $\frac{p'}{q'} \sim \frac{p}{q}$ and $\frac{r'}{s'} \sim \frac{r}{s}$ then

$$\begin{aligned} \frac{p'}{q'} + \frac{r'}{s'} = \frac{p's' + q'r'}{q's'} \quad &\text{is equivalent to} \quad \frac{p}{q} + \frac{r}{s} = \frac{ps + qr}{qs} \\ \frac{p'}{q'} \cdot \frac{r'}{s'} = \frac{p'r'}{q's'} \quad &\text{is equivalent to} \quad \frac{p}{q} \cdot \frac{r}{s} = \frac{pr}{qs} \end{aligned}$$

Check that both statements are true using the definition (11) of fraction equivalence.
Hint: The result for products of fractions is *much* easier than that for sums; try it first. Both results must be proved by repeated use of the given identities $p'q = qp'$ and $r's = rs'$ (equivalence of fraction symbols). $\square$

It is easy to verify that the elements $\mathbf{0} = [\frac{0}{1}]$ and $\mathbf{1} = [\frac{1}{1}]$ in $\mathbb{Q}$ have the special properties

$$\begin{aligned} \mathbf{0} + \left[\frac{p}{q}\right] &= \left[\frac{p}{q}\right] \text{ for all } \left[\frac{p}{q}\right] \text{ in } \mathbb{Q} \\ \mathbf{1} \cdot \left[\frac{p}{q}\right] &= \left[\frac{p}{q}\right] \text{ for all } \left[\frac{p}{q}\right] \text{ in } \mathbb{Q} \end{aligned}$$

These elements are, respectively, the *additive zero element* and the *multiplicative identity element* in $(\mathbb{Q}, +, \cdot\,)$ The next exercise shows that $\mathbb{Q}$ contains a faithful copy of the integers $\mathbb{Z}$.

1.5.23 Exercise. Let $\psi : \mathbb{Z} \rightarrow \mathbb{Q} = \mathcal{F}/(\sim)$ be the map $\psi(m) = \left[\frac{m}{1}\right]$. Prove that

(a) ψ is a one-to-one map of $\mathbb{Z}$ into $\mathbb{Q}$, so $\psi(\mathbb{Z})$ is a faithful copy of $\mathbb{Z}$ in $\mathbb{Q}$.

(b) ψ intertwines the algebraic operations in $\mathbb{Z}$ and $\mathbb{Q}$:

$$\begin{aligned} \psi(a + b) &= \psi(a) + \psi(b) \text{ (sum of elements in } \mathbb{Q}) \ = \left[\tfrac{a}{1}\right] + \left[\tfrac{b}{1}\right] \\ \psi(a \cdot b) &= \psi(a) \cdot \psi(b) \text{ (product of elements in } \mathbb{Q}) \ = \left[\tfrac{a}{1}\right] \cdot \left[\tfrac{b}{1}\right] \end{aligned}$$

for all $a, b \in \mathbb{Z}$. $\square$

1.5.24 Exercise. Prove that every nonzero element $\mathbf{x} = \left[\frac{p}{q}\right]$ in $\mathbb{Q}$ has a multiplicative inverse $\mathbf{x}^{-1} = \left[\frac{r}{s}\right]$ such that $\mathbf{x}^{-1} \cdot \mathbf{x} = \mathbf{1}$. $\square$

This makes the system $\mathbb{Q}$ a "number field." The system of integers does not have this property; for instance the number "2" has no multiplicative inverse in $\mathbb{Z}$. In view of 1.5.23 the system of rationals is a natural "extension" $\mathbb{Q} \supseteq \mathbb{Z}$ in which all nonzero elements have multiplicative inverses (in $\mathbb{Q}$). That is precisely the point of constructing the system $\mathbb{Q}$.

1.5.25 Exercise. If we define a "positivity relation" $\left[\frac{p}{q}\right] > 0$ in $\mathbb{Q}$ to mean that $pq > 0$, prove that

(a) The relation ">" is well-defined on equivalence classes, independent of the representative $p/q \in \mathcal{F}$ – i.e. if $p/q \sim p'/q'$ then $pq > 0 \Leftrightarrow p'q' > 0$ in $\mathbb{Z}$.

(b) If $x = \left[\frac{p}{q}\right]$ and $y = \left[\frac{r}{s}\right]$ satisfy $x > 0$ and $y > 0$ in $\mathbb{Q}$ prove that $x + y > 0$ and $x{\cdot}y > 0$.

As we will see in Chapter 2, this means $(\mathbb{Q}, +, \cdot\,)$ becomes a "commutative ordered ring" when equipped with the ">" relation. $\square$