**EXAMPLE 0.23**

Jack sees Jill, who has just come in from outdoors. On observing that she is completely dry, he knows that it is not raining. His "proof" that it is not raining is that *if it were raining* (the assumption that the statement is false), *Jill would be wet* (the obviously false consequence). Therefore, it must not be raining. ■

Next, let's prove by contradiction that the square root of 2 is an irrational number. A number is ***rational*** if it is a fraction $\frac{m}{n}$, where $m$ and $n$ are integers; in other words, a rational number is the *ratio* of integers $m$ and $n$. For example, $\frac{2}{3}$ obviously is a rational number. A number is ***irrational*** if it is not rational.

**THEOREM 0.24**

$\sqrt{2}$ is irrational.

**PROOF** First, we assume for the purpose of later obtaining a contradiction that $\sqrt{2}$ is rational. Thus

$$\sqrt{2} = \frac{m}{n},$$

where $m$ and $n$ are integers. If both $m$ and $n$ are divisible by the same integer greater than 1, divide both by the largest such integer. Doing so doesn't change the value of the fraction. Now, at least one of $m$ and $n$ must be an odd number.

We multiply both sides of the equation by $n$ and obtain

$$n\sqrt{2} = m.$$

We square both sides and obtain

$$2n^2 = m^2.$$

Because $m^2$ is 2 times the integer $n^2$, we know that $m^2$ is even. Therefore, $m$, too, is even, as the square of an odd number always is odd. So we can write $m = 2k$ for some integer $k$. Then, substituting $2k$ for $m$, we get

$$\begin{aligned} 2n^2 &= (2k)^2 \\ &= 4k^2. \end{aligned}$$

Dividing both sides by 2, we obtain

$$n^2 = 2k^2.$$

But this result shows that $n^2$ is even and hence that $n$ is even. Thus we have established that both $m$ and $n$ are even. But we had earlier reduced $m$ and $n$ so that they were *not* both even—a contradiction.

## PROOF BY INDUCTION

Proof by induction is an advanced method used to show that all elements of an infinite set have a specified property. For example, we may use a proof by induction to show that an arithmetic expression computes a desired quantity for every assignment to its variables, or that a program works correctly at all steps or for all inputs.

To illustrate how proof by induction works, let's take the infinite set to be the natural numbers, $\mathcal{N} = \{1, 2, 3, \dots\}$, and say that the property is called $\mathcal{P}$. Our goal is to prove that $\mathcal{P}(k)$ is true for each natural number $k$. In other words, we want to prove that $\mathcal{P}(1)$ is true, as well as $\mathcal{P}(2)$, $\mathcal{P}(3)$, $\mathcal{P}(4)$, and so on.

Every proof by induction consists of two parts, the ***basis*** and the ***induction step***. Each part is an individual proof on its own. The basis proves that $\mathcal{P}(1)$ is true. The induction step proves that for each $i \geq 1$, if $\mathcal{P}(i)$ is true, then so is $\mathcal{P}(i+1)$.

When we have proven both of these parts, the desired result follows—namely, that $\mathcal{P}(i)$ is true for each $i$. Why? First, we know that $\mathcal{P}(1)$ is true because the basis alone proves it. Second, we know that $\mathcal{P}(2)$ is true because the induction step proves that if $\mathcal{P}(1)$ is true then $\mathcal{P}(2)$ is true, and we already know that $\mathcal{P}(1)$ is true. Third, we know that $\mathcal{P}(3)$ is true because the induction step proves that if $\mathcal{P}(2)$ is true then $\mathcal{P}(3)$ is true, and we already know that $\mathcal{P}(2)$ is true. This process continues for all natural numbers, showing that $\mathcal{P}(4)$ is true, $\mathcal{P}(5)$ is true, and so on.

Once you understand the preceding paragraph, you can easily understand variations and generalizations of the same idea. For example, the basis doesn't necessarily need to start with 1; it may start with any value $b$. In that case, the induction proof shows that $\mathcal{P}(k)$ is true for every $k$ that is at least $b$.

In the induction step, the assumption that $\mathcal{P}(i)$ is true is called the ***induction hypothesis***. Sometimes having the stronger induction hypothesis that $\mathcal{P}(j)$ is true for every $j \leq i$ is useful. The induction proof still works because when we want to prove that $\mathcal{P}(i+1)$ is true, we have already proved that $\mathcal{P}(j)$ is true for every $j \leq i$.

The format for writing down a proof by induction is as follows.

***Basis:*** Prove that $\mathcal{P}(1)$ is true.

$$\vdots$$

***Induction step:*** For each $i \geq 1$, assume that $\mathcal{P}(i)$ is true and use this assumption to show that $\mathcal{P}(i+1)$ is true.

$$\vdots$$

Now, let's prove by induction the correctness of the formula used to calculate the size of monthly payments of home mortgages. When buying a home, many people borrow some of the money needed for the purchase and repay this loan over a certain number of years. Typically, the terms of such repayments stipulate that a fixed amount of money is paid each month to cover the interest, as well as part of the original sum, so that the total is repaid in 30 years. The formula for calculating the size of the monthly payments is shrouded in mystery, but actually is quite simple. It touches many people's lives, so you should find it interesting. We use induction to prove that it works, making it a good illustration of that technique.

First, we set up the names and meanings of several variables. Let $P$ be the *principal*, the amount of the original loan. Let $I > 0$ be the yearly *interest rate* of the loan, where $I = 0.06$ indicates a 6% rate of interest. Let $Y$ be the monthly payment. For convenience, we use $I$ to define another variable $M$, the monthly multiplier. It is the rate at which the loan changes each month because of the interest on it. Following standard banking practice, the monthly interest rate is one-twelfth of the annual rate so $M = 1 + I/12$, and interest is paid monthly (monthly compounding).

Two things happen each month. First, the amount of the loan tends to increase because of the monthly multiplier. Second, the amount tends to decrease because of the monthly payment. Let $P_t$ be the amount of the loan outstanding after the $t$th month. Then $P_0 = P$ is the amount of the original loan, $P_1 = MP_0 - Y$ is the amount of the loan after one month, $P_2 = MP_1 - Y$ is the amount of the loan after two months, and so on. Now we are ready to state and prove a theorem by induction on $t$ that gives a formula for the value of $P_t$.

**THEOREM 0.25**

For each $t \geq 0$,

$$P_t = PM^t - Y\left(\frac{M^t - 1}{M - 1}\right).$$

**PROOF**

***Basis:*** Prove that the formula is true for $t = 0$. If $t = 0$, then the formula states that

$$P_0 = PM^0 - Y\left(\frac{M^0 - 1}{M - 1}\right).$$

We can simplify the right-hand side by observing that $M^0 = 1$. Thus we get

$$P_0 = P,$$

which holds because we have defined $P_0$ to be $P$. Therefore, we have proved that the basis of the induction is true.

***Induction step:*** For each $k \geq 0$, assume that the formula is true for $t = k$ and show that it is true for $t = k + 1$. The induction hypothesis states that

$$P_k = PM^k - Y\left(\frac{M^k - 1}{M - 1}\right).$$

Our objective is to prove that

$$P_{k+1} = PM^{k+1} - Y\left(\frac{M^{k+1} - 1}{M - 1}\right).$$

We do so with the following steps. First, from the definition of $P_{k+1}$ from $P_k$, we know that

$$P_{k+1} = P_k M - Y.$$

Therefore, using the induction hypothesis to calculate $P_k$,

$$P_{k+1} = \left[ PM^k - Y\left(\frac{M^k - 1}{M - 1}\right)\right] M - Y.$$

Multiplying through by $M$ and rewriting $Y$ yields

$$\begin{aligned} P_{k+1} &= PM^{k+1} - Y\left(\frac{M^{k+1} - M}{M - 1}\right) - Y\left(\frac{M - 1}{M - 1}\right) \\ &= PM^{k+1} - Y\left(\frac{M^{k+1} - 1}{M - 1}\right). \end{aligned}$$

Thus the formula is correct for $t = k + 1$, which proves the theorem.

Problem 0.15 asks you to use the preceding formula to calculate actual mortgage payments.

## EXERCISES

**0.1** Examine the following formal descriptions of sets so that you understand which members they contain. Write a short informal English description of each set.

- **a.** $\{1, 3, 5, 7, \dots\}$
- **b.** $\{\dots, -4, -2, 0, 2, 4, \dots\}$
- **c.** $\{n \mid n = 2m \text{ for some } m \text{ in } \mathcal{N}\}$
- **d.** $\{n \mid n = 2m \text{ for some } m \text{ in } \mathcal{N}, \text{ and } n = 3k \text{ for some } k \text{ in } \mathcal{N}\}$
- **e.** $\{w \mid w$ is a string of `0`s and `1`s and $w$ equals the reverse of $w\}$
- **f.** $\{n \mid n \text{ is an integer and } n = n + 1\}$

**0.2** Write formal descriptions of the following sets.

- **a.** The set containing the numbers 1, 10, and 100
- **b.** The set containing all integers that are greater than 5
- **c.** The set containing all natural numbers that are less than 5
- **d.** The set containing the string `aba`
- **e.** The set containing the empty string
- **f.** The set containing nothing at all