The opinions presented by Shafarevich and Hadamard represent two extreme positions on the role of proof and rigor within mathematics and indeed on the nature of mathematics itself. Both Hadamard (1865–1963) and Shafarevich (1923–) have made many significant contributions to mathematics; thus we are compelled to look carefully at the comments of each of them. To gain a better understanding of the place that proof occupies within mathematics, we explore the positions of Hadamard and Shafarevich in greater detail.

According to Shafarevich, the existence of proofs of mathematical statements distinguishes mathematics among all intellectual endeavors. In other scientific fields, investigators can at best propose conjectures about the essence of things and attempt to confirm these conjectures with experimental data or observation of natural phenomena. In fact, most scientific theories "explain" the events of nature in terms of other scientific or mathematical theories. For example, geologists account for earthquakes via the theory of plate tectonics, and physicists describe the motion of planets in our solar system in terms of a system of differential equations. However, because of the complex and haphazard way of the world, the fallibility of human observational methods, or many other factors, the possibility always exists that a scientific theory will have to be abandoned or modified because of empirical evidence.

In mathematics the situation is different. Mathematicians working in a particular field

1. agree on certain fundamental rules, i.e., the axioms or postulates,
2. introduce some auxiliary concepts, called definitions, and
3. deduce statements, called (depending on their importance) theorems, propositions, lemmas, or corollaries relating the items that are presented in the axioms or definitions.

A particular statement becomes a theorem (proposition, lemma) when it is justified or proved. The proof of a statement consists of a sequence of statements, beginning with an axiom or previously established statement, and proceeding through a sequence of statements where each is deducible by means of rules of logic from axioms, previous theorems, or previous statements in the sequence. Without the concept of proof, mathematics would be another empirical science. But, with this notion, mathematics becomes *the* deductive science; hence its uniqueness and its justification.

Excerpts from Galovich, S. (1989). *Introduction to Mathematical Structures*. San Diego, CA. Harcourt Brace Jovanovich.

Hadamard, on the other hand, believes that the essence of mathematics lies in its discovery of interesting and striking relationships among the objects of the mathematician's fancy—numbers, functions, curves, surfaces, groups, Boolean algebras, etc. Once the theorems are articulated, proofs must be given, but only to legalize the theorems. Their truth is visible to the experienced mathematician before the proofs are given. Some philosophers of mathematics extend this position to entire mathematical theories: They argue that in practice the axioms of a particular mathematical discipline are actually created last, as a postscript to the discovery of the theorems of the subject, even though in any formal exposition of the discipline (in a textbook or research paper) the axioms head the parade, and the theorems and their attendant proofs march faithfully behind. From this viewpoint, mathematics is closely akin to the sciences. Results are discovered, and then justified and organized into a comprehensible framework.

The debates ranging from the nature of mathematics to the role of proof within mathematics rage to this day. Of course, issues of this sort may never be resolved to the satisfaction of all parties. However, discussions such as the one outlined in the previous paragraph help us understand the purpose, practice, and essence of mathematics. From these discussions we obtain a more detailed portrait of mathematics and a clearer fix on its position relative to the other intellectual activities of humans.

On the basis of the preceding discussion, what can we conclude about the role of proof in mathematics?

On the one hand, no one familiar with mathematics will deny the importance of rigor and proof. Experience has convinced every mathematician that any assertion must be supported by a rigorous argument. Countless novice, apprentice, and master mathematicians have attempted to prove an intuitively obvious "theorem" only to watch it disintegrate into a false statement. Thus every mathematician must become proficient with proofs. He or she must learn to read mathematical proofs critically as they are presented in texts or research papers and must develop the ability to write valid proofs. Proofs are indeed one of the focal points of mathematical activity; hence they need to be mastered by any student of formal mathematics.

On the other hand, activities such as experimentation, discovery, and reasoning by analogy are important aspects of a mathematician's experience. Mathematicians investigate abstract phenomena in search of order and pattern. Employing a combination of informal reasoning and experimentation, they conjure up conjectures that describe the patterns they observe. At this point they either prove their conjectures formally, or disprove them by constructing counterexamples, in which case the process of investigation and conjecture repeats itself. From this point of view, mathematics encompasses a broad range of activities, requiring mathematicians to guess and to prove, to hypothesize and to criticize.

51

Direct Proof

A direct proof proceeds from the hypothesis P and deduces that Q must hold. In concocting a direct proof, we are free to use all the hypotheses that are given and any statement that has been previously established. Here is an elementary example.

Example 1.3.1 Prove: The product of two odd integers is an odd integer.

First, let us translate this statement into an implication. Our initial attempts will not contain any symbols.

(i) If the product of two odd integers is taken, then that product is an odd integer.
(ii) If two odd integers are given, then their product is an odd integer.

Now let us state a version using some variables:

(iii) If a and b are odd integers, then $a \cdot b$ is an odd integer.

To make the quantification on a and b explicit, we have the following version:

(iv) For all integers a and b, if a and b are odd, then $a \cdot b$ is an odd integer.

All these statements describe a property of the set of integers; hence none is any more "mathematical" than any of the others. Although the third and fourth sentences might appear to be the most mathematical of the four, they differ from the others mainly in their conciseness and sophistication. For example, the use of "$a \cdot b$" in the conclusion must be interpreted by the reader to mean "the product of a and b." Now to the proof. We take as our definition of an odd integer the following: An integer a is odd if there exists an integer m such that $a = 2 \cdot m + 1$.

Proof By definition, since a and b are odd, there exist integers m and n such that $a = 2 \cdot m + 1$ and $b = 2 \cdot n + 1$. We must show that there exists an integer k such that $a \cdot b = 2 \cdot k + 1$.

By the properties of addition and multiplication of real numbers described in Section 1.2,

$$\begin{aligned} a \cdot b &= (2m + 1)(2n + 1) \\ &= (2m + 1) \cdot 2n + (2m + 1) \cdot 1 \\ &= 2m \cdot 2n + 2n + 2m + 1 \\ &= 4mn + 2m + 2n + 1 \\ &= 2(2mn + m + n) + 1. \end{aligned}$$

Thus $a \cdot b = 2k + 1$ where k is the integer $2mn + m + n$. This proves that $a \cdot b$ is odd if a and b are odd. ■

52

Next we give a direct proof of an important property of the real number system.

Theorem 1.3.1 Cancellation Law for Multiplication. *If a, b, and c are real numbers such that $a \neq 0$ and $ab = ac$, then $b = c$.*

Proof Suppose a, b, and c are arbitrary real numbers such that $a \neq 0$ and $ab = ac$. Since $a \neq 0$, the multiplicative inverse of a, a^{-1}, exists. Thus

$$a^{-1} \cdot (a \cdot b) = a^{-1} \cdot (a \cdot c).$$

Hence, by the associative law for multiplication,

$$(a^{-1} \cdot a) \cdot b = (a^{-1} \cdot a) \cdot c.$$

Thus

$$1 \cdot b = 1 \cdot c$$

or

$$b = c. \qquad ■$$

The following result can be either derived from Theorem 1.3.1 or proved via a similar argument. We leave the proof as an exercise. (See Exercise 1.3.2.)

Corollary 1.3.2 *If a and b are real numbers such that $ab = 0$, then either $a = 0$ or $b = 0$.*

Excerpts from Galovich, S. (1989). *Introduction to Mathematical Structures*. San Diego, CA. Harcourt Brace Jovanovich.