The Axiom of Choice allows you to select one element from each set in a collection and have it executed as an example to the others.

My math teacher was a big believer in proof by intimidation.
Last class: Inference Rules for Quantifiers

\[ P(c) \text{ for some } c \]
\[ \therefore \exists x \ P(x) \]

\[ \forall x \ P(x) \]
\[ \therefore P(a) \text{ for any } a \]

“Let } a \text{ be arbitrary}*”...P(a)
\[ \therefore \forall x \ P(x) \]

\[ \exists x \ P(x) \]
\[ \therefore P(c) \text{ for some } \text{special}** \ c \]

* in the domain of P.

** c is a NEW name.
These rules need some caveats...

There are extra conditions on using these rules:

1. **Intro** $\forall$ “Let $a$ be arbitrary***”... $P(a)$
   $\therefore \forall x \ P(x)$

2. **Elim** $\exists$ $\exists x \ P(x)$
   $\therefore P(c)$ for some special*** $c$

   * in the domain of $P$

   ** $c$ has to be a NEW name.

Over integer domain: $\forall x \ \exists y \ (y \geq x)$ is True but $\exists y \forall x \ (y \geq x)$ is False

**BAD “PROOF”**

1. $\forall x \ \exists y \ (y \geq x)$ Given
2. Let $a$ be an arbitrary integer
3. $\exists y \ (y \geq a)$ Elim $\forall$: 1
4. $b \geq a$ Elim $\exists$: 3 ($b$)
5. $\forall x \ (b \geq x)$ Intro $\forall$: 2, 4
6. $\exists y \forall x \ (y \geq x)$ Intro $\exists$: 5
These rules need some caveats...

There are extra conditions on using these rules:

\[
\begin{array}{ll}
\text{Intro } \forall & \text{“Let } a \text{ be arbitrary*”} \ldots P(a) \\
\therefore & \forall x \ P(x) \\
\end{array}
\]

\[
\begin{array}{ll}
\text{Elim } \exists & \exists x \ P(x) \\
\therefore & P(c) \text{ for some special** } c \\
\end{array}
\]

* in the domain of \( P \)

** \( c \) has to be a NEW name.

Over integer domain: \( \forall x \ \exists y \ (y \geq x) \) is True but \( \exists y \forall x \ (y \geq x) \) is False

BAD “PROOF”

1. \( \forall x \ \exists y \ (y \geq x) \)  Given
2. Let \( a \) be an arbitrary integer
3. \( \exists y \ (y \geq a) \)  Elim \( \forall \): 1
4. \( b \geq a \)  Elim \( \exists \): 3 \((b)\)
5. \( \forall x \ (b \geq x) \)  Intro \( \forall \): 2, 4
6. \( \exists y \forall x \ (y \geq x) \)  Intro \( \exists \): 5

Can’t get rid of \( a \) since another name in the same line, \( b \), depends on it!
These rules need some caveats...

There are extra conditions on using these rules:

1. “Let a be arbitrary*”...\( P(a) \)
   \[ \therefore \forall x \ P(x) \]
   * in the domain of \( P \). No other name in \( P \) depends on \( a \)

2. \( \exists x \ P(x) \)
   \[ \therefore P(c) \text{ for some special** } c \]
   ** \( c \) is a NEW name. List all dependencies for \( c \).

Over integer domain: \( \forall x \ \exists y \ (y \geq x) \) is True but \( \exists y \forall x \ (y \geq x) \) is False

BAD “PROOF”

1. \( \forall x \ \exists y \ (y \geq x) \) Given
2. Let \( a \) be an arbitrary integer
3. \( \exists y \ (y \geq a) \) Elim \( \forall \): 1
4. \( b \geq a \) Elim \( \exists \): 3 (\( b \))
5. \( \forall x \ (b \geq x) \) Intro \( \forall \): 2, 4
6. \( \exists y \forall x \ (y \geq x) \) Intro \( \exists \): 5

Can’t get rid of \( a \) since another name in the same line, \( b \), depends on it!
Over integer domain: $\forall x \exists y (y \geq x)$ is True but $\exists y \forall x (y \geq x)$ is False

b depends on a since it appears inside the expression “$\exists y (y \geq a)$”

BAD “PROOF”
1. $\forall x \exists y (y \geq x)$ Given
2. Let a be an arbitrary integer
3. $\exists y (y \geq a)$ Elim $\forall$: 1
4. $b \geq a$ Elim $\exists$: 3 (b depends on a)
5. $\forall x (b \geq x)$ Intro $\forall$: 2,4
6. $\exists y \forall x (y \geq x)$ Intro $\exists$: 5

Can’t Intro $\forall$ with “Let a be an arbitrary ... P(a)” because $P(a) = “b \geq a”$ uses object b, which depends on a!
Over integer domain: $\forall x \exists y (y \geq x)$ is True but $\exists y \forall x (y \geq x)$ is False

b depends on a since it appears inside the expression “$\exists y (y \geq a)$”

BAD “PROOF”
1. $\forall x \exists y (y \geq x)$ Given
2. Let $a$ be an arbitrary integer
3. $\exists y (y \geq a)$ Elim $\forall$: 1
4. $b \geq a$ Elim $\exists$: 3 ($b$ depends on $a$)
5. $\forall x (b \geq x)$ Intro $\forall$: 2,4
6. $\exists y \forall x (y \geq x)$ Intro $\exists$: 5

Have instead shown $\forall x (b(x) \geq x)$
where $b(x)$ is a number that is possibly different for each $x$
Formal Proofs

• In principle, formal proofs are the standard for what it means to be “proven” in mathematics
  – almost all math (and theory CS) done in Predicate Logic

• But they are tedious and impractical
  – e.g., applications of commutativity and associativity
  – Russell & Whitehead’s formal proof that $1+1 = 2$ is several hundred pages long
    we allowed ourselves to cite “Arithmetic”, “Algebra”, etc.

• Similar situation exists in programming...
Programming

a := ADD(i, 1)
b := MOD(a, n)
c := ADD(arr, b)
d := LOAD(c)
e := ADD(arr, i)
STORE(e, d)

arr[i] = arr[(i+1) % n];
Programming vs Proofs

Given

Elim \land: 1
Elim \lor: 3, 5
Modus Ponens: 2, 6

Assembly Language for Programs
Assembly Language for Proofs

\[ a := \text{ADD}(i, 1) \]
\[ b := \text{MOD}(a, n) \]
\[ c := \text{ADD}(\text{arr}, b) \]
\[ d := \text{LOAD}(c) \]
\[ e := \text{ADD}(\text{arr}, i) \]
\[ \text{STORE}(e, d) \]
Proofs

<table>
<thead>
<tr>
<th>Given</th>
<th>what is the “Java” for proofs?</th>
</tr>
</thead>
<tbody>
<tr>
<td>$\land$ Elim: 1</td>
<td></td>
</tr>
<tr>
<td>Double Negation: 4</td>
<td></td>
</tr>
<tr>
<td>$\lor$ Elim: 3, 5</td>
<td></td>
</tr>
<tr>
<td>MP: 2, 6</td>
<td></td>
</tr>
</tbody>
</table>

- **Assembly Language for Proofs**
- **High-level Language for Proofs**
Proofs

Given
Given
\( \land \) Elim: 1
Double Negation: 4
\( \lor \) Elim: 3, 5
MP: 2, 6

Assembly Language for Proofs

High-level Language for Proofs

English?
Proofs

Given
Given
\( \land \) Elim: 1
Double Negation: 4
\( \lor \) Elim: 3, 5
MP: 2, 6

Assembly Language for Proofs
High-level Language for Proofs
Proofs

• Formal proofs follow simple well-defined rules and should be easy for a machine to check
  – as assembly language is easy for a machine to execute

• English proofs correspond to those rules but are designed to be easier for humans to read
  – also easy to check with practice
    (almost all actual math and theory CS is done this way)
  – English proof is correct if the reader believes they could translate it into a formal proof
    (the reader is the “compiler” for English proofs)
Last class: Even and Odd

Prove: “The square of every even number is even.”

Formal proof of: \( \forall x \ (\text{Even}(x) \rightarrow \text{Even}(x^2)) \)

1. Let \( a \) be an arbitrary integer
   
   2.1 \( \text{Even}(a) \) Assumption
   
   2.2 \( \exists y \ (a = 2y) \) Definition of Even
   
   2.3 \( a = 2b \) Elim \( \exists \): \( b \) special depends on \( a \)
   
   2.4 \( a^2 = 4b^2 = 2(2b^2) \) Algebra
   
   2.5 \( \exists y \ (a^2 = 2y) \) Intro \( \exists \) rule
   
   2.6 \( \text{Even}(a^2) \) Definition of Even

2. \( \text{Even}(a) \rightarrow \text{Even}(a^2) \) Direct Proof

3. \( \forall x \ (\text{Even}(x) \rightarrow \text{Even}(x^2)) \) Intro \( \forall \): 1,2

Even(x) \( \equiv \exists y \ (x = 2y) \)
Odd(x) \( \equiv \exists y \ (x = 2y + 1) \)
Domain: Integers
Prove “The square of every even integer is even.”

Let \( a \) be an arbitrary integer.

1. Let \( a \) be an arbitrary integer.

Suppose \( a \) is even.

\[ 2.1 \quad \text{Even}(a) \quad \text{Assumption} \]

Then, by definition, \( a = 2b \) for some integer \( b \) (dep on \( a \)).

\[ 2.2 \quad \exists y \ (a = 2y) \quad \text{Definition} \]
\[ 2.3 \quad a = 2b \quad \text{b special depends on } a \]

2.4 Squaring both sides, we get
\[ a^2 = 4b^2 = 2(2b^2) \quad \text{Algebra} \]

So \( a^2 \) is, by definition, even.

\[ 2.5 \quad \exists y \ (a^2 = 2y) \quad \text{Definition} \]
\[ 2.6 \quad \text{Even}(a^2) \quad \text{Definition} \]

Since \( a \) was arbitrary, we have shown that the square of every even number is even.

\[ 2. \quad \text{Even}(a) \rightarrow \text{Even}(a^2) \]
\[ 3. \quad \forall x \ (\text{Even}(x) \rightarrow \text{Even}(x^2)) \]
English Proof: Even and Odd

Prove “The square of every even integer is even.”

**Proof:** Let \( a \) be an arbitrary integer.

Suppose \( a \) is even. Then, by definition, \( a = 2b \) for some integer \( b \) (depending on \( a \)). Squaring both sides, we get \( a^2 = 4b^2 = 2(2b^2) \). So \( a^2 \) is, by definition, is even.

Since \( a \) was arbitrary, we have shown that the square of every even number is even. ■
Prove “The square of every even integer is even.”

**Proof:** Let \( a \) be an arbitrary even integer.

Then, by definition, \( a = 2b \) for some integer \( b \) (dep on \( a \)). Squaring both sides, we get \( a^2 = 4b^2 = 2(2b^2) \). So \( a^2 \) is, by definition, is even.

Since \( a \) was arbitrary, we have shown that the square of every even number is even. ■

\[ \forall x \ (\text{Even}(x) \rightarrow \text{Even}(x^2)) \]
Prove “The sum of two odd numbers is even.”

Formally, prove  \( \forall x \forall y ((\text{Odd}(x) \land \text{Odd}(y)) \rightarrow \text{Even}(x+y)) \)
**Predicate Definitions**

<table>
<thead>
<tr>
<th>Even(x)</th>
<th>Odd(x)</th>
</tr>
</thead>
<tbody>
<tr>
<td>$\exists y \ (x = 2y)$</td>
<td>$\exists y \ (x = 2y + 1)$</td>
</tr>
</tbody>
</table>

**Domain of Discourse**

Integers

---

Prove “The sum of two odd numbers is even.”

Formally, prove $\forall x \forall y \ ((\text{Odd}(x) \land \text{Odd}(y)) \rightarrow \text{Even}(x+y))$

Let $x$ and $y$ be arbitrary integers.

1. Let $x$ be an arbitrary integer
2. Let $y$ be an arbitrary integer

Since $x$ and $y$ were arbitrary, the sum of any odd integers is even.

3. $(\text{Odd}(x) \land \text{Odd}(y)) \rightarrow \text{Even}(x+y)$
4. $\forall x \forall y \ ((\text{Odd}(x) \land \text{Odd}(y)) \rightarrow \text{Even}(x+y))$ Intro $\forall$
Prove “The sum of two odd numbers is even.”

Formally, prove \( \forall x \forall y ((\text{Odd}(x) \land \text{Odd}(y)) \rightarrow \text{Even}(x+y)) \)

Let \( x \) and \( y \) be arbitrary integers.

Suppose that both are odd.

so \( x+y \) is even.

Since \( x \) and \( y \) were arbitrary, the sum of any odd integers is even.
Prove “The sum of two odd numbers is even.”

Formally, prove \( \forall x \forall y ((\text{Odd}(x) \land \text{Odd}(y)) \rightarrow \text{Even}(x+y)) \)

Let \( x \) and \( y \) be arbitrary integers.

Suppose that both are odd.

so \( x+y \) is even.

Since \( x \) and \( y \) were arbitrary, the sum of any odd integers is even.

1. Let \( x \) be an arbitrary integer
2. Let \( y \) be an arbitrary integer
3.1 Odd(\( x \)) \land Odd(\( y \)) Assumption
3.2 Odd(\( x \)) Elim \( \land \): 2.1
3.3 Odd(\( y \)) Elim \( \land \): 2.1
3.9 Even(\( x+y \))
3. (Odd(\( x \)) \land Odd(\( y \))) \rightarrow Even(\( x+y \)) DPR
4. \( \forall x \forall y ((\text{Odd}(x) \land \text{Odd}(y)) \rightarrow \text{Even}(x+y)) \) Intro \( \forall \)
English Proof: Even and Odd

Prove “The sum of two odd numbers is even.”

Let x and y be arbitrary integers.  
1. Let x be an arbitrary integer
2. Let y be an arbitrary integer

Suppose that both are odd.
3.1 Odd(x) ∧ Odd(y)  Assumption
3.2 Odd(x)  Elim ∧: 2.1
3.3 Odd(y)  Elim ∧: 2.1

Then, x = 2a+1 for some integer a (depending on x) and y = 2b+1 for some integer b (depending on y).
3.4 ∃z (x = 2z+1)  Def of Odd: 2.2
3.5 x = 2a+1  Elim ∃: 2.4 (a dep x)
3.6 ∃z (y = 2z+1)  Def of Odd: 2.3
3.7 y = 2b+1  Elim ∃: 2.5 (b dep y)

so x+y is, by definition, even.
3.9 ∃z (x+y = 2z)  Intro ∃: 2.4
3.10 Even(x+y)  Def of Even

Since x and y were arbitrary, the sum of any odd integers is even.
3.  (Odd(x) ∧ Odd(y)) → Even(x+y)  DPR
4.  ∀x ∀y ((Odd(x) ∧ Odd(y)) → Even(x+y))  Intro ∀
Prove “The sum of two odd numbers is even.”

Let \( x \) and \( y \) be arbitrary integers.

1. Let \( x \) be an arbitrary integer
2. Let \( y \) be an arbitrary integer

Suppose that both are odd.

Then, \( x = 2a+1 \) for some integer \( a \) (depending on \( x \)) and \( y = 2b+1 \) for some integer \( b \) (depending on \( y \)).

Their sum is \( x+y = \ldots = 2(a+b+1) \) so \( x+y \) is, by definition, even.

Since \( x \) and \( y \) were arbitrary, the sum of any odd integers is even.
Prove “The sum of two odd numbers is even.”

Proof: Let x and y be arbitrary integers. Suppose that both are odd. Then, \( x = 2a+1 \) for some integer a (depending on x) and \( y = 2b+1 \) for some integer b (depending on x). Their sum is \( x+y = (2a+1) + (2b+1) = 2a+2b+2 = 2(a+b+1) \), so \( x+y \) is, by definition, even. Since x and y were arbitrary, the sum of any two odd integers is even. ■
Prove “The sum of two odd numbers is even.”

Proof: Let \( x \) and \( y \) be arbitrary odd integers. Then, \( x = 2a+1 \) for some integer \( a \) (depending on \( x \)) and \( y = 2b+1 \) for some integer \( b \) (depending on \( x \)). Their sum is \( x+y = (2a+1) + (2b+1) = 2a+2b+2 = 2(a+b+1) \), so \( x+y \) is, by definition, even.

Since \( x \) and \( y \) were arbitrary, the sum of any two odd integers is even. \( \blacksquare \)

\[ \forall x \, \forall y \, ((\text{Odd}(x) \land \text{Odd}(y)) \to \text{Even}(x+y)) \]
Rational Numbers

- A real number $x$ is *rational* iff there exist integers $a$ and $b$ with $b \neq 0$ such that $x = a/b$.

$\text{Rational}(x) := \exists a \, \exists b \, (((\text{Integer}(a) \land \text{Integer}(b)) \land (x = a/b)) \land b \neq 0)$
Rationality

Predicate Definitions

\[
\text{Rational}(x) := \exists a \ \exists b \ (\text{Integer}(a) \land \text{Integer}(b) \land (x = a/b) \land (b \neq 0))
\]

Prove: “The product of two rationals is rational.”
Formally, prove \( \forall x \ \forall y ((\text{Rational}(x) \land \text{Rational}(y)) \rightarrow \text{Rational}(xy)) \)
Rationality

Proof:

Let x and y be arbitrary rationals.

Since x and y were arbitrary, we have shown that the product of any two rationals is rational. ■
Rationality

Prove: “The product of two rationals is rational.”

Proof: Let \( x \) and \( y \) be arbitrary rationals. Then, \( x = a/b \) for some integers \( a, b \), where \( b \neq 0 \), and \( y = c/d \) for some integers \( c, d \), where \( d \neq 0 \).

Since \( x \) and \( y \) were arbitrary, we have shown that the product of any two rationals is rational. \( \blacksquare \)
Prove: “The product of two rationals is rational.”

Proof: Let $x$ and $y$ be arbitrary rationals. Then, $x = a/b$ for some integers $a$, $b$, where $b \neq 0$, and $y = c/d$ for some integers $c,d$, where $d \neq 0$. Multiplying, we get that $xy = (a/b)(c/d) = (ac)/(bd)$. Since $b$ and $d$ are both non-zero, so is $bd$. Furthermore, $ac$ and $bd$ are integers. By definition, then, $xy$ is rational. Since $x$ and $y$ were arbitrary, we have shown that the product of any two rationals is rational. ■
Rationality

Prove: “The product of two rationals is rational.”
OR “If x and y are rational, then xy is rational.”

Recall that unquantified variables (not constants) are implicitly for-all quantified.

∀x ∀y ((Rational(x) ∧ Rational(y)) → Rational(xy))
Prove: “If \( x \) and \( y \) are rational, then \( xy \) is rational.”

Proof: Let \( x \) and \( y \) be arbitrary rationals.

Suppose \( x \) and \( y \) are rational.

Then, \( x = a/b \) for some integers \( a, b \), where \( b \neq 0 \), and \( y = c/d \) for some integers \( c, d \), where \( d \neq 0 \).

Multiplying, we get that \( xy = (a/b)(c/d) = (ac)/(bd) \).

Since \( b \) and \( d \) are both non-zero, so is \( bd \). Furthermore, \( ac \) and \( bd \) are integers. By definition, then, \( xy \) is rational.

Since \( x \) and \( y \) were arbitrary, we have shown that the product of any two rationals is rational. ■

Predicate Definitions

\[
\text{Rational}(x) := \exists a \ \exists b \ (\text{Integer}(a) \land \text{Integer}(b) \land (x = a/b) \land (b \neq 0))
\]
Rationality

Prove: “If x and y are rational, then xy is rational.”

Suppose x and y are rational.

Then, x = a/b for some integers a, b, where b ≠ 0 and y = c/d for some integers c, d, where d ≠ 0.

Rational(x) := ∃a ∃b (Integer(a) ∧ Integer(b) ∧ (x = a/b) ∧ (b ≠ 0))

Predicate Definitions

1.1 Rational(x) ∧ Rational(y) Assumption

1.4 ∃p ∃q ((x = p/q) ∧ Integer(p) ∧ Integer(q) ∧ (q ≠ 0)) Def Rational: 1.2

1.5 (x = a/b) ∧ Integer(a) ∧ Integer(b) ∧ (b ≠ 0) Elim ∃: 1.4

1.6 ∃p ∃q ((x = p/q) ∧ Integer(p) ∧ Integer(q) ∧ (q ≠ 0)) Def Rational: 1.3

1.7 (y = c/d) ∧ Integer(c) ∧ Integer(d) ∧ (d ≠ 0) Elim ∃: 1.4
Rationality

Suppose $x$ and $y$ are rational.

Then, $x = \frac{a}{b}$ for some integers $a, b$, where $b \neq 0$ and $y = \frac{c}{d}$ for some integers $c, d$, where $d \neq 0$.

Rationality

Domain of Discourse

Real Numbers

 Predicate Definitions

| Rational(x) := $\exists a \exists b \ (\text{Integer}(a) \land \text{Integer}(b) \land (x = \frac{a}{b}) \land (b \neq 0))$ |

Prove: “If $x$ and $y$ are rational, then $xy$ is rational.”

1.1 $\text{Rational}(x) \land \text{Rational}(y)$ Assumption

??

1.4 $\exists p \exists q ((x = \frac{p}{q}) \land \text{Integer}(p) \land \text{Integer}(q) \land (q \neq 0))$ Def Rational: 1.2

1.5 $(x = \frac{a}{b}) \land \text{Integer}(a) \land \text{Integer}(b) \land (b \neq 0)$ Elim $\exists$: 1.4

1.6 $\exists p \exists q ((x = \frac{p}{q}) \land \text{Integer}(p) \land \text{Integer}(q) \land (q \neq 0))$ Def Rational: 1.3

1.7 $(y = \frac{c}{d}) \land \text{Integer}(c) \land \text{Integer}(d) \land (d \neq 0)$ Elim $\exists$: 1.4
### Rationality

**Predicate Definitions**

\[
\text{Rational}(x) := \exists a \exists b \left( \text{Integer}(a) \land \text{Integer}(b) \land \left( x = \frac{a}{b} \right) \land \left( b \neq 0 \right) \right)
\]

Prove: “If \( x \) and \( y \) are rational, then \( xy \) is rational.”

Suppose \( x \) and \( y \) are rational.

Then, \( x = a/b \) for some integers \( a, b \), where \( b \neq 0 \) and \( y = c/d \) for some integers \( c, d \), where \( d \neq 0 \).

<table>
<thead>
<tr>
<th>1.1</th>
<th>( \text{Rational}(x) \land \text{Rational}(y) )</th>
<th>Assumption</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.2</td>
<td>( \text{Rational}(x) )</td>
<td>Elim ( \land ): 1.1</td>
</tr>
<tr>
<td>1.3</td>
<td>( \text{Rational}(y) )</td>
<td>Elim ( \land ): 1.1</td>
</tr>
<tr>
<td>1.4</td>
<td>( \exists p \exists q \left( (x = p/q) \land \text{Integer}(p) \land \text{Integer}(q) \land (q \neq 0) \right) )</td>
<td>Def Rational: 1.2</td>
</tr>
<tr>
<td>1.5</td>
<td>( (x = a/b) \land \text{Integer}(a) \land \text{Integer}(b) \land (b \neq 0) )</td>
<td>Elim ( \exists ): 1.4</td>
</tr>
<tr>
<td>1.6</td>
<td>( \exists p \exists q \left( (x = p/q) \land \text{Integer}(p) \land \text{Integer}(q) \land (q \neq 0) \right) )</td>
<td>Def Rational: 1.3</td>
</tr>
<tr>
<td>1.7</td>
<td>( (y = c/d) \land \text{Integer}(c) \land \text{Integer}(d) \land (d \neq 0) )</td>
<td>Elim ( \exists ): 1.4</td>
</tr>
</tbody>
</table>
Rationality

<table>
<thead>
<tr>
<th>Predicate Definitions</th>
</tr>
</thead>
<tbody>
<tr>
<td>Rational(x) := ∃a ∃b (Integer(a) ∧ Integer(b) ∧ (x = a/b) ∧ (b ≠ 0))</td>
</tr>
</tbody>
</table>

Prove: “If x and y are rational, then xy is rational.”

\[ xy = \frac{ac}{bd} \]

1.5 \( (x = a/b) \land \text{Integer}(a) \land \text{Integer}(b) \land (b \neq 0) \)

1.7 \( (y = c/d) \land \text{Integer}(c) \land \text{Integer}(d) \land (d \neq 0) \)

Multiplying, we get \( xy = \frac{ac}{bd} \).
Rationality

Prove: “If x and y are rational, then xy is rational.”

```
| 1.5 | (x = a/b) ∧ Integer(a) ∧ Integer(b) ∧ (b ≠ 0) |
| 1.7 | (y = c/d) ∧ Integer(c) ∧ Integer(d) ∧ (d ≠ 0) |
```

Multiplying, we get $xy = \frac{ac}{bd}$.

```
| 1.10 | $xy = \frac{a/b}{c/d} = \frac{ac}{bd} = \frac{ac}{bd}$ |
```

Algebra
Rationality

Predicate Definitions

Rational(x) := \exists a \exists b (\text{Integer}(a) \land \text{Integer}(b) \land (x = a/b) \land (b \neq 0))

Prove: “If x and y are rational, then xy is rational.”

Multiplying, we get xy = (ac)/(bd).

\begin{align*}
1.5 & \quad (x = a/b) \land \text{Integer}(a) \land \text{Integer}(b) \land (b \neq 0) \\
1.7 & \quad (y = c/d) \land \text{Integer}(c) \land \text{Integer}(d) \land (d \neq 0) \\
1.8 & \quad x = a/b \quad \text{Elim } \wedge: 1.5 \\
1.9 & \quad y = c/d \quad \text{Elim } \wedge: 1.7 \\
1.10 & \quad xy = (a/b)(c/d) = (ac/bd) = (ac)/(bd) \quad \text{Algebra}
\end{align*}
Rationality

Prove: “If x and y are rational, then xy is rational.”

\[
\begin{align*}
\text{Rational}(x) &:= \exists a \exists b (\text{Integer}(a) \land \text{Integer}(b) \land (x = a/b) \land (b \neq 0)) \\
\hline
\end{align*}
\]

\[
\begin{align*}
1.5 & \quad (x = a/b) \land \text{Integer}(a) \land \text{Integer}(b) \land (b \neq 0) \\
1.7 & \quad (y = c/d) \land \text{Integer}(c) \land \text{Integer}(d) \land (d \neq 0) \\
1.11 & \quad b \neq 0 \quad \text{Elim } \land: 1.5^* \\
1.12 & \quad d \neq 0 \quad \text{Elim } \land: 1.7 \\
1.13 & \quad bd \neq 0 \quad \text{Prop of Integer Mult} \\
\end{align*}
\]

Since b and d are non-zero, so is bd.

* Oops, I skipped steps here...
Prove: “If x and y are rational, then xy is rational.”

\[ x = a/b \land (\text{Integer}(a) \land \text{Integer}(b) \land (b \neq 0)) \]

\[ y = c/d \land (\text{Integer}(c) \land \text{Integer}(d) \land (d \neq 0)) \]

\[ \text{Integer}(a) \land (\text{Integer}(b) \land (b \neq 0)) \]  

Elim \land: 1.5

\[ \text{Integer}(b) \land (b \neq 0) \]  

Elim \land: 1.11

\[ b \neq 0 \]  

Elim \land: 1.12

We left out the parentheses...
Rationality

Prove: “If x and y are rational, then xy is rational.”

\[ \text{Rational}(x) := \exists a \exists b \ (\text{Integer}(a) \land \text{Integer}(b) \land (x = a/b) \land (b \neq 0)) \]

Since b and d are non-zero, so is bd.

\[
\begin{align*}
1.5 & \quad (x = a/b) \land \text{Integer}(a) \land \text{Integer}(b) \land (b \neq 0) \\
1.7 & \quad (y = c/d) \land \text{Integer}(c) \land \text{Integer}(d) \land (d \neq 0) \\
1.13 & \quad b \neq 0 \quad \text{Elim } \land: 1.5 \\
1.16 & \quad d \neq 0 \quad \text{Elim } \land: 1.7 \\
1.17 & \quad bd \neq 0 \quad \text{Prop of Integer Mult}
\end{align*}
\]
Prove: “If x and y are rational, then xy is rational.”

Furthermore, ac and bd are integers.

1.5 \((x = a/b) \land \text{Integer}(a) \land \text{Integer}(b) \land (b \neq 0)\)

1.7 \((y = c/d) \land \text{Integer}(c) \land \text{Integer}(d) \land (d \neq 0)\)

1.19 \text{Integer}(a) \quad \text{Elim} \land: 1.5^*

1.22 \text{Integer}(b) \quad \text{Elim} \land: 1.5^*

1.24 \text{Integer}(c) \quad \text{Elim} \land: 1.7^*

1.27 \text{Integer}(d) \quad \text{Elim} \land: 1.7^*

1.28 \text{Integer}(ac) \quad \text{Prop of Integer Mult}

1.29 \text{Integer}(bd) \quad \text{Prop of Integer Mult}
Prove: “If x and y are rational, then xy is rational.”

\[ xy = \frac{a}{b} \frac{c}{d} = \frac{ac}{bd} = \frac{ac}{bd} \]

\[ 1.10 \]

\[ 1.17 \quad bd \neq 0 \quad \text{Prop of Integer Mult} \]

\[ 1.28 \quad \text{Integer}(ac) \quad \text{Prop of Integer Mult} \]
\[ 1.29 \quad \text{Integer}(bd) \quad \text{Prop of Integer Mult} \]

\[ 1.30 \quad \text{Integer}(bd) \land (bd \neq 0) \quad \text{Intro} \land: 1.29, 1.17 \]
\[ 1.31 \quad \text{Integer}(ac) \land \text{Integer}(bd) \land (bd \neq 0) \quad \text{Intro} \land: 1.28, 1.30 \]

\[ 1.32 \quad (xy = \frac{a}{b} / (c/d)) \land \text{Integer}(ac) \land \text{Integer}(bd) \land (bd \neq 0) \quad \text{Intro} \land: 1.10, 1.31 \]

\[ 1.33 \quad \exists p \exists q \left( (xy = p/q) \land \text{Integer}(p) \land \text{Integer}(q) \land (q \neq 0) \right) \quad \text{Intro} \exists: 1.32 \]

\[ 1.34 \quad \text{Rational}(xy) \quad \text{Def of Rational: 1.32} \]
Rationality

Predicate Definitions

Rational(x) := ∃a ∃b (Integer(a) ∧ Integer(b) ∧ (x = a/b) ∧ (b ≠ 0))

Prove: “If x and y are rational, then xy is rational.”

Suppose x and y are rational.

| 1.1  | Rational(x) ∧ Rational(y)   | Assumption       |
|      |                               |                  |
|      | 1.10 xy = (a/b)(c/d) = (ac/bd) = (ac)/(bd) |                  |
|      | 1.17 bd ≠ 0                   | Prop of Integer Mult |

Furthermore, ac and bd are integers.

| 1.28 | Integer(ac)                   | Prop of Integer Mult |
|      | 1.29 Integer(bd)              | Prop of Integer Mult |

By definition, then, xy is rational.

| 1.34 | Rational(xy)                  | Def of Rational: 1.32 |

And finally...
Rational(x) := ∃a ∃b (Integer(a) ∧ Integer(b) ∧ (x = a/b) ∧ (b ≠ 0))

Prove: “If x and y are rational, then xy is rational.”

Suppose that x and y are rational.

1.1 Rational(x) ∧ Rational(y) Assumption

1.10 xy = (a/b)(c/d) = (ac/bd) = (ac)/(bd)

1.17 bd ≠ 0 Prop of Integer Mult

Furthermore, ac and bd are integers.

1.28 Integer(ac) Prop of Integer Mult

1.29 Integer(bd) Prop of Integer Mult

By definition, then, xy is rational.

1.34 Rational(xy) Def of Rational: 1.32

1. Rational(x) ∧ Rational(y) → Rational(xy) Direct Proof
Prove: “If $x$ and $y$ are rational, then $xy$ is rational.”

Proof: Suppose $x$ and $y$ are rational.

Then, $x = \frac{a}{b}$ for some integers $a$, $b$, where $b \neq 0$, and $y = \frac{c}{d}$ for some integers $c,d$, where $d \neq 0$.

Multiplying, we get that $xy = \frac{ac}{bd}$. Since $b$ and $d$ are both non-zero, so is $bd$. Furthermore, $ac$ and $bd$ are integers. By definition, then, $xy$ is rational. $\blacksquare$
English Proofs

• High-level language let us work more quickly
  – should not be necessary to spill out every detail
  – reader checks that the writer is not skipping too much
  – examples so far
    skipping Intro \( \land \) and Elim \( \land \)
    not stating existence claims (immediately apply Elim \( \exists \) to name the object)
    not stating that the implication has been proven (“Suppose X... Thus, Y.” says it already)
  – (list will grow over time)

• English proof is correct if the reader believes they could translate it into a formal proof
  – the reader is the “compiler” for English proofs