Direct Proofs

1 Example 1

Definition. An integer n is even if and only if there exists and integer k such that $2k = n$

Let n be an integer. If n is even then n^2 is even.

1.1 Proof in Symbols

Given	Inferred	Rule of Inference
n is even	$\exists k \in \mathbb{Z} \vert 2k = n$	*modus ponens using Definition of "even" and given*
	k is an integer such that $2k = n$.	*existential instantiation (Table 2, p174)*
	$4k^2 = n^2$	*algebra — square* $2k = n$
	$2 \cdot 2k^2 = n^2$	*algebra — factor out 2*
	Let l be an integer such that $l = 2k^2$.	*closure of integers*
	$2l = n^2$	*algebra — substitute* l *for* $2k^2$
	$\exists l \in \mathbb{Z} \vert 2l = n^2$	*existential generalization(Table 2, p174)*
	n^2 is even	*Inferred (6) and definition of "even"*

1.2 Proof in words

We assume that n is even. From the definition of even, we know that there is an integer k such that

$$2k = n \tag{1}$$

We can square both sides of equation 1 to see that $4k^2 = n^2$. We can then factor out a 2 and get:

$$2 \cdot 2k^2 = n^2 \tag{2}$$

Because the integers are closed under addition and multiplication, we know that there exists an integer l such that $2k^2 = l$. When we substitute l into equation 2 we see that $2l = n^2$. Because we have found an integer l such that $2l = n^2$, the definition of even tells us that n^2 is even. ■

2 Example 2

Definition: A number s is *rational* if and only if there exists two integers x and y such that $\frac{x}{y} = s$.

If s and t are rational numbers, then $s + t$ is also rational.

2.1 Proof in Symbols

Given	Inferred	Rule of Inference
s is rational	$\exists a, b \in \mathbb{Z} \| \frac{a}{b} = s$	*definition of "Rational"*
t is rational	$\frac{a}{b} = s$ for some $a, b \in \mathbb{Z}$.	*existential instantiation (Table 2, p174)*
	$\exists c, d \in \mathbb{Z} \| \frac{c}{d} = t$	*definition of "Rational"*
	$\frac{a}{b} = t$ for some $c, d \in \mathbb{Z}$	*existential instantiation (Table 2, p174)*
	$s + t = \frac{a}{b} + \frac{c}{d}$	*algebra — substitution*
	$s + t = \frac{ad+bc}{bd}$	*algebra — multiplication of fractions*
	Let n be an integer such that $n = ad + bc$	*closure of integers*
	Let m be an integer such that $m = bd$	*closure of integers*
	$s + t = \frac{n}{m}$	*algebra — substitution*
	$s + t$ is rational	*definition of "Rational"*

2.2 Proof in words

Let s and t be rational numbers. From the definition of rational, we know that there exist integers a and b such that $s = \frac{a}{b}$. Likewise, we know that there exist integers c and d such that $t = \frac{c}{d}$. From here we can substitute $\frac{a}{b}$ for s and $\frac{b}{c}$ for t and see that $s + t = \frac{a}{b} + \frac{c}{d}$. This is equivalent to saying that $s + t = \frac{ad+bc}{bd}$. Let $n = ad + bc$ and let $m = bd$. Because the integers are closed under addition and multiplication, we know that n and m are integers. Thus, we have found two integer m and n such hat $\frac{n}{m} = s + t$. Hence, we know that $s + t$ is rational by definition. ■

3 Example 3

Definition: Let a, and b be integers. We say a divides b (written $a|b$ if and only if $\exists k \in \mathbb{Z} | ak = b$.

Let a, b, and c be integers. If $a|b$ and $a|c$, then $a|bc$.

3.1 Proof in Symbols

Given: $a|b$, $a|c$

	Inferred	Rule of Inference
1	$\exists k \in \mathbb{Z} \| ak = b$	*definition of divices*
2	$\exists l \in \mathbb{Z} \| al = c$	*definition of divides*
3	$ak = b$ for some $k \in \mathbb{Z}$	*existential instantiation*
4	$aj = c$ for some $j \in \mathbb{Z}$	*existential instantiation*
5	$bc = akaj$	*algebra — multiply 4 and 5*
6	$bc = a(kaj)$	*algebra — associtivity of integers*
7	Let $l \in \mathbb{Z} = kaj$	*closure of integers under multiplication*
8	$bc = al$	*algebra — substitue 7 into 6*
9	$a\|bc$	*definition of divides*

4 Proof in words

We will prove that, given integers a, b, and c, if $a|b$ and $a|c$, then $a|bc$. We will do this by finding an integer j such that $aj = bc$.nc

The definition of divides tells us that

$$ak = b \tag{3}$$

for some integer k. Likewise, we know that

$$al = c \tag{4}$$

for some integer c. We can multiply equations 3 and 4 to get

$$bc = akal \tag{5}$$

Now let j be an integer such that $j = kal$. When we substitute j for kal in equation 5, we see that $bc = aj$. Thus, we have found an integer j such that $aj = bc$. Therefore, the definition of divides tells us that $a|bc$. ■

5 Another Proof in Words

Given that a, b and c are integers, we wish to show that $a|bc$. From the definition of divides, we know that there exist integers k and l such that $ak = b$ and $al = c$. We can multiply these two equations to see that $bc = akal = a(kal)$. Let j be an integer such that $j = kal$. We can subsitite j into the equation $bc = akal$ to see that $bc = aj$. Finally, the definition of divides tells us that $a|bc$. ■