Chapter 2. Mathematical Proof

2.1 Remark: At the end of the last chapter we raised the following questions. Given first-order formulas F and G, how can we determine whether $F \cong G$? Given a set of formulas S and a formula K, how can we determine whether $S \models K$? There is, in general, no routine algorithmic procedure to solve these two problems, but sometimes we can construct a **mathematical proof**. Just as a mathematical statement (normally expressed using a combination of mathematical symbols and words from a natural language such as English) can be expressed as a formula in a very precise formal symbolic language, so too a mathematical proof can be translated into a very precise symbolic form of proof called a **derivation**. In this chapter we shall describe two formal proof systems, one for deriving equivalences and one for deriving valid arguments.

2.2 Note: To state our proof rules precisely, we need to introduce one somewhat subtle concept, namely the concept of **substitution**, which is used in many mathematical proofs. For example, if we know that $a \leq x$ for every $x \in S$ and we know that $b \in S$, then we can conclude that $a \leq b$. In a detailed proof, we would break this into two steps, as follows.

1. Since $\forall x(x \in S \to a \leq x)$ it follows that $b \in S \to a \leq b$.
2. Since $b \in S$ and $b \in S \to a \leq b$ it follows that $a \leq b$.

In the first step, we used a substitution. In the formula $F \equiv (x \in S \to a \leq x)$ we replaced x by b. If write $[F]_{x \mapsto t}$ to denote the formula obtained from F by replacing the variable symbol x by the term t, then the proof rule that was invoked at step 1 was as follows: from $\forall x F$ we can conlude $[F]_{x \mapsto b}$.

When we define $[F]_{x \mapsto t}$, we want it to be the case that (once an interpretation has been chosen) the formula $[F]_{x \mapsto t}$ has the same meaning about t as the original formula F had about x. In general, this cannot be accomplished by simply replacing each occurrence of the symbol x by the term t. For example, in the interpretation $\mathbf{Z}$, the statement "x divides y" can be expressed using the formula $F \equiv \exists z\ y = x \times z$. We would like the formula $[F]_{x \mapsto u}$ to mean "u divides y", and this can be accomplished simply by replacing x by u to obtain $[F]_{x \mapsto u} \equiv \exists z\ y = u \times z$. But we would also like the formula $[F]_{x \mapsto z}$ to mean "z divides y" and if we simply replace x by z the formula becomes $\exists z\ y = z \times z$ which has a totally different meaning (it means "y is a perfect square"). To obtain the desired formula $[F]_{x \mapsto z}$ we first replace the bound variable z in F by the next available variable symbol u, then replace x by z afterwards, as follows

$$[F]_{x \mapsto z} \equiv \big[\exists z\ y = x \times z\big]_{x \mapsto z} \equiv \exists u \big[y = x \times u\big]_{x \mapsto z} \equiv \exists u\ y = z \times u.$$

2.3 Definition: Given a formula F, a variable symbol x, and a term t, we define the formula $[F]_{x \mapsto t}$ as follows. When F is obtained using rule F1 or F2, the formula $[F]_{x \mapsto t}$ is obtained from F by replacing all occurrences of the symbol x by the term t. To deal with rules F3 and F4 we define $\big[\neg F\big]_{x \mapsto t} \equiv \neg [F]_{x \mapsto t}$ and for $* \in \{\wedge, \vee, \to, \leftrightarrow\}$ we define $\big[(F * G)\big]_{x \mapsto t} \equiv \big([F]_{x \mapsto t} * [G]_{x \mapsto t}\big)$. To deal with rule F5, for $K \in \{\forall, \exists\}$ we define $\big[Kx\, F\big]_{x \mapsto t} \equiv Kx\, F$ (note that we do not need to change the formula when all occurrences of x are bound), and for a variable symbol y (which is different than x) we define $\big[Ky\, F\big]_{x \mapsto t}$ as follows. If y does not occur in t, we define $\big[Ky\, F\big]_{x \mapsto t} \equiv Ky[F]_{x \mapsto t}$. If y does occur in t, we define $\big[Ky\, F\big]_{x \mapsto t} \equiv Ku\big[[F]_{y \mapsto u}\big]_{x \mapsto t}$ where u is the first variable symbol which is not x and does not occur in F or in t. The formula $[F]_{x \mapsto t}$ is called the formula obtained from F by **substitution**, by replacing (free occurrences of) x by t.

2.4 Definition: For any formulas F, G and H, and any terms s and t, and any variables x and y, we have the following logical equivalences which are called the **basic equivalences**. The first 24 of these can be verified using truth-tables and the others are accepted axiomatically, without proof.

(Identity)	E1.	$F \cong F$
(Double Negation)	E2.	$F \cong \neg\neg F$
(Commutativity)	E3.	$F \wedge G \cong G \wedge F$
	E4.	$F \vee G \cong G \vee F$
(Associativity)	E5.	$F \wedge (G \wedge H) \cong (F \wedge G) \wedge H$
	E6.	$F \vee (G \vee H) \cong (F \vee G) \vee H$
(DeMorgan's Law)	E7.	$\neg(F \wedge G) \cong (\neg F \vee \neg G)$
	E8.	$\neg(F \vee G) \cong (\neg F \wedge \neg G)$
(Distributivity)	E9.	$F \wedge (G \vee H) \cong (F \wedge G) \vee (F \wedge H)$
	E10.	$F \vee (G \wedge H) \cong (F \vee G) \wedge (F \vee H)$
(Idempotence)	E11.	$F \wedge F \cong F$
	E12.	$F \vee F \cong F$
(Absorption)	E13.	$F \wedge (F \vee G) \cong F$
	E14.	$F \vee (F \wedge G) \cong F$
(Tautology)	E15.	$F \wedge (G \vee \neg G) \cong F$
	E16.	$F \vee (G \vee \neg G) \cong G \vee \neg G$
(Contradiction)	E17.	$F \wedge (G \wedge \neg G) \cong G \wedge \neg G$
	E18.	$F \vee (G \wedge \neg G) \cong F$
(Contrapositive)	E19.	$F \to G \cong \neg G \to \neg F$
(Implication)	E20.	$F \to G \cong \neg F \vee G$
	E21.	$\neg(F \to G) \cong F \wedge \neg G$
(If and Only If)	E22.	$F \leftrightarrow G \cong (F \wedge G) \vee (\neg F \wedge \neg G)$
	E23.	$F \leftrightarrow G \cong (\neg F \vee G) \wedge (F \vee \neg G)$
	E24.	$F \leftrightarrow G \cong (F \to G) \wedge (G \to F)$
(Equality)	E25.	$s = t \ \cong \ t = s$
(Double Quantifier)	E26.	$\forall x \, \forall y \, F \cong \forall y \, \forall x \, F$
	E27.	$\exists x \, \exists y \, F \cong \exists y \, \exists x \, F$
(Negate Quantifier)	E28.	$\neg\forall x \, F \cong \exists x \neg F$
	E29.	$\neg\exists x \, F \cong \forall x \, \neg F$
(Separate Quantifier)	E30.	$\forall x \, (F \wedge G) \cong \forall x \, F \wedge \forall x \, G$
	E31.	$\exists x \, (F \vee G) \cong \exists x \, F \vee \exists x \, G$
(Unused Variable)	E32.	$\forall x \, F \cong F$ if x is not free in F
	E33.	$\exists x \, F \cong F$ if x is not free in F
(Changing Variables)	E34.	$\forall x \, F \cong \forall y \, [F]_{x \mapsto y}$ if y is not free in F
	E35.	$\exists x \, F \cong \exists y \, [F]_{x \mapsto y}$ if y is not free in F

When $F \cong G$ (or $G \cong F$) is one of the above basic equivalences, and H is a formula which contains F as a sub-formula, and K is the formula obtained from H by replacing F by G, we say that K is obtained from G by **applying the basic equivalence** $F \cong G$ (or the equivalence $G \cong F$).

2.5 Definition: Given equivalent formulas F and G, a **derivation** of the equivalence $F \cong G$ is a list of formulas $F_1, F_2, \cdots, F_l$ with $F_1 = F$ and $F_l = G$ such that each formula F_{k+1} is obtained from the previous formula F_k by applying one of the basic equivalences.

2.6 Example: Let F and G be formulas. Make a derivation for $F \wedge (F \to G) \cong F \wedge G$.

Solution: Here is one possible derivation.

$F \wedge (F \to G)$	$\cong F \wedge (\neg F \vee G)$	Implication E20
	$\cong (F \wedge \neg F) \vee (F \wedge G)$	Distributivity E9
	$\cong (F \wedge G) \vee (F \wedge \neg F)$	Commutativity E4
	$\cong F \wedge G$	Contradiction E18

2.7 Example: Let F, G and H be formulas. Find a derivation for distributivity of $\vee$ over $\wedge$ from the right, that is for the logical equivalence $(F \wedge G) \vee H \cong (F \vee H) \wedge (G \vee H)$.

Solution: Here is a derivation.

$(F \wedge G) \vee H$	$\cong H \vee (F \wedge G)$	Commutativity E4
	$\cong (H \vee F) \wedge (H \vee G)$	Distributivity E10
	$\cong (F \vee H) \wedge (H \vee G)$	Commutativity E4
	$\cong (F \vee H) \wedge (G \vee H)$	Commutativity E4

2.8 Example: Derive the logical equivalence $F \to (G \to H) \cong (F \wedge G) \to H$.

Solution:

$F \to (G \to H)$	$\cong \neg F \vee (G \to H)$	Implication E20
	$\cong \neg F \vee (\neg G \vee H)$	Implication E20
	$\cong (\neg F \vee \neg G) \vee H$	Associativity E6
	$\cong \neg(F \wedge G) \vee H$	DeMorgan's Law E7
	$\cong (F \wedge G) \to H$	Implication E20

2.9 Example: Derive the logical equivalence $(F \wedge G) \to H \cong (F \to H) \vee (G \to H)$.

Solution:

$(F \wedge G) \to H$	$\cong \neg(F \wedge G) \vee H$	Implication E20
	$\cong (\neg F \vee \neg G) \vee H$	DeMorgan's Law E7
	$\cong (\neg F \vee \neg G) \vee (H \vee H)$	Idempotence E12
	$\cong ((\neg F \vee \neg G) \vee H) \vee H$	Associativity E6
	$\cong (\neg F \vee (\neg G \vee H)) \vee H$	Associativity E6
	$\cong (\neg F \vee (H \vee \neg G)) \vee H$	Commutativity E4
	$\cong ((\neg F \vee H) \vee \neg G) \vee H$	Associativity E6
	$\cong (\neg F \vee H) \vee (\neg G \vee H)$	Associativity E6
	$\cong (F \to H) \vee (\neg G \vee H)$	Implication E20
	$\cong (F \to H) \vee (G \to H)$	Implication E20

2.10 Example: Make a derivation for the equivalence $\exists x\,(F \to G) \cong \forall x\,F \to \exists x\,G$.

Solution: Here is a derivation.

$\exists x\,(F \to G)$	$\cong \exists x\,(\neg F \vee G)$	Implication E20
	$\cong \exists x \neg F \vee \exists x\,G$	Separating Quantifier E30
	$\cong \neg \forall x\,F \vee \exists x\,G$	Negating Quantifier E27
	$\cong \forall x\,F \to \exists x\,G$	Implication E20

2.11 Remark: We now give several examples of proofs which use standard mathematical language and notation. As an exercise, you should try to justify each step in each proof. Some steps make use of a definition, and other steps use one or more of the basic equivalences. In Example 2.15, two of the steps make use of the fact that $\alpha(F), \alpha(G) \in \{0, 1\}$.

We make several remarks about the symbols used in these proofs. Many of the symbols used in our formal symbolic language are not normally used in more standard mathematical language. The symbols $\rightarrow$ and $\leftrightarrow$ are more commonly written as $\Longrightarrow$ and $\Longleftrightarrow$. The symbols $\wedge$ and $\vee$ are more commonly expressed using the words "and" and "or". The negation symbol $\neg$ is usually either expressed in words (using expressions involving the word "not") or is indicated by crossing out a binary relation symbol, for example by writing $\neg\, s{=}t$ as $s \neq t$ and by writing $\neg\, s{\in}t$ as $s \notin t$. Also note that the same symbol $\Longleftrightarrow$ which is used in place of the symbol $\rightarrow$ is also often used to replace the symbol $\cong$.

2.12 Example: Let A and B be sets. Show that $A = B$ if and only if $A \subseteq B$ and $B \subseteq A$.

Solution: We have

$$\begin{aligned} A = B &\Longleftrightarrow \forall x \left(x \in A \Longleftrightarrow x \in B\right) \\ &\Longleftrightarrow \forall x \left((x \in A \Longrightarrow x \in B) \text{ and } (x \in B \Longrightarrow x \in A)\right) \\ &\Longleftrightarrow \forall x \,(x \in A \Longrightarrow x \in B) \text{ and } \forall x (x \in B \Longrightarrow x \in A) \\ &\Longleftrightarrow A \subseteq B \text{ and } B \subseteq A. \end{aligned}$$

2.13 Example: Prove that for all sets A, B and C we have $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$ (this is part of Theorem 1.4).

Solution: Let A, B and C be sets. Then for all x we have

$$\begin{aligned} x \in A \cap (B \cup C) &\Longleftrightarrow x \in A \text{ and } x \in (B \cup C) \\ &\Longleftrightarrow x \in A \text{ and } \left(x \in B \text{ or } x \in C\right) \\ &\Longleftrightarrow \left(x \in A \text{ and } x \in B\right) \text{ or} \left(x \in A \text{ and } x \in C\right) \\ &\Longleftrightarrow x \in A \cap B \text{ or } x \in A \cap C \\ &\Longleftrightarrow x \in (A \cap B) \cup (A \cap C). \end{aligned}$$

2.14 Example: Prove that for sets $A, B \subseteq X$ we have $X \setminus (A \cup B) = (X \setminus A) \cap (X \setminus B)$ (this is also part of Theorem 1.4).

Solution: Let A, B and X be sets with $A, B \subseteq X$. Then for all x we have

$$\begin{aligned} x \in X \setminus (A \cup B) &\Longleftrightarrow x \in X \text{ and } x \notin (A \cup B) \\ &\Longleftrightarrow x \in X \text{ and } \left(x \notin A \text{ and } x \notin B\right) \\ &\Longleftrightarrow \left(x \in X \text{ and } x \in X\right) \text{ and } \left(x \notin A \text{ and } x \notin B\right) \\ &\Longleftrightarrow \left(x \in X \text{ and } x \notin A\right) \text{ and } \left(x \in X \text{ and } x \notin B\right) \\ &\Longleftrightarrow x \in X \setminus A \text{ and } x \in X \setminus B \\ &\Longleftrightarrow x \in (X \setminus A) \cap (X \setminus B). \end{aligned}$$

2.15 Example: Prove that for all formulas F and G, $F \cong G \Longleftrightarrow \left(F \models G \text{ and } G \models F\right)$ (this is part of Theorem 1.20),

Solution: Let F and G be formulas. Then

$$\begin{aligned} \left(F \models G \text{ and } G \models F\right) \Longleftrightarrow &\text{ for all assignments } \alpha \ \left(\alpha(F){=}1 \Longrightarrow \alpha(G){=}1\right) \\ &\text{and for all assignments } \alpha \ \left(\alpha(G){=}1 \Longrightarrow \alpha(F){=}1\right) \end{aligned}$$

$\iff$ for all assignments α $\big(\big(\alpha(F)=1 \Longrightarrow \alpha(G)=1\big)$ and $\big(\alpha(G)=1 \Longrightarrow \alpha(F)=1\big)\big)$

$\iff$ for all assignments α $\big(\alpha(F)=1 \iff \alpha(G)=1\big)$

$\iff$ for all assignments α $\big(\big(\alpha(F)=1$ and $\alpha(G)=1\big)$ or $\big(\alpha(F) \neq 1$ and $\alpha(G) \neq 1\big)\big)$

$\iff$ for all assignments α $\big(\big(\alpha(F)=1$ and $\alpha(G)=1\big)$ or $\big(\alpha(F) = 0$ and $\alpha(G) = 0\big)\big)$

$\iff$ for all assignments α $\alpha(F) = \alpha(G)$

$\iff F \cong G$.

2.16 Definition: For any formulas F, G and H, any sets of formulas $\mathcal{S}$ and $\mathcal{T}$, any terms s and t, and any variable symbols x and y, the following rules are called the **basic validity rules**. We accept these rules axiomatically, without proof.

(Premise)	V1.	If $F \in \mathcal{S}$ then $\mathcal{S} \models F$
(Adding Premises)	V2.	If $\mathcal{S} \models F$ and $\mathcal{S} \subseteq \mathcal{T}$ then $\mathcal{T} \models F$
(The Chain Rule)	V3.	If $\mathcal{S} \models F$ and $\mathcal{S} \cup \{F\} \models G$ then $\mathcal{S} \models G$
(Proof by Cases)	V4.	If $\mathcal{S} \cup \{F\} \models G$ and $\mathcal{S} \cup \{\neg F\} \models G$ then $\mathcal{S} \models G$
(Contradiction)	V5.	If $\mathcal{S} \cup \{\neg F\} \models G$ and $\mathcal{S} \cup \{\neg F\} \models \neg G$ then $\mathcal{S} \models F$
	V6.	If $\mathcal{S} \cup \{F\} \models G$ and $\mathcal{S} \cup \{F\} \models \neg G$ then $\mathcal{S} \models \neg F$
(Conjunction)	V7.	If $\mathcal{S} \models F$ and $\mathcal{S} \models G$ then $\mathcal{S} \models F \wedge G$
	V8.	If $\mathcal{S} \cup \{F, G\} \models H$ then $\mathcal{S} \cup \{F \wedge G\} \models H$
	V9.	If $\mathcal{S} \models F \wedge G$ then $\mathcal{S} \models F$
	V10.	If $\mathcal{S} \models F \wedge G$ then $\mathcal{S} \models G$
(Disjunction)	V11.	If $\mathcal{S} \cup \{\neg F\} \models G$ then $\mathcal{S} \models F \vee G$
	V12.	If $\mathcal{S} \cup \{\neg G\} \models F$ then $\mathcal{S} \models F \vee G$
	V13.	If $\mathcal{S} \cup \{F\} \models H$ and $\mathcal{S} \cup \{G\} \models H$ then $\mathcal{S} \cup \{F \vee G\} \models H$
	V14.	If $\mathcal{S} \models F$ then $\mathcal{S} \models F \vee G$
	V15.	If $\mathcal{S} \models G$ then $\mathcal{S} \models F \vee G$
	V16.	If $\mathcal{S} \models F \vee G$ and $\mathcal{S} \models \neg F$ then $\mathcal{S} \models G$
	V17.	If $\mathcal{S} \models F \vee G$ and $\mathcal{S} \models \neg G$ then $\mathcal{S} \models F$
(Implication)	V18.	If $\mathcal{S} \cup \{F\} \models G$ then $\mathcal{S} \models F \to G$
	V19.	If $\mathcal{S} \cup \{\neg G\} \models \neg F$ then $\mathcal{S} \models F \to G$
	V20.	If $\mathcal{S} \cup \{\neg F\} \models H$ and $\mathcal{S} \cup \{G\} \models H$ then $\mathcal{S} \cup \{F \to G\} \models H$
	V21.	If $\mathcal{S} \models \neg F$ then $\mathcal{S} \models F \to G$
	V22.	If $\mathcal{S} \models G$ then $\mathcal{S} \models F \to G$
	V23.	If $\mathcal{S} \models F \to G$ and $\mathcal{S} \models F$ then $\mathcal{S} \models G$
	V24.	If $\mathcal{S} \models F \to G$ and $\mathcal{S} \models \neg G$ then $\mathcal{S} \models \neg F$
(If and Only If)	V25.	If $\mathcal{S} \models F \to G$ and $\mathcal{S} \models G \to F$ then $\mathcal{S} \models F \leftrightarrow G$
	V26.	If $\mathcal{S} \cup \{F, G\} \models H$ and $\mathcal{S} \cup \{\neg F, \neg G\} \models H$ then $\mathcal{S} \cup \{F \leftrightarrow G\} \models H$
	V27.	If $\mathcal{S} \models F$ and $\mathcal{S} \models G$ then $\mathcal{S} \models F \leftrightarrow G$
	V28.	If $\mathcal{S} \models \neg F$ and $\mathcal{S} \models \neg G$ then $\mathcal{S} \models F \leftrightarrow G$
	V29.	If $\mathcal{S} \models F \leftrightarrow G$ and $\mathcal{S} \models F$ then $\mathcal{S} \models G$
	V30.	If $\mathcal{S} \models F \leftrightarrow G$ and $\mathcal{S} \models G$ then $\mathcal{S} \models F$
	V31.	If $\mathcal{S} \models F \leftrightarrow G$ and $\mathcal{S} \models \neg F$ then $\mathcal{S} \models \neg G$
	V32.	If $\mathcal{S} \models F \leftrightarrow G$ and $\mathcal{S} \models \neg G$ then $\mathcal{S} \models \neg F$

(Equality) V33 $\mathcal{S} \models t = t$
V34 If $\mathcal{S} \models s = t$ then $\mathcal{S} \models t = s$
V35 If $\mathcal{S} \models r = s$ and $\mathcal{S} \models s = t$ then $\mathcal{S} \models r = t$
V36 If $S \models s = t$ and $\mathcal{S} \models [F]_{x \mapsto s}$ then $\mathcal{S} \models [F]_{x \mapsto t}$

(Forall) V37 If $S \models [F]_{x \mapsto y}$ where y is not free in $\mathcal{S} \cup \{\forall x\, F\}$, then $\mathcal{S} \models \forall x\, F$
V38 If $\mathcal{S} \cup \left\{[F]_{x \mapsto t}\right\} \models G$ then $\mathcal{S} \cup \{\forall x\, F\} \models G$
V39 If $\mathcal{S} \models \forall x\, F$ then $\mathcal{S} \models [F]_{x \mapsto t}$

(Exists) V40. If $\mathcal{S} \models [F]_{x \mapsto t}$ then $\mathcal{S} \models \exists x\, F$
V41. If $\mathcal{S} \cup \left\{[F]_{x \mapsto y}\right\} \models G$ where y is not free in $\mathcal{S} \cup \{G, \exists x\, F\}$, then $\mathcal{S} \cup \{\exists x\, F\} \models G$

(Equivalence) V42. If $F \cong G$ and $\mathcal{S} \models F$ then $\mathcal{S} \models G$
V43. If $F \cong G$ and $\mathcal{S} \cup \{F\} \models H$ then $\mathcal{S} \cup \{G\} \models H$

Rule V13 is also called **Proof by Cases**, Rule V19 is called the **Contrapositive Rule**, Rule V23 is called **Modus Ponens**, and rule V36 is called the **Substitution Rule**.

2.17 Definition: Given a set of formulas $\mathcal{S}$ and a formula F such that $\mathcal{S} \models F$, a **derivation** of the valid argument $\mathcal{S} \models F$ is a list of valid arguments $\mathcal{S}_1 \models F_1$, $\mathcal{S}_2 \models F_2$, $\cdots$, $\mathcal{S}_l \models F_l$ with $\mathcal{S}_l = \mathcal{S}$ and $F_l = F$, such that each valid argument $\mathcal{S}_k \models F_k$ is obtained from previous valid arguments $\mathcal{S}_j \models F_j$ with $j < k$ using one of the Basic Validity Rules. The equivalence rules V42 and V43 are only used in the case that the equivalence $F \cong G$ is obtained by applying one of the 35 basic equivalences. Except for the equivalence rules, the Basic Validity Rules are not applied to subformulas.

2.18 Note: The basic validity rules correspond to standard methods of proof which are used routinely in mathematics. Here are the basic validity rules stated less formally (and less precisely) in standard mathematical language.

V1 (Premise) If we suppose F then we can conclude F.
V2 (Adding Premises) If we can prove G without F then we can prove G with F.
V3 (Chain Rule) If we can prove F and, with F we can prove G, then we can prove G.
V4 (Proof by Cases) To prove F by cases, choose a formula G, then consider two cases. For the first case, suppose that G is true then prove F and, for the second case, suppose that G is false then prove F.

V5 (Contradiction 1) To prove that F is true we can suppose, for a contradiction, that F is false, choose a formula G, then prove that G is true and that G is false.
V6 (Contradiction 2) To prove that F is false we can suppose, for a contradiction, that F is true, choose a formula G, then prove that G is true and that G is false.

V7 (Conjunction 1) To prove $F \wedge G$, we prove F and we prove G.
V8 (Conjunction 2) To prove that $F \wedge G$ implies H we suppose F and G then prove H.
V9 (Conjunction 3) From $F \wedge G$ we can conclude F.
V10 (Conjunction 4) From $F \wedge G$ we can conclude G.

V11 (Disjunction 1) To prove $F \vee G$ we can suppose that F is false then prove G.
V12 (Disjunction 2) To prove $F \vee G$ we can suppose that G is false then prove F.
V13 (Disjunction 3) To prove that $F \vee G$ implies H we consider two cases. For the first case, we suppose F then prove H and, for the second case, we suppose G then prove H.
V14 (Disjunction 4) From F we can conclude $F \vee G$.
V15 (Disjunction 5) From G we can conclude $F \vee G$.
V16 (Disjunction 6) From $F \vee G$ and $\neg F$ we can conclude G.
V17 (Disjunction 7) From $F \vee G$ and $\neg G$ we can conclude F.

V18 (Implication 1) To prove $F \to G$ we can suppose F then prove G.
V19 (Implication 2) To prove $F \to G$ we can suppose $\neg G$ then prove $\neg F$.
V20 (Implication 3) To prove that $F \to G$ implies H, we consider two cases. For the first case, suppose $\neg F$ then prove H and, for the second case, suppose G then prove H.
V21 (Implication 4) From $\neg F$ we can conclude $F \to G$.
V22 (Implication 5) From G we can conclude $F \to G$.
V23 (Implication 6) From $F \to G$ and F we can conclude G.
V24 (Implication 7) From $F \to G$ and $\neg G$ we can conclude $\neg F$.

V25 (If and Only If 1) To prove $F \leftrightarrow G$, we prove $F \to G$ and we prove $G \to F$
V26 (If and Only If 2) To prove that $F \leftrightarrow G$ implies H, first we suppose that F and G are both true then prove H, and then we suppose that F and G are both false then prove H.
V27 (If and Only If 3) From F and G we can conclude $F \leftrightarrow G$.
V28 (If and Only If 4) From $\neg F$ and $\neg G$ we can conclude $F \leftrightarrow G$.
V29 (If and Only If 5) From $F \leftrightarrow G$ and F we can conclude G.
V30 (If and Only If 6) From $F \leftrightarrow G$ and G we can conclude F.
V31 (If and Only If 7) From $F \leftrightarrow G$ and $\neg F$ we can conclude $\neg G$.
V32 (If and Only If 8) From $F \leftrightarrow G$ and $\neg G$ we can conclude $\neg F$.
V33 (Equality 1) We can always conclude that $t = t$.
V34 (Equality 2) From $s = t$ we can conclude that $t = s$.
V35 (Equality 3) From $r = s$ and $s = t$ we can conclude that $r = t$.
V36 (Substitution) From $s = t$ and $[F]_{x \mapsto s}$ we can conclude $[F]_{x \mapsto t}$.

V37 (Forall 1) To prove $\forall x\, F$, we choose a variable symbol y about which we have not made any assumptions (in the case that we have not made any assumptions about x we can take $y \equiv x$) and we write "let y be arbitrary", then we prove the statement $[F]_{x \mapsto y}$.
V38 (Forall 2) To prove that $\forall x\, F$ implies G, we choose a term t, suppose that $[F]_{x \mapsto t}$ is true, then prove G.
V39 (Forall 3) From $\forall x F$ we can conclude $[F]_{x \mapsto t}$.

V40 (Exists 1) To prove $\exists x\, F$, we choose a term t then we prove the statement $[F]_{x \mapsto t}$.
V41 (Exists 2) To prove that $\exists x\, F$ implies G, we choose a variable symbol y about which we have made no assumptions and which does not occur in G (in the case that we have not made any assumptions about x and x does not occur in G we can take $y \equiv x$), we suppose $[F]_{x \mapsto y}$ and write "choose y so that $[F]_{x \mapsto y}$ is true", then we prove G.

V42 (Equivalence 1) If F is equivalent to G, then to prove F we can prove G.
V43 (Equivalence 2) If F is equivalent to G, then we can replace the premise F by G.

2.19 Note: Recall that the statement $\forall\, x \in A\ F$ can be expressed as $\forall x\big(x \in A \to F\big)$. To prove this statement, in the case that we have made no assumptions about x, we write "let x be arbitrary" [to use V37] then we suppose $x \in A$ [to use V18] then we prove F (in the case that we have made assumptions about x, we write "let y be arbitrary", suppose $y \in A$, then prove $[F]_{x \mapsto y}$). Rather than writing "let x be arbitrary and suppose $x \in A$" we usually write "let $x \in A$ be arbitrary" or simply "let $x \in A$". Similarly, to prove a statement of the form "for every function $f : A \to B$ we have F" we would begin the proof by writing "let $f : A \to B$ be arbitrary" or simply "let $f : A \to B$".

2.20 Note: In standard mathematical proofs, the proof rules are often used implicitly, but in the next few examples we shall state explicitly (in square brackets) which rule is being used at each step in our proof.

2.21 Example: Let F, G and H be formulas. Prove that $\{F \to (G \wedge H), (F \wedge G) \vee H\} \models H$.

Solution: We need to prove that for every assignment α, if $\alpha\big(F \to (G \wedge H)\big) = 1$ and $\alpha\big((F \wedge G) \vee H\big) = 1$ then $\alpha(H) = 1$. Here is a step-by-step proof in which we indicate which proof rule is being used at each step.

1. Let α be an arbitrary assignment [to use V37 and V18].
2. Suppose that $F \to (G \wedge H)$ is true (under α), and that $(F \wedge G) \vee H$ is true [to use V8].
3. Suppose, for a contradiction, that H is false [to use V5].
4. Since $(F \wedge G) \vee H$ is true and H is false, it follows that $F \wedge G$ is true [by V17].
5. Since $F \wedge G$ is true, F is true [by V9].
6. Since F is true and $F \to (G \wedge H)$ is true, it follows that $G \wedge H$ is true [by V23].
7. Since $G \wedge H$ is true, H is true [by V10].
8. Since H true and H false, we have the desired contradiction. Thus H is true [by V5].
9. Thus if $\alpha\big(F \to (G \wedge H)\big) = 1$ and $\alpha\big((F \wedge G) \vee H\big) = 1$ then $\alpha(H) = 1$ [by V8].
10. Since α was arbitrary, we have $\{F \to (G \wedge H), (F \wedge G) \vee H\} \models H$ [by V37 and V18].

Now here is the same proof presented in the form of a derivation of valid arguments.

1.	$\{F \to (G \wedge H), (F \wedge G) \vee H\,,\, \neg H\} \models \neg H$	V1
2.	$\{F \to (G \wedge H), (F \wedge G) \vee H\,,\, \neg H\} \models (F \wedge G) \vee H$	V1
3.	$\{F \to (G \wedge H), (F \wedge G) \vee H\,,\, \neg H\} \models (F \wedge G)$	V17 on lines 2 and 1
4.	$\{F \to (G \wedge H), (F \wedge G) \vee H\,,\, \neg H\} \models F$	V9 on 3
5.	$\{F \to (G \wedge H), (F \wedge G) \vee H\,,\, \neg H\} \models F \to (G \wedge H)$	V1
6.	$\{F \to (G \wedge H), (F \wedge G) \vee H\,,\, \neg H\} \models G \wedge H$	V23 on 5 and 4
7.	$\{F \to (G \wedge H), (F \wedge G) \vee H\,,\, \neg H\} \models H$	V10 on 6
8.	$\{F \to (G \wedge H), (F \wedge G) \vee H\} \models H$	V5 on 7 and 1

2.22 Example: Prove that $\{((F \vee \neg G) \to H)\,,\, (F \leftrightarrow (G \wedge \neg H))\} \models H \wedge \neg F$.

Solution: Here is a derivation of valid arguments.

1.	$\{((F \vee \neg G) \to H)\,,\, (F \leftrightarrow (G \wedge \neg H))\,,\, \neg H\} \models \neg H$	V1
2.	$\{((F \vee \neg G) \to H)\,,\, (F \leftrightarrow (G \wedge \neg H))\,,\, \neg H\} \models \neg(F \vee \neg G)$	V1
3.	$\{((F \vee \neg G) \to H)\,,\, (F \leftrightarrow (G \wedge \neg H))\,,\, \neg H\} \models (F \vee \neg G) \to H$	V23 on 1 and 2
4.	$\{((F \vee \neg G) \to H)\,,\, (F \leftrightarrow (G \wedge \neg H))\,,\, \neg H\} \models \neg F \wedge \neg\neg G$	V42 with E8 on 3
5.	$\{((F \vee \neg G) \to H)\,,\, (F \leftrightarrow (G \wedge \neg H))\,,\, \neg H\} \models \neg F$	V9 on 4
6.	$\{((F \vee \neg G) \to H)\,,\, (F \leftrightarrow (G \wedge \neg H))\,,\, \neg H\} \models \neg\neg G$	V10 on 4
7.	$\{((F \vee \neg G) \to H)\,,\, (F \leftrightarrow (G \wedge \neg H))\,,\, \neg H\} \models G$	V42 with E2 on 6
8.	$\{((F \vee \neg G) \to H)\,,\, (F \leftrightarrow (G \wedge \neg H))\,,\, \neg H\} \models G \wedge \neg H$	V7 on 7 and 1
9.	$\{((F \vee \neg G) \to H)\,,\, (F \leftrightarrow (G \wedge \neg H))\,,\, \neg H\} \models F \leftrightarrow (G \wedge \neg H)$	V1
10.	$\{((F \vee \neg G) \to H)\,,\, (F \leftrightarrow (G \wedge \neg H))\,,\, \neg H\} \models F$	V30 on 9
11.	$\{((F \vee \neg G) \to H)\,,\, (F \leftrightarrow (G \wedge \neg H))\} \models H$	V5 on 10 and 5
12.	$\{((F \vee \neg G) \to H)\,,\, (F \leftrightarrow (G \wedge \neg H))\} \models \neg\neg H$	V42 with E2 on 11
13.	$\{((F \vee \neg G) \to H)\,,\, (F \leftrightarrow (G \wedge \neg H))\} \models \neg G \vee \neg\neg H$	V15 on 12
14.	$\{((F \vee \neg G) \to H)\,,\, (F \leftrightarrow (G \wedge \neg H))\} \models \neg(G \wedge \neg H)$	V42 with E7 on 13
15.	$\{((F \vee \neg G) \to H)\,,\, (F \leftrightarrow (G \wedge \neg H))\} \models F \leftrightarrow (G \wedge \neg H)$	V1 (or V2 on 9)
16.	$\{((F \vee \neg G) \to H)\,,\, (F \leftrightarrow (G \wedge \neg H))\} \models H$	V5 on 10 and 5
17.	$\{((F \vee \neg G) \to H)\,,\, (F \leftrightarrow (G \wedge \neg H))\} \models \neg F$	V32 on 16
18.	$\{((F \vee \neg G) \to H)\,,\, (F \leftrightarrow (G \wedge \neg H))\} \models H$	V7 on 11 and 17

2.23 Example: Prove that $\models \forall x\, \exists y\, \big(\neg y = f(x) \to yRf(x)\big)$.

Solution: We need to prove that for every non-empty set U, for every function $f : U \to U$, and for every binary relation relation $R \subseteq U^2$, for all $x \in U$ there exists $y \in U$ such that if $y \neq f(x)$ then $(y, f(x)) \in R$. Here is a step-by-step proof.

1. Let U be a set, let $f : U \to U$ and let $R \subseteq U^2$ [to use V37 and V18].
2. Let $x \in U$ be arbitrary [to use V37].
3. Choose $y = f(x)$ [to use V40 where the chosen term is $t = f(x)$].
4. Since $y = f(x)$, the formula $\neg y = f(x)$ is false. [by V42 with E2]
5. Since $\neg y = f(x)$ is false, the statement $\neg y = f(x) \to (y, f(x)) \in R$ is true [by V21].
6. This proves that there exists $y \in U$ such that if $y \neq f(x)$ then $(y, f(x)) \in R$ [by V40].
7. Since $x \in U$ was arbitrary, we have proven that for all $x \in U$ there exists $y \in U$ such that if $y \neq f(x)$ then $(y, f(x)) \in R$ [by V37].
8. Since U and f and R were arbitrary, our proof is complete [by V37 and V18].

Here is the same proof presented formally as a derivation of valid arguments.

1.	$\models f(x) = f(x)$	V33
2.	$\models \neg\neg\, f(x) = f(x)$	V42 with E2 on 1
3.	$\models \big(\neg\, f(x) = f(x) \to f(x)Rf(x)\big)$	V24 on 2
4.	$\models \exists y\big(\neg\, y = f(x) \to yRf(x)\big)$	V40 with $t = f(x)$ on 3
5.	$\models \forall x\, \exists y\, \big(\neg y = f(x) \to yRf(x)\big)$	V37 on 4

2.24 Exercise: Prove that $\models \forall x\big(\exists y\ \neg xRy \vee \exists y\ yRx\big)$.

2.25 Example: Prove that $\big\{\forall x\ g(x, a) = x\big\} \models \forall x\, \big(\forall y\ g(x, y) = y \to x = a\big)$.

Solution: First we provide a proof using standard mathematical language. Let U be a nonempty set, let $a \in U$ and let $g : U^2 \to U$. Suppose that for all $x \in U$ we have $g(x, a) = x$. We need to prove that for all $x \in U$, if $g(x, y) = y$ for every $y \in U$ then $x = a$. Let $x \in U$ be arbitrary, and note that $g(x, a) = x$. Suppose that for every $y \in U$ we have $g(x, y) = y$. Then in particular, taking $y = a$, we have $g(x, a) = a$. Thus $x = g(x, a) = a$, as required.

We now convert the above proof into a derivation of valid arguments:

1.	$\big\{\forall x\ g(x, a) = x\,,\ \forall y\ g(x, y) = y\big\} \models\ \forall y\ g(x, y) = y$	V1
2.	$\big\{\forall x\ g(x, a) = x\,,\ \forall y\ g(x, y) = y\big\} \models\ g(x, a) = a$	V39 on 1
3.	$\big\{\forall x\ g(x, a) = x\,,\ \forall y\ g(x, y) = y\big\} \models\ \forall x\ g(x, a) = x$	V1
4.	$\big\{\forall x\ g(x, a) = x\,,\ \forall y\ g(x, y) = y\big\} \models\ g(x, a) = x$	V39 on 3
5.	$\big\{\forall x\ g(x, a) = x\,,\ \forall y\ g(x, y) = y\big\} \models\ x = g(x, a)$	V34 on 4
6.	$\big\{\forall x\ g(x, a) = x\,,\ \forall y\ g(x, y) = y\big\} \models\ x = a$	V35 on 5, 2
7.	$\big\{\forall x\ g(x, a) = x\big\} \models\ (\forall y\, g(x, y) = y \to x = a)$	V18 on 6
8.	$\big\{\forall x\ g(x, a) = x\big\} \models\ \forall x\, (\forall y\ g(x, y) = y \to x = a)$	V37 on 7

Note that, at the final step, we were able to apply Rule V37 on line 7 because the variable symbol x is not free in the formula $\forall x\ g(x, a) = x$.

2.26 Note: Any statement of the form $\forall\, x \in \emptyset\ F$ is true. Indeed the statement $\forall\, x \in \emptyset\ F$ is equivalent (by definition) to the statement $\forall x(x \in \emptyset \to F)$. For every x, the statement $x \in \emptyset$ is false, and so the statement $x \in \emptyset \to F$ is true. A statement of this form is said to be **vacuously true**.

2.27 Exercise: Let F be a formula and let the symbol $\emptyset$ be a constant symbol. Make a derivation of valid arguments to show that $\{\forall x \neg x \in \emptyset\} \models \forall x (x \in \emptyset \to F)$.

2.28 Exercise: Let F be a formula and let $\emptyset$ be the empty set. Prove that $\models F \iff \emptyset \models F$.

2.29 Example: Prove that the class of all sets is not a set.

Solution: Here is a proof in standard mathematical language.

1. Let u be the class of all sets.
2. Suppose, for a contradiction, that u is a set .
3. Let $w = \{x \in u | x \notin x\}$ and note that w is a set by a Separation Axiom.
4. We claim that $w \in w$. Suppose, for a contradiction, that $w \notin w$.
5. Since $w \in u$ and $w \notin w$ we have $w \in w$ by the definition of w.
6. Since $w \in w$ and $w \notin w$ we have the desired contradiction, so $w \in w$, as claimed.
7. We claim that $w \notin w$. Suppose, for a contradiction, that $w \in w$.
8. Since $w \in u$ and $w \in w$ we have $w \notin w$, by the definition of w.
9. Since $w \in w$ and $w \notin w$ we have the desired contradiction, so $w \notin w$, as claimed.
10. Since $w \in w$ and $w \notin w$, we have the desired contradiction, so u is not a set, as claimed.

Note that the statement "the class u of all sets is a set" can be expressed as $\exists u \forall x \; x \in u$. Also, note that on line 3 we used the Separation Axiom $\forall u \exists w \forall x \left(x \in w \leftrightarrow (x \in u \wedge \neg x \in x\right)$. The above proof can be converted into a derivation of the valid argument

$$\left\{\forall u \exists w \forall x \left(x \in w \leftrightarrow (x \in u \wedge \neg x \in x)\right)\right\} \models \neg \exists u \forall x \; x \in u \, .$$

Here is a derivation which is a bit similar to the above proof.

1.	$\left\{w \in w \leftrightarrow (w \in u \wedge \neg w \in w) \, , \, w \in u \, , \, w \in w\right\} \models w \in w$	V1
2.	$\left\{w \in w \leftrightarrow (w \in u \wedge \neg w \in w) \, , \, w \in u \, , \, w \in w\right\} \models w \in w \leftrightarrow (w \in u \wedge \neg w \in w)$	V1
3.	$\left\{w \in w \leftrightarrow (w \in u \wedge \neg w \in w) \, , \, w \in u \, , \, w \in w\right\} \models (w \in u \wedge \neg w \in w)$	V29
4.	$\left\{w \in w \leftrightarrow (w \in u \wedge \neg w \in w) \, , \, w \in u \, , \, w \in w\right\} \models \neg w \in w$	V12
5.	$\left\{w \in w \leftrightarrow (w \in u \wedge \neg w \in w) \, , \, w \in u\right\} \models \neg w \in w$	V6
6.	$\left\{w \in w \leftrightarrow (w \in u \wedge \neg w \in w) \, , \, w \in u\right\} \models w \in u$	V1
7.	$\left\{w \in w \leftrightarrow (w \in u \wedge \neg w \in w) \, , \, w \in u\right\} \models w \in u \wedge \neg w \in w$	V10
8.	$\left\{w \in w \leftrightarrow (w \in u \wedge \neg w \in w) \, , \, w \in u\right\} \models w \in w \leftrightarrow (w \in u \wedge \neg w \in w)$	V1
9.	$\left\{w \in w \leftrightarrow (w \in u \wedge \neg w \in w) \, , \, w \in u\right\} \models w \in w$	V30
10.	$\left\{w \in w \leftrightarrow (w \in u \wedge \neg w \in w)\right\} \models \neg w \in u$	V6
11.	$\left\{w \in w \leftrightarrow (w \in u \wedge \neg w \in w)\right\} \models \exists x \neg x \in u$	V40
12.	$\left\{\forall x \left(x \in w \leftrightarrow (x \in u \wedge \neg x \in x)\right)\right\} \models \exists x \neg x \in u$	V38
13.	$\left\{\exists w \forall x \left(x \in w \leftrightarrow (x \in u \wedge \neg x \in x)\right)\right\} \models \exists x \neg x \in u$	V41
14.	$\left\{\forall u \exists w \forall x \left(x \in w \leftrightarrow (x \in u \wedge \neg x \in x)\right)\right\} \models \exists x \neg x \in u$	V39
15.	$\left\{\forall u \exists w \forall x \left(x \in w \leftrightarrow (x \in u \wedge \neg x \in x)\right)\right\} \models \forall u \exists x \neg x \in u$	V37
16.	$\left\{\forall u \exists w \forall x \left(x \in w \leftrightarrow (x \in u \wedge \neg x \in x)\right)\right\} \models \forall u \neg \forall x \, x \in u$	V45, E28
17.	$\left\{\forall u \exists w \forall x \left(x \in w \leftrightarrow (x \in u \wedge \neg x \in x)\right)\right\} \models \neg \exists u \forall x \, x \in u$	V45, E29

2.30 Example: For $a, b \in \mathbf{Z}$ we write $a \big| b$ when a is a factor of b, Prove that for $a, b, c \in \mathbf{Z}$, if $a|b$ and $b|c$ then $a|c$.

Solution: Here is a proof, in standard mathematical language, in which we do not bother to explicitly list all of our assumptions and we do not bother to indicate which proof rules are being used.

1. Suppose that $a|b$ and that $b|c$.
2. Since $a|b$ we can choose $k \in \mathbf{Z}$ so that $b = ak$.
3. Since $b|c$ we can choose $l \in \mathbf{Z}$ so that $c = bl$.
4. Then we have $c = bl = (ak)l = a(kl)$.
5. Thus $a|c$.

Note that $a|b$ can be expressed as $\exists x\ b = a \times x$ and $b|c$ can be expressed as $\exists x\ c = b \times x$ and $a|c$ can be expressed as $\exists x\ c = a \times x$. Also notice that on line 4 of the above proof, we implicitly made use of the fact that multiplication is associative which can be expressed as $\forall x\, \forall y\, \forall z\ (x \times y) \times z = x \times (y \times z)$. We now translate the above standard mathematical proof into a more detailed step-by-step proof which shows that

$$\big\{\exists x\ b = (a \times x)\,,\ \exists x\ c = b \times x\,,\ \forall x\, \forall y\, \forall z\ ((x \times y) \times z) = (x \times (y \times z))\big\} \models \exists x\ c = a \times x\,.$$

We need to prove that for every non-empty set U, for every binary function $\times$, and for every choice of $a \in U$ and $b \in U$, if there exists $x \in U$ such that $b = a \times x$ and if there exists $x \in U$ such that $c = b \times x$ and if for all $x, y, z \in U$ we have $(x \times y) \times z = x \times (y \times z)$, then there exists $x \in U$ such that $c = a \times x$. Here is a proof.

1. Let U be a set, let $\times$ be a binary function on U, and let $a, b \in U$ [to use V37 and V18].
2. Suppose $\exists\, x\ b = a \times x$, suppose $\exists\, x\ c = b \times x$, and suppose $\forall x\, \forall y\, \forall z\ (x \times y) \times z = x \times (y \times z)$ [to use V8 and V18].
3. Since $\exists x\ b = a \times x$ we can choose x so that $b = a \times x$ [to use V41].
4. Since $\exists x\ c = b \times x$ we can choose y so that $c = b \times y$ [to use V41].
5. Since $c = b \times y$ and $b = a \times x$ it follows that $c = (a \times x) \times y$ [by V36].
6. Since $\forall x\, \forall y\, \forall z\ (x \times y) \times z = x \times (y \times z)$, we have $\forall y\, \forall z\ (a \times y) \times z = a \times (y \times z)$ [by V39].
7. Since $\forall y\, \forall z\ (a \times y) \times z = a \times (y \times z)$, it follows that $\forall z\ (a \times x) \times z = a \times (x \times z)$ [by V39].
8. Since $\forall z\ (a \times x) \times z = a \times (x \times z)$ it follows that $(a \times x) \times y = a \times (x \times y)$ [by V39].
9. Since $c = (a \times x) \times y$ and $(a \times x) \times y = a \times (x \times y)$, it follows that $c = a \times (x \times y)$ [by V35].
10. Since $c = a \times (x \times y)$ it follows that $\exists x\ c = a \times x$ [by V40].
11. Since U and $\times$ and a and b were arbitrary, the proof is complete [by V37, V8 and V18].

Here is a similar proof presented formally as a derivation of valid arguments.

1.	$\big\{b = a \times x\,,\ c = b \times y\,,\ (a \times x) \times y = a \times (x \times y)\big\} \models\ b = a \times x$	V1
2.	$\big\{b = a \times x\,,\ c = b \times y\,,\ (a \times x) \times y = a \times (x \times y)\big\} \models\ c = b \times y$	V1
3.	$\big\{b = a \times x\,,\ c = b \times y\,,\ (a \times x) \times y = a \times (x \times y)\big\} \models\ c = (a \times x) \times y$	V36
4.	$\big\{b = a \times x\,,\ c = b \times y\,,\ (a \times x) \times y = a \times (x \times y)\big\} \models\ (a \times x) \times y = a \times (x \times y)$	V1
5.	$\big\{b = a \times x\,,\ c = b \times y\,,\ (a \times x) \times y = a \times (x \times y)\big\} \models\ c = a \times (x \times y)$	V35
6.	$\big\{b = a \times x\,,\ c = b \times y\,,\ (a \times x) \times y = a \times (x \times y)\big\} \models\ \exists x\ c = a \times x$	V40
7.	$\big\{b = a \times x\,,\ c = b \times y\,,\ \forall z\ (a \times x) \times z = a \times (x \times z)\big\} \models\ \exists x\ c = a \times x$	V38
8.	$\big\{b = a \times x\,,\ c = b \times y\,,\ \forall y\, \forall z\ (a \times y) \times z = a \times (y \times z)\big\} \models\ \exists x\ c = a \times x$	V38
9.	$\big\{b = a \times x\,,\ c = b \times y\,,\ \forall x\, \forall y\, \forall z\ (x \times y) \times z = x \times (y \times z)\big\} \models\ \exists x\ c = a \times x$	V38
10.	$\big\{b = a \times x\,,\ \exists x\ c = b \times x\,,\ \forall x\, \forall y\, \forall z\ (x \times y) \times z = x \times (y \times z)\big\} \models\ \exists x\ c = a \times x$	V41
11.	$\big\{\exists x\ b = a \times x\,,\ \exists x\ c = b \times x\,,\ \forall x\, \forall y\, \forall z\ (x \times y) \times z = x \times (y \times z)\big\} \models\ \exists x\ c = a \times x$	V41

2.31 Example: Prove that for $a, b \in \mathbf{Z}$, if $a|b$ and $b|a$ then $b = \pm a$.

Proof: Here is a proof in standard mathematical language.

1. Suppose that $a|b$ and $b|a$.
2. Since $a|b$ we can choose $k \in \mathbf{Z}$ so that $b = ak$.
3. Since $b|a$ we can choose $l \in \mathbf{Z}$ so that $a = bl$.
4. Then we have $a = bl = (ak)l = a(kl)$, that is $a \cdot 1 = a \cdot kl$.
5. Since $a \cdot 1 = a \cdot kl$, it follows that either $a = 0$ or $1 = kl$.
6. In the case that $a = 0$ we have $b = a \cdot k = 0 \cdot k = 0$ and so $b = a$.
7. In the case that $1 = kl$, it follows that either $k = l = 1$ or $k = l = -1$.
8. When $k = l = 1$ we have $b = a \cdot k = a \cdot 1 = a$ and
9. when $k = l = -1$ we have $b = a \cdot k = a \cdot (-1) = -a$.
10. In all cases, either $b = a$ or $b = -a$, that is $b = \pm a$.

It is a bit challenging to convert the above proof into a derivation of valid arguments, not because the proof itself is particularly difficult, but because the proof makes use of many algebraic properties of the integers and, because we are so familiar with those algebraic properties, it is easy to overlook the fact that some of these properties need to be included as premises in order to obtain a valid argument. Also it is difficult to decide exactly which properties need to be included as premises and which properties can then be proven from those premises. Here are some of the properties that were used implicitly in the proof.

On line 4 we used associativity of multiplication to obtain $(ak)l = a(kl)$ and we used the fact that $a = a \cdot 1$. On line 5 we used the fact that if $au = av$ then either $a = 0$ or $u = v$. On line 6 we used the fact that $0 \cdot k = 0$. On line 7 we used the fact that if $kl = 1$ then either $k = l = 1$ or $k = l = -1$ (incidentally, this algebraic property does not hold in $\mathbf{Q}$ or in $\mathbf{R}$). On line 8 we used the fact that $a \cdot 1 = a$ (which was also used on line 5) and on line 9 we used the fact that $a \cdot (-1) = -a$.

Another slight complication is that, in a derivation of valid arguments, all of the statements must be expressed as formulas in a first-order language, say first-order number theory. On several lines in our proof we use some mathematical notation, with which all students will no doubt be familiar, but which is not used explicitly in first order number theory. Namely, we use the negative sign $-$ to write -1 and $-a$. The statement $b = -a$ can be expressed by the formula $b + a = 0$, and the statement $k = l = -1$ can be expressed as $\big(k = l \ \wedge \ l + 1 = 0\big)$, but it is more challenging to decide how to express the statement $a \cdot (-1) = -a$ as a formula; since our proof uses the fact that if $k = -1$ then $a \cdot k = -a$, we might choose to express the statement using the formula $\big(k + 1 = 0 \ \rightarrow \ a \times k + a = 0\big)$.

2.32 Remark: In the next chapter, we shall carefully gather together and list all of the basic algebraic properties of $\mathbf{Z}$, $\mathbf{Q}$ and $\mathbf{R}$ which are needed in all of the subsequent proofs in this course. They are also needed in all proofs in all other mathematics courses. These algebraic properties can either be accepted axiomatically, without proof, or they can all be painstakingly proven. Our approach will be to accept them axiomatically.

In order to prove all of the basic algebraic properties, it would be necessary to begin by carefully and precisely defining the sets $\mathbf{Z}$, $\mathbf{Q}$ and $\mathbf{R}$ (by constructing them explicitly using the ZFC axioms of set theory), and then also carefully and precisely defining all of the algebraic operations, such as addition and multiplication, which are used in these sets. Only after the operations have been defined is it possible to prove that they satisfy their well-known algebraic properties. The procedure by which one can define the sets $\mathbf{Z}$, $\mathbf{Q}$ and $\mathbf{R}$ along with their operations $+$ and $\times$, and also their ordering $\leq$, is outlined briefly in Appendix 1.