3. Proofs

The purpose of this chapter is give the definition of a mathematical proof, and give the simplest proofs which will be needed in proving the completeness theorem in the next chapter. Given a set Γ of formulas in a first-order language, and a formula φ in that language, we explain what it means to have a proof of φ from Γ.

The following formulas are the *logical axioms*. Here φ, ψ, χ are arbitrary formulas unless otherwise indicated.

(L1a) $\varphi \to (\psi \to \varphi)$.
(L1b) $[\varphi \to (\psi \to \chi)] \to [(\varphi \to \psi) \to (\varphi \to \chi)]$.
(L1c) $(\neg\varphi \to \neg\psi) \to (\psi \to \varphi)$.
(L2) $\forall v_i(\varphi \to \psi) \to (\forall v_i\varphi \to \forall v_i\psi)$, for any $i \in \omega$.
(L3) $\varphi \to \forall v_i\varphi$ for any $i \in \omega$ such that v_i does not occur in φ.
(L4) $\exists v_i(v_i = \sigma)$ if σ is a term and v_i does not occur in σ.
(L5) $\sigma = \tau \to (\sigma = \rho \to \tau = \rho)$, where σ, τ, ρ are terms.
(L6) $\sigma = \tau \to (\rho = \sigma \to \rho = \tau)$, where σ, τ, ρ are terms.
(L7) $\sigma = \tau \to \mathbf{F}\xi_0 \dots \xi_{i-1}\sigma\xi_{i+1} \dots \xi_{m-1} = \mathbf{F}\xi_0 \dots \xi_{i-1}\tau\xi_{i+1} \dots \xi_{m-1}$, where $\mathbf{F}$ is an m-ary function symbol, $i < m$, and $\sigma, \tau, \xi_0, \dots, \xi_{i-1}, \xi_{i+1}, \dots \xi_{m-1}$ are terms.
(L8) $\sigma = \tau \to (\mathbf{R}\xi_0 \dots \xi_{i-1}\sigma\xi_{i+1} \dots \xi_{m-1} \to \mathbf{R}\xi_0 \dots \xi_{i-1}\tau\xi_{i+1} \dots \xi_{m-1})$, where $\mathbf{R}$ is an m-ary relation symbol, $i < m$, and $\sigma, \tau, \xi_0, \dots, \xi_{i-1}, \xi_{i+1}, \dots \xi_{m-1}$ are terms.

Theorem 3.1. *Every logical axiom is universally valid.*

Proof. (L1a–c): Universally valid by Theorem 2.9.
(L2): Assume that

(1) $\overline{A} \models \forall v_i(\varphi \to \psi)[a]$ and
(2) $\overline{A} \models \forall v_i\varphi[a]$;

We want to show that $\overline{A} \models \forall v_i\psi[a]$. To this end, take any $b \in A$; we want to show that $\overline{A} \models \varphi[a^i_b]$. Now by (1) we have $\overline{A} \models (\varphi \to \psi)[a^i_b]$, hence $\overline{A} \models \varphi[a^i_b]$ implies that $\overline{A} \models \psi[a^i_b]$. Now by (2) we have $\overline{A} \models \varphi[a^i_b]$, so $\overline{A} \models \psi[a^i_b]$.

(L3): We prove by induction on φ that if v_i does not occur in φ, and if $a, b : \omega \to A$ are such that $a(j) = b(j)$ for all $j \neq i$, then $\overline{A} \models \varphi[a]$ iff $\overline{A} \models \varphi[b]$. This will imply that (L3) is universally valid.

• φ is $\sigma = \tau$. Thus v_i does not occur in σ or in τ. Then

$$\begin{aligned} \overline{A} \models (\sigma = \tau)[a] \quad &\text{iff} \quad \sigma^{\overline{A}}(a) = \tau^{\overline{A}}(a) \\ &\text{iff} \quad \sigma^{\overline{A}}(b) = \tau^{\overline{A}}(b) \quad \text{by Proposition 2.4} \\ &\text{iff} \quad \overline{A} \models (\sigma = \tau)[b]. \end{aligned}$$

• φ is $\mathbf{R}\sigma_0 \dots \sigma_{m-1}$ for some m-ary relation symbol and some terms $\sigma_0, \dots, \sigma_{m-1}$. We leave this case to an exercise.

• φ is $\neg\psi$ (inductively).

$$\begin{array}{lll} \overline{A} \models \varphi[a] & \text{iff} & \text{not}(\overline{A} \models \psi[a]) \\ & \text{iff} & \text{not}(\overline{A} \models \psi[b]) \quad \text{(inductive hypothesis)} \\ & \text{iff} & \overline{A} \models \varphi[b]. \end{array}$$

• φ is $\psi \to \chi$ (inductively).

$$\begin{array}{lll} \overline{A} \models \varphi[a] & \text{iff} & (\overline{A} \models \psi[a] \text{ implies that } \overline{A} \models \chi[a]) \\ & \text{iff} & (\overline{A} \models \psi[b] \text{ implies that } \overline{A} \models \chi[b]) \\ & & \text{(inductive hypothesis)} \\ & \text{iff} & \overline{A} \models \varphi[b]. \end{array}$$

• φ is $\forall v_k \psi$ (inductively). By symmetry it suffices to prove just one direction. Suppose that $\overline{A} \models \varphi[a]$; we want to show that $\overline{A} \models \varphi[b]$. To this end, suppose that $u \in A$; we want to show that $\overline{A} \models \psi[b^k_u]$. Since $\overline{A} \models \varphi[a]$, we have $\overline{A} \models \psi[a^k_u]$. Now $k \neq i$, since v_i does not occur in φ. Hence $(a^k_u)(j) = (b^k_u)(j)$ for all $j \neq i$. Hence $\overline{A} \models \psi[b^k_u]$ by the inductive hypothesis, as desired.

This finishes our proof by induction of the statement made above. Now assume that $\overline{A} \models \varphi[a]$ and $u \in A$; we want to show that $\overline{A} \models \varphi[a^i_u]$. This holds by the statement above.

This finishes the proof of (L3).

(L4): Suppose that σ is a term and v_i does not occur in σ. To prove that $\overline{A} \models (\exists v_i(v_i = \sigma))[a]$, we want to find $u \in A$ such that $\overline{A} \models (v_i = \sigma)[a^i_u]$. Let $u = \sigma^{\overline{A}}(a)$. Then

$$(v_i)^{\overline{A}}[a^i_u] = u = \sigma^{\overline{A}}(a) = \sigma^{\overline{A}}(a^i_u)$$

by Proposition 2.4 (since v_i does not occur in σ, hence $a(j) = a^i_u(j)$ for all j such that v_j occurs in σ). Hence $\overline{A} \models (v_i = \sigma)[a^i_u]$.

(L5): Assume that $\overline{A} \models (\sigma = \tau)[a]$ and $\overline{A} \models (\sigma = \rho)[a]$. Then $\sigma^{\overline{A}}(a) = \tau^{\overline{A}}(a)$ and $\sigma^{\overline{A}}(a) = \rho^{\overline{A}}(a)$, so $\tau^{\overline{A}}(a) = \rho^{\overline{A}}(a)$, hence $\overline{A} \models (\tau = \rho)[a]$.

(L6): Left as an exercise.

(L7): Assume that $\overline{A} \models (\sigma = \tau)[a]$. Then $\sigma^{\overline{A}}(a) = \tau^{\overline{A}}(a)$, and so

$$\begin{aligned} (\mathbf{F}\xi_0 \dots \xi_{i-1}\sigma\xi_{i+1} \dots \xi_{m-1})^{\overline{A}}(a) &= \mathbf{F}^{\overline{A}}(\xi_0^{\overline{A}}(a), \dots, \xi_{i-1}^{\overline{A}}(a), \sigma^{\overline{A}}(a), \xi_{i+1}^{\overline{A}}(a), \dots, \xi_{m-1}^{\overline{A}}(a)) \\ &= \mathbf{F}^{\overline{A}}(\xi_0^{\overline{A}}(a), \dots, \xi_{i-1}^{\overline{A}}(a), \tau^{\overline{A}}(a), \xi_{i+1}^{\overline{A}}(a), \dots, \xi_{m-1}^{\overline{A}}(a)) \\ &= (\mathbf{F}\xi_0 \dots \xi_{i-1}\tau\xi_{i+1} \dots \xi_{m-1})^{\overline{A}}(a); \end{aligned}$$

it follows that $\overline{A} \models (\mathbf{F}\xi_0 \dots \xi_{i-1}\sigma\xi_{i+1} \dots \xi_{m-1} = \mathbf{F}\xi_0 \dots \xi_{i-1}\tau\xi_{i+1} \dots \xi_{m-1})[a]$, hence (L7) is universally valid.

(L8): Left as an exercise. □

Now let Γ be a set of formulas. A Γ-*proof* is a finite sequence $\langle \varphi_0, \dots, \varphi_{m-1} \rangle$ of formulas such that for each $i < m$ one of the following conditions holds:

(I1) φ_i is a logical axiom
(I2) $\varphi_i \in \Gamma$.
(I3) (modus ponens) There are $j, k < i$ such that φ_j is the formula $\varphi_k \to \varphi_i$.
(I4) (generalization) There exist $j < i$ and $k \in \omega$ such that φ_i is the formula $\forall v_k \varphi_j$.

Then we say that Γ *proves* φ, in symbols $\Gamma \vdash \varphi$, provided that φ is an entry in some Γ-proof. We write $\vdash \varphi$ in place of $\emptyset \vdash \varphi$.

Theorem 3.2. *If* $\Gamma \vdash \varphi$, *then* $\Gamma \models \varphi$.

Proof. Recall the notion $\Gamma \models \varphi$ from Chapter 2: it says that for every structure $\overline{A}$ for the implicit language we are dealing with, if $\overline{A} \models \psi[a]$ for all $\psi \in \Gamma$ and all $a : \omega \to A$, then $\overline{A} \models \varphi[a]$ for every $a : \omega \to A$. Now it suffices to take a Γ-proof $\langle \psi_0, \ldots, \psi_{m-1} \rangle$ and prove by complete induction on i that $\Gamma \models \psi_i$ for each $i < m$.

Case 1. ψ_i is a logical axiom. Then the result follows by Theorem 3.1.

Case 2. $\psi_i \in \Gamma$. Obviously then $\Gamma \models \psi_i$.

Case 3. There are $j, k < i$ such that φ_j is $\varphi_k \to \varphi_i$. Suppose that $\overline{A}$ is a model of Γ and $a : \omega \to A$. Then $\overline{A} \models \varphi_k[a]$ by the inductive hypothesis, and also $\overline{A} \models (\varphi_k \to \varphi_i)[a]$ by the inductive hypothesis. Thus $\overline{A} \models \varphi_k[a]$ implies that $\overline{A} \models \varphi_i[a]$, so $\overline{A} \models \varphi_i[a]$.

Case 3. There exist $j < i$ and $k \in \omega$ such that φ_i is $\forall v_k \varphi_j$. Given $u \in A$, we want to show that $\overline{A} \models \varphi_j[a^k_u]$; but this follows from the inductive hypothesis. □

One form of the completeness theorem, proved in the next chapter, is that, conversely, $\Gamma \models \varphi$ implies that $\Gamma \vdash \varphi$.

The standard foundation of mathematics is embodied in the set $\Gamma = \mathrm{ZFC}$ of the Zermelo-Fraenkel axioms for set theory with choice. The logical facts in this chapter form a prerequisite for a rigorous treatment of set theory. The language for set theory has just one non-logical constant, a binary relation symbol $\in$. Instead of $\in v_i v_j$ we write $v_i \in v_j$. ZFC consists of the following formulas.

Axiom 1. (Extensionality) If two sets have the same members, then they are equal. Formally:

$$\forall v_0 \forall v_1 [\forall v_2 (v_2 \in v_0 \leftrightarrow v_2 \in v_1) \to v_0 = v_1].$$

Axiom 2. (Comprehension) Given any set z and any property φ, there is a subset of z consisting of those elements of z with the property φ.

Formally, for any formula φ in which v_1 does not appear,

$$\exists v_1 \forall v_0 (v_0 \in v_1 \leftrightarrow v_0 \in v_2 \wedge \varphi).$$

Axiom 3. (Pairing) For any sets x, y there is a set which has them as members (possibly along with other sets). Formally:

$$\exists v_2 (v_0 \in v_2 \wedge v_1 \in v_2).$$

Axiom 4. (Union) For any family $\mathscr{A}$ of sets, we can form a new set A which has as elements all elements which are in at least one member of $\mathscr{A}$ (maybe A has even more elements). Formally:

$$\exists v_0 \forall v_1 \forall v_2 (v_2 \in v_1 \wedge v_1 \in v_3 \to v_1 \in v_0).$$

Axiom 5. (Power set) For any set x, there is a set which has as elements all subsets of x, and again possibly has more elements. Formally:

$$\exists v_1 \forall v_2 [\forall v_3 (v_3 \in v_2 \to v_3 \in v_0) \to v_2 \in v_1].$$

Axiom 6. (Infinity) There is a set which intuitively has infinitely many elements:

$$\begin{aligned}&\exists v_0 [\exists v_1 [v_1 \in v_0 \wedge \forall v_2 (\neg (v_2 \in v_1))] \wedge \\ &\forall v_1 [v_1 \in v_0 \to \exists v_2 [v_2 \in v_0 \wedge \forall v_3 (v_3 \in v_2 \leftrightarrow v_3 \in v_1 \vee v_3 = v_1)]]].\end{aligned}$$

If we take the smallest set v_0 with these properties we get the natural numbers.

Axiom 7. (Replacement) If a function has domain a set, then its range is also a set. Here we use the intuitive notion of a function.

$$\forall v_0 [v_0 \in v_1 \to \exists v_2 [\varphi \wedge \forall v_3 [\varphi' \to v_2 = v_3]]] \to \exists v_4 \forall v_0 [v_0 \in v_1 \to \exists v_2 \in v_4 \wedge \varphi].$$

Here φ is a formula in which v_3 and v_4 do not occur, and φ' is obtained from φ by replacing all occurrences of v_2 by v_3.

Axiom 8. (Foundation) Every nonempty set v_0 has a member y which has no elements in common with v_0. This is a somewhat mysterious axiom which rules out such anti-intuitive situations as $a \in a$ or $a \in b \in a$.

$$\forall v_0 [\exists v_1 (v_1 \in v_0) \to \exists v_1 [v_1 \in v_0 \wedge \forall v_2 (v_2 \in v_1 \to \neg (v_2 \in v_0))]]$$

Axiom 9. (Choice) For any family $\mathscr{A}$ of nonempty sets such that no two members of $\mathscr{A}$ have an element in common, there is a set B having exactly one element in common with each member of $\mathscr{A}$.

$$\begin{aligned}&\forall v_1 \in v_0 \exists v_2 (v_2 \in v_1) \wedge \forall v_1 \forall v_2 [v_1 \in v_0 \wedge v_2 \in v_0 \wedge \neg (v_1 = v_2) \to \forall v_3 [v_3 \in v_1 \to \neg (v_3 \in v_2)] \\ &\to \exists v_1 \forall v_2 [v_2 \in v_0 \to \exists v_3 [v_3 \in v_1 \wedge v_3 \in v_2 \wedge \forall v_4 [v_4 \in v_1 \wedge v_4 \in v_2 \to v_4 = v_3]]]]\end{aligned}$$

In principle, any theorem in mathematics is a formula φ such that ZFC $\vdash \varphi$. A course in set theory usually develops the purely set-theoretical portion of mathematics, to the extent needed for the rest of mathematics.

In this chapter we will show that many definite formulas φ are such that $\vdash \varphi$. We begin with tautologies.

Lemma 3.3. *$\vdash \varphi$ for any first-order tautology φ.*

Proof. Let χ be a sentential tautology, and let $\langle \psi_0, \psi_1, \ldots \rangle$ be a sequence of first-order formulas such that φ is obtained from χ by replacing each sentential variable S_i by ψ_i. For each sentential formula θ, let θ' be obtained from θ by replacing each sentential variable S_i by ψ_i. By Theorem 1.20, $\vdash \chi$ (in the sentential sense). Hence there is a sentential proof $\langle \theta_0, \ldots, \theta_m \rangle$ with $\theta_m = \chi$. We claim that $\langle \theta'_0, \ldots, \theta'_m \rangle$ is a first-order proof. Since $\theta'_m = \chi' = \varphi$, this will prove the lemma. If $i \leq m$ and θ_i is a (sentential) axiom, then θ'_i is the corresponding first-order axiom:

$$[\rho \to (\sigma \to \rho)]' = [\rho' \to (\sigma' \to \rho')];$$
$$[[\rho \to (\sigma \to \tau] \to [(\rho \to \sigma) \to (\rho \to \tau)]]' =$$
$$[[\rho' \to (\sigma' \to \tau')] \to [(\rho' \to \sigma') \to (\rho' \to \tau')]];$$
$$[(\neg\rho \to \neg\sigma) \to (\sigma \to \rho)]' = [(\neg\rho' \to \neg\sigma') \to (\sigma' \to \rho')].$$

If $j, k < i$ and θ_k is $\theta_j \to \theta_i$, then θ'_k is $\theta'_j \to \theta'_i$. □

We proceed with simple theorems concerning equality.

Proposition 3.4. $\vdash \sigma = \sigma$ *for any term* σ.

Proof. The following is a $\emptyset$-proof; on the left is the entry number, and on the right a justification. Let v_i be a variable not occurring in σ.

(1)	$v_i = \sigma \to (v_i = \sigma \to \sigma = \sigma)$	(L5)
(2)	$[v_i = \sigma \to (v_i = \sigma \to \sigma = \sigma)] \to [\neg(\sigma = \sigma) \to \neg(v_i = \sigma)]$	(taut.)
(3)	$\neg(\sigma = \sigma) \to \neg(v_i = \sigma)$	((1), (2), MP)
(4)	$\forall v_i[\neg(\sigma = \sigma) \to \neg(v_i = \sigma)]$	((3), gen.)
(5)	$\forall v_i[\neg(\sigma = \sigma) \to \neg(v_i = \sigma)] \to [\forall v_i \neg(\sigma = \sigma) \to \forall v_i \neg(v_i = \sigma)]$	(L2)
(6)	$\forall v_i \neg(\sigma = \sigma) \to \forall v_i \neg(v_i = \sigma)$	(4), (5), MP
(7)	$\neg(\sigma = \sigma) \to \forall v_i \neg(\sigma = \sigma)$	(L3)
(8)	$(7) \to [(6) \to [\neg(\sigma = \sigma) \to \forall v_i \neg(v_i = \sigma)]$	(taut.)
(9)	$(6) \to [\neg(\sigma = \sigma) \to \forall v_i \neg(v_i = \sigma)]$	(7), (8), MP
(10)	$\neg(\sigma = \sigma) \to \forall v_i \neg(v_i = \sigma)$	(6), (9), MP
(11)	$(10) \to [\exists v_i (v_i = \sigma) \to \sigma = \sigma]$	(taut.)
(12)	$\exists v_i (v_i = \sigma) \to \sigma = \sigma$	(10), (11), MP
(13)	$\exists v_i (v_i = \sigma)$	(L4)
(14)	$(13) \to [(12) \to \sigma = \sigma]$	(L1)
(15)	$(12) \to \sigma = \sigma$	((13), (14), MP)
(16)	$\sigma = \sigma$	((12), (15), MP)

□

Proposition 3.5. $\vdash \sigma = \tau \to \tau = \sigma$ *for any terms* σ, τ.

Proof. By (L5) we have

$$\vdash \sigma = \tau \to (\sigma = \sigma \to \tau = \sigma);$$

and by Proposition 3.4 we have $\vdash \sigma = \sigma$. Now

$$\sigma = \sigma \to ([\sigma = \tau \to (\sigma = \sigma \to \tau = \sigma)] \to (\sigma = \tau \to \tau = \sigma))$$

is a tautology, so $\vdash \sigma = \tau \to \tau = \sigma$. □

Proposition 3.6. $\vdash \sigma = \tau \to (\tau = \rho \to \sigma = \rho)$ *for any terms* σ, τ, ρ.

Proof. By (L5), $\vdash \tau = \sigma \to (\tau = \rho \to \sigma = \rho)$. By Propostition 3.5, $\vdash \sigma = \tau \to \tau = \sigma$. Now

$$(\sigma = \tau \to \tau = \sigma) \to ([\tau = \sigma \to (\tau = \rho \to \sigma = \rho)] \to [\sigma = \tau \to (\tau = \rho \to \sigma = \rho)])$$

is a tautology, so $\vdash \sigma = \tau \to (\tau = \rho \to \sigma = \rho)$. □

Proposition 3.7. *If* $\mathbf{F}$ *is an* m*-ary function symbol and* $\sigma_0, \ldots, \sigma_{m-1}$ *and* $\tau_0, \ldots, \tau_{m-1}$ *are terms, then*

$$\vdash \bigwedge_{i<m} (\sigma_i = \tau_i) \to \mathbf{F}\sigma_0 \ldots \sigma_{m-1} = \mathbf{F}\tau_0 \ldots \tau_{m-1}.$$

Proof. For each $i < m$ let φ_i be the following instance of (L7):

$$\sigma_i = \tau_i \to \mathbf{F}\tau_0 \ldots \tau_{i-1}\sigma_i\sigma_{i+1} \ldots \sigma_{m-1} = \mathbf{F}\tau_0 \ldots \tau_{i-1}\tau_i\sigma_{i+1} \ldots \sigma_{m-1}.$$

Note that φ_0 is

$$\sigma_0 = \tau_0 \to \mathbf{F}\sigma_0 \ldots \sigma_{m-1} = \mathbf{F}\tau_0\sigma_1 \ldots \sigma_{m-1}$$

and φ_{m-1} is

$$\sigma_{m-1} = \tau_{m-1} \to \mathbf{F}\tau_0 \ldots \tau_{m-2}\sigma_{m-1} = \mathbf{F}\tau_0 \ldots \tau_{m-1}.$$

Now we claim that for all $j \leq m$,

$$(*) \qquad \vdash \bigwedge_{i<m} (\sigma_i = \tau_i) \to \mathbf{F}\sigma_0 \ldots \sigma_{m-1} = \mathbf{F}\tau_0 \ldots \tau_{j-1}\sigma_j\sigma_{j+1} \ldots \sigma_{m-1}.$$

We prove this by induction on j. For $j = 0$, $(*)$ is

$$\vdash \bigwedge_{i<m} (\sigma_i = \tau_i) \to \mathbf{F}\sigma_0 \ldots \sigma_{m-1} = \mathbf{F}\sigma_0 \ldots \sigma_{m-1},$$

and this is true by Proposition 3.4 and a tautology. Now assume that $(*)$ holds for j, with $j < m$. Now the following is an instance of Proposition 3.6:

$$\begin{aligned}\vdash &\mathbf{F}\sigma_0 \ldots \sigma_{m-1} = \mathbf{F}\tau_0 \ldots \tau_{j-1}\sigma_j\sigma_{j+1} \ldots \sigma_{m-1} \to \\ &[\mathbf{F}\tau_0 \ldots \tau_{j-1}\sigma_j\sigma_{j+1} \ldots \sigma_{m-1} = \mathbf{F}\tau_0 \ldots \tau_j\sigma_{j+1} \ldots \sigma_{m-1} \to \\ &\mathbf{F}\sigma_0 \ldots \sigma_{m-1} = \mathbf{F}\tau_0 \ldots \tau_j\sigma_{j+1} \ldots \sigma_{m-1}].\end{aligned}$$

Hence a tautology and φ_j gives $(*)$ for $j+1$. This finishes the inductive proof of $(*)$. The case $j = m$ gives the assertion of the proposition. $\square$

The following proposition is very similar, in statement and proof, to Proposition 3.7.

Proposition 3.8. *If* $\mathbf{R}$ *is an* m*-ary function symbol and* $\sigma_0, \ldots, \sigma_{m-1}$ *and* $\tau_0, \ldots, \tau_{m-1}$ *are terms, then*

$$\vdash \bigwedge_{i<m} (\sigma_i = \tau_i) \to (\mathbf{R}\sigma_0 \ldots \sigma_{m-1} \leftrightarrow \mathbf{R}\tau_0 \ldots \tau_{m-1}).$$

Proof. First we claim that for each $i < m$ we have

$$(1) \qquad \vdash \sigma_i = \tau_i \to (\mathbf{R}\tau_0 \ldots \tau_{i-1}\sigma_i\sigma_{i+1} \ldots \sigma_{m-1} \leftrightarrow \mathbf{R}\tau_0 \ldots \tau_{i-1}\tau_i\sigma_{i+1} \ldots \sigma_{m-1}).$$

In fact, two instances of (L8) are as follows:

$$(2) \qquad \sigma_i = \tau_i \to (\mathbf{R}\tau_0 \ldots \tau_{i-1}\sigma_i\sigma_{i+1} \ldots \sigma_{m-1} \to \mathbf{R}\tau_0 \ldots \tau_{i-1}\tau_i\sigma_{i+1} \ldots \sigma_{m-1}).$$

$$(3) \qquad \tau_i = \sigma_i \to (\mathbf{R}\tau_0 \ldots \tau_i\sigma_{i+1} \ldots \sigma_{m-1} \to \mathbf{R}\tau_0 \ldots \tau_{i-1}\sigma_i\sigma_{i+1} \ldots \sigma_{m-1}).$$

Now the following is a tautology: $(\sigma_i = \tau_i \to \tau_i = \sigma_i) \to [(2) \to ((3) \to (1))]$. Hence from (2) and (3) and Proposition 3.5 we obtain (1). Let the formula in (1) be φ_i.

Note that φ_0 is

$$\sigma_0 = \tau_0 \to (\mathbf{R}\sigma_0 \ldots \sigma_{m-1} \leftrightarrow \mathbf{R}\tau_0\sigma_1 \ldots \sigma_{m-1})$$

and φ_{m-1} is

$$\sigma_{m-1} = \tau_{m-1} \to (\mathbf{R}\tau_0 \ldots \tau_{m-2}\sigma_{m-1} \leftrightarrow \mathbf{R}\tau_0 \ldots \tau_{m-1}).$$

Now we claim that for all $j \leq m$,

$$(*) \qquad \vdash \bigwedge_{i<m} (\sigma_i = \tau_i) \to (\mathbf{R}\sigma_0 \ldots \sigma_{m-1} \leftrightarrow \mathbf{R}\tau_0 \ldots \tau_{j-1}\sigma_j\sigma_{j+1} \ldots \sigma_{m-1}).$$

We prove this by induction on j. For $j = 0$, $(*)$ is

$$\vdash \bigwedge_{i<m} (\sigma_i = \tau_i) \to (\mathbf{R}\sigma_0 \ldots \sigma_{m-1} \leftrightarrow \mathbf{R}\sigma_0 \ldots \sigma_{m-1}),$$

and this is a tautology. Now assume that $(*)$ holds for j, with $j < m$. Now the following is a tautology:

$$\begin{aligned}\vdash &(\mathbf{R}\sigma_0 \ldots \sigma_{m-1} \leftrightarrow \mathbf{R}\tau_0 \ldots \tau_{j-1}\sigma_j\sigma_{j+1} \ldots \sigma_{m-1}) \to \\ &[(\mathbf{R}\tau_0 \ldots \tau_{j-1}\sigma_j\sigma_{j+1} \ldots \sigma_{m-1} \leftrightarrow \mathbf{R}\tau_0 \ldots \tau_j\sigma_{j+1} \ldots \sigma_{m-1}) \to \\ &(\mathbf{R}\sigma_0 \ldots \sigma_{m-1} \leftrightarrow \mathbf{R}\tau_0 \ldots \tau_j\sigma_{j+1} \ldots \sigma_{m-1})].\end{aligned}$$

Hence a tautology and φ_j give $(*)$ for $j+1$. This finishes the inductive proof of $(*)$. The case $j = m$ gives the assertion of the proposition. □

We now give several results expressing the principle of substitution of equals for equals. The main fact is expressed in Theorem 3.18, which says that under certain conditions the formula $\sigma = \tau \to (\varphi \leftrightarrow \psi)$ is provable, where ψ is obtained from φ by replacing some occurrences of σ by τ.

Lemma 3.9. *If σ and τ are terms, φ and ψ are formulas, v_i is a variable not occurring in σ or τ, and $\vdash \sigma = \tau \to (\varphi \to \psi)$, then $\vdash \sigma = \tau \to (\forall v_i \varphi \to \forall v_i \psi)$.*

Proof.

(1)	$\vdash \forall v_i[\sigma = \tau \to (\varphi \to \psi)]$	(hypothesis, gen.)
(2)	$\vdash \forall v_i(\sigma = \tau) \to \forall v_i(\varphi \to \psi)]$	(from (1), using (L2))
(3)	$\vdash \forall v_i(\varphi \to \psi) \to (\forall v_i \varphi \to \forall v_i \psi)$	((L2))
(4)	$\vdash \sigma = \tau \to \forall v_i(\sigma = \tau)$.	((L3))

Now putting (2)–(4) together with a tautology gives the lemma. □

To proceed further we need to discuss the notion of free and bound occurrences of variables and terms. This depends on the notion of a subformula. Recall that a formula is just a finite sequence of positive integers, subject to certain conditions. Atomic equality formulas have the form $\sigma = \tau$ for some terms σ, τ, and $\sigma = \tau$ is defined to be $\langle 3 \rangle^\frown \sigma^\frown \tau$. Atomic non-equality formulas have the form $\mathbf{R}\sigma_0 \dots \sigma_{m-1}$ for some m, some m-ary relation symbol $\mathbf{R}$, and some terms $\sigma_0, \dots, \sigma_{m-1}$. $\mathbf{R}$ is actually some positive integer k greater than 5 and not divisible by 5, and $\mathbf{R}\sigma_0 \dots \sigma_{m-1}$ is the sequence $\langle k \rangle^\frown \sigma_0^\frown \cdots^\frown \sigma_{m-1}$. Non-atomic formulas have the form

$\neg\varphi = \langle 1 \rangle^\frown \varphi$,
$\varphi \to \psi = \langle 2 \rangle^\frown \varphi^\frown \psi$, or
$\forall v_s \varphi = \langle 4, 5(s+1) \rangle^\frown \varphi$.

Thus every formula begins with one of the integers 1,2,3,4 or some positive integer greater than 5 not divisible by 5 which is a relation symbol. This helps motivate the following propositions.

Proposition 3.10. *If $\sigma = \langle \sigma_0, \dots, \sigma_{k-1} \rangle$ is a term, then each σ_i is either of the form $5m$ with m a positive integer, or it is an odd integer greater than 5 which is a function symbol or individual constant.*

Proof. We prove this by induction on σ, thus using Proposition 2.1. The proposition is obvious if σ is a variable or individual constant. Suppose that $\mathbf{F}$ is a function symbol of rank m, $\tau_0, \dots, \tau_{m-1}$ are terms, and σ is $\mathbf{F}\tau_0 \dots \tau_{m-1}$, where we assume the truth of the proposition for $\tau_0, \dots, \tau_{m-1}$. Suppose that $i < k$. If $i = 0$, then σ_i is $\mathbf{F}$, a function symbol. If $i > 0$, then σ_i is an entry in some τ_j, and the desired conclusion follows by the inductive hypothesis. □

Proposition 3.11. *Let $\varphi = \langle \varphi_0, \dots \varphi_{k-1} \rangle$ be a formula, suppose that $i < k$, and φ_i is one of the integers 1,2,3,4 or a positive integer greater than 5 which is a relation symbol. Then there is a unique segment $\langle \varphi_i, \varphi_{i+1}, \dots, \varphi_j \rangle$ of φ which is a formula.*

Proof. We prove this by induction on φ, thus using Proposition 2.5. We assume the hypothesis of the proposition. First suppose that φ is an atomic equality formula $\sigma = \tau$ with σ and τ terms. Thus $\sigma = \tau$ is the sequence $\langle 1 \rangle^\frown \sigma^\frown \tau$. Now by Proposition 2.2(ii), no entry of a term is among the integers $1, 2, 3, 4$ or is a positive integer greater than 5 which is a relation symbol. It follows from the assumption about i that $i = 0$, and hence the desired segment of φ is φ itself. It is unique by Proposition 2.6(iii). Second suppose that φ is an atomic non-equality formula $\mathbf{R}\sigma_0 \dots \sigma_{m-1}$ with $\mathbf{R}$ an m-ary relation symbol and $\sigma_0, \dots, \sigma_{m-1}$ terms. This is very similar to the first case. $\mathbf{R}\sigma_0 \dots \sigma_{m-1}$ is the sequence $\langle \mathbf{R} \rangle^\frown \sigma_0^\frown \cdots^\frown \sigma_{m-1}$. By Proposition 2.2(ii) i must be 0, and hence the desired segment of φ is φ itself. It is unique by Proposition 2.6(iii).

Now assume inductively that φ is $\neg\psi$; so φ is $\langle 1 \rangle^\frown \psi$. If $i = 0$, then φ itself is the desired segment, unique by Proposition 2.6(iii). If $i > 0$, then $\varphi_i = \psi_{i-1}$, where $\psi = \langle \psi_0, \dots, \psi_{k-1} \rangle$. By the inductive hypothesis there is a segment $\langle \psi_{i-1}, \psi_i, \dots, \psi_j \rangle$ of ψ which is a formula. This gives a segment $\langle \varphi_i, \varphi_{i+1}, \dots, \varphi_{j+1} \rangle$ of φ which is a formula; it is unique by Proposition 2.6(iii).

Assume inductively that φ is $\psi \to \chi$ for some formulas ψ, χ. So φ is $\langle 2 \rangle^\frown \psi^\frown \chi$. If $i = 0$, then φ itself is the required segment, unique by Proposition 2.6(iii). Now suppose that $i > 0$. Now we have $\psi = \langle \varphi_1, \dots, \varphi_m \rangle$ and $\chi = \langle \varphi_{m+1}, \dots, \varphi_{k-1} \rangle$ for some m. If $1 \leq i \leq m$, then by the inductive assumption there is a segment $\langle \varphi_i, \varphi_{i+1}, \dots, \varphi_n \rangle$ of ψ which is a formula. This is also a segment of φ, and it is unique by Proposition 2.6(iii). If $m + 1 \leq i \leq k - 1$, a similar argument with χ gives the desired result.

Finally, assume inductively that φ is $\forall v_s \psi$ with ψ some formula and $s \in \omega$. We leave this case to an exercise. □

The segment of φ asserted to exist in Proposition 3.11 is called the *subformula of* φ beginning at i. For example, consider the formula $\varphi \stackrel{\text{def}}{=} \forall v_0 [v_0 = v_2 \to v_0 = v_2]$. The formula $v_0 = v_1$ occurs in two places in φ. In detail, φ is the sequence $\langle 4, 5, 2, 3, 5, 15, 3, 5, 15 \rangle$. Thus

$\varphi_0 = 4$;
$\varphi_1 = 5$;
$\varphi_2 = 2$;
$\varphi_3 = 3$;
$\varphi_4 = 5$;
$\varphi_5 = 15$;
$\varphi_6 = 3$;
$\varphi_7 = 5$;
$\varphi_8 = 15$;

On the other hand, $v_0 = v_2$ is the formula $\langle 3, 5, 15 \rangle$. It occurs in φ beginning at 3, and also beginning at 6.

Now a variable v_s is said to *occur bound* in φ at the j-th position iff with $\varphi = \langle \varphi_0, \dots, \varphi_{m-1} \rangle$, we have $\varphi_j = v_s$ and there is a subformula of φ of the form $\forall v_s \psi =$

$\langle \varphi_i, \varphi_{i+1}, \ldots, \varphi_m \rangle$ with $i+1 \leq j \leq m$. If a variable v_s occurs at the j-th position of φ but does not occur bound there, then that occurrence is said to be *free*. We give some examples. Let φ be the formula $v_0 = v_1 \to v_1 = v_2$. All the occurrences of v_0, v_1, v_2 are free occurrences in φ. Note that as a sequence φ is $\langle 2, 3, 5, 10, 3, 10, 15 \rangle$; so $\varphi_0 = 2$, $\varphi_1 = 3$, $\varphi_2 = 5$, $\varphi_3 = 10$, $\varphi_4 = 3$, $\varphi_5 = 10$, and $\varphi_6 = 15$. The variable v_0, which is the integer 5, occurs free at the 2-nd position. The variable v_1, which is the integer 10, occurs free at the 3rd and 5th positions. The variable v_2, which is the integer 15, occurs free at the 6th position.

Now let ψ be the formula $v_0 = v_1 \to \forall v_1(v_1 = v_2)$. Then the first occurence of v_1 is free, but the other two occurrences are bound. As a sequence, ψ is $\langle 2, 3, 5, 10, 4, 10, 3, 10, 15 \rangle$. The variable v_1 occurs free at the 3rd position, and bound at the 5th and 7th positions.

We also need the notion of a term occurring in another term, or in a formula. The following two propositions are proved much like 3.11.

Proposition 3.12. *If $\sigma = \langle \sigma_0, \ldots, \sigma_{m-1} \rangle$ is a term and $i < m$, then there is a unique term τ which is a segment of σ beginning at i.*

Proof. We prove this by induction on σ. For σ a variable or individual constant, we have $m = 1$ and so $i = 0$, and σ itself is the only possibility for τ. Now suppose that the proposition is true for terms $\tau_0, \ldots \tau_{n-1}$, $\mathbf{F}$ is an n-ary function symbol, and σ is $\mathbf{F}\tau_0 \ldots \tau_{n-1}$. If $i = 0$, then σ itself begins at i, and it is the only term beginning at i by Proposition 2.2(iii). If $i > 0$, then i is inside some term τ_k, and so by the inductive assumption there is a term which is a segment of τ_k beginning there; this term is a segment of σ too, and it is unique by Proposition 2.2(iii). □

Under the assumptions of Proposition 3.12, we say that τ occurs in σ beginning at i.

Proposition 3.13. *If $\varphi = \langle \varphi_0, \ldots, \varphi_{m-1} \rangle$ is a formula, $i < m$, and φ_i is a variable, an individual constant, or a function symbol, then there is a unique segment of φ beginning at i which is a term.*

Proof. We prove this by induction on φ. First suppose that φ is an atomic equality formula $\sigma = \tau$ for some terms σ, τ. Thus φ is $\langle 3 \rangle^\frown \sigma^\frown \tau$. So $i > 0$, and hence i is inside σ or τ. If i is inside σ, then by Proposition 3.12, there is a term which is a segment of σ beginning at i; it is also a segment of φ, and it is unique by Proposition 2.2(iii). Similarly for τ.

We leave the other parts of the proof to an exercise. □

Under the assumptions of Proposition 3.12, we say that the indicated segment occurs in φ beginning at i.

We now extend the notions of free and bound occurrences to terms. Let σ be a term which occurs as a segment in a formula φ. Say that $\varphi = \langle \varphi_0, \ldots, \varphi_{m-1} \rangle$ and $\sigma = \langle \varphi_i, \ldots \varphi_k \rangle$. We say that this occurrence of σ in φ is *bound* iff there is a variable v_s which occurs bound in φ at some place t with $i \leq t \leq k$; the occurrence of σ is *free* iff there is no such variable.

We give some examples. The term $v_0 + v_1$ is bound in its only occurrence in the formula $\forall v_0(v_0 + v_1 = v_2)$. The same term is bound in its first occurrence and free in its second occurrence in the formula $\forall v_0(v_0 + v_1 = v_2) \wedge v_0 + v_1 = v_0$.

Suppose that σ, τ, ρ are terms, and τ occurs in σ beginning at i. By the *result of replacing that occurrence of τ by ρ* we mean the following sequence ξ. Say σ, τ, ρ have domains (lengths) m, n, p respectively. Then ξ is the sequence

$$\langle \sigma_0, \ldots, \sigma_{i-1}, \rho_0, \ldots, \rho_{p-1}, \sigma_{i+n}, \ldots, \sigma_{m-1} \rangle.$$

Put another way, if σ is $\theta^\frown\tau^\frown\eta$ with θ of length i, then ξ is $\theta^\frown\rho^\frown\eta$.

Proposition 3.14. *Suppose that σ, τ, ρ are terms, and the sequence ξ is obtained from ρ by replacing one occurrence of σ by τ. Then ξ is a term.*

Proof. We prove this by induction on ρ, thus by using Proposition 2.1. If ρ is a variable or an individual constant, then σ must be ρ itself, and ξ is τ, which is a term. Now suppose that ρ is $\mathbf{F}\eta_0 \ldots \eta_{m-1}$ for some m-ary function symbol $\mathbf{F}$ and some terms $\eta_0, \ldots, \eta_{m-1}$, and the proposition holds for $\eta_0, \ldots, \eta_{m-1}$. Say the occurrence of σ in ρ begins at i. If $i = 0$, then σ equals ρ, and hence ξ equals τ, which is a term. If $i > 0$, then i is inside some η_j, and hence the occurrence of σ is actually an occurrence in η_j by Proposition 2.2(iii). Replacing this occurrence of σ in η_j by τ we obtain a term by the inductive hypothesis; call this term η'_j. It follows that ξ is $\mathbf{F}\eta_0 \ldots \eta_{j-1}\eta'_j, \eta_{j+1} \ldots \eta_{m-1}$, which is a term. □

As an example, consider the term $v_0 \bullet (v_1 + v_2)$ in the language for $(\mathbb{Q}, +, \cdot)$. Replacing the occurrence of v_1 by $v_0 \bullet v_1$ we obtain the term $v_0 \bullet ((v_0 \bullet v_1) + v_2)$. Writing this out in detail, we start with the sequence $\langle 9, 5, 7, 10, 15 \rangle$ and end with the sequence $\langle 9, 5, 7, 9, 5, 10, 15 \rangle$.

Our first form of subsitution of equals for equals only involves terms:

Theorem 3.15. *If σ, τ, ρ are terms, and ξ is a sequence obtained from ρ by replacing an occurrence of σ in ρ by τ, then ξ is a term and $\vdash \sigma = \tau \to \rho = \xi$.*

Proof. ξ is a term by Proposition 3.14. Now we proceed by induction on ρ. If ρ is a variable or an individual constant, then σ must be the same as ρ, since ρ has length 1 and σ occurs in ρ. Then ξ is τ, and $\sigma = \tau \to \rho = \xi$ is $\sigma = \tau \to \sigma = \tau$, a tautology. So the proposition is true in this case.

Now assume inductively that ρ is $\mathbf{F}\eta_0 \ldots \eta_{m-1}$ with $\mathbf{F}$ an m-ary function symbol and $\eta_0, \ldots, \eta_{m-1}$ terms. There are two possibilities for the occurrence of σ. First, possibly σ is the same as ρ. Then ξ is τ, and again we have the tautology $\sigma = \tau \to \sigma = \tau$, Second, the occurrence of σ is within some η_i. Then by the inductive hypothesis, $\vdash \sigma = \tau \to \eta_i = \eta'_i$, where η'_i is obtained from η_i by replacing the indicated occurrence of σ by τ. Now an instance of (L7) is

$$\eta_i = \eta'_i \to \mathbf{F}\eta_0 \ldots \eta_{i-1} \ldots \eta_i\eta_{i+1} \ldots \eta_{m-1} = \mathbf{F}\eta_0 \ldots \eta_{i-1} \ldots \eta'_i\eta_{i+1} \ldots \eta_{m-1}.$$

Putting this together with $\vdash \sigma = \tau \to \eta_i = \eta'_i$ and a tautology gives $\vdash \sigma = \tau \to \rho = \xi$. □

Proposition 3.16. *Suppose that φ is a formula and σ, τ are terms. Suppose that σ occurs at the i-th place in φ, and if $i > 0$ and $\varphi_{i-1} = \forall$, then τ is a variable. Let the sequence ψ be obtained from φ by replacing that occurrence of σ by τ. Then ψ is a formula.*

Proof. Exercise. □

For the exact definition of ψ see the description before Proposition 3.14.

Lemma 3.17. *Suppose that σ and τ are terms, φ is a formula, and ψ is obtained from φ by replacing one free occurrence of σ in φ by τ, such that the occurrence of τ that results is free in ψ. Then $\vdash \sigma = \tau \to (\varphi \leftrightarrow \psi)$.*

Proof. We proceed by induction on φ. First suppose that φ is an atomic equality formula $\rho = \xi$. If the occurrence of σ that is replaced is in ρ, let ρ' be the resulting term. Then by Proposition 3.15, $\vdash \sigma = \tau \to \rho = \rho'$. Now (L5) gives $\vdash \rho = \rho' \to (\rho = \xi \to \rho' = \xi)$. Putting these two together with a tautology gives $\vdash \sigma = \tau \to (\rho = \xi \to \rho' = \xi)$. By symmetry, $\vdash \sigma = \tau \to (\rho' = \xi \to \rho = \xi)$. Hence $\vdash \sigma = \tau \to (\rho = \xi \leftrightarrow \rho' = \xi)$.

If the occurrence of σ that is replaced is in ξ, a similar argument using (L6) works.

Second, suppose that φ is an atomic non-equality formula $\mathbf{R}\rho_0 \dots \rho_{m-1}$, with $\mathbf{R}$ an m-ary relation symbol and $\rho_0, \dots, \rho_{m-1}$ terms. Say that the occurrence of σ that is replaced by τ is in ρ_i, the resulting term being ρ_i'. Then by Proposition 3.15, $\vdash \sigma = \tau \to \rho_i = \rho_i'$. By (L8) we have

$$\vdash \rho_i = \rho_i' \to (\mathbf{R}\rho_0 \dots \rho_{m-1} \to \mathbf{R}\rho_0 \dots \rho_{i-1}\rho_i'\rho_{i+1} \dots \rho_{m-1}),$$

so by a tautology we get from these two facts

$$\vdash \sigma = \tau \to (\mathbf{R}\rho_0 \dots \rho_{m-1} \to \mathbf{R}\rho_0 \dots \rho_{i-1}\rho_i'\rho_{i+1} \dots \rho_{m-1}),$$

and by symmetry

$$\vdash \sigma = \tau \to (\mathbf{R}\rho_0 \dots \rho_{i-1}\rho_i'\rho_{i+1} \dots \rho_{m-1} \to \mathbf{R}\rho_0 \dots \rho_{m-1}),$$

and then another tautology gives

$$\vdash \sigma = \tau \to (\mathbf{R}\rho_0 \dots \rho_{m-1} \leftrightarrow \mathbf{R}\rho_0 \dots \rho_{i-1}\rho_i'\rho_{i+1} \dots \rho_{m-1}),$$

This finishes the atomic cases. Now suppose inductively that φ is $\neg\chi$. The occurrence of σ in φ that is replaced actually occurs in χ; let χ' be the result of replacing that occurrence of σ by τ. Now the occurrence of σ in χ is free in χ. In fact, suppose that $\forall v_i\theta$ is a subformula of χ which has as a segment the indicated occurrence of σ, and v_i occurs in σ. Then $\forall v_i\theta$ is also a subformula of φ, contradicting the assumption that the occurrence of σ is free in φ. Similarly the occurrence of τ in χ' which replaced the occurrence of σ is free. So by the inductive hypothesis, $\vdash \sigma = \tau \to (\chi \leftrightarrow \chi')$, and hence a tautology gives $\vdash \sigma = \tau \to (\neg\chi \leftrightarrow \neg\chi')$, i.e., $\vdash \sigma = \tau \to (\varphi \leftrightarrow \psi)$.

We leave the case of an implication to an exercise.

Finally, suppose that φ is $\forall v_i \rho$. Then the occurrence of σ in φ that is replaced is in ρ. Let ρ' be obtained from ρ by replacing that occurrence of σ by τ. The occurrence of σ in ρ must be free since it is free in φ, as in the treatment of $\neg$ above; similarly for τ and ρ'. Hence by the inductive hypothesis, $\vdash \sigma = \tau \to (\rho \leftrightarrow \rho')$. Now since the occurrence of σ in φ is free, the variable v_i does not occur in σ. Similarly, it does not occur in τ. Hence by Proposition 3.9 and tautologies we get $\vdash \sigma = \tau \to (\forall v_i \rho \leftrightarrow \forall v_i \rho')$, i.e., $\vdash \sigma = \tau \to (\varphi \leftrightarrow \psi)$. □

The hypothesis that the term τ is still free in the result of the replacement in this proposition is necessary for the truth of the proposition. See an exercise. This hypothesis is equivalent to saying that the occurrence of σ which is replaced is not inside a subformula of φ of the form $\forall v_i \chi$ with v_i a variable occurring in τ.

Theorem 3.18. (Substitution of equals for equals) *Suppose that φ is a formula, σ is a term, and σ occurs freely in φ starting at indices $i(0) < \cdots < i(m-1)$. Also suppose that τ is a term. Let ψ be obtained from φ by replacing each of these occurrences of σ by τ, and each such occurrence of τ is free in ψ. Then $\vdash \sigma = \tau \to (\varphi \leftrightarrow \psi)$.*

Proof. We prove this by induction on m. If $m = 0$, then φ is the same as ψ, and the conclusion is clear. Now assume the result for m, for any φ. Now assume that σ occurs freely in φ starting at indices $i(0) < \cdots < i(m)$, and no such occurrence is inside a subformula of φ of the form $\forall v_j \chi$ with v_j a variable occurring in τ. Let θ be obtained from φ by replacing the last occurrence of σ, the one beginning at $i(m)$, by τ. By Proposition 3.17, $\vdash \sigma = \tau \to (\varphi \leftrightarrow \theta)$. Now we apply the inductive hypothesis to θ and the occurrences of σ starting at $i(0), \ldots, i(m-1)$; this gives $\vdash \sigma = \tau \to (\theta \leftrightarrow \psi)$. Hence a tautology gives $\vdash \sigma = \tau \to (\varphi \leftrightarrow \psi)$, finishing the inductive proof. □

Proposition 3.19. *Suppose that φ, ψ, χ are formulas, and the sequence θ is obtained from φ by replacing an occurrence of ψ in φ by χ. Then θ is a formula.*

Proof. Exercise. □

For the exact meaning of θ see the description before Proposition 3.14.

Another form of the substitution of equals by equals principle is as follows:

Theorem 3.20. *Let φ, χ, ρ be formulas, and let ψ be obtained from φ by replacing an occurrence of χ in φ by ρ. Suppose that $\vdash \chi \leftrightarrow \rho$. Then $\vdash \varphi \leftrightarrow \psi$.*

Proof. Induction on φ. If φ is atomic, then ψ is the same as ρ, and the conclusion is clear. Suppose inductively that φ is $\neg\varphi'$. If χ is equal to φ, then ψ is equal to ρ and the conclusion is clear. Suppose that χ occurs within φ', and let ψ' be obtained from φ' by replacing that occurrence by ρ. Assume that $\vdash \chi \leftrightarrow \rho$. Then by the inductive hypothesis $\vdash \varphi' \leftrightarrow \psi'$, so $\vdash \neg\varphi' \leftrightarrow \neg\psi'$, as desired.

The case in which φ is $\varphi' \to \varphi''$ is similar. Finally, suppose that φ is $\forall v_i \varphi'$, and χ occurs within φ'. Let ψ' be obtained from φ' by replacing that occurrence by ρ. Assume that $\vdash \chi \leftrightarrow \rho$. Then $\vdash \varphi' \leftrightarrow \psi'$ by the inductive assumption. So by a tautology, $\vdash \varphi' \to \psi'$,

and then by generalization $\vdash \forall v_i(\varphi' \to \psi')$. Using (L2) we then get $\vdash \forall v_i\varphi' \to \forall v_i\psi'$. Similarly, $\vdash \forall v_i\psi' \to \forall v_i\varphi'$. Hence using a tautology, $\vdash \forall v_i\varphi' \leftrightarrow \forall v_i\psi'$. □

Now we work to prove two important logical principles: changing bound variables, and dropping a universal quantifier in favor of a term.

For any formula φ, $i \in \omega$, and term σ by $\mathrm{Subf}_\sigma^{v_i}\varphi$ we mean the result of replacing each free occurrence of v_i in φ by σ. We now work towards showing that under suitable conditions, the formula $\forall v_i\varphi \to \mathrm{Subf}_\sigma^{v_i}\varphi$ is provable. The supposition expressed in the first sentence of the following lemma will be eliminated later on.

Lemma 3.21. *Suppose that v_i does not occur bound in φ, and does not occur in the term σ.*

Assume that no free occurrence of v_i in φ is within a subformula of φ of the form $\forall v_j\chi$ with v_j a variable occurring in σ. Then $\vdash \forall v_i\varphi \to \mathrm{Subf}_\sigma^{v_i}\varphi$.

Proof.

(1)	$\vdash v_i = \sigma \to (\varphi \to \mathrm{Subf}_\sigma^{v_i}\varphi)$	(by Proposition 3.18 and a tautology)
(2)	$\vdash \varphi \to (\neg\mathrm{Subf}_\sigma^{v_i}\varphi \to \neg(v_i = \sigma))$	(using a tautology)
(3)	$\vdash \forall v_i[\varphi \to (\neg\mathrm{Subf}_\sigma^{v_i}\varphi \to \neg(v_i = \sigma))]$	(generalization)
(4)	$\vdash \forall v_i\varphi \to \forall v_i(\neg\mathrm{Subf}_\sigma^{v_i}\varphi \to \neg(v_i = \sigma))$	(using (L2))
(5)	$\vdash \forall v_i(\neg\mathrm{Subf}_\sigma^{v_i}\varphi \to \neg(v_i = \sigma)) \to (\forall v_i\neg\mathrm{Subf}_\sigma^{v_i}\varphi \to \forall v_i\neg(v_i = \sigma))$	((L2))
(6)	$\vdash \forall v_i\varphi \to (\forall v_i\neg\mathrm{Subf}_\sigma^{v_i}\varphi \to \forall v_i\neg(v_i = \sigma))$	((4), (5), a tautology)
(7)	$\vdash \neg\forall v_i\neg(v_i = \sigma) \to (\forall v_i\varphi \to \neg\forall v_i\neg\mathrm{Subf}_\sigma^{v_i}\varphi)$	((6), a tautology)
(8)	$\vdash \neg\forall v_i\neg(v_i = \sigma)$	((L4))
(9)	$\vdash \forall v_i\varphi \to \neg\forall v_i\neg\mathrm{subf}_\sigma^{v_i}\varphi)$	((7), (8), modus ponens)
(10)	$\vdash \neg\mathrm{Subf}_\sigma^{v_i}\varphi \to \forall v_i\neg\mathrm{Subf}_\sigma^{v_i}\varphi$	((L3))
(11)	$\vdash \forall v_i\varphi \to \mathrm{Subf}_\sigma^{v_i}\varphi$	((9), (10), a tautology)

□

Lemma 3.22. *If $i \neq j$, φ is a formula, v_i does not occur bound in φ, and v_j does not occur in φ at all, then $\vdash \forall v_i\varphi \to \forall v_j\mathrm{Subf}_{v_j}^{v_i}\varphi$.*

Proof.

$\vdash \forall v_i\varphi \to \mathrm{Subf}_{v_j}^{v_i}\varphi$	(by Lemma 3.21)
$\vdash \forall v_j\forall v_i\varphi \to \forall v_j\mathrm{Subf}_{v_j}^{v_i}\varphi$	(using (L2) and a tautology)
$\vdash \forall v_i\varphi \to \forall v_j\forall v_i\varphi$ (by (L3))	
$\vdash \forall v_i\varphi \to \forall v_j\mathrm{Subf}_{v_j}^{v_i}\varphi$	

□

Lemma 3.23. *If $i \neq j$, φ is a formula, v_i does not occur bound in φ, and v_j does not occur in φ at all, then $\vdash \forall v_i\varphi \leftrightarrow \forall v_j\mathrm{Subf}_{v_j}^{v_i}\varphi$.*

Proof. By Proposition 3.22 we have $\vdash \forall v_i\varphi \to \forall v_j\mathrm{Subf}_{v_j}^{v_i}\varphi$. Now v_j does not occur bound in $\mathrm{Subf}_{v_j}^{v_i}\varphi$ and v_i does not occur in $\mathrm{Subf}_{v_j}^{v_i}\varphi$ at all. Hence by Proposition 3.22 again, $\vdash \forall v_j\mathrm{Subf}_{v_j}^{v_i}\varphi \to \forall v_i\mathrm{Subf}_{v_i}^{v_j}\mathrm{Subf}_{v_j}^{v_i}\varphi$. Now $\mathrm{Subf}_{v_i}^{v_j}\mathrm{Subf}_{v_j}^{v_i}\varphi$ is actually just φ itself; so $\vdash \forall v_j\mathrm{Subf}_{v_j}^{v_i}\varphi \to \forall v_i\varphi$. Hence the proposition follows. □

For $i, j \in \omega$ and φ a formula, by $\mathrm{Subb}^{v_i}_{v_j}\varphi$ we mean the result of replacing all bound occurrences of v_i in φ by v_j. By Proposition 3.16 this gives another formula.

Proposition 3.24. *If v_i occurs bound in a formula φ, then there is a subformula $\forall v_i\psi$ of φ such that v_i does not occur bound in ψ.*

Proof. Induction on φ. Note that the statement to be proved is an implication. If φ is atomic, then v_i cannot occur bound in φ; thus the hypothesis of the implication is false, and so the implication itself is true. Now suppose inductively that φ is $\neg\chi$, and v_i occurs bound in φ. Then it occurs bound in χ, and so by the inductive hypothesis, χ has a subformula $\forall v_i\psi$ such that v_i does not occur bound in ψ. This is also a subformula of φ. The implication case is similar. Finally, suppose that φ is $\forall v_k\chi$, and v_i occurs bound in φ. If it occurs bound in χ, then by the inductive hypothesis χ has a subformula $\forall v_i\psi$ such that v_i does not occur bound in ψ; this is also a subformula of φ. If v_i does not occur bound in χ, then we must have $i = k$ since v_i occurs bound in φ, and then φ itself is the desired subformula. □

Theorem 3.25. (Change of bound variables) *If ψ_j does not occur in φ, then $\vdash \varphi \leftrightarrow \mathrm{Subb}^{v_i}_{v_j}\varphi$.*

Proof. We proceed by induction on the number m of bound occurrences of v_i in φ. If $m = 0$, then $\mathrm{Subb}^{v_i}_{v_j}\varphi$ is just φ itself, and the conclusion is clear. Now assume that $m > 0$ and the conclusion is known for all formulas with fewer than m bound occurrences of v_i. By Proposition 3.24, let $\forall v_i\psi$ be a formula occurring in φ such that v_i does not occur bound in ψ. Let k be such that v_k does not occur in φ, and hence also does not occur in ψ, and with $k \neq j$. Note that $k \neq i$ since v_k does not occur in φ while v_i does. Then by Proposition 3.23 we have

$$\vdash \forall v_i\psi \leftrightarrow \forall v_k\mathrm{Subf}^{v_i}_{v_k}\psi. \tag{1}$$

Let φ' be obtained from φ by replacing an occurrence of $\forall v_i\psi$ by $\forall v_k\mathrm{Subf}^{v_i}_{v_k}\psi$. By Theorem 3.20,

$$\vdash \varphi \leftrightarrow \varphi'. \tag{2}$$

Now v_j does not occur in φ', and φ' has fewer than m bound occurrences of v_i. Hence by the inductive hypothesis,

$$\vdash \varphi' \leftrightarrow \mathrm{Subb}^{v_i}_{v_j}\varphi'. \tag{3}$$

Now $k \neq i, j$ and v_k does not occur bound in $\mathrm{Subf}^{v_i}_{v_k}\psi$. Moreover, v_j does not occur in $\mathrm{Subf}^{v_i}_{v_k}\psi$ at all. Hence by Proposition 3.22,

$$\vdash \forall v_k\mathrm{Subf}^{v_i}_{v_k}\psi \leftrightarrow \forall v_j\mathrm{Subf}^{v_k}_{v_j}\mathrm{Subf}^{v_i}_{v_k}\psi.$$

Now clearly $\mathrm{Subf}^{v_k}_{v_j}\mathrm{Subf}^{v_i}_{v_k}\psi = \mathrm{Subf}^{v_i}_{v_j}\psi$; so

$$\vdash \forall v_k\mathrm{Subf}^{v_i}_{v_k}\psi \leftrightarrow \forall v_j\mathrm{Subf}^{v_i}_{v_j}\psi. \tag{4}$$

Now $\mathrm{Subb}^{v_i}_{v_j}\varphi$ can be obtained from $\mathrm{Subb}^{v_i}_{v_j}\varphi'$ by replacing an occurrence of $\forall v_k \mathrm{Subf}^{v_i}_{v_k}\psi$ by $\forall v_j \mathrm{Subf}^{v_i}_{v_j}\psi$. Hence by (4) and Theorem 3.20 we get

$$\vdash \mathrm{Subb}^{v_i}_{v_j}\varphi \leftrightarrow \mathrm{Subb}^{v_i}_{v_j}\varphi'. \tag{5}$$

(2), (3), and (5) now give the desired result, finishing the inductive proof. □

We can now strengthen Lemma 3.21 by eliminating one of its hypotheses; the remaining inessential hypothesis will be eliminated next.

Lemma 3.26. *Suppose that v_i does not occur in the term σ.*

Assume that no free occurrence of v_i in a formula φ is within a subformula of φ of the form $\forall v_j \chi$ with v_j a variable occurring in σ. Then $\vdash \forall v_i \varphi \to \mathrm{Subf}^{v_i}_{\sigma}\varphi$.

Proof. Choose j so that v_j does not occur in φ or in σ, with $i \neq j$. Then by the change of bound variables theorem 3.25, $\vdash \varphi \leftrightarrow \mathrm{Subb}^{v_i}_{v_j}\varphi$. From this, using generalization and (L2) we obtain

$$\vdash \forall v_i \varphi \leftrightarrow \forall v_i \mathrm{Subb}^{v_i}_{v_j}\varphi. \tag{1}$$

Now v_i does not occur bound in $\mathrm{Subb}^{v_i}_{v_j}\varphi$, and no free occurrence of v_i in $\mathrm{Subb}^{v_i}_{v_j}\varphi$ is in a subformula of $\mathrm{Subb}^{v_i}_{v_j}\varphi$ of the form $\forall v_k \psi$, with v_k a variable occurring in σ. This is true since it is true of φ, and v_j does not occur in σ. Hence by Lemma 3.21 we get

$$\vdash \forall v_i \mathrm{Subb}^{v_i}_{v_j}\varphi \to \mathrm{Subf}^{v_i}_{\sigma}\mathrm{Subb}^{v_i}_{v_j}\varphi. \tag{2}$$

Now v_i does not occur at all in $\mathrm{Subf}^{v_i}_{\sigma}\mathrm{Subb}^{v_i}_{v_j}\varphi$, so by change of bound variable,

$$\vdash \mathrm{Subf}^{v_i}_{\sigma}\mathrm{Subb}^{v_i}_{v_j}\varphi \leftrightarrow \mathrm{Subb}^{v_j}_{v_i}\mathrm{Subf}^{v_i}_{\sigma}\mathrm{Subb}^{v_i}_{v_j}\varphi. \tag{3}$$

But clearly $\mathrm{Subb}^{v_j}_{v_i}\mathrm{Subf}^{v_i}_{\sigma}\mathrm{Subb}^{v_i}_{v_j}\varphi = \mathrm{Subf}^{v_i}_{\sigma}\varphi$. Hence from (1)–(3) and tautologies we get the result of the lemma. □

Theorem 3.27. (Universal specification) *Assume that no free occurrence of v_i in a formula φ is within a subformula of φ of the form $\forall v_j \chi$ with v_j a variable occurring in a term σ. Then $\vdash \forall v_i \varphi \to \mathrm{Subf}^{v_i}_{\sigma}\varphi$.*

Proof. Choose j so that v_j does not occur in φ or in σ, with $j \neq i$. Then by Lemma 3.26, $\vdash \forall v_i \varphi \to \mathrm{Subf}^{v_i}_{v_j}\varphi$. Hence using (L2) we easily get

$$\vdash \forall v_j \forall v_i \varphi \to \forall v_j \mathrm{Subf}^{v_i}_{v_j}\varphi. \tag{1}$$

By (L3) we have

$$\vdash \forall v_i \varphi \to \forall v_j \forall v_i \varphi. \tag{2}$$

Now no free occurrence of v_j in $\mathrm{Subf}^{v_i}_{v_j}\varphi$ is within a subformula of $\mathrm{Subf}^{v_i}_{v_j}\varphi$ of the form $\forall v_k\psi$ with v_k occurring in σ; this is true because it holds for φ. Also, v_j does not occur in σ. Hence by Lemma 3.26 we have

$$\vdash \forall v_j \mathrm{Subf}^{v_i}_{v_j}\varphi \to \mathrm{Subf}^{v_j}_{\sigma}\mathrm{Subf}^{v_i}_{v_j}\varphi. \tag{3}$$

Clearly $\mathrm{Subf}^{v_j}_{\sigma}\mathrm{Subf}^{v_i}_{v_j}\varphi = \mathrm{Subf}^{v_i}_{\sigma}\varphi$, so from (1)–(3) the desired result follows. □

This finishes the fundamental things that can be proved. We now give various corollaries.

Corollary 3.28. $\vdash \forall v_i\varphi \to \varphi$. □

Proposition 3.29. *If v_i does not occur free in φ, then $\vdash \varphi \leftrightarrow \forall v_i\varphi$.*

Proof. By Corollary 3.28 we have

$$\vdash \forall v_i\varphi \to \varphi. \tag{1}$$

Now let v_j be a variable not occurring in φ. Then by a change of bound variable,

$$\vdash \varphi \leftrightarrow \mathrm{Subb}^{v_i}_{v_j}\varphi. \tag{2}$$

Hence using (L2) we easily get

$$\vdash \forall v_i \mathrm{Subb}^{v_i}_{v_j}\varphi \to \forall v_i\varphi. \tag{3}$$

Now note that v_i does not occur in $\mathrm{Subb}^{v_i}_{v_j}\varphi$. Hence by (L3) we get

$$\vdash \mathrm{Subb}^{v_i}_{v_j}\varphi \to \forall v_i \mathrm{Subb}^{v_i}_{v_j}\varphi. \tag{4}$$

Now from (1)–(4) the desired result easily follows. □

Proposition 3.30. $\vdash \forall v_i\forall v_j\varphi \leftrightarrow \forall v_j\forall v_i\varphi$, *for any formula φ and any $i, j \in \omega$.*

Proof.

$\vdash \forall v_i\forall v_j\varphi \to \varphi$	by Corollary 3.28 twice
$\vdash \forall v_i\forall v_i\forall v_j\varphi \to \forall v_i\varphi$	by (L2)
$\vdash \forall v_i\forall v_j\varphi \to \forall v_i\forall v_i\forall v_j\varphi$	using Prop. 3.29
$\vdash \forall v_i\forall v_j\varphi \to \forall v_i\varphi$	
$\vdash \forall v_j\forall v_i\forall v_j\varphi \to \forall v_j\forall v_i\varphi$	by (L2)
$\vdash \forall v_i\forall v_j\varphi \to \forall v_j\forall v_i\forall v_j\varphi$	using Prop. 3.29
$\vdash \forall v_i\forall v_j\varphi \to \forall v_j\forall v_i\varphi$	
$\vdash \forall v_j\forall v_i\varphi \to \forall v_i\forall v_j\varphi$	similarly
$\vdash \forall v_i\forall v_j\varphi \leftrightarrow \forall v_j\forall v_i\varphi$	□

Recall that $\exists v_i \varphi$ is defined to be the formula $\neg \forall v_i \neg \varphi$. The following simple propositions expand on this.

Proposition 3.31. $\vdash \neg \forall v_i \varphi \leftrightarrow \exists v_i \neg \varphi$ *for any formula* φ *and any* $i \in \omega$.

Proof. Exercise. □

Proposition 3.32. $\vdash \neg \exists v_i \varphi \leftrightarrow \forall v_i \neg \varphi$ *for any formula* φ *and any* $i \in \omega$.

Proof. Exercise. □

Some important results concerning $\exists$ are as follows.

Theorem 3.33. *If no free occurrence of* v_i *in a formula* φ *is within a subformula of the form* $\forall v_k \psi$ *with* v_k *occurring in a term* σ*, then* $\vdash \mathrm{Subf}_\sigma^{v_i} \varphi \rightarrow \exists v_i \varphi$.

Proof. Exercise. □

Corollary 3.34. $\vdash \varphi \rightarrow \exists v_i \varphi$ *for any formula* φ. □

Corollary 3.35. $\vdash \forall v_i \varphi \rightarrow \exists v_i \varphi$.

Proof. Exercise. □

Proposition 3.36. *If* v_i *does not occur free in* φ*, then* $\vdash \varphi \leftrightarrow \exists v_i \varphi$.

Proof. Exercise. □

Theorem 3.37. $\vdash \exists v_i \forall v_j \varphi \rightarrow \forall v_j \exists v_i \varphi$ *for any formula* φ.

Proof.

$\vdash \varphi \rightarrow \exists v_i \varphi$	by Corollary 3.34
$\vdash \forall v_j \varphi \rightarrow \forall v_j \exists v_i \varphi$	generalization, (L2)
$\vdash \neg \forall v_j \exists v_i \varphi \rightarrow \neg \forall v_j \varphi$	tautology
$\vdash \forall v_i [\neg \forall v_j \exists v_i \varphi \rightarrow \neg \forall v_j \varphi]$	generalization
$\vdash \forall v_i [\neg \forall v_j \exists v_i \varphi \rightarrow \neg \forall v_j \varphi] \rightarrow [\forall v_i \neg \forall v_j \exists v_i \varphi \rightarrow \forall v_i \neg \forall v_j \varphi]$	(L2)
$\vdash \forall v_i \neg \forall v_j \exists v_i \varphi \rightarrow \forall v_i \neg \forall v_j \varphi$	
$\vdash \neg \forall v_j \exists v_i \varphi \rightarrow \forall v_i \neg \forall v_j \varphi$	by Proposition 3.29
$\vdash \exists v_i \forall v_j \varphi \rightarrow \forall v_j \exists v_i \varphi$	tautology

□

Now we prove several results involving two formulas φ and ψ, and some variable v_i which is not free in one of them.

Proposition 3.38. *If* v_i *does not occur free in the formula* φ*, and* ψ *is any formula, then* $\vdash \forall v_i (\varphi \rightarrow \psi) \rightarrow (\varphi \rightarrow \forall v_i \psi)$.

Proof. By Proposition 3.29,

(1) $$\vdash \varphi \to \forall v_i \varphi.$$

By (L2) we have $\vdash \forall v_i(\varphi \to \psi) \to (\forall v_i \varphi \to \forall v_i \psi)$, and hence by a tautology

(2) $$\vdash \forall v_i \varphi \to [\forall v_i(\varphi \to \psi) \to \forall v_i \psi]$$

By a tautology, from (1) and (2) we get

$$\vdash \varphi \to [\forall v_i(\varphi \to \psi) \to \forall v_i \psi],$$

and then another tautology gives the desired result. □

Proposition 3.39. *If v_i does not occur free in the formula ψ, then $\vdash \forall v_i(\varphi \to \psi) \to (\exists v_i \varphi \to \psi)$.*

Proof.

(1)	$\vdash (\varphi \to \psi) \to (\neg\psi \to \neg\varphi)$	(taut.)
(2)	$\vdash \forall v_i(\varphi \to \psi) \to \forall v_i(\neg\psi \to \neg\varphi)$	((1), gen., (L2))
(3)	$\vdash \forall v_i(\neg\psi \to \neg\varphi) \to (\neg\psi \to \forall v_i \neg\varphi)$	(Prop. 3.38)
(4)	$\vdash (\neg\psi \to \forall v_i \neg\varphi) \to (\exists v_i \varphi \to \psi)$	(taut.)
	$\vdash \forall v_i(\varphi \to \psi) \to (\exists v_i \varphi \to \psi)$	((2)–(4), taut.)

□

Lemma 3.40. *If φ and ψ are formulas and v_i does not occur free in ψ, then $\vdash \forall v_i \varphi \vee \psi \leftrightarrow \forall v_i(\varphi \vee \psi)$.*

Proof.

$\vdash \forall v_i \varphi \vee \psi \leftrightarrow (\neg\psi \to \forall v_i \varphi)$	taut.
$\vdash (\neg\psi \to \forall v_i \varphi) \leftrightarrow \forall v_i(\neg\psi \to \varphi)$	by Prop. 3.38
$\vdash (\neg\psi \to \varphi) \leftrightarrow \varphi \vee \psi$	taut.
$\vdash \forall v_i(\neg\psi \to \varphi) \leftrightarrow \forall v_i(\varphi \vee \psi)$	gen., (L2)

Now the lemma follows. □

Proposition 3.41. $\vdash \forall v_i(\varphi \wedge \psi) \leftrightarrow \forall v_i \varphi \wedge \forall v_i \psi$, *for any formulas φ, ψ.*

Proof.

$\vdash \forall v_i(\varphi \wedge \psi) \to \varphi \wedge \psi$	by Corollary 3.28
$\vdash \forall v_i(\varphi \wedge \psi) \to \varphi$	using a tautology
$\vdash \forall v_i \forall v_i(\varphi \wedge \psi) \to \forall v_i \varphi$	using (L2)
$\vdash \forall v_i(\varphi \wedge \psi) \to \forall v_i \varphi$	using Proposition 3.29

$$
\begin{array}{lll}
 & \vdash \forall v_i(\varphi \wedge \psi) \to \forall v_i \psi & \text{similarly} \\
(1) & \vdash \forall v_i(\varphi \wedge \psi) \to \forall v_i \varphi \wedge \forall v_i \psi & \text{a tautology} \\
 & \vdash \forall v_i \varphi \to \varphi & \text{by Corollary 3.28} \\
 & \vdash \forall v_i \psi \to \psi & \text{by Corollary 3.28} \\
 & \vdash \forall v_i \varphi \wedge \forall v_i \psi \to \varphi \wedge \psi & \text{by a tautology} \\
 & \vdash \forall v_i(\forall v_i \varphi \wedge \forall v_i \psi) \to \forall v_i(\varphi \wedge \psi) & \text{using (L2)} \\
 & \vdash \forall v_i \varphi \wedge \forall v_i \psi \to \forall v_i(\varphi \wedge \psi). & \text{using Proposition 3.29}
\end{array}
$$

Now the desired result follows using (1) and a tautology. □

Proposition 3.42. *If φ and ψ are formulas and v_i does not occur free in ψ, then $\vdash \exists v_i \varphi \wedge \psi \leftrightarrow \exists v_i(\varphi \wedge \psi)$.*

Proof.

$$
\begin{array}{ll}
\vdash \neg \exists v_i \varphi \vee \neg \psi \leftrightarrow \forall v_i \neg \varphi \vee \neg \psi & \text{by Prop. 3.32} \\
\vdash \forall v_i \neg \varphi \vee \neg \psi \leftrightarrow \forall v_i(\neg \varphi \vee \neg \psi) & \text{by Prop. 3.40} \\
\vdash (\neg \varphi \vee \neg \psi) \leftrightarrow \neg(\varphi \wedge \psi) & \text{taut.} \\
\vdash \forall v_i(\neg \varphi \vee \neg \psi) \leftrightarrow \forall v_i \neg(\varphi \wedge \psi) & \text{gen., (L2)} \\
\vdash \forall v_i \neg(\varphi \wedge \psi) \leftrightarrow \neg \exists v_i(\varphi \wedge \psi). &
\end{array}
$$

From these facts we get $\vdash \neg \exists v_i \varphi \vee \neg \psi \leftrightarrow \neg \exists v_i(\varphi \wedge \psi)$. The proposition follows by a tautology. □

Proposition 3.43. *If $\vdash \varphi \leftrightarrow \psi$, then $\vdash \forall v_i \varphi \leftrightarrow \forall v_i \psi$.*

Proof. Exercise. □

Proposition 3.44. *If $\vdash \varphi \leftrightarrow \psi$, then $\vdash \exists v_i \varphi \leftrightarrow \exists v_i \psi$.*

Proof. Exercise. □

Proposition 3.45. $\vdash \exists v_i(\varphi \vee \psi) \leftrightarrow \exists v_i \varphi \vee \exists v_i \psi$ *for any formulas φ, ψ.*

Proof.

$$
\begin{array}{ll}
\vdash \neg(\varphi \vee \psi) \leftrightarrow \neg \varphi \wedge \neg \psi & \text{a tautology} \\
\vdash \forall v_i \neg(\varphi \vee \psi) \leftrightarrow \forall v_i(\neg \varphi \wedge \neg \psi) & \text{by Proposition 3.43} \\
\vdash \forall v_i(\neg \varphi \wedge \neg \psi) \leftrightarrow \forall v_i \neg \varphi \wedge \forall v_i \neg \psi & \text{by Proposition 3.41} \\
\vdash \neg \forall v_i \neg(\varphi \vee \psi) \leftrightarrow \neg \forall v_i \neg \varphi \vee \neg \forall v_i \neg \psi; & \text{a tautology}
\end{array}
$$

this gives the desired result. □

Now we work towards a major result concerning first-order logic, the prenex normal form theorem.

We define $\forall^d v_i = \exists v_i$ and $\exists^d v_i = \forall v_i$. In terms of our official definition, this means that $\langle 4, 5(i+1)\rangle^d = \langle 1, 4, 5(i+1), 1\rangle$ and $\langle 1, 4, 5(i+1), 1\rangle^d = \langle 4, 5(i+1)\rangle$.

Proposition 3.46. *Let $\langle Q_0, \ldots, Q_{m-1}\rangle$ be a sequence of quantifiers ($\forall$ or $\exists$), $\langle v_{i(0)}, \ldots, v_{i(m-1)}\rangle$ a sequence of variables, and φ a formula. Then*

$$\vdash \neg Q_0 v_{i(0)} \cdots Q_{m-1} v_{i(m-1)} \varphi \leftrightarrow Q_0^d v_{i(0)} \cdots Q_{m-1}^d v_{i(m-1)} \neg\varphi.$$

Proof. Induction on m. For $m = 0$ the assertion is just $\vdash \neg\varphi \leftrightarrow \neg\varphi$, which is a tautology. Now assume the result for m, and suppose given a sequence $\langle Q_0, \ldots, Q_m\rangle$ of quantifiers, a sequence $\langle v_{i(0)}, \ldots, v_{i(m)}\rangle$ of variables, and a formula φ. Then by the inductive hypothesis,

(1) $$\vdash \neg Q_1 v_{i(1)} \cdots Q_m v_{i(m)} \varphi \leftrightarrow Q_1^d v_{i(1)} \cdots Q_m^d v_{i(m)} \neg\varphi.$$

Now by Proposition 3.31 we have

(2) $$\vdash \neg\forall v_{i(0)} Q_1 v_{i(1)} \cdots Q_{m-1} v_{i(m-1)} \varphi \leftrightarrow \exists v_{i(0)} \neg Q_1 v_{i(1)} \cdots Q_m v_{i(m)} \varphi.$$

By (1) and Proposition 3.44 we have

$$\vdash \exists v_{i(0)} \neg Q_1 v_{i(1)} \cdots Q_m v_{i(m)} \varphi \leftrightarrow \exists v_{i(0)} Q_1 v_{i(1)} \cdots Q_m^d v_{i(m)} \neg\varphi.$$

If Q_0 is $\forall$, then (2) gives the desired conclusion. A similar argument works if Q_0 is $\exists$. □

Proposition 3.47. *Suppose that:*
(i) $\langle Q_0, \ldots, Q_{m-1}\rangle$ is a sequence of quantifiers,
(ii) $\langle v_{i(0)}, \ldots v_{i(m-1)}\rangle$ is a sequence of variables,
(iii) φ and ψ are formulas,
(iv) for every $j < m$, $v_{i(j)}$ does not occur free in ψ.
Then

$$\vdash Q_0 v_{i(0)} \cdots Q_{m-1} v_{i(m-1)} \varphi \vee \psi \leftrightarrow Q_0 v_{i(0)} \cdots Q_{m-1} v_{i(m-1)} (\varphi \vee \psi).$$

Proof. Induction on m. For $m = 0$ the assertion is $\vdash \varphi \vee \psi \leftrightarrow \varphi \vee \psi$, which is a tautology. Now suppose that the statement is true for m, and $\langle Q_0, \ldots, Q_m\rangle$ is a sequence of quantifiers, $\langle v_{i(0)}, \ldots v_{i(m)}\rangle$ is a sequence of variables, φ and ψ are formulas, and for every $j \leq m$, $v_{i(j)}$ does not occur free in ψ. Then by the inductive hypothesis,

(1) $$\vdash Q_1 v_{i(1)} \cdots Q_m v_{i(m)} \varphi \vee \psi \leftrightarrow Q_1 v_{i(1)} \cdots Q_m v_{i(m)} (\varphi \vee \psi).$$

Suppose that Q_0 is $\forall$. Then by (1) and Proposition 3.43,

(2) $$\vdash \forall v_{i(0)} [Q_1 v_{i(1)} \cdots Q_m v_{i(m)} \varphi \vee \psi] \leftrightarrow \forall v_{i(0)} Q_1 v_{i(1)} \cdots Q_m v_{i(m)} (\varphi \vee \psi).$$

By Proposition 3.40,

$$\vdash \forall v_{i(0)}[Q_1 v_{i(1)} \cdots Q_m v_{i(m)} \varphi \vee \psi] \leftrightarrow \forall v_{i(0)} Q_1 v_{i(1)} \cdots Q_m v_{i(m)} \varphi \vee \psi.$$

Together with (2) this gives

$$\vdash \forall v_{i(0)} Q_1 v_{i(1)} \cdots Q_m v_{i(m)} \varphi \vee \psi \leftrightarrow \forall v_{i(0)} Q_1 v_{i(1)} \cdots Q_m v_{i(m)} (\varphi \vee \psi). \tag{3}$$

Similarly we get

$$\vdash \exists v_{i(0)} Q_1 v_{i(1)} \cdots Q_m v_{i(m)} \varphi \vee \psi \leftrightarrow \exists v_{i(0)} Q_1 v_{i(1)} \cdots Q_m v_{i(m)} (\varphi \vee \psi).$$

This finishes the inductive proof. □

Proposition 3.48. *Suppose that:*
(i) $\langle Q_0, \ldots, Q_{m-1} \rangle$ *is a sequence of quantifiers,*
(ii) $\langle v_{i(0)}, \ldots v_{i(m-1)} \rangle$ *is a sequence of variables,*
(iii) φ *and* ψ *are formulas,*
(iv) for every $j < m$, $v_{i(j)}$ *does not occur free in* ψ.
Then

$$\vdash \psi \vee Q_0 v_{i(0)} \cdots Q_{m-1} v_{i(m-1)} \varphi \leftrightarrow Q_0 v_{i(0)} \cdots Q_{m-1} v_{i(m-1)} (\psi \vee \varphi).$$

Proof.

(1) $\vdash \psi \vee Q_0 v_{i(0)} \cdots Q_{m-1} v_{i(m-1)} \varphi \leftrightarrow Q_0 v_{i(0)} \cdots Q_{m-1} v_{i(m-1)} \varphi \vee \psi$ (taut.)
(2) $\vdash Q_0 v_{i(0)} \cdots Q_{m-1} v_{i(m-1)} \varphi \vee \psi \leftrightarrow Q_0 v_{i(0)} \cdots Q_{m-1} v_{i(m-1)} (\varphi \vee \psi)$ (Prop. 3.47)
(3) $\vdash \varphi \vee \psi \leftrightarrow \psi \vee \varphi$ (taut.)
(4) $\vdash Q_0 v_{i(0)} \cdots Q_{m-1} v_{i(m-1)} (\varphi \vee \psi) \leftrightarrow Q_0 v_{i(0)} \cdots Q_{m-1} v_{i(m-1)} (\psi \vee \varphi)$ ((3),Props. 3.43, 3.44)

Now the proposition follows by (1)–(3). □

A formula φ is *quantifier-free* iff the symbol $\forall$ does not occur in it. (More precisely, if the integer 4 is not among the entries of the sequence φ.) A formula φ is in *prenex normal form* iff there is a natural number m, a sequence $\langle v_{i(j)} : j < m \rangle$ of distinct variables, a quantifier-free formula ψ, and a sequence $\langle Q_0, \ldots, Q_{m-1} \rangle$ of $\forall$ and $\exists$ such that φ is the formula

$$Q_0 v_{i(0)} \ldots Q_{m-1} v_{i(m-1)} \psi.$$

Some examples of formulas in prenex normal form are

$$v_0 + v_1 = v_0,$$
$$\forall v_0 \exists v_1 \forall v_2 [v_0 + v_2 = v_0 \rightarrow v_1 = v_1],$$
$$\forall v_0 \forall v_1 (v_0 < v_1).$$

Theorem 3.49. *For any formula* φ *there is a formula* ψ *in prenex normal form with the same free variables as* φ *such that* $\vdash \varphi \leftrightarrow \psi$.

Proof. Induction on φ. For φ atomic, φ is already itself in prenex normal form. Now assume inductively that φ is $\neg\psi$. By the inductive hypothesis, say

$$\vdash \psi \leftrightarrow Q_0 v_{i(0)} \dots Q_{m-1} v_{i(m-1)} \chi, \tag{1}$$

with each Q_k either $\forall$ or $\exists$, χ quantifier free, and $Q_0 v_{i(0)} \dots Q_{m-1} v_{i(m-1)} \chi$ has the same free variables as ψ. By Proposition 3.46 we have

$$\vdash \neg Q_0 v_{i(0)} \cdots Q_{m-1} v_{i(m-1)} \chi \leftrightarrow Q_0^d v_{i(0)} \cdots Q_{m-1}^d v_{i(m-1)} \neg\chi.$$

Using (1) and a tautology gives

$$\vdash \varphi \leftrightarrow Q_0^d v_{i(0)} \cdots Q_{m-1}^d v_{i(m-1)} \neg\chi,$$

as desired.

Now assume inductively that φ is $\psi \to \chi$. By the inductive hypothesis, say

$$\begin{aligned} &\vdash \psi \leftrightarrow Q_0 v_{i(0)} \dots Q_{m-1} v_{i(m-1)} \psi' \quad \text{and} \\ &\vdash \chi \leftrightarrow R_0 v_{j(0)} \dots R_{n-1} v_{j(n-1)} \chi', \end{aligned}$$

with each Q_k and R_k either $\forall$ or $\exists$ and with ψ' and χ' quantifier free; ψ has the same free variables as $Q_0 v_{i(0)} \dots Q_{m-1} v_{i(m-1)} \psi'$, and χ has the same free variables as $R_0 v_{j(0)} \dots R_{n-1} v_{j(n-1)} \chi'$. Now $\vdash \varphi \leftrightarrow \neg\psi \vee \chi$, so

$$\vdash \varphi \leftrightarrow \neg Q_0 v_{i(0)} \dots Q_{m-1} v_{i(m-1)} \psi' \vee R_0 v_{j(0)} \dots R_{n-1} v_{j(n-1)} \chi'. \tag{2}$$

Now by Proposition 3.46 we obtain from (2)

$$\vdash \varphi \leftrightarrow Q_0^d v_{i(0)} \dots Q_{m-1}^d v_{i(m-1)} \neg\psi' \vee R_0 v_{j(0)} \dots R_{n-1} v_{j(n-1)} \chi'. \tag{3}$$

Let k be greater than any l such that v_l occurs in the above formula. Let ψ'' be obtained from ψ' by replacing each variable $v_{i(l)}$ by v_{k+l}, and let χ'' be obtained from χ' by replacing each variable $v_{j(l)}$ by v_{k+m+l}. Then by the change of bound variable theorem we get from (3)

$$\vdash \varphi \leftrightarrow Q_0^d v_k \dots Q_{m-1}^d v_{k+m-1} \neg\psi'' \vee R_0 v_{k+m} \dots R_{n-1} v_{k+m+n-1} \chi''. \tag{4}$$

Now by Proposition 3.47 we have

$$\begin{aligned} &\vdash Q_0^d v_k \dots Q_{m-1}^d v_{k+m-1} \neg\psi'' \vee R_0 v_{k+m} \dots R_{n-1} v_{k+m+n-1} \chi'' \\ &\leftrightarrow Q_0^d v_k \dots Q_{m-1}^d v_{k+m-1} (\neg\psi'' \vee R_0 v_{k+m} \dots R_{n-1} v_{k+m+n-1} \chi'') \end{aligned} \tag{5}$$

By Proposition 3.48 we get

$$\begin{aligned} &\vdash \neg\psi'' \vee R_0 v_{k+m} \dots R_{n-1} v_{k+m+n-1} \chi'' \\ &\leftrightarrow R_0 v_{k+m} \dots R_{n-1} v_{k+m+n-1} (\neg\psi'' \vee \chi''). \end{aligned}$$

Then using Props. 3.43 and 3.44, from this we get

$$\begin{aligned}&\vdash Q_0^d v_k \dots Q_{m-1}^d v_{k+m-1}(\neg\psi'' \vee R_0 v_{k+m} \dots R_{n-1} v_{k+m+n-1}\chi'')\\ &\leftrightarrow Q_0^d v_k \dots Q_{m-1}^d v_{k+m-1} R_0 v_{k+m} \dots R_{n-1} v_{k+m+n-1}(\neg\psi'' \vee \chi'').\end{aligned}$$

Putting this together with (4) and (5) we have

$$\vdash \varphi \leftrightarrow Q_0^d v_k \dots Q_{m-1}^d v_{k+m-1} R_0 v_{k+m} \dots R_{n-1} v_{k+m+n-1}(\neg\psi'' \vee \chi'').$$

This finishes the case when φ is $\psi \to \chi$.

Finally, suppose inductively that φ is $\forall v_k \psi$. By the inductive hypothesis, say

$$\vdash \psi \leftrightarrow Q_0 v_{i(0)} \dots Q_{m-1} v_{i(m-1)} \chi,$$

with each Q_k either $\forall$ or $\exists$, χ quantifier free, the variables $v_{i(j)}$ distinct, and $Q_0 v_{i(0)} \dots Q_{m-1} v_{i(m-1)}\chi$ has the same free variables as ψ. Then by Prop. 3.43 we have

$$\vdash \varphi \leftrightarrow \forall v_k Q_0 v_{i(0)} \dots Q_{m-1} v_{i(m-1)} \chi. \qquad \square$$

EXERCISES

E3.1. Do the case $\mathbf{R}\sigma_0 \dots \sigma_{m-1}$ for some m-ary relation symbol and terms $\sigma_0, \dots, \sigma_{m-1}$ in the proof of Theorem 3.1, (L3).

E3.2. Prove that (L6) is universally valid, in the proof of Theorem 3.1.

E3.3. Prove that (L8) is universally valid, in the proof of Theorem 3.1.

E3.3. Finish the proof of Proposition 3.11.

E3.5. Indicate which occurrences of the variables are bound and which ones free for the following formulas.

$\exists v_0(v_0 < v_1) \wedge \forall v_1(v_0 = v_1)$.
$v_4 + v_2 = v_0 \wedge \forall v_3(v_0 = v_1)$.
$\exists v_2(v_4 + v_2 = v_0)$.

E3.6. Finish the proof of Proposition 3.13.

E3.7. Indicate all free and bound occurrences of terms in the formula $v_0 = v_1 + v_1 \to \exists v_2(v_0 + v_2 = v_1)$.

E3.8. Prove Proposition 3.16

E3.9. Show that the condition in Proposition 3.17 that the resulting occurrence of τ is free is necessary. Hint: use Theorem 3.2; describe a specific formula of the type in Proposition 3.17, but with τ not free, such that the formula is not universally valid.

E3.10. Prove Proposition 3.19.

E3.11. Prove that the hypothesis of Theorem 3.27 is necessary.

E3.12. Prove Proposition 3.31.

E3.13. Prove Proposition 3.32.

E3.14. Prove Proposition 3.33.

E3.15. Prove Proposition 3.35.

E3.16. Prove Proposition 3.36.

E3.17. Prove Proposition 3.43.

E3.18. Prove Proposition 3.44.

E3.19. Find a formula in prenex normal form equivalent to the following formula:

$$\forall v_0 \exists v_1 (v_0 < v_1) \wedge \exists v_1 \forall v_0 (v_0 < v_1).$$

E3.20. Find a formula in prenex normal form equivalent to the following formula:

$$\forall v_0 [v_0 < v_1 \leftrightarrow \exists v_1 (v_1 < v_0)].$$

E3.21. Prove that

$$\vdash \forall v_0 \forall v_1 (v_0 = v_1) \rightarrow \forall v_0 (v_0 = v_1 \vee v_0 = v_2).$$

E3.22. Prove that

$$\vdash \exists v_0 (\neg v_0 = v_1 \wedge \neg v_0 = v_2) \rightarrow \exists v_0 \exists v_1 (\neg v_0 = v_1).$$