

5.7 Equality

Sections 5.3 to 5.6 gave the four quantifier rules, and with them every logical symbol of the language of Section 5.2 (the connectives, $\perp$, the quantifiers, and equality) has rules, except one. So far the equals sign has been treated like a predicate symbol: $a = b$ was an atomic formula like $P(a)$, and no rule looked inside it. Yet almost every calculation in mathematics is a chain of equations, and every use of “the” (the limit, the supremum, the inverse) quietly asserts that something is unique. This section adds the two rules for equality, $=I$ and $=E$, which say together that *equals may be replaced by equals*. Section 5.8 applies them to the phrase “there is exactly one”, which is an existential statement together with an equation. This section ends by completing the table of rules, phrases, and Lean tactics that Chapter 1 began.

5.7.1 What the rules so far cannot do with an equation

Here is the first line of a calculation any reader has written:

Since $a = b$ and $a + a = 2a$, we have $b + b = 2b$.

Nothing could be simpler, and nothing in Sections 5.3–5.6 derives it: so far the rules treat $=$ as they treat any two-place predicate symbol, and from $R(a, b)$ and $P(a)$ no rule gives $P(b)$. Reading $R(a, b)$ as $a < b$ and $P(x)$ as $x < 1$ over $\mathbb{Z}$, with $a = 0$ and $b = 5$, both premises are true and $P(b)$ is false.

What makes the step correct is what $=$ means: a and b are names of **the same object**. Any statement true of the object is true of it whichever name is used. Two things follow, and they are the two rules of this section.

1. Every term names the same object as itself. Nothing needs to be assumed to write $t = t$.
2. If t_1 and t_2 name the same object, then a statement about t_1 may be rewritten as the same statement about t_2 .

The first rule is unusual: it cites no earlier line at all. Chapter 1 anticipated this when it defined rules (Section 1.2): the definition of a rule schema (Definition 1.2.1) was worded so that a rule of Chapter 5 could have no given lines at all. This is that rule.

5.7.2 The rules for equality

Everything is equal to itself, and equals may be replaced by equals.

Definition 5.7.1. Rules for Equality

			i	$t_1 = t_2$	
k	$ $	$t = t$	$=I$	j	$\varphi[t_1/x]$
			k	$\varphi[t_2/x]$	$=E \ i, j$

The rule $=I$ (**equality introduction**, or reflexivity) writes $t = t$ for **any** term t , at any line, citing nothing. The rule $=E$ (**equality elimination**, or substitution of equals) cites an equation $t_1 = t_2$ on line i and a line j of the form $\varphi[t_1/x]$, both available at line k , and writes $\varphi[t_2/x]$ on line k . Here φ is **any** formula and x any variable, subject to one side condition:

both t_1 and t_2 are free for x in φ (Definition 5.2.6).

In words: $=I$ says that every term equals itself. $=E$ says that when $t_1 = t_2$ is known, a line that says something about t_1 may be rewritten as the same thing said about t_2 . The formula φ is the “something”: a statement with a hole x , which line j fills with t_1 and line k fills with t_2 .

Mark the holes first. To use $=E$ with $t_1 = t_2$, write down the line you have and draw a box round each occurrence of t_1 you want to replace. The boxes are the holes: φ is the line with a variable in each box, and the new line puts t_2 in every box. With $a = b$:

$$\boxed{a} + \boxed{a} = 2 \cdot \boxed{a} \text{ gives } b + b = 2 \cdot b, \quad \boxed{a} + a = 2 \cdot a \text{ gives } b + a = 2 \cdot a.$$

Occurrences without a box stay as they are.

Read the definition clause by clause.

1. **$=I$ cites nothing.**
 - *Schema*: the left block above, $t = t$, citing nothing.
 - *Reading*: every term equals itself, so the line may stand anywhere, even first in a derivation with no premises.
 - *Example*: “ $a + b = a + b \text{ — } =I$ ”, the first line of every chain below.
2. **The equation is read from left to right.** The cited equation $t_1 = t_2$ licenses replacing t_1 by t_2 , and not the other way round. From $a = b$ and $P(b)$, the rule does **not** give $P(a)$, because $P(b)$ is $\varphi[b/x]$ for $\varphi = P(x)$, and the equation would have to be $b = a$. The reverse direction needs one more step, symmetry, which we derive below.
3. **Some or all occurrences.** The choice of φ decides which occurrences of t_1 are replaced: exactly those that φ marks with x (the boxes above). Occurrences of t_1 that φ writes out are left alone. Choosing φ is the whole art of using the rule.
4. **Free for x .** Neither term may have a variable captured by a quantifier of φ , the condition of Definition 5.2.6 that the rules of Sections 5.3 and 5.5 also carry. The nonexample below shows what goes wrong without it.

One line, many readings. Take the equation $a = b$ and the line $a + a = 2 \cdot a$. The term a occurs three times in the line, and φ may mark any of them. Some of the choices:

φ	$\varphi[a/x]$ (the cited line)	$\varphi[b/x]$ (the new line)
$x + a = 2 \cdot a$	$a + a = 2 \cdot a$	$b + a = 2 \cdot a$
$a + x = 2 \cdot a$	$a + a = 2 \cdot a$	$a + b = 2 \cdot a$
$a + a = 2 \cdot x$	$a + a = 2 \cdot a$	$a + a = 2 \cdot b$
$x + x = 2 \cdot x$	$a + a = 2 \cdot a$	$b + b = 2 \cdot b$

Each of the three occurrences is marked or not, so there are $2^3 = 8$ choices in all, and each is a legal step. The fourth row is the step of the opening calculation.

○ **Second reading** · *Degenerate choices*

One more row belongs to the table:

φ	$\varphi[a/x]$ (the cited line)	$\varphi[b/x]$ (the new line)
$a + a = 2 \cdot a$	$a + a = 2 \cdot a$	$a + a = 2 \cdot a$

This row is the **degenerate** choice: φ contains no x , so $\varphi[a/x]$ and $\varphi[b/x]$ are both φ , and the rule copies the line unchanged. It is legal and useless, and it shows that “some occurrences” includes “none”. Another degenerate case: the equation may be $t = t$ itself, and then $=E$ again returns the cited line.

Quick check. From the equation $x_0 = 3$ and the line $x_0 \cdot x_0 > x_0$, which formula φ makes $=E$ give $3 \cdot 3 > x_0$? Which gives $x_0 \cdot 3 > 3$?

Solution. For $3 \cdot 3 > x_0$, take $\varphi = (z \cdot z > x_0)$, with a variable z that appears nowhere else: $\varphi[x_0/z]$ is the cited line and $\varphi[3/z]$ is $3 \cdot 3 > x_0$. For $x_0 \cdot 3 > 3$, take $\varphi = (x_0 \cdot z > z)$. The hole has to be a variable other than x_0 , since the occurrences of x_0 that stay must be written out in φ .

Quick check. From $a = b$ and the line $a \cdot a = a + 1$, which occurrences do you box to get $a \cdot b = b + 1$?

Solution. The second and the third a : $\varphi = (a \cdot z = z + 1)$, and $\varphi[a/z]$ is the given line, $\varphi[b/z]$ the new one.

A nonexample: capture. Take the equation $a = y$, with y a variable, and the line $\exists y (y < a)$. It is tempting to “substitute y for a ” and write $\exists y (y < y)$. With $\varphi = \exists y (y < x)$, the cited line is $\varphi[a/x]$, and the new line would be $\varphi[y/x]$. But y is **not** free for x in φ : the x sits inside $\exists y$, and the y put there would be captured. The side condition fails, and rightly. Read over $\mathbb{Z}$, with a and y both naming 0, the premises say “ $a = y$ ” (true) and “some integer is less than 0” (true), while $\exists y (y < y)$ says that some integer is less than itself (false).

1	$a = y$	
2	$\exists y (y < a)$	
3	$\exists y (y < y)$	$=E$ 1, 2

Line 3 breaks the side condition of [Definition 5.7.1](#). What the argument meant to say needs a different name for the bound variable: $\exists z (z < a)$, which is the same sentence up to renaming (Section 5.2), becomes $\exists z (z < y)$, which is true when y names 0.

Why these two rules. They are exactly the two facts about “same object” listed above, and nothing else about equality needs to be assumed. Symmetry ($s = t$ gives $t = s$), transitivity ($s = t$ and $t = u$ give $s = u$), and “applying the same function to both sides” are all derived below. So the two rules play for $=$ the part that the introduction and elimination rules played

for each connective: one builds an equation, one uses it.

Warning. **A bound variable is not a place to substitute.** From $x = 0$ and $\forall x (x = x)$, the line $\forall x (0 = x)$ does **not** follow: the x 's of $\forall x (x = x)$ are bound, and $=E$ replaces only free occurrences. Over $\mathbb{Z}$, with x naming 0, the premises are true and $\forall x (0 = x)$ is false.

🕒 **Second reading** · *Why no choice of the hole works*

To write $\forall x (x = x)$ as $\varphi[x/z]$, either z does not occur free in φ , and then $\varphi[0/z]$ is the unchanged line, or z occurs free in φ (for instance, φ is $\forall x (z = x)$), and then every free z lies inside $\forall x$, so x is not free for z in φ and the side condition fails.

5.7.3 Symmetry, transitivity and congruence

Everything we expect of equality now follows from the two rules. Each derivation below is short, and the only thought in each is the choice of φ .

It turns out that the equation in $=E$ may be read in either direction after all, at the cost of two extra lines (an $=I$ and an $=E$; after the abbreviation (sym) below, just one), and that equations chain:

Proposition 5.7.1. Equality Is Symmetric and Transitive

For all terms s, t, u :

- (a) $s = t \vdash t = s$;
- (b) $s = t, t = u \vdash s = u$.

Idea. For (a), the goal $t = s$ must be the last line of an $=E$ that uses the premise $s = t$ (it is the only equation available), so it has the form $\varphi[t/x]$, and the cited line $\varphi[s/x]$ must already be on a line. Try $\varphi = (x = s)$: then $\varphi[t/x]$ is $t = s$, the goal, and $\varphi[s/x]$ is $s = s$, which $=I$ supplies for free. For (b), rewrite the t of the first premise using the second: $\varphi = (s = x)$.

Proof.

- (a) With $\varphi := (x = s)$, for a variable x that occurs in neither s nor t , the line $s = s$ is $\varphi[s/x]$ and the goal $t = s$ is $\varphi[t/x]$. Both terms are free for x in φ , since φ has no quantifier. So the following is a derivation:

1	$s = t$	
2	$s = s$	$=I$
3	$t = s$	$=E\ 1, 2$

- (b) With $\varphi := (s = x)$, for a variable x that does not occur in s , the first premise $s = t$ is $\varphi[t/x]$ and the goal $s = u$ is $\varphi[u/x]$; again φ has no quantifier. So the following is a

derivation:

$$\begin{array}{l|l}
 1 & s = t \\
 2 & t = u \\
 \hline
 3 & s = u \quad =E\ 2, 1
 \end{array}$$

Line 3 of (b) cites the equation $t = u$ on line 2 as the rule's line i , and $s = t$ on line 1 as its line j . This proves (a) and (b). ■

Notice where the “reflexivity” line went in (a): the equation $s = t$ was not rewritten at all. It was the **tool**, and the line it rewrote, $s = s$, was manufactured for the purpose. This is the typical use of $=I$: it supplies a line for $=E$ to work on.

From now on, symmetry and transitivity may be used as one line, with the justifications “(sym)” and “(trans)”: each abbreviates the three-line derivation above with the given terms in place of s, t, u . This is the license of Definition 2.3.1, extended from statement letters to terms. The extension is harmless for the same reason: the derivations above used nothing about s, t, u except that they are terms, so they can be pasted in with any terms.

The next derivation is the rule behind “apply f to both sides”. Let f be a one-place function symbol, and a, b constants.

$$\begin{array}{l|l}
 1 & a = b \\
 2 & f(a) = f(a) \quad =I \\
 3 & f(a) = f(b) \quad =E\ 1, 2
 \end{array}$$

Here $\varphi = (f(a) = f(x))$: it keeps the first a and marks the second. With $\varphi = (f(x) = f(x))$ instead, the same two lines would give $f(b) = f(b)$, which is true and useless. Nothing is special about f : the same three lines give $a^2 = b^2$ from $a = b$, or $a + c = b + c$, or $|a| = |b|$. Every “do the same thing to both sides of an equation” is this derivation.

The last result of this group has no premises. It says that equals share every property, and it is called **Leibniz’s Law**.

Proposition 5.7.2. Leibniz’s Law

For every one-place predicate symbol P , $\vdash \forall x \forall y (x = y \rightarrow (P(x) \rightarrow P(y)))$.

In words: whatever is true of x is true of anything equal to it. The rule $=E$ is this law for every formula at once; the seven-line derivation is in the fold below.

🕒 **Second reading** · *Leibniz’s Law, derived*

Proof. Finding it. The goal is $\forall x$, so the search method of Section 3.1, with the step of Section 5.4, opens a flagged box for x_0 ; the new goal $\forall y (\dots)$ opens a second flagged box, for y_0 . The goal $x_0 = y_0 \rightarrow (P(x_0) \rightarrow P(y_0))$ is an implication, so a box opens with $x_0 = y_0$,

and the new goal $P(x_0) \rightarrow P(y_0)$ opens another, with $P(x_0)$. Now the goal is $P(y_0)$, the resources are $x_0 = y_0$ and $P(x_0)$, and one $=E$ with $\varphi = P(x)$ finishes. Every line but one was written by a goal-directed step.

1	x_0	y_0	$x_0 = y_0$	asm, for $\rightarrow I$
2			$P(x_0)$	asm, for $\rightarrow I$
3			$P(y_0)$	$=E$ 1, 2
4			$P(x_0) \rightarrow P(y_0)$	$\rightarrow I$ 2–3
5			$x_0 = y_0 \rightarrow (P(x_0) \rightarrow P(y_0))$	$\rightarrow I$ 1–4
6			$\forall y (x_0 = y \rightarrow (P(x_0) \rightarrow P(y)))$	$\forall I$ 1–5
7			$\forall x \forall y (x = y \rightarrow (P(x) \rightarrow P(y)))$	$\forall I$ 1–6

The two $\forall I$ lines cite the flagged boxes as 1–5 and 1–6: each flagged box immediately contains another box, so its range starts at that box’s first line (the convention of Section 5.4). At line 6 the name y_0 appears in no premise (there are none), in no open assumption (the boxes on lines 1 and 2 have closed), and not in the conclusion; at line 7 the same holds for x_0 . The derivation has 7 lines. ■

The claim is one of the classical “axioms of equality”, often taken as a starting point in place of $=E$. Here it is a consequence. Conversely, with the claim as a premise, $\forall E$ twice and $\rightarrow E$ twice would do the work of $=E$ for the formula $P(x)$; the rule does it for every formula at once.

Warning. Words about knowledge are not formulas. $=E$ rewrites formulas of the language, and “it is obvious that ...”, “the pupil checked that ...”, “it is known that ...” are not among its connectives. A pupil checked that $7 \cdot 13 = 91$, and indeed $7 \cdot 13 = 91$. Replacing $7 \cdot 13$ by 91 inside the report gives “the pupil checked that $91 = 91$ ”, a different claim about what the pupil did. Inside a formula every free occurrence of a term may be rewritten, subject to the side condition of [Definition 5.7.1](#); inside words about what someone knows or checked, none may.

5.7.3.1 Equal sets have the same elements

Example. Equal Sets Have the Same Elements

Read the domain as consisting of sets, with $\in$ a two-place predicate symbol written between its terms (shorthand rule 1 of Section 5.2). Show that $\vdash \forall x \forall y (x = y \rightarrow \forall z (z \in x \leftrightarrow z \in y))$.

Solution.

1	x_0	y_0	$x_0 = y_0$	asm, for $\rightarrow$ I
2			z_0 $z_0 \in x_0$	asm, for $\leftrightarrow$ I
3			$z_0 \in x_0$	asm, for $\leftrightarrow$ I
4			$z_0 \in x_0 \leftrightarrow z_0 \in x_0$	$\leftrightarrow$ I 2–2, 3–3
5			$z_0 \in x_0 \leftrightarrow z_0 \in y_0$	$=$ E 1, 4
6			$\forall z (z \in x_0 \leftrightarrow z \in y_0)$	$\forall$ I 2–5
7			$x_0 = y_0 \rightarrow \forall z (z \in x_0 \leftrightarrow z \in y_0)$	$\rightarrow$ I 1–6
8			$\forall y (x_0 = y \rightarrow \forall z (z \in x_0 \leftrightarrow z \in y))$	$\forall$ I 1–7
9			$\forall x \forall y (x = y \rightarrow \forall z (z \in x \leftrightarrow z \in y))$	$\forall$ I 1–8

The two boxes of line 4 are one-line boxes, as $P \rightarrow P$ is shown, and each flagged box immediately contains another box and is cited from its first line. Line 5 is $=$ E with $\varphi = (z_0 \in x_0 \leftrightarrow z_0 \in w)$: line 4 is $\varphi[x_0/w]$, and the equation of line 1 refills the hole with y_0 ; as in the proof of symmetry, $\leftrightarrow$ I manufactured a line for $=$ E to rewrite.

The converse, $\forall z (z \in x \leftrightarrow z \in y) \rightarrow x = y$, breaks. Here is a counter-reading to it: two dots a and b , with nothing an element of anything. With x naming a and y naming b , both sides of $z \in x \leftrightarrow z \in y$ are false for every z , so the hypothesis is true; and $a = b$ is false. For sets, the converse is taken as an axiom, the axiom of extensionality: a set is determined by its elements.

5.7.4 Calculations are chains of substitutions

A calculation in a proof looks like this:

$$a + b = 2 \cdot b + b = 2 \cdot 3 + 3 = 9,$$

written under the premises $a = 2 \cdot b$ and $b = 3$. The chain is a single statement to the eye, but logically it is several equations, each obtained from the last. Here is the derivation it abbreviates, with one line of arithmetic, justified “arith” as in Section 5.3.

A chain as a derivation. From $b = 3$ and $a = 2 \cdot b$, derive $a + b = 9$.

1	$b = 3$	
2	$a = 2 \cdot b$	
3	$a + b = a + b$	$=$ I
4	$a + b = 2 \cdot b + b$	$=$ E 2, 3
5	$a + b = 2 \cdot 3 + 3$	$=$ E 1, 4
6	$2 \cdot 3 + 3 = 9$	arith
7	$a + b = 9$	$=$ E 6, 5

The choices of φ , with z a variable not occurring in the terms:

- line 4: $\varphi = (a + b = z + b)$, rewriting the a on the **right** of line 3 and keeping the one on

the left;

- line 5: $\varphi = (a + b = 2 \cdot z + z)$, rewriting **both** remaining b 's on the right at once;
- line 7: $\varphi = (a + b = z)$, rewriting the whole right-hand side by the equation of line 6.

The pattern is general. A chain $t_1 = t_2 = \dots = t_n$ starts with $t_1 = t_1$ by =I, keeps t_1 fixed on the left, and rewrites the right-hand side once per link, each time by =E with the equation that justifies the link. Each link is either a premise, as on lines 4 and 5, or an arithmetic fact, as on line 7. The last line is $t_1 = t_n$. Transitivity (Proposition 5.7.1 (b)) is the same move made once; a chain makes it $n - 1$ times.

A **mixed chain**, such as $a^2 + 1 = 10 \leq 10 + b^2$ with $a = 3$, is not made of =E alone. Its = links are =E steps as above, and a $\leq$ link needs a fact about $\leq$: here that $b^2 \geq 0$, so that adding b^2 does not decrease a number. The = link before it then carries over by one more =E, with $\varphi = (z \leq 10 + b^2)$ and the equation $a^2 + 1 = 10$ turned round by symmetry (Proposition 5.7.1 (a)); transitivity of $\leq$ is needed only where two $\leq$ links meet, as in $x \leq y \leq z$. Those are facts about order, not about equality. They enter derivations as “arith” lines, one per link.

Quick check. Line 5 of the chain rewrites both b 's on the right of line 4 at once. Which φ would rewrite only the b inside $2 \cdot b$, and what line would it give? How would the chain then reach line 5?

Solution. Take $\varphi = (a + b = 2 \cdot z + b)$. Then line 4 is $\varphi[b/z]$, and =E 1, 4 gives $\varphi[3/z]$, the line $a + b = 2 \cdot 3 + b$. One more =E with the same equation $b = 3$ and $\varphi = (a + b = 2 \cdot 3 + z)$ then gives $a + b = 2 \cdot 3 + 3$, which is line 5. Marking both occurrences at once saves that line.

Quick check. Under the premise $a = 2$, the chain $a + 1 = 2 + 1 = 3 \leq 4$ has three links. Which is an =E step, and which are “arith” lines?

Solution. The first link is =E: from $a + 1 = a + 1$ (=I) and $a = 2$, with $\varphi = (a + 1 = z + 1)$, it writes $a + 1 = 2 + 1$. The links $2 + 1 = 3$ and $3 \leq 4$ are facts of school arithmetic, written as “arith” lines, and each is then carried into the chain by one more =E (with $\varphi = (a + 1 = z)$, then with $\varphi = (z \leq 4)$ and the equation turned round); the last link is about order, not equality.

5.7.5 What equality sounds like in a proof

In a written proof, =E is the word “substituting”, or no word at all: the chain $a + b = 2b + b = 9$ is read as a sequence of substitutions, and the reader supplies the φ of each link. “By symmetry” or “rewriting the equation as $t = s$ ” is Proposition 5.7.1 (a). “Applying f to both sides”, “squaring both sides”, “adding c to both sides” are the congruence derivation above. And =I is almost never written, because $t = t$ goes without saying; it is visible only in the first line of a formal chain, and in a proof assistant, where `rfl` proves $t = t$.

Here is a proof from school algebra, read link by link.

Claim. If $a + b = 0$ and $a + c = 0$, then $b = c$.

Proof. $b = b + 0 = b + (a + c) = (b + a) + c = (a + b) + c = 0 + c = c$.

The first link is the fact $y + 0 = y$ for every y , applied at $y = b$ (an instance by $\forall E$) and read from right to left: the chain needs $b = b + 0$, which is the instance $b + 0 = b$ turned round by symmetry. The second link rewrites the 0 by the premise $a + c = 0$, again turned round, since the chain needs 0 to become $a + c$. The third and fourth are instances of associativity and commutativity. The fifth rewrites $a + b$ by the premise $a + b = 0$ in the direction written. The last is the instance $0 + c = c$. So the claim says that a number has **at most one** additive inverse; the facts it uses are the field axioms, here school algebra.

5.7.6 The search method: one more step

Each of Sections 5.3 to 5.6 added a step to the search method of Section 3.1. Equality adds one.

- **An equation.** When an equation $t_1 = t_2$ is available and the goal differs from an available line only in some occurrences of t_1 and t_2 , look for the φ that makes one $=E$ turn the line into the goal: mark with x exactly the places where they differ. If the equation points the wrong way, turn it round first (sym). If no available line will do, make one with $=I$, as the proof of Proposition 5.7.1 did.

In the Givens/Goal table, $=E$ turns a Given into a new Given with some holes refilled, and $=I$ adds $t = t$ to the Givens at no cost.

Example. Instances of $=E$

In each row the hole is z ; the cited line fills it with the left side of the equation, the new line with the right side.

Equation $t_1 = t_2$	φ	Cited line $\varphi[t_1/z]$	New line $\varphi[t_2/z]$
$f(c) = g(c) + 1$	$P(z) \wedge R(f(c), c)$	$P(f(c)) \wedge R(f(c), c)$	$P(g(c) + 1) \wedge R(f(c), c)$
$\varepsilon/2 = \delta$	$ x - a < z \rightarrow h(x) - h(a) < \varepsilon$	$ x - a < \varepsilon/2 \rightarrow h(x) - h(a) < \varepsilon$	$ x - a < \delta \rightarrow h(x) - h(a) < \varepsilon$
$a + b = b + a$	$\forall y (z \cdot y = y \cdot (a + b))$	$\forall y ((a + b) \cdot y = y \cdot (a + b))$	$\forall y ((b + a) \cdot y = y \cdot (a + b))$

In the first row the $f(c)$ inside $R(f(c), c)$ is written out in φ and stays; in the third the hole sits under $\forall y$, and both terms are free for z because neither contains y .

Not an instance. From $2 = 1 + 1$ and the line $2^5 = 32$, the line $(1 + 1)^5 = 3(1 + 1)$, which treats the digit 2 of 32 as an occurrence of the term 2, is not written by $=E$: the numeral 32 is one constant, with no occurrence of the term 2 inside it; $\varphi = (z^5 = 32)$ gives only $(1 + 1)^5 = 32$.

5.7.7 The rule, phrase and Lean table, completed

Chapter 1 began a table that pairs each rule with the sentence that performs it in a written proof and, for readers who use a proof assistant, with the Lean code that does the same (Sections 1.2–1.6), and Chapter 2 added the rows for negation, the biconditional, and the classical rules (Sections 2.1–2.5). Sections 5.3–5.6 added a row for each quantifier rule, and this section adds

the two rows for equality. Here is the whole table for the calculus of this volume.

Rule	Shape	You write
$\wedge I$	$\varphi, \psi \Longrightarrow \varphi \wedge \psi$	“We show P , and we show Q .”
$\wedge E$	$\varphi \wedge \psi \Longrightarrow \varphi$ (or ψ)	“In particular, P .”
$\rightarrow E$	$\varphi \rightarrow \psi, \varphi \Longrightarrow \psi$	“Since P implies Q , and P holds, Q .”
$\rightarrow I$	$\text{box } \varphi \dots \psi \Longrightarrow \varphi \rightarrow \psi$	“Assume P Hence Q .”
R	φ (available) $\Longrightarrow \varphi$, copied	“As shown above, P .”
$\vee I$	$\varphi \Longrightarrow \varphi \vee \psi$ (or $\psi \vee \varphi$)	“So P or Q holds.”
$\vee E$	$\varphi \vee \psi, \text{box } \varphi \dots \chi, \text{box } \psi \dots \chi \Longrightarrow \chi$	“Case 1: P so R . Case 2: Q so R . In either case, R .”
$\neg E$	$\varphi, \neg\varphi \Longrightarrow \perp$	“... , which contradicts ...”
$\perp E$	$\perp \Longrightarrow \text{any } \varphi$	“This case cannot occur.” “So there is nothing to prove.”
$\neg I$	$\text{box } \varphi \dots \perp \Longrightarrow \neg\varphi$	“Suppose φ This is a contradiction. Hence not φ .”
$\leftrightarrow I$	$\text{box } \varphi \dots \psi, \text{box } \psi \dots \varphi \Longrightarrow \varphi \leftrightarrow \psi$	“ $(\Rightarrow)$ Suppose P so Q . “ $(\Leftarrow)$ Suppose Q so P .”
$\leftrightarrow E$	$\varphi \leftrightarrow \psi, \varphi \Longrightarrow \psi$ (or with ψ, φ)	“Since P holds if and only if Q does, and P holds, so does Q .”
RAA	$\text{box } \neg\varphi \dots \perp \Longrightarrow \varphi$	“Suppose, for a contradiction, that φ fails. ... This is impossible. Hence φ .”
$\forall E$	$\forall x \varphi \Longrightarrow \varphi[t/x]$	“In particular, for $x = t$, ...”; “applying the hypothesis to t , ...”
$\forall I$	$\text{box } [x_0] \dots \varphi[x_0/x] \Longrightarrow \forall x \varphi$	“Let x be arbitrary. ... Since x was arbitrary, ...”
$\exists I$	$\varphi[t/x] \Longrightarrow \exists x \varphi$	“Take $x = t$. Then ...”
$\exists E$	$\exists x \varphi, \text{box } [x_0] \varphi[x_0/x] \dots \chi \Longrightarrow \chi$	“Choose x with Then ...”
$=I$	$\text{nothing} \Longrightarrow t = t$	(usually unwritten) “ $t = t$.”
$=E$	$t_1 = t_2, \varphi[t_1/x] \Longrightarrow \varphi[t_2/x]$	“Substituting t_2 for t_1 , ...”; a chain $t_1 = t_2 = \dots = t_n$

Remark (For Lean users). $\wedge I$ constructor; $\wedge E$ h.1, h.2; $\rightarrow E$ exact h hp; $\rightarrow I$ intro hp; R exact hp; $\vee I$ left, right (or Or.inl hp); $\vee E$ Or.elim h (or cases h); $\neg E$ exact hn hp (goal False); $\perp E$ exfalse; $\neg I$ intro hp (goal False); $\leftrightarrow I$ constructor; $\leftrightarrow E$ h.mp hp, h.mpr hq; RAA by_contra h; $\forall E$ h t (or specialize h t); $\forall I$ intro x; $\exists I$ use t (or Exists.intro t h); $\exists E$ obtain (or Exists.elim h); $=I$ rfl; $=E$ rw [h], chains calc. Nothing later depends on these.

Of the derived rules of Chapter 2, MT, CP and DS have their rows in Section 2.3, and $\neg\neg E$ and

LEM in Section 2.5; the derived sequents that searches use most are collected in Section 3.1. With the two equality rows, every rule of the calculus has its phrase.

Warning (Not allowed: $=E$). Each step breaks the clause of the reading of Definition 5.7.1, or the warning, shown.

- “From $c = f(b)$ and $Q(f(b))$, write $Q(c)$ ”: the equation is read left to right and rewrites c into $f(b)$; turn it round first, by (sym) (clause 2).
- “From $x = 0$ and $\forall x (x \geq x)$, write $\forall x (0 \geq 0)$ ”: only free occurrences are replaced, and both x ’s of $x \geq x$ are bound (the warning “A bound variable is not a place to substitute”).
- “From $b = z + 1$ and $\forall z (z \leq b)$, write $\forall z (z \leq z + 1)$ ”: with $\varphi = \forall z (z \leq w)$, the z of $z + 1$ is captured (clause 4).
- “Rewrite a term inside ‘it is obvious that ...’”: that is not a formula (the warning “Words about knowledge are not formulas”).

Remark (Looking ahead). Chapter 8 turns the “You write” column of this table into a full dictionary of proof phrases.

5.7.8 Exercises

5.7.8.1 A. Check your understanding

Exercise. A1

- (a) State $=I$ and $=E$ as schemas, with the side condition of $=E$.
 (b) In the derivation below, name for each of lines 4, 5, 6, and 8 the rule, the cited lines, and the formula φ (with a variable z as its hole).

1	$a = b + 1$	
2	$b = 2$	
3	$a \cdot a = a \cdot a$	$=I$
4	$a \cdot a = (b + 1) \cdot a$	$=E$ 1, 3
5	$a \cdot a = (b + 1) \cdot (b + 1)$	$=E$ 1, 4
6	$a \cdot a = (2 + 1) \cdot (2 + 1)$	$=E$ 2, 5
7	$(2 + 1) \cdot (2 + 1) = 9$	arith
8	$a \cdot a = 9$	$=E$ 7, 6

- (c) In the same derivation, could lines 4 and 5 be replaced by one line? With which φ ?
 (d) True or false, with a reason: from the lines $a = b$ and $P(b)$, one application of $=E$ gives $P(a)$.
 (e) True or false, with a reason: from $a = b$ and the line $\forall x (x = a \rightarrow P(x))$, one application of $=E$ gives $\forall x (x = b \rightarrow P(x))$.

Solution. (a) =I: at any line k , write $t = t$, for any term t , citing nothing. =E: from $t_1 = t_2$ on line i and $\varphi[t_1/x]$ on line j , both available at line k , write $\varphi[t_2/x]$ on line k ; side condition: t_1 and t_2 are both free for x in φ .

(b) Line 4: =E 1, 3, with $\varphi = (a \cdot a = z \cdot a)$, which rewrites the first a on the right. Line 5: =E 1, 4, with $\varphi = (a \cdot a = (b + 1) \cdot z)$. Line 6: =E 2, 5, with $\varphi = (a \cdot a = (z + 1) \cdot (z + 1))$, which rewrites both b 's at once. Line 8: =E 7, 6, with $\varphi = (a \cdot a = z)$. In each case the left-hand side $a \cdot a$ is written out in φ , so it is kept.

(c) Yes: =E 1, 3 with $\varphi = (a \cdot a = z \cdot z)$ gives $a \cdot a = (b + 1) \cdot (b + 1)$ in one step, rewriting both a 's on the right and keeping the two on the left.

(d) False. With the equation $a = b$, =E passes from $\varphi[a/x]$ to $\varphi[b/x]$. The line $P(b)$ is $\varphi[b/x]$ for $\varphi = P(x)$, so the rule would need the equation $b = a$. One application of symmetry first (Proposition 5.7.1 (a)) gives $b = a$, and then =E gives $P(a)$.

(e) True. Take $\varphi = \forall x (x = z \rightarrow P(x))$: the cited line is $\varphi[a/z]$ and the new line is $\varphi[b/z]$. The terms a and b are constants, so both are free for z , although the hole lies under $\forall x$.

Exercise. A2: Drill

Each part takes a line or two. The parts run from single steps, through a missing line and a justification column, to judging steps and short derivations. Letters a, b, c, d are constants.

- What does =I cite?
- From $a = b$ and $P(a, a)$, box the holes to get $P(a, b)$.
- From $c = d + 1$ and the line $R(c, c \cdot c)$, write the =E line that rewrites only the last c .
- From $x_0 = 2$ and $x_0 + x_0 = 4$, which φ gives $2 + x_0 = 4$?
- Line 6 is $f(b) + b = 7$, justified "=E 2, 5", and line 2 is $a = b$. Give two possible lines 5.
- Justify each line: 1 $a = b$, premise; 2 $\forall x (P(x) \rightarrow x = c)$, premise; 3 $P(a)$, premise; 4 $P(a) \rightarrow a = c$; 5 $a = c$; 6 $a = a$; 7 $b = a$; 8 $b = c$.
- From $a = b$ and $P(b)$, does one =E give $P(a)$?
- From $a = y$ and $\exists y (y < a)$, is $\exists y (y < y)$ a legal =E line?
- From $x_0 = 0$ and the line $\forall y (x_0 \leq y)$, is $\forall y (0 \leq y)$ a legal =E line? From $y = 0$ and the same line, is $\forall y (x_0 \leq 0)$?
- Derive $a = b \vdash f(b) = f(a)$.
- Derive $a = b, b = c \vdash a = c$ in one step.
- Derive $\forall x R(x, x) \vdash \forall x \forall y (x = y \rightarrow R(x, y))$.

Solution.

- Nothing.
- Box the second a only: $\varphi = P(a, z)$.
- $R(c, c \cdot (d + 1))$, with $\varphi = R(c, c \cdot z)$.
- $\varphi = (z + x_0 = 4)$.
- Any two of $f(a) + a = 7$ ($\varphi = (f(z) + z = 7)$), $f(b) + a = 7$ ($\varphi = (f(b) + z = 7)$),

- $f(a) + b = 7$ ($\varphi = (f(z) + b = 7)$); and the degenerate $f(b) + b = 7$ itself.
- (f) 4 $\forall E$ 2 (at a); 5 $\rightarrow E$ 4, 3; 6 $=I$; 7 $=E$ 1, 6 ($\varphi = (z = a)$); 8 $=E$ 5, 7 ($\varphi = (b = z)$).
- (g) No, clause 2: the equation rewrites a into b . Turn it round first (sym), then $=E$.
- (h) No, clause 4: the y put in would be captured by $\exists y$.
- (i) The first is legal: $\varphi = \forall y (z \leq y)$, and 0 is free for z . The second is not: with $\varphi = \forall y (x_0 \leq z)$, the term y of the equation is not free for z in φ (clause 4); the y would be captured.
- (j) 2 $f(a) = f(a)$, $=I$; 3 $f(b) = f(a)$, $=E$ 1, 2, with $\varphi = (f(z) = f(a))$.
- (k) 3 $a = c$, $=E$ 2, 1, with $\varphi = (a = z)$.
- (l) A flagged box x_0 , inside it a flagged box y_0 : 2 $x_0 = y_0$, assumption; 3 $R(x_0, x_0)$, $\forall E$ 1; 4 $R(x_0, y_0)$, $=E$ 2, 3 ($\varphi = R(x_0, z)$); 5 $x_0 = y_0 \rightarrow R(x_0, y_0)$, $\rightarrow I$ 2–4; 6 $\forall y (x_0 = y \rightarrow R(x_0, y))$, $\forall I$ 2–5; 7 $\forall x \forall y (x = y \rightarrow R(x, y))$, $\forall I$ 2–6. (A reflexive relation contains equality.)

5.7.8.2 B. Practice

Exercise. B1: The identity is unique

A set with an operation $\cdot$ has an **identity** e if $e \cdot x = x$ and $x \cdot e = x$ for every x . Derive

$$\forall x (e \cdot x = x \wedge x \cdot e = x), \quad \forall x (e' \cdot x = x \wedge x \cdot e' = x) \vdash e = e',$$

where e and e' are constants. Which half of “there is exactly one identity” does this prove?

Hint: look at the one element that both premises can say something about.

Solution. The goal is an equation between e and e' , and the only term that both premises can connect to both is the product $e \cdot e'$. Instantiate the first premise at e' and the second at e ($\forall E$, reading the terms off the goal):

1	$\forall x (e \cdot x = x \wedge x \cdot e = x)$	
2	$\forall x (e' \cdot x = x \wedge x \cdot e' = x)$	
3	$e \cdot e' = e' \wedge e' \cdot e = e'$	$\forall E$ 1
4	$e \cdot e' = e'$	$\wedge E$ 3
5	$e' \cdot e = e \wedge e \cdot e' = e$	$\forall E$ 2
6	$e \cdot e' = e$	$\wedge E$ 5
7	$e = e'$	$=E$ 6, 4

Line 7 uses the equation $e \cdot e' = e$ of line 6 to rewrite the left side of line 4, with $\varphi = (z = e')$: $\varphi[e \cdot e'/z]$ is line 4, and $\varphi[e/z]$ is $e = e'$. In prose: $e = e \cdot e' = e'$, the first equation because e' is an identity and the second because e is.

This is the “at most one” half: any two identities are equal. It says nothing about whether an identity exists. Section 5.8 shows how such an argument combines with existence.

Exercise. B2: Rewrite, and turn round

A search for $a = b$, $b = c$, $P(a) \vdash P(c) \wedge c = a$ has reached the stage below. Name the move, then complete it, giving for each $=E$ line its holes.

1		$a = b$	
2		$b = c$	
3		$P(a)$	
		$\vdots$	
9		$P(c) \wedge c = a$	?

Solution. The move is the search step “An equation” of this section: mark the holes, and turn the equation round with an $=I$ line if it points the wrong way.

1		$a = b$	
2		$b = c$	
3		$P(a)$	
4		$P(b)$	$=E\ 1, 3$
5		$P(c)$	$=E\ 2, 4$
6		$a = c$	$=E\ 2, 1$
7		$a = a$	$=I$
8		$c = a$	$=E\ 6, 7$
9		$P(c) \wedge c = a$	$\wedge I\ 5, 8$

Lines 4 and 5: $\varphi = P(z)$. Line 6: $\varphi = (a = z)$, so line 1 is $\varphi[b/z]$ and the equation $b = c$ refills the hole with c . Line 8: $\varphi = (z = a)$; line 7 is $\varphi[a/z]$, and the equation $a = c$ refills the box with c . Lines 7–8 are (sym) written out; with the abbreviation of the text, line 8 is “ $c = a$ (sym) 6”.

Exercise. B3: Derive or break

For each claim, derive it with the rules of Chapters 1–2 and of this chapter, or break it with a counter-reading.

- (a) $f(a) = b, a = c \vdash f(c) = b$.
- (b) $f(a) = f(b) \vdash a = b$.
- (c) $\forall x (f(x) = x) \vdash f(f(c)) = c$.
- (d) $\forall x \forall y (f(x) = f(y) \rightarrow x = y), f(a) = f(b) \vdash a = b$.
- (e) $a \neq b, b \neq c \vdash a \neq c$.
- (f) $a = b, b \neq c \vdash a \neq c$.
- (g) $f(a) = a \vdash f(f(a)) = a$.

(h) $f(f(a)) = a \vdash f(a) = a$.

Solution.

(a) Derive. One $=E$, with $\varphi = (f(z) = b)$:

1		$f(a) = b$	
2		$a = c$	
3		$f(c) = b$	$=E\ 2, 1$

(b) Break. Counter-reading: the domain $\{0, 1\}$, f sending both to 0, a naming 0 and b naming 1. Then $f(a) = 0 = f(b)$, and $a = b$ is false.

(c) Derive. Instantiate at the compound term $f(c)$ as well as at c :

1		$\forall x (f(x) = x)$	
2		$f(f(c)) = f(c)$	$\forall E\ 1$
3		$f(c) = c$	$\forall E\ 1$
4		$f(f(c)) = c$	$=E\ 3, 2$

Line 4 has $\varphi = (f(f(c)) = z)$.

(d) Derive.

1		$\forall x \forall y (f(x) = f(y) \rightarrow x = y)$	
2		$f(a) = f(b)$	
3		$\forall y (f(a) = f(y) \rightarrow a = y)$	$\forall E\ 1$
4		$f(a) = f(b) \rightarrow a = b$	$\forall E\ 3$
5		$a = b$	$\rightarrow E\ 4, 2$

(e) Break. Counter-reading: the domain $\{0, 1\}$, a and c naming 0, b naming 1. Then $a \neq b$ and $b \neq c$ are true, and $a \neq c$ is false: two different letters, one object.

(f) Derive.

1		$a = b$	
2		$b \neq c$	
3			asm, for $\neg I$
4			
5			
6			

Line 4 has $\varphi = (z = c)$.

(g) Derive.

1		$f(a) = a$	
2		$f(f(a)) = f(f(a))$	$=I$
3		$f(f(a)) = f(a)$	$=E\ 1, 2$
4		$f(f(a)) = a$	$=E\ 1, 3$

Line 3 has $\varphi = (f(f(a)) = f(z))$, and line 4 has $\varphi = (f(f(a)) = z)$.

- (h) Break. Counter-reading: the domain $\{0, 1\}$, f exchanging 0 and 1, a naming 0. Then $f(f(0)) = f(1) = 0$, so the premise is true, and $f(0) = 1$, so $f(a) = a$ is false.
- (i) and (d) differ by the premise that f is one-to-one; (e) and (f) look alike, and $\neq$ is not transitive, since different letters may name one object; (g) and (h) are converses. Worked example types: [Proposition 5.7.1](#); the chain derivation of “Calculations are chains of substitutions”; the congruence derivation.

Marking scheme. (10 points) 1 for each of the eight claims (a derivation with every φ named, or a counter-reading with the domain and every symbol’s value); 2 for the closing comparison, with the point about (e) and (f) stated. Fatal errors (0 for the claim): an $=E$ with the equation read right to left; a counter-reading in which two letters that must differ (by a premise) name one object.

5.7.8.3 C. Going deeper

Exercise. C1: Two different objects

- (a) Derive $\exists x \exists y (x \neq y) \vdash \forall x \exists y (x \neq y)$, and name the line that uses a classical rule.
- (b) Read both formulas aloud. Derive the converse, or break it.

Solution.

- (a) Read off the goal and the premise. The premise is an existential (twice), so both $\exists E$ boxes open first, with names x_0 and y_0 . The goal is universal, so a flagged box u_0 opens inside them. The new goal $\exists y (u_0 \neq y)$ is postponed, and no available line decides whether u_0 is x_0 , so the search splits by LEM:

1	$\exists x \exists y (x \neq y)$	
2	$x_0 \mid \exists y (x_0 \neq y)$	asm, for $\exists E$
3	$y_0 \mid x_0 \neq y_0$	asm, for $\exists E$
4	$u_0 \mid u_0 = x_0 \vee u_0 \neq x_0$	LEM
5	$u_0 = x_0$	asm, for $\vee E$
6	$u_0 = y_0$	asm, for $\neg I$
7	$x_0 = y_0$	=E 5, 6
8	$\perp$	$\neg E$ 7, 3
9	$u_0 \neq y_0$	$\neg I$ 6–8
10	$\exists y (u_0 \neq y)$	$\exists I$ 9
11	$u_0 \neq x_0$	asm, for $\vee E$
12	$\exists y (u_0 \neq y)$	$\exists I$ 11
13	$\exists y (u_0 \neq y)$	$\vee E$ 4, 5–10, 11–12
14	$\forall x \exists y (x \neq y)$	$\forall I$ 4–13
15	$\forall x \exists y (x \neq y)$	$\exists E$ 2, 3–14
16	$\forall x \exists y (x \neq y)$	$\exists E$ 1, 2–15

Line 7 is =E with $\varphi = (z = y_0)$: line 6 is $\varphi[u_0/z]$, and the equation $u_0 = x_0$ refills the hole with x_0 . The classical line is line 4, LEM, a derived rule whose derivation uses RAA (Section 2.5). At line 14, u_0 appears in no premise, in neither open assumption (lines 2 and 3) and not in line 14. At lines 15 and 16 the witnesses y_0 and x_0 appear neither in the last lines, nor in the existentials, nor in the open assumptions.

- (b) The premise says “there are two different objects”; the conclusion says “every object has one different from it”. The converse derives: 2 $\exists y (x \neq y)$, $\forall E$ 1 (at x); 3 $\exists x \exists y (x \neq y)$, $\exists I$ 2 (witness x). Over a one-element domain both are false; over larger ones both are true.

Marking scheme. (10 points) 2: two $\exists E$ boxes with different names, each aimed at the goal it must reach. 2: a flagged box u_0 for the $\forall$ (inside or outside the $\exists E$ boxes), and the goal postponed. 3: the split on $u_0 = x_0$, with the first case reaching $u_0 \neq y_0$ by $\neg I$ and =E, and the second giving the witness x_0 at once. 1: the classical line named, with the reason. 2: (b), the converse derived, with both readings. An RAA box on $\neg \exists y (u_0 \neq y)$ in place of the LEM split earns full marks if correct, its RAA line then named as the classical one. Fatal errors (0 for the step): the flag u_0 chosen as x_0 ; an $\exists E$ box closed on a line that mentions its witness.