

2.4 Iff, Equivalence, and What a Definition Says

One connective is still without rules: “if and only if”. Theorems say “ n is odd if and only if n^2 is odd”, and every definition, though written with a plain “if”, is used as an “if and only if”. Section 1.1 warned that “if” means different things in a theorem and in a definition; this section explains why. The one new thing here is the pair of rules for $\leftrightarrow$; the rest of the section (provable equivalence, the layout of an “iff” proof, the convention about definitions, chains of equivalences) is what the rules are used for.

2.4.1 The rules for “if and only if”

“ P if and only if Q ” combines “ P if Q ”, which is $Q \rightarrow P$, with “ P only if Q ”, which is $P \rightarrow Q$, as Section 1.1 explained. A proof of it travels both ways; a use of it, either way. An implication is proved by a box, opened on the hypothesis and closed on the conclusion (Definition 1.4.1); an “if and only if” needs two such boxes.

An “if and only if” is two implications, and proving it takes two proofs.

Definition 2.4.1. Rules for the Biconditional

i	φ	asm, for $\leftrightarrow I$
	$\vdots$	
j	ψ	
k	ψ	asm, for $\leftrightarrow I$
	$\vdots$	
l	φ	
m	$\varphi \leftrightarrow \psi$	$\leftrightarrow I$ $i-j, k-l$

i	$\varphi \leftrightarrow \psi$		i	$\varphi \leftrightarrow \psi$	
j	φ		j	ψ	
k	ψ	$\leftrightarrow E$ i, j	k	φ	$\leftrightarrow E$ i, j

The first schema is the rule $\leftrightarrow I$ (**iff-introduction**); its two assumptions are discharged when their boxes close, and each box’s last line (ψ in the first, φ in the second) is a line **of that box itself**, not of a box inside it. The two schemas below it are the two forms of $\leftrightarrow E$ (**iff-elimination**).

As in every schema (Definition 1.2.1), φ and ψ stand for any statements, replaced consistently, and i, j, k, l, m for line numbers. Read the rules clause by clause.

1. **Two boxes.** $\leftrightarrow I$ needs two available boxes: one opened by φ and ending in ψ , the other opened by ψ and ending in φ , each last line a line of its own box. Each is exactly the box $\rightarrow I$ would need for one direction. Their order does not matter, but both must be there: a single box from φ to ψ proves $\varphi \rightarrow \psi$ and nothing more. Each box’s assumption is printed

- “asm, for $\leftrightarrow$ I”; in a written proof the two boxes are the paragraphs ($\Rightarrow$) and ($\Leftarrow$).
2. **Separate boxes.** The boxes are siblings, not nested, so nothing in the second may cite a line of the first (the scope rule of Definition 1.4.2). Each direction is a proof on its own.
 3. **Citation.** The justification cites both boxes as ranges, as in $\leftrightarrow$ I 2–4, 5–7.
 4. **Elimination, either way.** From $\varphi \leftrightarrow \psi$ and φ on available lines, $\leftrightarrow$ E writes ψ ; from $\varphi \leftrightarrow \psi$ and ψ , it writes φ . It is modus ponens in whichever direction we need, citing the biconditional first.

In the Givens/Goal table, $\leftrightarrow$ I splits a row in two: φ added to the Givens with the goal ψ , and ψ added with the goal φ .

2.4.2 First derivations with iff

The section’s goal-directed move: **a goal $\varphi \leftrightarrow \psi$ opens two boxes**, one on each side, and each box’s goal is the other side.

Example. An iff read both ways

- (a) Show that $P \leftrightarrow Q \vdash Q \leftrightarrow P$.
- (b) Show that $P \leftrightarrow Q, \neg Q \vdash \neg P$.

Solution.

- (a) *Idea.* The goal is an iff, so the last line is $\leftrightarrow$ I, and we need a box from Q to P and a box from P to Q . Each box’s goal is one $\leftrightarrow$ E away: the premise crosses from its assumption to the other side.

The goal at the foot (left), then its two boxes (right).

1	$P \leftrightarrow Q$	
2	Q	asm, for $\leftrightarrow$ I
	$\vdots$	
3	P	
4	P	asm, for $\leftrightarrow$ I
	$\vdots$	
5	Q	
6	$Q \leftrightarrow P$	$\leftrightarrow$ I 2–3, 4–5

The finished derivation:

1	$P \leftrightarrow Q$	
2	Q	asm, for $\leftrightarrow$ I
3	P	$\leftrightarrow$ E 1, 2
4	P	asm, for $\leftrightarrow$ I
5	Q	$\leftrightarrow$ E 1, 4
6	$Q \leftrightarrow P$	$\leftrightarrow$ I 2–3, 4–5

Line 3 uses the second form of $\leftrightarrow$ E (right to left), line 5 the first.

- (b) *Idea.* The goal $\neg P$ is a negation, so open a box on P and aim at $\perp$ (Section 2.2). Inside, the premise $P \leftrightarrow Q$ turns P into Q , and Q clashes with $\neg Q$.

1		$P \leftrightarrow Q$	
2		$\neg Q$	
3			asm, for $\neg$ I
4			
5			
6		$\neg P$	$\neg$ I 3–5

This is the derivation of Proposition 2.3.1 with $\leftrightarrow$ E on line 4: if two statements are equivalent and one fails, so does the other.

The rules say nothing that the two implications do not say. The next result makes this exact.

Proposition 2.4.1. An Iff Is Two Implications

$P \leftrightarrow Q \vdash (P \rightarrow Q) \wedge (Q \rightarrow P)$, and $(P \rightarrow Q) \wedge (Q \rightarrow P) \vdash P \leftrightarrow Q$.

Idea. Each goal chooses its rule. For the first, the goal is a conjunction of two implications: $\wedge$ I needs both, and each is built in its own $\rightarrow$ I box, crossing the premise with $\leftrightarrow$ E inside. For the second, the goal is an iff: open its two boxes. The premise is a conjunction, so take it apart first (premise-directed), and cross each box with one of its halves by $\rightarrow$ E.

First claim: the two implications as goals (left), then their boxes (right).

1		$P \leftrightarrow Q$	
		$\vdots$	
4		$P \rightarrow Q$	
		$\vdots$	
7		$Q \rightarrow P$	
8		$(P \rightarrow Q) \wedge (Q \rightarrow P)$	$\wedge$ I 4, 7

1	$P \leftrightarrow Q$	
2	P	asm, for $\rightarrow$ I
	$\vdots$	
3	Q	
4	$P \rightarrow Q$	$\rightarrow$ I 2–3
5	Q	asm, for $\rightarrow$ I
	$\vdots$	
6	P	
7	$Q \rightarrow P$	$\rightarrow$ I 5–6
8	$(P \rightarrow Q) \wedge (Q \rightarrow P)$	$\wedge$ I 4, 7

Second claim: the premise taken apart (left), then the two boxes (right).

1	$(P \rightarrow Q) \wedge (Q \rightarrow P)$	
2	$P \rightarrow Q$	$\wedge$ E 1
3	$Q \rightarrow P$	$\wedge$ E 1
	$\vdots$	
8	$P \leftrightarrow Q$	

1	$(P \rightarrow Q) \wedge (Q \rightarrow P)$	
2	$P \rightarrow Q$	$\wedge$ E 1
3	$Q \rightarrow P$	$\wedge$ E 1
4	P	asm, for $\leftrightarrow$ I
	$\vdots$	
5	Q	
6	Q	asm, for $\leftrightarrow$ I
	$\vdots$	
7	P	
8	$P \leftrightarrow Q$	$\leftrightarrow$ I 4–5, 6–7

Proof. For the first claim, the following is a derivation with premise $P \leftrightarrow Q$ and last line $(P \rightarrow Q) \wedge (Q \rightarrow P)$.

1	$P \leftrightarrow Q$	
2	P	asm, for $\rightarrow$ I
3	Q	$\leftrightarrow$ E 1, 2
4	$P \rightarrow Q$	$\rightarrow$ I 2–3
5	Q	asm, for $\rightarrow$ I
6	P	$\leftrightarrow$ E 1, 5
7	$Q \rightarrow P$	$\rightarrow$ I 5–6
8	$(P \rightarrow Q) \wedge (Q \rightarrow P)$	$\wedge$ I 4, 7

For the second claim, the following is a derivation with premise $(P \rightarrow Q) \wedge (Q \rightarrow P)$ and last line $P \leftrightarrow Q$.

1	$(P \rightarrow Q) \wedge (Q \rightarrow P)$	
2	$P \rightarrow Q$	$\wedge$ E 1
3	$Q \rightarrow P$	$\wedge$ E 1
4	P	asm, for $\leftrightarrow$ I
5	Q	$\rightarrow$ E 2, 4
6	Q	asm, for $\leftrightarrow$ I
7	P	$\rightarrow$ E 3, 6
8	$P \leftrightarrow Q$	$\leftrightarrow$ I 4–5, 6–7

Lines 2 and 3 lie in no box, so both boxes may cite them. This proves both claims. ■

🔄 **Second reading** · *Why iff keeps its own rules*

So $\leftrightarrow$ could have been an abbreviation for $(P \rightarrow Q) \wedge (Q \rightarrow P)$. We keep it as a connective with its own rules, so that every connective is proved by an introduction rule and used by an elimination rule.

Example. Negating both sides of an iff

Show that $P \leftrightarrow Q \vdash \neg P \leftrightarrow \neg Q$.

Solution. Idea. The goal is an iff, so there are two boxes, one opened by $\neg P$ and reaching $\neg Q$, the other the reverse. Each box's goal is a negation, so each contains a $\neg$ I box: the goal-directed move applied twice, one inside the other. Inside the inner box, $\leftrightarrow$ E crosses from one side of the premise to the other, and the result clashes with the outer assumption. The second half is part (b) of [Example \(An iff read both ways\)](#), run inside a box; the first is

its mirror image, with the other form of $\leftrightarrow E$.

The outer boxes (left), then a $\neg I$ box inside each (right).

1	$P \leftrightarrow Q$		1	$P \leftrightarrow Q$	
2	$\neg P$	asm, for $\leftrightarrow I$	2	$\neg P$	asm, for $\leftrightarrow I$
	$\vdots$		3	Q	asm, for $\neg I$
6	$\neg Q$			$\vdots$	
7	$\neg Q$	asm, for $\leftrightarrow I$	5	$\perp$	
	$\vdots$		6	$\neg Q$	$\neg I$ 3–5
11	$\neg P$		7	$\neg Q$	asm, for $\leftrightarrow I$
12	$\neg P \leftrightarrow \neg Q$	$\leftrightarrow I$ 2–6, 7–11	8	P	asm, for $\neg I$
				$\vdots$	
			10	$\perp$	
			11	$\neg P$	$\neg I$ 8–10
			12	$\neg P \leftrightarrow \neg Q$	$\leftrightarrow I$ 2–6, 7–11

The finished derivation:

1	$P \leftrightarrow Q$	
2	$\neg P$	asm, for $\leftrightarrow I$
3	Q	asm, for $\neg I$
4	P	$\leftrightarrow E$ 1, 3
5	$\perp$	$\neg E$ 4, 2
6	$\neg Q$	$\neg I$ 3–5
7	$\neg Q$	asm, for $\leftrightarrow I$
8	P	asm, for $\neg I$
9	Q	$\leftrightarrow E$ 1, 8
10	$\perp$	$\neg E$ 9, 7
11	$\neg P$	$\neg I$ 8–10
12	$\neg P \leftrightarrow \neg Q$	$\leftrightarrow I$ 2–6, 7–11

The two halves are mirror images.

Quick check. In the derivation of [Example \(Negating both sides of an iff\)](#), which line does line 5 cite as $\neg\varphi$, and why may it?

Solution. Line 2, $\neg P$, the assumption of the outer box 2–6, which is still open at line 5.

The derivation uses only the rules of this section and of Sections 2.1–2.2. Its converse, $\neg P \leftrightarrow \neg Q \vdash P \leftrightarrow Q$, is also derivable, with the rule of Section 2.5: in the box of P it must produce the **positive** statement Q , and the natural box, on $\neg Q$, closes to $\neg\neg Q$, not Q .

Example (Negating both sides of an iff) negated both sides of an iff. Can one side be the negation of the other, a statement equivalent to its own negation?

Lemma 2.4.2. No Statement Is Equivalent to Its Negation

$\vdash \neg(P \leftrightarrow \neg P)$.

Idea. The goal is a negation: open a $\neg$ I box on $P \leftrightarrow \neg P$, with goal $\perp$. $\leftrightarrow$ E needs one side of the iff on a line, and neither is. So make $\neg P$ a subgoal, by a $\neg$ I box on P : inside it $\leftrightarrow$ E gives $\neg P$, which clashes with P . With $\neg P$ in hand, $\leftrightarrow$ E the other way gives P , and the two clash again.

The outer box (left), then the subgoal $\neg P$ with its box (right).

1		$P \leftrightarrow \neg P$	asm, for $\neg$ I
		$\vdots$	
7		$\perp$	
8		$\neg(P \leftrightarrow \neg P)$	$\neg$ I 1–7

1		$P \leftrightarrow \neg P$	asm, for $\neg$ I
2		P	asm, for $\neg$ I
		$\vdots$	
4		$\perp$	
5		$\neg P$	$\neg$ I 2–4
		$\vdots$	
7		$\perp$	
8		$\neg(P \leftrightarrow \neg P)$	$\neg$ I 1–7

Proof. The following is a derivation with no premises and last line $\neg(P \leftrightarrow \neg P)$.

1		$P \leftrightarrow \neg P$	asm, for $\neg$ I
2		P	asm, for $\neg$ I
3		$\neg P$	$\leftrightarrow$ E 1, 2
4		$\perp$	$\neg$ E 2, 3
5		$\neg P$	$\neg$ I 2–4
6		P	$\leftrightarrow$ E 1, 5
7		$\perp$	$\neg$ E 6, 5
8		$\neg(P \leftrightarrow \neg P)$	$\neg$ I 1–7

Line 5 may be cited at lines 6 and 7: it lies in the box 1–7, as they do. No rule of Section 2.5 is used.

■

In words: no statement is equivalent to its own negation; a definition that made a term mean the failure of that very term would define nothing.

For an instance, let x be a real number. The sentence “ $x > 0$ if and only if $x \leq 0$ ” is false whatever x is: by the convention of Section 2.1, $x \leq 0$ is $\neg(x > 0)$, so the sentence is an instance of $P \leftrightarrow \neg P$, and the lemma, used as a derived rule, refutes every instance.

Quick check. In the proof of [Lemma 2.4.2](#), which two lines use the biconditional, and in which direction?

Solution. Line 3, from the left side P (line 2) to the right side $\neg P$; and line 6, from the right side $\neg P$ (line 5) back to the left side P .

2.4.3 Provable equivalence

[Proposition 2.4.1](#) is a pair of sequents, one in each direction. It is not the first such pair: [Proposition 1.4.2](#) and [Proposition 1.6.1](#) are pairs too. When two statements can each be derived from the other, either may stand in for the other in any derivation, and the situation deserves a name.

Two statements are provably equivalent when each can be derived from the other.

Definition 2.4.2. Provable Equivalence

Statements P and Q are **provably equivalent**, written $P \dashv\vdash Q$, if $P \vdash Q$ and $Q \vdash P$.

In words: there is a derivation with premise P and last line Q , and **another** with premise Q and last line P . The symbol is the turnstile of [Definition 1.2.3](#) written twice, back to back; two derivations prove the claim.

A first example is $P \wedge Q \dashv\vdash Q \wedge P$: [Proposition 1.2.1](#) derives $Q \wedge P$ from $P \wedge Q$, and the same derivation with P and Q exchanged derives $P \wedge Q$ from $Q \wedge P$. By the same exchange, [Example \(First derivations with “or”\)](#) gives $P \vee Q \dashv\vdash Q \vee P$, and part (a) of [Example \(An iff read both ways\)](#) gives $P \leftrightarrow Q \dashv\vdash Q \leftrightarrow P$.

🔄 **Second reading** · *Edge cases of provable equivalence*

The degenerate example is $P \dashv\vdash P$: the one-line derivation of part (a) of [Example \(Derivations, simplest first\)](#) serves in both directions.

A minimal change gives a one-way street. [Example \(Two negations from one premise\)](#) derived $P \vdash \neg\neg P$, but the converse, $\neg\neg P \vdash P$, would have to remove two negations, and no rule met

so far removes one. So we cannot claim $P \dashv\vdash \neg\neg P$: the clause “ $Q \vdash P$ ” is the one missing. (It holds once Section 2.5 adds its rule.) Likewise Proposition 2.3.2 derives $\neg Q \rightarrow \neg P$ from $P \rightarrow Q$, but not yet the reverse.

The connective $\leftrightarrow$ and the relation $\dashv\vdash$ are two sides of one idea; the next result makes the link exact, and shows that $\dashv\vdash$ behaves as an equivalence should.

Proposition 2.4.3. Provable Equivalence and the Biconditional

For all statements P, Q, R :

- (a) $P \dashv\vdash Q$ if and only if $\vdash P \leftrightarrow Q$;
- (b) $P \dashv\vdash P$; if $P \dashv\vdash Q$, then $Q \dashv\vdash P$; and if $P \dashv\vdash Q$ and $Q \dashv\vdash R$, then $P \dashv\vdash R$.

In words: one derivation of $P \leftrightarrow Q$ from no premises is worth two derivations, one each way; and $\dashv\vdash$ can be used like $=$ in a calculation.

🕒 **Second reading** • *The proof: copying derivations*

Idea. Everything here moves whole derivations around. To prove $\vdash P \leftrightarrow Q$, the two boxes of $\leftrightarrow$ I are the two given derivations, with their premises turned into the boxes’ assumptions. To use $\vdash P \leftrightarrow Q$, write out its derivation and apply $\leftrightarrow$ E. For transitivity, run one derivation into the next: the last line of the first is the premise of the second.

Proof. We use one observation twice. Let D be a derivation, and copy its lines, in order and with their numbers shifted, to some place in another derivation, with every line of the copy inside the same boxes as that place. Then every citation inside the copy is still available: if line i of D is available at line k of D , every box of D containing line i contains line k , and the boxes added around the copy contain both lines. Closed boxes cited in D are handled the same way. So each copied line is justified by the same rule as before.

($\Rightarrow$) in (a). Suppose $P \vdash Q$ and $Q \vdash P$, by derivations D_1 and D_2 . Build a derivation with no premises as follows. Open a box with the assumption P and, below it, copy D_1 , turning each of its premise lines P into a repetition of the assumption by (D3) of Definition 1.4.2. By the observation, the copy is justified, and its last line Q is a line of the box itself, since the last line of D_1 lies in none of D_1 ’s boxes. Close the box. Open a second box with Q , copy D_2 in the same way, and close it on P . Then $\leftrightarrow$ I on the two boxes gives $P \leftrightarrow Q$. So $\vdash P \leftrightarrow Q$.

($\Leftarrow$) in (a). Suppose $\vdash P \leftrightarrow Q$, by a derivation D with no premises. For $P \vdash Q$, start with the premise P , copy D below it, and write Q by $\leftrightarrow$ E from the last line of the copy, $P \leftrightarrow Q$, and line 1. Both cited lines lie in no box, so both are available. For $Q \vdash P$, do the same with premise Q , using the other form of $\leftrightarrow$ E. So $P \dashv\vdash Q$.

- (b) The one-line derivation consisting of the premise P shows $P \vdash P$, in both directions, so $P \dashv\vdash P$. Symmetry holds because Definition 2.4.2 says the same thing about P, Q as about Q, P . For transitivity it is enough to show that $P \vdash Q$ and $Q \vdash R$ give $P \vdash R$,

since the reverse direction is the same statement with P and R exchanged. Take a derivation D_1 of Q from P , and below its last line copy a derivation D_2 of R from Q , turning each premise line Q of D_2 into a repetition of the last line of D_1 . That line lies in no box, so it is available everywhere below it, and by the observation the rest of the copy is justified. The result has premise P and last line R . This proves the proposition. ■

Here are equivalences derived so far. Each row gives two derived rules (Definition 2.3.1), one in each direction.

Provable equivalence	Derived in
$P \wedge Q \dashv\vdash Q \wedge P$	Proposition 1.2.1, with the letters exchanged for the converse
$P \vee Q \dashv\vdash Q \vee P$	Example (First derivations with “or”), likewise
$(P \wedge Q) \rightarrow R \dashv\vdash P \rightarrow (Q \rightarrow R)$	Proposition 1.4.2
$P \wedge (Q \vee R) \dashv\vdash (P \wedge Q) \vee (P \wedge R)$	Proposition 1.6.1
$(P \rightarrow R) \wedge (Q \rightarrow R) \dashv\vdash (P \vee Q) \rightarrow R$	Example (Cases on a hypothesis are two implications) and Example (A disjunctive hypothesis splits into two implications)
$P \leftrightarrow Q \dashv\vdash (P \rightarrow Q) \wedge (Q \rightarrow P)$	Proposition 2.4.1
$P \leftrightarrow Q \dashv\vdash Q \leftrightarrow P$	Example (An iff read both ways) (a), with the letters exchanged
$\neg\neg\neg P \dashv\vdash \neg P$	Example (Three negations become one), and Example (Two negations from one premise) (a) with $\neg P$ for P

The fourth row is distributivity of $\wedge$ over $\vee$ as a provable equivalence. Some familiar laws are not in the table, because the text has derived them in one direction only; associativity of $\vee$ is one (Example (Regrouping a disjunction)).

Warning. A sequent in one direction is not an equivalence. $P \wedge Q \vdash P$ holds by $\wedge E$, but the form “from P conclude $P \wedge Q$ ” breaks: take P : “ $2 > 1$ ” and Q : “ $1 > 2$ ”, and the premise is true while the conclusion is false. Before writing $\dashv\vdash$, check that **both** derivations exist.

2.4.4 Proving an iff: two directions

In a written proof, the two boxes of $\leftrightarrow I$ become two paragraphs: $(\Rightarrow)$ assumes the left side and reaches the right, $(\Leftarrow)$ the reverse. Neither may borrow the other’s assumption: they are two separate boxes.

The first example completes the story of parity. We use the facts (E1)–(E3) of Section 2.1: every integer is even or odd; no integer is both even and odd; the square of an odd integer is odd.

Theorem 2.4.4. Odd Square, Odd Number

Let n be an integer. Then n is odd if and only if n^2 is odd.

Idea. Two boxes. Forwards is (E3). Backwards, “ n^2 is odd” gives nothing to compute with, so split on (E1) and show the even case impossible, as in Example (An impossible case).

Proof. ($\Rightarrow$) This is (E3).

($\Leftarrow$) Suppose n^2 is odd [assumption for the second box]. By (E1), n is even or odd, and we argue by cases [$\vee$ E]. If n is odd, we are done. If n is even, say $n = 2k$ with k an integer, then $n^2 = 2(2k^2)$ is even; so n^2 is both even and odd [$\wedge$ I], which contradicts (E2) [$\neg$ E]. So this case cannot occur, and n is odd in it too [$\perp$ E]. In both cases n is odd.

This proves the theorem [$\leftrightarrow$ I].

■

With the derived rules of Section 2.3, ($\Leftarrow$) fits in one breath, “ n cannot be even, since then n^2 would be even; so n is odd”: $\neg$ I with (E2), then MT, then DS on (E1).

The next example is about real numbers, and its two directions do different work. Each hypothesis is needed: dropping either one breaks one of the two directions, as the remark after the proof shows.

Theorem 2.4.5. Squaring Preserves Order

Let x and y be real numbers with $x \geq 0$ and $y \geq 0$. Then

$$x \leq y \iff x^2 \leq y^2.$$

Idea. Forwards, multiply $x \leq y$ by $x \geq 0$ and by $y \geq 0$, and chain. Backwards, nothing undoes squaring without square roots, so we split instead: either $x \leq y$, which is the goal, or $y < x$. In the second case the forward argument, run with a strict inequality, gives $y^2 < x^2$, which clashes with the hypothesis: an impossible case, closed by $\perp$ E.

Proof. ($\Rightarrow$) Suppose $x \leq y$. Multiplying by $x \geq 0$ gives $x^2 \leq xy$, and multiplying by $y \geq 0$ gives $xy \leq y^2$. Hence $x^2 \leq y^2$.

($\Leftarrow$) Suppose $x^2 \leq y^2$. For real numbers, $x \leq y$ or $y < x$, and we argue by cases [$\vee$ E]. If $x \leq y$, we are done. If $y < x$, then $x > y \geq 0$, so $x > 0$. Multiplying $y < x$ by $x > 0$ gives $xy < x^2$, and multiplying $y < x$ by $y \geq 0$ gives $y^2 \leq xy$. Hence $y^2 < x^2$, which contradicts $x^2 \leq y^2$ [$\neg$ E]; so this case cannot occur, and $x \leq y$ holds in it [$\perp$ E]. In both cases $x \leq y$.

This proves the theorem [$\leftrightarrow$ I].

■

Remark. Each hypothesis has a job. The direction $(\Rightarrow)$ needs $x \geq 0$, and fails without it: $x = -2$, $y = 1$ gives $x \leq y$ but $x^2 = 4 > 1 = y^2$. (Its proof also multiplied by $y \geq 0$, but there $y \geq 0$ already follows from $y \geq x \geq 0$.) The direction $(\Leftarrow)$ used only $y \geq 0$, and fails without it: $x = 1$, $y = -2$ gives $x^2 = 1 \leq 4 = y^2$ but $x > y$.

A payoff comes at once. For $a, b \geq 0$, apply [Theorem 2.4.5](#) to $x = \sqrt{a}$ and $y = \sqrt{b}$: $\sqrt{a} \leq \sqrt{b}$ if and only if $a \leq b$. Taking square roots preserves order, a fact used constantly in estimates. (That square roots of non-negative numbers exist is a school fact here.)

Quick check. Here is a proof of the statement “for a real number x , $x^2 = 1$ if and only if $x = 1$ or $x = -1$ ”.

If $x = 1$, then $x^2 = 1 \cdot 1 = 1$. If $x = -1$, then $x^2 = (-1)(-1) = 1$. This proves the claim.

Which direction has been proved, and which is missing? Supply the missing one.

Solution. The proof assumes the right side, “ $x = 1$ or $x = -1$ ”, splits it into its two cases, and reaches $x^2 = 1$ in both. So it proves $(\Leftarrow)$, by $\vee$ E. The direction $(\Rightarrow)$ is missing.

$(\Rightarrow)$ Suppose $x^2 = 1$. Then $(x - 1)(x + 1) = x^2 - 1 = 0$. A product of real numbers is zero only if one of the factors is zero, so $x - 1 = 0$ or $x + 1 = 0$, that is, $x = 1$ or $x = -1$.

Warning. A proof of an iff can prove one direction twice and look complete. For “ n is odd if and only if n^2 is odd”, a proof that shows “if n is odd, then n^2 is odd” and then “if n^2 is not odd, then n is not odd” has proved $(\Rightarrow)$ and its contrapositive (Proposition 2.3.2), which is $(\Rightarrow)$ again. The direction $(\Leftarrow)$, “if n^2 is odd, then n is odd”, is still missing; its contrapositive would be “if n is not odd, then n^2 is not odd”. Before writing “this proves the theorem”, check that one paragraph assumes each side.

2.4.5 What a definition says

Here is a definition written the way this book and most others write definitions.

A function $f: \mathbb{R} \rightarrow \mathbb{R}$ is **strictly increasing** if, for all real numbers x and y , $x < y$ implies $f(x) < f(y)$.

Grammatically the sentence is an implication, “ f is strictly increasing **if** [condition]”, and read as a theorem it would allow only one move, from the condition to the term. But a definition is not a theorem. It introduces a new term, and the new term means **exactly** the condition: no more, since nothing else was said about the term, and no less, since the condition is all the term was made to express. So the definition is used in both directions, as an $\leftrightarrow$ between the term and the condition, and $\leftrightarrow$ E is how it is used.

In a definition, “if” means “if and only if”.

This is a convention of mathematical language, not a rule of logic. Some books write “iff” or $:\Leftrightarrow$

in definitions; this book, like most, writes “if” and puts the term defined in **bold**, which signals that the “if” is an “iff”. Here it is used three ways.

Example. A definition used in both directions

- (a) Show that $f(x) = 3x - 5$ defines a strictly increasing function $f: \mathbb{R} \rightarrow \mathbb{R}$.
- (b) Suppose $g: \mathbb{R} \rightarrow \mathbb{R}$ is strictly increasing. Show that $g(1) < g(2)$.
- (c) Show that $h(x) = x^2$ does not define a strictly increasing function $h: \mathbb{R} \rightarrow \mathbb{R}$.

Solution.

- (a) Let x and y be real numbers with $x < y$. Multiplying by $3 > 0$ gives $3x < 3y$, and subtracting 5 gives $3x - 5 < 3y - 5$, that is, $f(x) < f(y)$. So f satisfies the condition, and by the definition, read from right to left, f is strictly increasing [$\leftrightarrow$ E].
- (b) Since g is strictly increasing, the definition, read from left to right, says that $x < y$ implies $g(x) < g(y)$ for all real x and y [$\leftrightarrow$ E]. Taking $x = 1$ and $y = 2$, and using $1 < 2$, we get $g(1) < g(2)$ [$\rightarrow$ E].
- (c) Suppose h were strictly increasing [assumption for $\neg$ I]. By the definition read from left to right, as in (b), $-1 < 0$ would give $h(-1) < h(0)$, that is, $1 < 0$, which is false [$\neg$ E]. So h is not strictly increasing [$\neg$ I].

Part (a) uses the definition from the condition to the term; parts (b) and (c) use it from the term to the condition. A definition read only as an “if” would permit (a) and nothing else. Because the term means exactly the condition, a candidate condition is judged against the intended meaning. Had the definition said “ $x < y$ implies $f(x) \leq f(y)$ ”, it would be too broad: the constant function $f(x) = 0$ would count as strictly increasing. Had it said “ $x < y$ implies $f(y) - f(x) \geq 1$ ”, it would be too narrow: $f(x) = x$ would not count, since $0 < \frac{1}{2}$ and $\frac{1}{2} - 0 < 1$.

Warning. The convention is for **definitions only**. In a theorem, “if” means “if”, one direction. The theorem “if $6 \mid n$, then n is even” is true for every integer n : $n = 6k = 2(3k)$. Its converse, “if n is even, then $6 \mid n$ ”, breaks at $n = 4$. Reading a theorem’s “if” as “iff” means proving its converse without a proof, which is the error of Argument B in Section 1.1.

🕒 **Second reading** · *The same slip in calculus*

A familiar theorem of calculus says: if f is differentiable at a , then f is continuous at a . Its converse is false. The function $f(x) = |x|$ is continuous at 0, but it is not differentiable there, since its graph has a corner: the quotient $|h|/h$ is 1 for $h > 0$ and -1 for $h < 0$.

Quick check. Write the converse of “if a real number x satisfies $x > 2$, then $x^2 > 4$ ”, and break it.

Solution. The converse is “if $x^2 > 4$, then $x > 2$ ”. The value $x = -3$ breaks it: $(-3)^2 = 9 > 4$, and $-3 > 2$ fails.

2.4.6 Chains of equivalences

“The following are equivalent: (a), (b), (c)” means that any two of the three are equivalent: three iff statements, or six implications. Three implications suffice, if they go round in a cycle:

$$(a) \Rightarrow (b) \Rightarrow (c) \Rightarrow (a).$$

Once the cycle is proved, any condition leads to any other by following the arrows round. Here is the derivation behind that sentence.

Proposition 2.4.6. Proving Equivalence by a Cycle

$P \rightarrow Q$, $Q \rightarrow R$, $R \rightarrow P \vdash P \leftrightarrow Q$. Likewise, from the same three premises, $Q \leftrightarrow R$ and $R \leftrightarrow P$ are derivable.

Idea. The goal is an iff, so there are two boxes. From P , one step along the cycle reaches Q . From Q , the cycle reaches P the long way round, through R : a backward chain of $\rightarrow$ E, as in Section 1.3. The other two equivalences need no new work, because the three premises do not change when the letters are rotated.

The goal at the foot (left), then its two boxes (right).

1	$P \rightarrow Q$	1	$P \rightarrow Q$	
2	$Q \rightarrow R$	2	$Q \rightarrow R$	
3	$R \rightarrow P$	3	$R \rightarrow P$	
		4	P	asm, for $\leftrightarrow$ I
	$\vdots$		$\vdots$	
		5	Q	
9	$P \leftrightarrow Q$	6	Q	asm, for $\leftrightarrow$ I
			$\vdots$	
		8	P	
		9	$P \leftrightarrow Q$	$\leftrightarrow$ I 4–5, 6–8

Proof. The following is a derivation with the three premises and last line $P \leftrightarrow Q$.

1	$P \rightarrow Q$	
2	$Q \rightarrow R$	
3	$R \rightarrow P$	
4	P	asm, for $\leftrightarrow$ I
5	Q	$\rightarrow$ E 1, 4
6	Q	asm, for $\leftrightarrow$ I
7	R	$\rightarrow$ E 2, 6
8	P	$\rightarrow$ E 3, 7
9	$P \leftrightarrow Q$	$\leftrightarrow$ I 4–5, 6–8

Now replace P, Q, R throughout by Q, R, P respectively. The premises $P \rightarrow Q, Q \rightarrow R, R \rightarrow P$ become $Q \rightarrow R, R \rightarrow P, P \rightarrow Q$, the same three statements in a different order, and every line remains justified by the same rule, since the letters stood for any statements (as in clause 2 after Definition 2.3.1). So the renamed derivation derives $Q \leftrightarrow R$ from the same premises. Rotating once more gives $R \leftrightarrow P$. This proves the proposition. ■

In a cycle every condition reaches every other along the arrows; longer cycles work the same way, with longer chains of $\rightarrow$ E in the boxes.

Warning. Two arrows back and forth are not a cycle through three conditions. Proving (a) $\Rightarrow$ (b) and (b) $\Rightarrow$ (a) shows that (a) and (b) are equivalent and says nothing about (c): no arrow enters or leaves it. For a real number x , take (a) “ $x > 0$ ”, (b) “ $2x > 0$ ”, and (c) “ $x > 1$ ”. Both arrows between (a) and (b) are true, and (c) is not equivalent to them: $x = \frac{1}{2}$ satisfies (a) and (b) but not (c). Every condition in the list must lie on the cycle.

Example. Three descriptions of the unit interval

Let x be a real number. Prove that the following are equivalent.

- (a) $0 < x < 1$.
- (b) $x^2 < x$.
- (c) $x > 0$ and $1/x > 1$.

Solution. By Proposition 2.4.6 it suffices to prove (a) $\Rightarrow$ (b) $\Rightarrow$ (c) $\Rightarrow$ (a).

(a) $\Rightarrow$ (b). Suppose $0 < x < 1$. Multiplying $x < 1$ by $x > 0$ gives $x^2 < x$.

(b) $\Rightarrow$ (c). Suppose $x^2 < x$. First, $x > 0$: otherwise $x \leq 0$, and then $x \leq 0 \leq x^2$, so $x \leq x^2$, which contradicts $x^2 < x$. (In rules: we have $x \leq 0$ or $x > 0$; the first is refuted by a $\neg$ I box, and DS (Proposition 2.3.4) leaves the second.) Since $x > 0$, we may divide $x^2 < x$ by x , which gives $x < 1$, and then divide $x < 1$ by x , which gives $1 < 1/x$. So $x > 0$ and $1/x > 1$.

(c) $\Rightarrow$ (a). Suppose $x > 0$ and $1/x > 1$. Multiplying $1 < 1/x$ by $x > 0$ gives $x < 1$. So

$$0 < x < 1.$$

The order of the cycle was a choice, made so that each arrow was short: (b) $\Rightarrow$ (c) carried the only case split. The reverse cycle would also do, with different arrows to prove.

2.4.7 The rule card

Before the card, the two rules at work on large statements.

Example. Instances of $\leftrightarrow$ I and $\leftrightarrow$ E

Rule	Letters replaced	Cited	New line
$\leftrightarrow$ I	$\varphi := P \wedge Q,$ $\psi := Q \wedge P$	box $P \wedge Q \dots$ $Q \wedge P$, box $Q \wedge P \dots$ $P \wedge Q$	$(P \wedge Q) \leftrightarrow (Q \wedge P)$
$\leftrightarrow$ E	$\varphi := \neg P,$ $\psi := Q \rightarrow R$	$\neg P \leftrightarrow (Q \rightarrow R),$ $Q \rightarrow R$	$\neg P$ (the second form)
$\leftrightarrow$ E	$\varphi := P \vee Q, \psi := \neg R$	$(P \vee Q) \leftrightarrow \neg R,$ $P \vee Q$	$\neg R$

Not an instance. From two lines $P \rightarrow Q$ and $Q \rightarrow P$, the line “ $P \leftrightarrow Q$ — $\leftrightarrow$ I” is not an instance: $\leftrightarrow$ I cites two boxes, not two implications. The two lines give the iff through [Proposition 2.4.1](#) used as a derived rule (after $\wedge$ I), or by opening the two boxes.

Chapter 1’s seven rules are on the card at the end of Section 1.6; here are this chapter’s so far.

Rule	Shape	You write	Lean
$\neg$ E	$\varphi, \neg\varphi \Rightarrow \perp$	“..., which contradicts ...”	<code>exact hn hp</code> (goal <code>False</code>)
$\perp$ E	$\perp \Rightarrow \text{any } \varphi$	“This case cannot occur.” “So there is nothing to prove.”	<code>exfalso</code>
$\neg$ I	box $\varphi \dots \perp \Rightarrow \neg\varphi$	“Suppose P This is a contradiction. Hence not P .”	<code>intro hp</code> (goal <code>False</code>)
MT	$\varphi \rightarrow \psi, \neg\psi \Rightarrow \neg\varphi$ (derived)	“Since Q fails, so does P .”	<code>mt h hnq</code>
CP	$\varphi \rightarrow \psi \Rightarrow \neg\psi \rightarrow \neg\varphi$ (derived)	“We prove the contrapositive: suppose not Q ; ... so not P .”	<code>mt</code>
DS	$\varphi \vee \psi, \neg\varphi \Rightarrow \psi$ (derived)	“ P is impossible, so Q .”	<code>h.resolve_left hnp</code>
$\leftrightarrow$ I	box $\varphi \dots \psi$, box $\psi \dots \varphi \Rightarrow \varphi \leftrightarrow \psi$	“ $(\Rightarrow)$ Suppose P so Q . $(\Leftarrow)$ Suppose Q so P .”	<code>constructor</code>

Rule	Shape	You write	Lean
$\leftrightarrow E$	$\varphi \leftrightarrow \psi, \varphi \implies \psi$ (or with ψ, φ)	“Since P holds if and only if Q does, and P holds, so does Q .”	<code>h.mp hp / h.mpr hq</code>

The rows for this section’s rules complete the table for the connectives. The Lean names in the last column come from the two fields of an iff, `mp` (“modus ponens”, left to right) and `mpr` (right to left).

Warning (Not allowed: $\leftrightarrow I$ and $\leftrightarrow E$). Each step below is wrong; the tag names the clause it breaks.

- Close $\leftrightarrow I$ with one box: clause 1, two boxes (a single box proves $\varphi \rightarrow \psi$ only).
- In the second box, cite a line of the first: clause 2, the boxes are siblings (the pair below).
- Write $\neg\psi$ by $\leftrightarrow E$ from $\varphi \leftrightarrow \psi$ and $\neg\varphi$: clause 4, $\leftrightarrow E$ needs one side itself; $\neg\psi$ takes a $\neg I$ box.
- Write $\varphi \leftrightarrow \psi$ by $\leftrightarrow I$ citing two implication lines: clause 3, the rule cites boxes, as ranges (the look-alike of [Example \(Instances of \$\leftrightarrow I\$ and \$\leftrightarrow E\$ \)](#)).

Clause 2 is where the rule bites: WRONG beside RIGHT, with premises $P \rightarrow Q$, R and $(Q \wedge R) \rightarrow P$. On the left, line 7 copies P from the closed first box.

1	$P \rightarrow Q$		1	$P \rightarrow Q$	
2	R		2	R	
3	$(Q \wedge R) \rightarrow P$		3	$(Q \wedge R) \rightarrow P$	
4	$\begin{array}{ c} P \end{array}$	asm, for $\leftrightarrow I$	4	$\begin{array}{ c} P \end{array}$	asm, for $\leftrightarrow I$
5	$\begin{array}{ c} Q \end{array}$	$\rightarrow E$ 1, 4	5	$\begin{array}{ c} Q \end{array}$	$\rightarrow E$ 1, 4
6	$\begin{array}{ c} Q \end{array}$	asm, for $\leftrightarrow I$	6	$\begin{array}{ c} Q \end{array}$	asm, for $\leftrightarrow I$
7	$\begin{array}{ c} P \end{array}$	R 4	7	$\begin{array}{ c} Q \wedge R \end{array}$	$\wedge I$ 6, 2
8	$P \leftrightarrow Q$	$\leftrightarrow I$ 4–5, 6–7	8	$\begin{array}{ c} P \end{array}$	$\rightarrow E$ 3, 7
			9	$P \leftrightarrow Q$	$\leftrightarrow I$ 4–5, 6–8

The left list never cites premises 2 and 3, so it would show $P \rightarrow Q \vdash P \leftrightarrow Q$, which breaks: with P : “ $x > 5$ ” and Q : “ $x > 3$ ”, at $x = 4$ the premise is true and $P \leftrightarrow Q$ is false.

Remark (Looking ahead). Chapter 5 uses the lemma $\neg(P \leftrightarrow \neg P)$ to show that no barber can shave exactly those who do not shave themselves, and in what sense no set can contain exactly the sets that do not contain themselves. *Analysis on the Real Line*, Chapter 1 proves from its axioms that every non-negative real number has a square root, the school fact behind the square-root payoff above.

2.4.8 Exercises

2.4.8.1 A. Check your understanding

Exercise. A1

- (a) State the rules $\leftrightarrow I$ and $\leftrightarrow E$, and the definition of $P \dashv\vdash Q$.
- (b) For a real number $x \geq 0$, consider “ $x^2 = x$ if and only if $x = 0$ or $x = 1$ ”. Write the directions $(\Rightarrow)$ and $(\Leftarrow)$ as implications. Which one would a proof begin with “Suppose $x^2 = x$ ”?
- (c) True or false, with a reason: from the definition “an integer n is **even** if there is an integer k with $n = 2k$ ” and the fact that 10 is even, we may conclude that $10 = 2k$ for some integer k .
- (d) True or false, with a reason: from the theorem “if $x > 1$, then $x^2 > 1$ ” and the fact that $x^2 > 1$, we may conclude that $x > 1$.

Solution.

- (a) $\leftrightarrow I$: from a box $\varphi \dots \psi$ and a box $\psi \dots \varphi$, both available, write $\varphi \leftrightarrow \psi$. $\leftrightarrow E$: from $\varphi \leftrightarrow \psi$ and either side, write the other (Definition 2.4.1). $P \dashv\vdash Q$ means $P \vdash Q$ and $Q \vdash P$ (Definition 2.4.2).
- (b) $(\Rightarrow)$: if $x^2 = x$, then $x = 0$ or $x = 1$. $(\Leftarrow)$: if $x = 0$ or $x = 1$, then $x^2 = x$. The direction $(\Rightarrow)$ begins “Suppose $x^2 = x$ ”, since it assumes the left side.
- (c) True. A definition’s “if” means “if and only if”, so the definition may be used from the term “even” to the condition, by $\leftrightarrow E$. (Indeed $k = 5$.)
- (d) False. A theorem’s “if” is one direction only, and the conclusion would be its converse. The converse fails at $x = -2$: $x^2 = 4 > 1$ but $x < 1$.

Exercise. A2: Drill

The parts run from one step, through a missing line, a justification column and steps to judge, to short derivations.

- (a) Lines 1 $P \leftrightarrow Q$, 2 Q . What does “ $\leftrightarrow E$ 1, 2” write?
- (b) A box 3–6 runs from $P \vee Q$ to $\neg R$, and a box 7–9 from $\neg R$ to $P \vee Q$. What does “ $\leftrightarrow I$ 3–6, 7–9” write?
- (c) Write “ $x^2 = 4$ if and only if $x = 2$ or $x = -2$ ” as two implications. Which begins “Suppose $x^2 = 4$ ”?
- (d) Definition: “an integer n is a **multiple of 3** if $n = 3k$ for some integer k ”. From $12 = 3 \cdot 4$, what follows, reading the definition which way?
- (e) Line 6 is $Q \wedge R$, justified “ $\leftrightarrow E$ 2, 5”, and line 2 is $P \leftrightarrow (Q \wedge R)$. What is line 5?
- (f) Line 12 is $\neg P \leftrightarrow Q$, justified “ $\leftrightarrow I$ 4–7, 8–11”. What are lines 4, 7, 8 and 11?
- (g) Fill in the justifications (i)–(iv).

1		$P \leftrightarrow \neg Q$	
2		Q	
3			P (i)
4			$\neg Q$ (ii)
5			$\perp$ (iii)
6		$\neg P$	(iv)

- (h) Lines 1 $P \leftrightarrow Q$, 2 $\neg P$. Does $\leftrightarrow E$ give anything?
- (i) A box 2–4 runs from P to Q ; a box 5–7 from Q to P , and line 6 cites line 3. Is “ $P \leftrightarrow Q$ — $\leftrightarrow I$ 2–4, 5–7” correct?
- (j) One box runs from P to Q . What does it prove?
- (k) True or false: $P \dashv\vdash Q$ says no more than $\vdash P \rightarrow Q$.
- (l) A proof that (a), (b), (c) are equivalent proves (a) $\Rightarrow$ (b), (b) $\Rightarrow$ (a) and (b) $\Rightarrow$ (c). Is it complete?
- (m) Derive $P \leftrightarrow Q$, $P \vdash Q \wedge P$.
- (n) Derive $P \leftrightarrow Q$, $Q \leftrightarrow R$, $R \vdash P$.
- (o) Derive $P \leftrightarrow Q$, $\neg P \vdash \neg Q$.

Solution.

- (a) P , by the second form.
- (b) $(P \vee Q) \leftrightarrow \neg R$: the first box’s assumption on the left, its last line on the right.
- (c) ($\Rightarrow$) if $x^2 = 4$, then $x = 2$ or $x = -2$; ($\Leftarrow$) the converse. The direction ($\Rightarrow$) begins “Suppose $x^2 = 4$ ”.
- (d) 12 is a multiple of 3, reading the definition from the condition to the term ($\leftrightarrow E$).
- (e) P , the left side, so that the first form writes the right side $Q \wedge R$.
- (f) Line 4 is $\neg P$ and line 7 is Q (the first box); line 8 is Q and line 11 is $\neg P$ (the second).
- (g) (i) assumption, for $\neg I$; (ii) $\leftrightarrow E$ 1, 3; (iii) $\neg E$ 2, 4; (iv) $\neg I$ 3–5.
- (h) No: $\leftrightarrow E$ needs P or Q itself. $\neg Q$ comes by a $\neg I$ box, as in part (o).
- (i) No: line 6 cites line 3, inside the closed sibling box 2–4.
- (j) $P \rightarrow Q$, by $\rightarrow I$; not $P \leftrightarrow Q$.
- (k) False: it says $P \vdash Q$ and $Q \vdash P$, two derivations (equivalently $\vdash P \leftrightarrow Q$); $\vdash P \rightarrow Q$ is only half of it.
- (l) No: no arrow leaves (c). Add (c) $\Rightarrow$ (a) or (c) $\Rightarrow$ (b).
- (m) 3 Q , $\leftrightarrow E$ 1, 2; 4 $Q \wedge P$, $\wedge I$ 3, 2.
- (n) 4 Q , $\leftrightarrow E$ 2, 3; 5 P , $\leftrightarrow E$ 1, 4.
- (o) 3 Q , assumption, for $\neg I$; 4 P , $\leftrightarrow E$ 1, 3; 5 $\perp$, $\neg E$ 4, 2; 6 $\neg Q$, $\neg I$ 3–5.

2.4.8.2 B. Practice

Exercise. B1: Iff is transitive

Show that $P \leftrightarrow Q, Q \leftrightarrow R \vdash P \leftrightarrow R$.

Solution. The goal is an iff, so we open two boxes: P to R , and R to P . In each, the premises are used as bridges, one after the other, by $\leftrightarrow E$.

1		$P \leftrightarrow Q$	
2		$Q \leftrightarrow R$	
3			asm, for $\leftrightarrow I$
4		P	
5		Q	$\leftrightarrow E$ 1, 3
6		R	$\leftrightarrow E$ 2, 4
7		R	asm, for $\leftrightarrow I$
8		Q	$\leftrightarrow E$ 2, 6
9		P	$\leftrightarrow E$ 1, 7
10		$P \leftrightarrow R$	$\leftrightarrow I$ 3–5, 6–8

Lines 4 and 8 use $P \leftrightarrow Q$ in opposite directions, as do lines 5 and 7 with $Q \leftrightarrow R$.

Exercise. B2: A parity equivalence

Let n be an integer. Prove that n is even if and only if $n + 3$ is odd.

Solution. ($\Rightarrow$) Suppose n is even, say $n = 2k$ with k an integer. Then $n + 3 = 2k + 2 + 1 = 2(k + 1) + 1$, and $k + 1$ is an integer, so $n + 3$ is odd.

($\Leftarrow$) Suppose $n + 3$ is odd, say $n + 3 = 2j + 1$ with j an integer. Then $n = 2j - 2 = 2(j - 1)$, and $j - 1$ is an integer, so n is even.

This proves the equivalence.

Exercise. B3: Strict inequalities

Let x and y be real numbers with $x \geq 0$ and $y \geq 0$. Deduce from [Theorem 2.4.5](#) and [Example \(Negating both sides of an iff\)](#) that $x < y$ if and only if $x^2 < y^2$. You may use that, for real numbers a and b , $a < b$ holds exactly when $b \leq a$ fails.

- Apply [Theorem 2.4.5](#) with the roles of x and y exchanged. What does it say?
- Use [Example \(Negating both sides of an iff\)](#) as a derived rule on (a): with which statements in place of P and Q , and what does it give?
- Translate both sides of (b) with the fact quoted.
- What have you proved?

Solution.

- (a) The exchange is allowed, since both numbers are non-negative: $y \leq x$ if and only if $y^2 \leq x^2$.
- (b) With P : “ $y \leq x$ ” and Q : “ $y^2 \leq x^2$ ”, [Example \(Negating both sides of an iff\)](#), used as a derived rule (Definition 2.3.1), gives: $y \leq x$ fails if and only if $y^2 \leq x^2$ fails.
- (c) By the fact quoted, the left side says $x < y$ and the right side says $x^2 < y^2$.
- (d) That $x < y$ if and only if $x^2 < y^2$.

Exercise. B4: Both directions

A search for $P \leftrightarrow Q \vdash (P \wedge R) \leftrightarrow (Q \wedge R)$ has reached the stage below. *Name the move, then complete it.*

1	$P \leftrightarrow Q$	
	$\vdots$	
12	$(P \wedge R) \leftrightarrow (Q \wedge R)$	?

Solution. The move is *two boxes for an iff*: the goal’s main connective is $\leftrightarrow$, so line 12 will be $\leftrightarrow$ I, with a box from $P \wedge R$ to $Q \wedge R$ and a box back. Inside each, take the conjunction apart, cross with $\leftrightarrow$ E, and rebuild.

1	$P \leftrightarrow Q$	
2	$P \wedge R$	asm, for $\leftrightarrow$ I
3	P	$\wedge$ E 2
4	R	$\wedge$ E 2
5	Q	$\leftrightarrow$ E 1, 3
6	$Q \wedge R$	$\wedge$ I 5, 4
7	$Q \wedge R$	asm, for $\leftrightarrow$ I
8	Q	$\wedge$ E 7
9	R	$\wedge$ E 7
10	P	$\leftrightarrow$ E 1, 8
11	$P \wedge R$	$\wedge$ I 10, 9
12	$(P \wedge R) \leftrightarrow (Q \wedge R)$	$\leftrightarrow$ I 2–6, 7–11

The second box never cites a line of the first: line 10 gets P afresh from line 8.

Exercise. B5: Criticize the definition

For real numbers a, b, x , we want to define “ x lies **strictly between** a and b ”, meaning that one of a, b is less than x and x is less than the other. Here are five candidate conditions.

- (i) $a < x$ and $x < b$.
 - (ii) $a < x$ or $x < b$.
 - (iii) $(a < x \text{ and } x < b) \text{ or } (b < x \text{ and } x < a)$.
 - (iv) $(x - a)(x - b) < 0$.
 - (v) $x \leq a$ fails and $b \leq x$ fails.
- (a) For each, say whether it is too broad (it admits a triple a, b, x that should be excluded), too narrow (it excludes one that should be admitted), or right, giving a triple for each fault.
 - (b) A definition is read as an iff. Prove that (iii) and (iv) are equivalent.
 - (c) Which candidates would make “if x lies strictly between a and b , then x lies strictly between b and a ” false? Give one triple that shows it for all of them.

Solution.

- (a) (i) Too narrow: $a = 5, b = 2, x = 3$ lies between and fails (i). It is not too broad: (i) gives one of the wanted orders.
- (ii) Too broad: $a = 2, b = 5, x = 100$ satisfies $2 < 100$ but does not lie between. And too narrow: $a = 5, b = 2, x = 3$ lies between, but $5 < 3$ and $3 < 2$ both fail (the triple of (c)).
- (iii) Right: it lists the two possible orders.
- (iv) Right, by (b).
- (v) This is (i) in negative dress: by the convention of Section 2.1, “ $x \leq a$ fails” is $a < x$ and “ $b \leq x$ fails” is $x < b$. So it is too narrow, by the same triple as (i), and needlessly negative.
- (b) ($\Rightarrow$) In the case $a < x < b$, $x - a > 0$ and $x - b < 0$, so the product is negative. In the case $b < x < a$, $x - a < 0$ and $x - b > 0$, so again the product is negative. The two cases are $\vee$ E on (iii).
 ($\Leftarrow$) Suppose the product is negative. Then neither factor is 0, and the two factors cannot have the same sign, since a product of two positive or of two negative numbers is positive. So $x - a > 0 > x - b$, that is $a < x < b$, or $x - a < 0 < x - b$, that is $b < x < a$.
- (c) (i), (ii) and (v). With $a = 2, b = 5, x = 3$, each holds for the ends 2, 5 and fails for the ends 5, 2 (for (ii): $2 < 3$, while neither $5 < 3$ nor $3 < 2$). A definition of “between” should not depend on the order of the two ends; (iii) and (iv) do not, since exchanging a and b exchanges the two disjuncts of (iii) and the two factors of (iv).

Marking scheme. (10 points) - 4: (a), one point each for (i) and (v) with a correct triple, one for (ii) with **both** triples (too broad and too narrow), and one for calling (iii) and (iv) right. - 4: (b), each direction 2; the second must say why the factors have opposite signs. - 2: (c), (i), (ii) and (v) with one triple.

Fatal error (0 for (b)): proving only one direction and calling the conditions equivalent.

Exercise. B6: Four conditions, one cycle

Let n be an integer. Prove by one cycle of four implications that the following are equivalent.

- (i) n is odd.
- (ii) $n + 1$ is even.
- (iii) $8 \mid n^2 - 1$.
- (iv) n^2 is odd.

You may use [Theorem 2.4.4](#) and the fact that $k(k - 1)$ is even for every integer k . Then: a proof that proved only (i) $\Leftrightarrow$ (ii) and (iii) $\Leftrightarrow$ (iv) would be incomplete; which two implications would complete it most cheaply?

Solution. We prove the cycle (i) $\Rightarrow$ (ii) $\Rightarrow$ (iii) $\Rightarrow$ (iv) $\Rightarrow$ (i). It suffices by the argument of [Proposition 2.4.6](#): for any two conditions, each reaches the other by a chain of $\rightarrow$ E along the arrows, inside the two boxes of $\leftrightarrow$ I.

(i) $\Rightarrow$ (ii). If $n = 2k + 1$, then $n + 1 = 2(k + 1)$.

(ii) $\Rightarrow$ (iii). If $n + 1 = 2j$, then $n - 1 = 2(j - 1)$, so $n^2 - 1 = (n - 1)(n + 1) = 4j(j - 1)$. By the fact quoted, $j(j - 1) = 2m$ for an integer m , so $n^2 - 1 = 8m$.

(iii) $\Rightarrow$ (iv). If $n^2 - 1 = 8m$, then $n^2 = 2(4m) + 1$, which is odd.

(iv) $\Rightarrow$ (i). This is [Theorem 2.4.4](#), read from right to left.

(Exercise B3 of Section 1.6 met the fact (i) $\Rightarrow$ (iii) by another route.)

For the second question: (i) $\Rightarrow$ (iv) and (iv) $\Rightarrow$ (i). Both are [Theorem 2.4.4](#), so they cost nothing. Any two implications joining the two pairs, one in each direction, would do, for instance (ii) $\Rightarrow$ (iii) and (iv) $\Rightarrow$ (i); with them every condition reaches every other.

Marking scheme. (10 points) - 1: a cycle through all four conditions, citing the argument of [Proposition 2.4.6](#) or arguing that it suffices. - 8: 2 for each of the four arrows. - 1: the completion question.

Fatal errors (0 for the step): a “cycle” that omits a condition; (iii) $\Rightarrow$ (iv) or (iv) $\Rightarrow$ (i) argued by examples.

Exercise. B7: Derive or break

For each claim, derive it with the rules of Chapter 1 and Sections 2.1–2.4, or break it by statements about a real number x that make its counterexample set true.

- (a) $P \leftrightarrow Q \vdash (P \vee R) \leftrightarrow (Q \vee R)$.
- (b) $(P \vee R) \leftrightarrow (Q \vee R) \vdash P \leftrightarrow Q$.
- (c) $P \leftrightarrow (Q \wedge R) \vdash P \rightarrow Q$.
- (d) $P \leftrightarrow (Q \wedge R) \vdash Q \rightarrow P$.
- (e) $P \leftrightarrow Q, Q \leftrightarrow \neg R \vdash \neg(P \wedge R)$.
- (f) $P \leftrightarrow Q \vdash \neg(P \wedge \neg Q)$.

- (g) $\neg(P \wedge \neg Q) \vdash P \leftrightarrow Q$.
 (h) $P \leftrightarrow Q, P \vee Q \vdash P \wedge Q$.

Solution.

- (a) Derive. Two boxes for the iff, and a case split inside each.

1	$P \leftrightarrow Q$		
2		$P \vee R$	asm, for $\leftrightarrow$ I
3		P	asm, for $\vee$ E
4		Q	$\leftrightarrow$ E 1, 3
5		$Q \vee R$	$\vee$ I 4
6		R	asm, for $\vee$ E
7		$Q \vee R$	$\vee$ I 6
8		$Q \vee R$	$\vee$ E 2, 3–5, 6–7
9		$Q \vee R$	asm, for $\leftrightarrow$ I
10		Q	asm, for $\vee$ E
11		P	$\leftrightarrow$ E 1, 10
12		$P \vee R$	$\vee$ I 11
13		R	asm, for $\vee$ E
14		$P \vee R$	$\vee$ I 13
15		$P \vee R$	$\vee$ E 9, 10–12, 13–14
16	$(P \vee R) \leftrightarrow (Q \vee R)$		$\leftrightarrow$ I 2–8, 9–15

- (b) Break. Take P : “ $x > 0$ ”, Q : “ $x > 5$ ”, R : “ $x > -1$ ”. At $x = 1$, $P \vee R$ and $Q \vee R$ are both true, so the premise is true; P is true and Q false, so $P \leftrightarrow Q$ is false. The counterexample set (Definition 1.1.3) $(P \vee R) \leftrightarrow (Q \vee R), \neg(P \leftrightarrow Q)$ is true at $x = 1$.

- (c) Derive.

1		$P \leftrightarrow (Q \wedge R)$	
2			P asm, for $\rightarrow$ I
3			$Q \wedge R$ $\leftrightarrow$ E 1, 2
4			Q $\wedge$ E 3
5		$P \rightarrow Q$ $\rightarrow$ I 2–4	

- (d) Break. Take P : “ $x > 5$ ”, Q : “ $x > 0$ ”, R : “ $x > 3$ ”. At $x = 1$, $Q \wedge R$ and P are both false, so the premise is true, while $Q \rightarrow P$ is false, since Q is true and P false. The counterexample set is true at $x = 1$.

- (e) Derive.

1	$P \leftrightarrow Q$	
2	$Q \leftrightarrow \neg R$	
3	$P \wedge R$	asm, for $\neg$ I
4	P	$\wedge$ E 3
5	Q	$\leftrightarrow$ E 1, 4
6	$\neg R$	$\leftrightarrow$ E 2, 5
7	R	$\wedge$ E 3
8	$\perp$	$\neg$ E 7, 6
9	$\neg(P \wedge R)$	$\neg$ I 3–8

(f) Derive.

1	$P \leftrightarrow Q$	
2	$P \wedge \neg Q$	asm, for $\neg$ I
3	P	$\wedge$ E 2
4	Q	$\leftrightarrow$ E 1, 3
5	$\neg Q$	$\wedge$ E 2
6	$\perp$	$\neg$ E 4, 5
7	$\neg(P \wedge \neg Q)$	$\neg$ I 2–6

(g) Break. Take P : “ $x > 5$ ”, Q : “ $x > 0$ ”. At $x = 1$, $P \wedge \neg Q$ is false, since P is, so the premise is true; P is false and Q true, so $P \leftrightarrow Q$ is false. The counterexample set is true at $x = 1$.

(h) Derive. Split on the second premise; in each case $\leftrightarrow$ E supplies the other letter.

1	$P \leftrightarrow Q$	
2	$P \vee Q$	
3	P	asm, for $\vee$ E
4	Q	$\leftrightarrow$ E 1, 3
5	$P \wedge Q$	$\wedge$ I 3, 4
6	Q	asm, for $\vee$ E
7	P	$\leftrightarrow$ E 1, 6
8	$P \wedge Q$	$\wedge$ I 7, 6
9	$P \wedge Q$	$\vee$ E 2, 3–5, 6–8

(b) and (g) are the converses of (a) and (f), and (d) replaces the conclusion of (c) by its converse; each of the three breaks. (a) is the $\vee$ -twin of [Exercise \(B4: Both directions\)](#), with a case split inside each box.

Marking scheme. (16 points) For each claim: 1 for the verdict; 1 for a derivation every line of which checks, or for a choice of statements and one value of x at which every member of

the counterexample set is true. Fatal errors (0 for the claim): a “break” at which a premise fails; RAA in a derivation; a box of $\leftrightarrow$ I citing its sibling.

2.4.8.3 C. Going deeper

Exercise. C1: Divisibility by six

For integers d and n , write $d \mid n$ if $n = dk$ for some integer k . Let n be an integer. Prove that the following three conditions are equivalent, by a single cycle of three implications.

- (i) $6 \mid n$;
- (ii) $2 \mid n$ and $3 \mid n$;
- (iii) $6 \mid n^2$.

You may use Theorem 2.1.3 and part (a) of Exercise (B3: The square root of three, used later).

Solution (Hint 1). Choose the order of the cycle so that each arrow is short. The two results you may use both pass from a square to the number itself.

Solution (Hint 2). Try $(i) \Rightarrow (iii) \Rightarrow (ii) \Rightarrow (i)$. The last arrow is the one that needs an idea: the two halves of (ii) must be used together, not one at a time.

Solution. We prove $(i) \Rightarrow (iii) \Rightarrow (ii) \Rightarrow (i)$, which suffices by [Proposition 2.4.6](#).

$(i) \Rightarrow (iii)$. Suppose $n = 6k$. Then $n^2 = 36k^2 = 6(6k^2)$, so $6 \mid n^2$.

$(iii) \Rightarrow (ii)$. Suppose $n^2 = 6j$. Then $n^2 = 2(3j)$ is even, so n is even by Theorem 2.1.3, that is, $2 \mid n$. Also $n^2 = 3(2j)$, so $3 \mid n^2$, and by part (a) of Exercise (B3: The square root of three, used later), $3 \mid n$. Hence $2 \mid n$ and $3 \mid n$ $[\wedge]$.

$(ii) \Rightarrow (i)$. Suppose $2 \mid n$ and $3 \mid n$, and write $n = 3b$ with b an integer. The integer b is odd or even. If b were odd, then $n = 3b$ would be odd: writing $b = 2c + 1$ gives $3b = 6c + 3 = 2(3c + 1) + 1$. But n is even, and no integer is both, so this case cannot occur $[\neg E, \perp E]$. Hence b is even, say $b = 2c$, and $n = 6c$, so $6 \mid n$.

Marking scheme. (10 points) - 1: names a cycle through all three conditions and cites [Proposition 2.4.6](#) (or proves the needed implications explicitly). - 2: $(i) \Rightarrow (iii)$ by computation. - 3: $(iii) \Rightarrow (ii)$, citing Theorem 2.1.3 for the factor 2 and part (a) of Exercise (B3: The square root of three, used later) for the factor 3. - 4: $(ii) \Rightarrow (i)$, combining the two factors correctly (ruling out b odd, or $n = 3n - 2n$, or otherwise).

Fatal errors (0 for the step): a “cycle” that omits a condition; using “ $2 \mid n$ and $3 \mid n$ gives $6 \mid n$ ” without proof; using “ $6 \mid n^2$ implies $6 \mid n$ ” as known. Any other cycle through the three conditions earns full marks if each of its arrows is proved: 1 point for the cycle and its citation, and 3 points for each of its three arrows.

Exercise. C2: Dropping a hypothesis, and repairing the statement

- (a) Suppose only $y \geq 0$ is assumed in [Theorem 2.4.5](#), and x is an arbitrary real number. The remark after it says that $(\Leftarrow)$ survives. Which steps of its proof use $y \geq 0$, and why is $x \geq 0$ never needed? Refute $(\Rightarrow)$ with a new pair.
- (b) Prove that for **all** real numbers x and y , $|x| \leq |y|$ if and only if $x^2 \leq y^2$.

Hint: for (b), apply [Theorem 2.4.5](#) to the right pair of numbers.

Solution.

- (a) The proof of $(\Leftarrow)$ uses $y \geq 0$ twice: for $x > 0$ from $x > y$, and for $y^2 \leq xy$. Its other multiplication is by the derived $x > 0$, so $x \geq 0$ is never used. For $(\Rightarrow)$, take $x = -3$, $y = 1$: $x \leq y$ and $y \geq 0$, but $x^2 = 9 > 1 = y^2$.
- (b) Let x and y be real numbers. Then $|x| \geq 0$ and $|y| \geq 0$, so [Theorem 2.4.5](#) applies to the pair $|x|, |y|$ and gives $|x| \leq |y|$ if and only if $|x|^2 \leq |y|^2$. Finally $|x|^2 = x^2$, since $|x|$ is x or $-x$ and $(-x)^2 = x^2$, and likewise $|y|^2 = y^2$. This proves that $|x| \leq |y|$ if and only if $x^2 \leq y^2$.