

FOUNDATIONS

Course notes

Drew M. Schaffner

CONTENTS

CHAPTER 1: STATEMENTS AND PROOF	I
1 The conditional	I
2 Three ways to prove $P \implies Q$	2
CHAPTER 2: NUMBERS AND PARITY	2
3 The number systems	3
4 Even and odd	3
CHAPTER 3: RATIONAL AND IRRATIONAL NUMBERS	4
5 Arithmetic of the rationals	4
6 The irrationality of $\sqrt{2}$	5
7 The golden ratio	5

CHAPTER 1: STATEMENTS AND PROOF

The first kind of proof is the lowly conditional, $P \implies Q$, read “ P implies Q ” or “if P , then Q ”. To prove it, we take what we are given in P , together with what we already know to be true, and use it to reach Q . This chapter fixes what a conditional means and what may be traded for it.

I THE CONDITIONAL

DEFINITION 1.1 (*Conditional*). For statements P and Q , the conditional $P \implies Q$ is false when P is true and Q is false, and true in every other case. P is the *hypothesis* and Q the *conclusion*. Three related statements are

converse	$Q \implies P$,
inverse	$\neg P \implies \neg Q$,
contrapositive	$\neg Q \implies \neg P$.

Remark 1.2. A conditional with a false hypothesis is true, however odd its conclusion. “If $1 = 2$, then the moon is cheese” is a true statement. A conditional promises nothing when its hypothesis fails.

THEOREM 1.3 (*Contrapositive*). For any statements P and Q , the conditional $P \implies Q$ and its contrapositive $\neg Q \implies \neg P$ are logically equivalent: they are true in exactly the same cases.

PROOF. Compare the two in every case:

P	Q	$\neg P$	$\neg Q$	$P \implies Q$	$\neg Q \implies \neg P$
T	T	F	F	T	T
T	F	F	T	F	F
F	T	T	F	T	T
F	F	T	T	T	T

The last two columns agree in every row. ■

Remark 1.4. The converse is *not* equivalent to the conditional. In the second row of the table (P true, Q false), $P \implies Q$ is false but $Q \implies P$ is true. The inverse is the contrapositive of the converse, so it stands or falls with the converse.

2 THREE WAYS TO PROVE $P \implies Q$

DIRECT. Assume P and deduce Q step by step.

CONTRAPOSITIVE. Assume $\neg Q$ and deduce $\neg P$. By [Theorem 1.3](#), this proves $P \implies Q$.

CONTRADICTION. Assume P and $\neg Q$ together, and deduce something false. Then the case “ P true, Q false” cannot happen, and that is the only case in which $P \implies Q$ fails.

Each method appears in the next two chapters. The proof that n^2 even implies n even ([Theorem 4.4](#)) goes by contrapositive, and the irrationality of $\sqrt{2}$ ([Theorem 6.1](#)) by contradiction.

Exercise 2.1. Let n be an integer. State the converse, inverse and contrapositive of “if n is even, then n^2 is even”, and decide which of the four statements are true.

Solution. • Converse: if n^2 is even, then n is even.

• Inverse: if n is odd, then n^2 is odd.

• Contrapositive: if n^2 is odd, then n is odd.

Here “not even” is the same as “odd” by [Theorem 4.2](#). All four statements are true: the original and its contrapositive by [Theorem 4.3](#), and the converse and inverse by [Theorem 4.4](#). This is unusual. A conditional and its converse both hold exactly when P and Q are equivalent, as they are here. ◁

CHAPTER 2: NUMBERS AND PARITY

Before we can prove anything about numbers, we have to agree on what they are. Some of what follows comes from rather simple ideas, and some of it we simply have to accept: there is no substitute for it, and without it we can go no further. What we accept without proof is an *axiom*. What we merely agree to call something is a *definition*.

3 THE NUMBER SYSTEMS

We take for granted the natural numbers $\mathbb{N} = \{1, 2, 3, \dots\}$, the integers $\mathbb{Z} = \{\dots, -2, -1, 0, 1, 2, \dots\}$ with their usual arithmetic and order, and the real numbers $\mathbb{R}$, the points of the number line.

AXIOM 3.1 (*Well-ordering*). Every nonempty set of natural numbers has a least element.

DEFINITION 3.2 (*Rational and irrational numbers*). A real number q is *rational*, written $q \in \mathbb{Q}$, if

$$q = \frac{a}{b} \quad \text{for some } a, b \in \mathbb{Z} \text{ with } b \neq 0.$$

A real number that is not rational is *irrational*. The irrationals form the set $\mathbb{R} \setminus \mathbb{Q}$.

So $\mathbb{N} \subset \mathbb{Z} \subset \mathbb{Q} \subset \mathbb{R}$, since $n = n/1$. Examples of rationals are $-\frac{3}{13}$, -1 , 0 , 2 and $\frac{13}{2}$. The condition $b \neq 0$ matters, because $\frac{a}{0}$ is not a number. It is not obvious that irrational numbers exist at all; [Section 6](#) shows that $\sqrt{2}$ is one.

DEFINITION 3.3 (*Complex numbers*). Let i be a number with $i^2 = -1$. A *complex number* is one of the form

$$z = a + ib, \quad a, b \in \mathbb{R},$$

and the set of them is $\mathbb{C}$. Taking $b = 0$ shows that $\mathbb{R} \subset \mathbb{C}$.

Remark 3.4. Writing $i = \sqrt{-1}$ is common but risky. The rule $\sqrt{xy} = \sqrt{x}\sqrt{y}$, valid for $x, y \geq 0$, would give $-1 = i \cdot i = \sqrt{-1}\sqrt{-1} = \sqrt{1} = 1$. So $i^2 = -1$ is the safe definition.

It is unfortunate that i is called *imaginary*. In truth all numbers are imaginary, in the sense that we made them up, and i is no less real than $\sqrt{2}$ or -1 .

4 EVEN AND ODD

DEFINITION 4.1 (*Even and odd*). An integer a is *even* if $a = 2b$ for some $b \in \mathbb{Z}$, and *odd* if $a = 2b + 1$ for some $b \in \mathbb{Z}$.

THEOREM 4.2 (*Parity*). Every integer is either even or odd, and no integer is both.

PROOF. *At least one.* Let $n \in \mathbb{Z}$ and let q be the greatest integer with $2q \leq n$. Then $2(q+1) > n$, so $r = n - 2q$ satisfies $0 \leq r < 2$. If $r = 0$, then $n = 2q$ is even. If $r = 1$, then $n = 2q + 1$ is odd.

Not both. If $n = 2a = 2b + 1$ with $a, b \in \mathbb{Z}$, then $2(a - b) = 1$. But $2(a - b)$ is 0 if $a = b$, and at least 2 in absolute value otherwise. So it is never 1. ■

Because of [Theorem 4.2](#), “not even” and “odd” mean the same thing for integers. Every integer is exactly one of the two: even *exclusive or* odd.

THEOREM 4.3 (*Arithmetic of parity*). Let $m, n \in \mathbb{Z}$.

- (a) If m and n have the same parity, then $m + n$ is even. If they have different parities, then $m + n$ is odd.
 (b) If m is even, then mn is even. If m and n are both odd, then mn is odd.

PROOF. Write the even numbers as $2a$ and the odd ones as $2a + 1$.

- (a) $2a + 2b = 2(a + b)$ and $(2a + 1) + (2b + 1) = 2(a + b + 1)$ are even, while $2a + (2b + 1) = 2(a + b) + 1$ is odd.
 (b) $(2a)n = 2(an)$ is even, and $(2a + 1)(2b + 1) = 2(2ab + a + b) + 1$ is odd. ■

THEOREM 4.4 (*Parity of a square*). For $n \in \mathbb{Z}$, n^2 is even if and only if n is even.

PROOF. If n is even, then $n^2 = n \cdot n$ is even by **Theorem 4.3**. For the converse we prove the contrapositive (**Theorem 1.3**): if n is not even, then by **Theorem 4.2** it is odd, so n^2 is odd by **Theorem 4.3**, and hence not even, again by **Theorem 4.2**. ■

Exercise 4.5. Prove that the product of two consecutive integers is even.

PROOF. Let the integers be n and $n + 1$. By **Theorem 4.2**, n is even or odd. If n is even, then $n(n + 1)$ is even by **Theorem 4.3**(b). If n is odd, then $n + 1$ is even by **Theorem 4.3**(a), and again the product is even. ■

Exercise 4.6. Prove that $n^2 + n + 1$ is odd for every integer n .

PROOF. $n^2 + n = n(n + 1)$ is even by **Exercise 4.5**, so $n^2 + n + 1 = 2k + 1$ for some $k \in \mathbb{Z}$. ■

Remark 4.7. As a consequence, $x^2 + x + 1 = 0$ has no integer roots. Every integer input gives an odd output, and 0 is even.

CHAPTER 3: RATIONAL AND IRRATIONAL NUMBERS

The rationals are closed under arithmetic, and a little parity is enough to prove that $\sqrt{2}$ is not among them. Once one irrational number is known, many more follow, including the golden ratio.

5 ARITHMETIC OF THE RATIONALS

THEOREM 5.1 (*Closure of the rationals*). If $p, q \in \mathbb{Q}$, then $p + q$, $p - q$ and pq are rational, and so is p/q when $q \neq 0$.

PROOF. Write $p = a/b$ and $q = c/d$ with $a, b, c, d \in \mathbb{Z}$ and $b, d \neq 0$. Then

$$p \pm q = \frac{ad \pm bc}{bd}, \quad pq = \frac{ac}{bd}, \quad \frac{p}{q} = \frac{ad}{bc} \quad (c \neq 0),$$

and in each case the numerator and denominator are integers, with a nonzero denominator. ■

6 THE IRRATIONALITY OF $\sqrt{2}$

THEOREM 6.1 (*$\sqrt{2}$ is irrational*). There are no integers a and $b \neq 0$ with $(a/b)^2 = 2$.

PROOF. Suppose there are, and argue by contradiction. Replacing a and b by $-a$ and $-b$ if necessary, we may take $b > 0$. By well-ordering (Axiom 3.1), choose such a pair with b as small as possible. Then $a^2 = 2b^2$ is even, so a is even by Theorem 4.4. Write $a = 2c$. Then $4c^2 = 2b^2$, so $b^2 = 2c^2$ is even, and $b = 2d$ is even too. Now $(c/d)^2 = 2$ with $0 < d < b$, which contradicts the choice of b . ■

Remark 6.2. The proof is a contradiction (Section 2). The well-ordering axiom lets us start from the smallest possible denominator. The parity argument then produces a smaller one. Without well-ordering, the same argument would only show that any such pair can be halved forever.

THEOREM 6.3 (*Rational and irrational*). Let $q \in \mathbb{Q}$ and let $x \in \mathbb{R} \setminus \mathbb{Q}$. Then $q + x$ is irrational, and so is qx if $q \neq 0$.

PROOF. If $q + x = p$ were rational, then $x = p - q$ would be rational by Theorem 5.1. If $qx = p$ were rational with $q \neq 0$, then $x = p/q$ would be rational. Both contradict $x \notin \mathbb{Q}$. ■

Exercise 6.4. Show that $3 + \sqrt{2}$ and $\frac{\sqrt{2}}{2}$ are irrational.

Solution. 3 and $\frac{1}{2}$ are nonzero rationals and $\sqrt{2}$ is irrational (Theorem 6.1). By Theorem 6.3, so are $3 + \sqrt{2}$ and $\frac{1}{2}\sqrt{2}$. ◁

7 THE GOLDEN RATIO

Exercise 7.1. Prove that $\sqrt{5}$ is irrational, and hence that the golden ratio $\varphi = \frac{1+\sqrt{5}}{2}$ is irrational.

PROOF. Step 1: if $5 \mid a^2$ then $5 \mid a$. Divide a by 5, so that $a = 5q + r$ with $r \in \{0, 1, 2, 3, 4\}$. Then $a^2 = 5(5q^2 + 2qr) + r^2$, and $r^2 \in \{0, 1, 4, 9, 16\}$ leaves remainder 0, 1, 4, 4, 1 on division by 5. So $5 \mid a^2$ only when $r = 0$.

Step 2: $\sqrt{5}$ is irrational. Copy the proof of Theorem 6.1. Suppose $a^2 = 5b^2$ with $b > 0$ as small as possible. Step 1 gives $a = 5c$. Then $b^2 = 5c^2$, so $b = 5d$ with $0 < d < b$ and $(c/d)^2 = 5$, a contradiction.

Step 3: φ is irrational. $\frac{\sqrt{5}}{2}$ is irrational, and so is $\varphi = \frac{1}{2} + \frac{\sqrt{5}}{2}$, by two applications of Theorem 6.3. ■

Remark 7.2. An irrational number may still be the root of a polynomial with integer coefficients. $\sqrt{2}$ is a root of $x^2 - 2$, and φ is a root of $x^2 - x - 1$. Such numbers are *algebraic*. Numbers that are not algebraic are *transcendental*; e (Hermite, 1873) and π (Lindemann, 1882) are the classical examples. So φ is irrational but *not* transcendental. Those two theorems are much deeper than anything in this chapter.