

BRENDAN WHITAKER  
THE OHIO STATE UNIVERSITY  
MATHEMATICS

---

# HONORS ANALYSIS I (MATH 4181H)

---

*Instructor:*  
Liz Vivas  
Professor  
Dept. of Mathematics

August-December, 2018  
Lecture Notes



## SECTION 0.1

## INTRODUCTION

Office: MW710

Email: [vivas.3@osu.edu](mailto:vivas.3@osu.edu)

Office Hours: 10:15-11:15am (every day)

Mentoring Sessions: Ryan McConnell, Vilas Winstein (Thurs: 6:30-8:30pm, Sun: 2-4pm)

Starting tomorrow, all classes will be in MW154.



# CHAPTER 1

---

## PROLOGUE

---

### SECTION 1.1

#### BASIC PROPERTIES OF NUMBERS

**Tuesday, August 21st**

**Quick introduction to real numbers:**

$$(1.1) \quad \begin{aligned} \mathbb{N} &= \{ 1, 2, 3, 4, 5, \dots \} && \text{addition, subtraction} \\ \mathbb{Z} &= \{ \dots, -3, -2, -1, 0, 1, 2, 3, \dots \} && \text{multiplication, division} \\ \mathbb{Q} &= \left\{ \frac{p}{q} : p, q \in \mathbb{Z}, q \neq 0 \right\} \\ \mathbb{R} &= \left\{ \begin{array}{l} \boxed{\text{closed algebraic field}} \\ \boxed{\text{Dedekind cuts}} \end{array} \right\} . \end{aligned}$$

Note that we're being a bit imprecise here with our definition of  $\mathbb{Q}$ . With this construction,  $\frac{1}{2}$  and  $\frac{2}{4}$  are not the same element. But this does not reflect the true nature of  $\mathbb{Q}$ . In both cases with  $\mathbb{R}$ , we are talking about “limits”. Note  $\sqrt{2} \in \mathbb{R}$ ,  $\sqrt{2} \notin \mathbb{Q}$ .

**Axiomatic way:**

EXAMPLE 1.1. We define the natural numbers as the numbers we use for counting. A set has  $|n|$  elements. So the natural numbers are the space of all possible cardinalities of finite sets.

Then we start deducing properties.

EXAMPLE 1.2. Two sets that have  $m$  and  $n$  elements; when put together, they'll have  $m + n$  elements.

DEFINITION 1.3. The axiomatic properties of the natural numbers  $\mathbb{N}$ , i.e. the **Peano Axioms**. Let  $s : \mathbb{N} \rightarrow \mathbb{N}$  be the successor function.

- (1) Axiom 1:  $s : \mathbb{N} \rightarrow \mathbb{N}$  is injective.
- (2) Axiom 2:  $\mathbb{N} \setminus s(\mathbb{N}) = \{ a \in \mathbb{N} : a \notin s(\mathbb{N}) \}$  has exactly one element, which is called 1.
- (3) Axiom 3: If  $X \subseteq \mathbb{N}$ , is a set such that  $1 \in X$  and  $\forall x \in X, s(x) \in X$ , then  $X = \mathbb{N}$ .

So then we can say  $\mathbb{N} = \{1, 2, 3, \dots\} = \{1, s(1), s(s(1)), \dots\}$ . And we can define addition as

$$(1.2) \quad m + n = s(\dots s(s(n))),$$

where we have a composition of  $m$  instances of  $s$ .

**DEFINITION 1.4. Properties of Numbers (AXIOMS):** Given two numbers  $a$  and  $b$ , we define the sum of  $a$  and  $b$  and denote it by  $a + b$ .

(1) **P1 (Associativity):** If  $a, b, c$  are any numbers, then

$$(1.3) \quad (a + b) + c = a + (b + c).$$

Consequences:

$$(1.4) \quad \begin{aligned} a + b + c + d &= (a + b) + (c + d) \\ &= (a + (b + c)) + d. \end{aligned}$$

(2) **P2 (Identity):** There exists an element  $0$  such that if  $a$  is any number, then

$$(1.5) \quad a + 0 = 0 + a = a.$$

(3) **P3 (Inverses):** For every number  $a$ , there exists a number  $-a$  such that

$$(1.6) \quad a + (-a) = (-a) + a = 0.$$

**EXERCISE 1.** Prove that  $(a + b) + (c + d) = (a + (b + c)) + d$ .

**PROOF.** We'll use **P1**:  $(x + y) + z = x + (y + z)$ . So first let  $a + b = x$ ,  $c = y$ , and  $d = z$ . Then we get

$$(1.7) \quad ((a + b) + c) + d = (a + b) + (c + d).$$

Now let  $a = x$ ,  $b = y$ , and  $c = z$ . So then for the left hand side, we get

$$(1.8) \quad (a + b) + c = a + (b + c),$$

which tells us

$$(1.9) \quad \begin{aligned} (a + b) + (c + d) &= ((a + b) + c) + d \\ &= (a + (b + c)) + d. \end{aligned}$$

□

**EXERCISE 2.** The identity element  $0$  is unique. If there exists  $y$  such that for **some** (note that we do not need this to be true for all) number  $a$ ,  $a + y = a$ , then  $y = 0$ .

**PROOF.** Take  $a$  such that  $a + y = a$ . Since we know  $(-a)$  exists by **P3**, we have

$$(1.10) \quad (-a) + a + y = (-a) + a.$$

Note we have to add  $(-a)$  on the same side on both sides of the equation, because we do not know whether our addition operation is abelian or not. This tells us

$$(1.11) \quad y = 0$$

since by **P3**, we know  $(-a) + a = 0$ , and by **P2**, we know  $0 + y = y$ . □

**EXAMPLE 1.5.** Let  $\mathbb{F}_2 = \{0, 1\}$ . Define

$$(1.12) \quad \begin{aligned} 0 + 0 &= 0 \\ 0 + 1 &= 1 \\ 1 + 0 &= 1 \\ 1 + 1 &= 0. \end{aligned}$$

So prove that  $(\mathbb{F}_2, +)$  satisfies **P1-P3**.

**Wednesday, August 22nd**

We're listing properties **(P1) - P(12)**.

Note  $\mathbb{R}$  is a complete ordered field. "Complete" has to do with limits. The term "ordered" has to do with properties **(P10) - (P12)**. And the term field is defined via properties **(P1) - (P9)**.

$$\textbf{(P1)} \quad a + (b + c) = (a + b) + c.$$

$$\textbf{(P2)} \quad a + 0 = 0 + a = a.$$

**(P3)** For every  $a$  there exists  $-a$  such that

$$(1.13) \quad a + (-a) = (-a) + a = 0.$$

**Consequences:**

- 0 is unique.
- Additive inverse is unique.

$$\textbf{(P4)} \quad a + b = b + a.$$

EXAMPLE 1.6. Consider

$$(1.14) \quad M_{2 \times 2} = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} : a, b, c, d \in \mathbb{R} \right\}.$$

And we have the sum operation

$$(1.15) \quad \begin{pmatrix} a & b \\ c & d \end{pmatrix} + \begin{pmatrix} e & f \\ g & h \end{pmatrix} = \begin{pmatrix} a+e & b+f \\ c+g & d+h \end{pmatrix},$$

which satisfies **(P1) - (P4)**. Note

$$(1.16) \quad \begin{aligned} 0 &= \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix} \\ 1 &= \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}. \end{aligned}$$

DEFINITION 1.7. Any set which satisfies **(P1) - (P4)** is a group.

DEFINITION 1.8. **Multiplication:** given any two numbers  $a$  and  $b$ ,  $ab$  is the product of  $a, b$ .

$$\textbf{(P5)} \quad a \cdot (b \cdot c) = (a \cdot b) \cdot c.$$

**(P6)** There exists an identity element for multiplication, 1. And we have

$$(1.17) \quad a \cdot 1 = 1 \cdot a = a.$$

And we also require  $1 \neq 0$ . Why?

PROOF. Let  $1 = 0$ . Then the same element  $(*)$  satisfies **(P2)** and **(P6)**. Then we have

$$(1.18) \quad \begin{aligned} (*) + a &= a + (*) = a \\ a \cdot (*) &= (*) \cdot a = a. \end{aligned}$$

Thus every element is  $(*)$ . □

**(P7)** There exists a multiplicative inverse for  $a \neq 0$ .

$$\textbf{(P8)} \quad a \cdot b = b \cdot a.$$

$$\textbf{(P9)} \quad a \cdot (b + c) = a \cdot b + a \cdot c.$$

DEFINITION 1.9. We say any set which satisfies all 9 properties is called a **field**.

EXAMPLE 1.10. (1)  $\mathbb{N}$  is not a group.

(2)  $\mathbb{Z}$  is a group, but not a field, because it does not satisfy **(P7)**.

(3)  $\mathbb{Q}$  is a field. Recall

$$(1.19) \quad \mathbb{Q} = \left\{ \frac{p}{q} : p, q \in \mathbb{Z}, q \neq 0 \right\},$$

$$\frac{1}{q} = q^{-1}.$$

(4)  $M_{n \times m}$  matrices with real entries is a group under addition, not a field.

(5)  $\mathbb{F}_2$  is a field. BONUS: check that it is.

(6) Define

$$(1.20) \quad \mathbb{Q}(i) = \{ (a, b) : a, b \in \mathbb{Q} \}.$$

We define addition:

$$(1.21) \quad \begin{aligned} (a, b) + (c, d) &= (a + c, b + d) \\ (a, b) \cdot (c, d) &= (ac - bd, ad + bc). \end{aligned}$$

And  $\mathbb{Q}(i), +, \cdot$  is a field. If  $(c, d) = (1, 0)$ , then we have

$$(1.22) \quad (a, b) \cdot (1, 0) = (a - 0, 0 + b) = (a, b).$$

Every element  $(a, b) \neq (0, 0)$  has a multiplicative inverse. To find it, we solve

$$(1.23) \quad \begin{aligned} (a, b) \cdot (c, d) &= (1, 0) \\ ac - bd &= 1 \\ ad + bc &= 0. \end{aligned}$$

Solve for  $c$  and  $d$  in terms of  $a$  and  $b$ . You get

$$(1.24) \quad \begin{aligned} c &= \frac{a}{a^2 + b^2}, \\ d &= \frac{-b}{a^2 + b^2}. \end{aligned}$$

Consequences of **(P1)** - **(P9)**.

LEMMA 1.11. *Let  $K$  be a field (satisfies **(P1)** - **(P9)**). Then if  $a \cdot b = 0$ , then  $a = 0$  or  $b = 0$ , i.e.  $a$  field is torsion-free.*

PROOF. Let  $a \cdot b = 0$ , and suppose for contradiction that  $a \neq 0$ ,  $b \neq 0$ . Then both  $a^{-1}, b^{-1}$  exist. So then we may multiply both sides by  $a^{-1}$  to get

$$(1.25) \quad \begin{aligned} a^{-1} \cdot a \cdot b &= a^{-1} \cdot 0 \\ 1 \cdot b &= 0 \\ b &= 0. \end{aligned}$$

The proof follows similarly for  $a$ . □

EXERCISE 3. Prove that  $a \cdot (-b) = -(a \cdot b)$ .

PROOF. Note  $-(a \cdot b)$  is the additive inverse of  $a \cdot b$ . We already know this is unique, so what remains to be shown is that  $a \cdot (-b)$  is also this additive inverse. Observe

$$(1.26) \quad \begin{aligned} (a \cdot b) + (a \cdot (-b)) &= a \cdot (b + (-b)) \\ &= a \cdot 0 \\ &= 0. \end{aligned}$$

□

LEMMA 1.12. *Additive inverses are unique.*

PROOF. Suppose

$$(1.27) \quad \begin{aligned} a + b &= 0 & (*) \\ a + c &= 0 & (**) \end{aligned}$$

Then we have

$$(1.28) \quad \begin{aligned} (a + b) + c &= 0 + c \\ (b + a) + c &= c \\ b + (a + c) &= c & \text{by } (**) \\ b + 0 &= c \\ b &= c. \end{aligned}$$

□

EXERCISE 4. Prove that multiplicative inverses are also unique.

EXERCISE 5. Prove that  $(-a) \cdot (-b) = a \cdot b$ .

PROOF. By Exercise 3, we know

$$(1.29) \quad \begin{aligned} (-a) \cdot (-b) &= -((-a) \cdot b) \\ &= -(-(a \cdot b)) = a \cdot b. \end{aligned}$$

Then we need only show that  $-(-x) = x$ . Note that  $x + (-x) = (-x) + x = 0$ , so  $x$  is the additive inverse of  $(-x)$ . So  $-(-x) = x$ , since additive inverses are unique. □

Common mistake:  $a < b$  &  $c < d \Rightarrow ac < bd$ . This is WRONG.

Next class, we'll talk about the symbol  $<$ . The next 3 properties are about *order*.

**Thursday, August 23rd**

EXAMPLE 1.13. We give an example of a field. Consider

$$(1.30) \quad \begin{aligned} \mathbb{Q}(t) &= \left\{ \frac{p(t)}{q(t)} : p, q \in \mathbb{Q}[t], q \neq 0 \right\} \\ \frac{t^2}{1+t} + \frac{t^3-1}{2t} &= \frac{t^2(2t) + (t^3-1)(1+t)}{2t(1+t)} \\ \frac{p(t)}{q(t)} + \frac{r(t)}{s(t)} &= \frac{p(t)s(t) + r(t)q(t)}{q(t)s(t)}. \end{aligned}$$

DEFINITION 1.14. Let  $K$  be a field, thus **(P1)**-**(P9)** are satisfied, then we say  $k$  is an **ordered field** if there exists a subset  $P \subseteq K$  such that

**(P10)** Every  $a \in K$ , either

- (a)  $a \in P$ ,
- (b) or  $-a \in P$ ,
- (c) or  $a = 0$ .

**(P11)** If  $a, b \in P \Rightarrow a + b \in P$ .

**(P12)** If  $a, b \in P \Rightarrow a \cdot b \in P$ .

EXAMPLE 1.15. (1)  $\mathbb{Q}$  is a field. Let  $P \subseteq \mathbb{Q}$  such that  $P = \left\{ \frac{p}{q} > 0 \right\}$ .

(2)  $\mathbb{Q}(i) = \{ (a, b) : a, b \in \mathbb{Q} \}$ , as yesterday, is not an ordered field. Later we will prove it.

(3)  $\mathbb{Q}(t)$  is an ordered field. Define

$$(1.31) \quad P = \left\{ \frac{p(t)}{q(t)} : q \neq 0, \text{ largest coefficient of } (pq) \text{ is } > 0 \right\}.$$



So how can we check that something is an ordered field?

### Consequences of (P10)-(P12)

PROPOSITION 1.16.  $1 \in P$  and  $-1 \notin P$ .

PROOF. Let  $K$  be an ordered field. Recall that  $1 \neq 0$ . Then  $1 \in P$  or  $-1 \in P$ . By (P12), If  $1 \in P$ , then  $1 \cdot 1 \in P$ . So nothing important is found. Then suppose  $-1 \in P$ . Then we get  $(-1)(-1) \in P$ , so  $1 \in P$ . Then  $-1, 1 \in P$ . So  $1 + (-1) \in P \Rightarrow 0 \in P$ . This is impossible by (P10).  $\square$

PROPOSITION 1.17. For every  $a \in K$ ,  $a \neq 0 \Rightarrow a^2 \in P$ .

PROOF. Since  $a \neq 0$ , we know  $a \in P$  or  $-a \in P$ . In either case by (P12), we know that  $a \cdot a \in P$ , or  $(-a)(-a) \in P$ , which tells us  $a^2 \in P$ .  $\square$

PROPOSITION 1.18. In any ordered field,  $-1$  is not the square of any number.

PROOF. Note that if  $-1 = a^2$ , then  $-1 \in P$ . But this contradicts Proposition 1.16.  $\square$

We revisit Example 2. We discussed  $\mathbb{Q}(i)$ . We defined multiplication by

$$(1.32) \quad (a, b) \cdot (c, d) = (ac - bd, ad + bc).$$

And thus

$$(1.33) \quad (a, b) \cdot (1, 0) = (a, b).$$

Thus the zero element is  $(0, 0)$ . Then the  $-1$  element is  $(-1, 0)$ . And turns out that

$$(1.34) \quad (0, 1)^2 = (-1, 0).$$

Thus  $-1 = a^2$  for some  $a \in \mathbb{Q}(i)$ , so by Proposition 1.18,  $\mathbb{Q}(i)$  cannot be an ordered field.

EXAMPLE 1.19.  $\mathbb{F}_2$  is not an ordered field.

PROOF. Note that  $-1 = 1$ . And thus  $1 \in P$ , so  $1 + 1 \in P$ , and thus  $0 \in P$  which is impossible.  $\square$

### Application to $\mathbb{R}$ :

For real numbers,  $P = \{x > 0\}$ .

(P10) For every  $x \in \mathbb{R}$ , either  $x > 0$ , or  $-x > 0$ , or  $x = 0$ .

(P11) If  $x > 0, y > 0$ , then  $x + y > 0$ .

(P12) If  $x > 0, y > 0$ , then  $xy > 0$ .

REMARK 1.20. We say  $x < y$  if  $y - x \in P$ , i.e. if  $y - x > 0$ .

REMARK 1.21. **Transitivity:** If  $x < y$  and  $y < z$ , then  $x < z$ .

PROOF. Let  $x < y$  and  $y < z$ . Then we know  $y - x \in P$  and  $z - y \in P$ . We want to know if  $z - x \in P$ . But by (P11), we know

$$(1.35) \quad y - x + z - y = z - x \in P.$$

Thus  $x < z$ .  $\square$

REMARK 1.22. If  $x < y$  and  $z$  is any number, then  $x + z < y + z$ . (\*).

PROOF. Observe

$$\begin{aligned}
 (1.36) \quad & y - x \in P \\
 & (y + 0) - x \in P \\
 & (y + (z + (-z))) - x \in P \\
 & (y + z) + (-z - x) \in P \\
 & (y + z) - (x + z) \in P \\
 & x + z < y + z.
 \end{aligned}$$

□

REMARK 1.23. (1) If  $x < y$  and  $z \in P \Rightarrow xz < yz$ .  
 (2) If  $x < y$  and  $-z \in P \Rightarrow yz < xz$ .

PROOF. For (1),  $y - x \in P$ ,  $z \in P$  so

$$\begin{aligned}
 (1.37) \quad & (y - x) \cdot z \in P \\
 & yz - xz \in P \\
 & xz < yz.
 \end{aligned}$$

(2) follows similarly.

□

REMARK 1.24. Given  $x, y$ , then either  $y > x$ ,  $x > y$ , or  $x = y$ .

PROOF. Consider  $y - x$  is either in  $P$ , it's negative is in  $P$ , or it is 0, by (P10).

□

DEFINITION 1.25. For any ordered field  $k$ , we can define for  $x \in K$  a value that is called the **absolute value**  $|x|$ :

$$(1.38) \quad |x| = \begin{cases} x & x \in P \\ -x & -x \in P \\ 0 & x = 0 \end{cases}.$$

EXAMPLE 1.26. Consider  $\mathbb{Q}(t)$ . Take  $\alpha = \frac{1}{t}, \beta = \frac{2-t^2}{t^3} \in \mathbb{Q}(t)$ . Recall that  $P \subseteq \mathbb{Q}(t)$  is defined as

$$(1.39) \quad P = \{ a \in \mathbb{Q}(t) : \text{coefficient of } pq \text{ with largest degree is positive} \}.$$

Note that

$$\begin{aligned}
 (1.40) \quad & \alpha \in P \quad (1t = t; 1 > 0) \\
 & \beta \notin P \quad (2t^3 - t^5; -1 < 0).
 \end{aligned}$$

So we have

$$\begin{aligned}
 (1.41) \quad & \left| \frac{1}{t} \right| = \frac{1}{t}, \\
 & \left| \frac{2-t^2}{t^3} \right| = \frac{t^2-2}{t^3}.
 \end{aligned}$$

DEFINITION 1.27. We say  $x \leq y$  if  $x < y$  or  $x = y$ .

THEOREM 1.28. Let  $x, y \in K$  for some ordered field  $K$ . Then

$$(1.42) \quad |x + y| \leq |x| + |y|.$$

PROOF. If  $x = 0 \Rightarrow |x + y| = |y|$ , then  $|x| = 0$ , and we are done. Same if  $y = 0$ .

If  $x, y \in P$ , then  $|x| = x, |y| = y$ , then  $x + y \in P$ , and so  $|x + y| = x + y$ . The proof for when  $-x, -y \in P$  is the same. Two more cases. □

**Friday, August 24th**

**THEOREM 1.29.** *Let  $F$  be an ordered field. Then  $|a + b| \leq |a| + |b|$ .*

**PROOF.** Let  $a > 0$  and  $b < 0$ . Then we have  $|a| = a$  and  $|b| = -b$ . Then we have three cases:

$$(1.43) \quad |a + b| = \begin{cases} a + b & \leq a - b \\ -a - b & \leq a - b \end{cases}$$

**Case 1:**  $a > 0, b < 0$ . Since  $b < 0 \Rightarrow -b \in P$ .

$$\Rightarrow (-b) + (-b) \in P$$

$$\Rightarrow (-b) + (-b) > 0$$

$$\Rightarrow b + ((-b) + (-b)) > b$$

$$\Rightarrow (b + (-b)) + (-b) > b$$

$$\Rightarrow -b > b \Rightarrow a - b > a + b$$

But  $|a| + |b| = a - b$ , so  $|a| + |b| > a + b$ . We also know that since  $a > 0$ ,  $a \in P$ , we have  $\Rightarrow a + a \in P$

$$\Rightarrow a + a > 0$$

$$\Rightarrow (a + a) + (-a) > -a$$

$$a > -a$$

$\Rightarrow a - b > -a - b$ . So we have  $|a| + |b| > -a - b$ . But we also have  $|a| + |b| > a + b$ . And since

$$(1.44) \quad |a + b| = \begin{cases} a + b \\ -a - b \end{cases},$$

We know that  $|a + b| < |a| + |b|$  in this case. □

**PROPOSITION 1.30.** *For all  $a, b \in F$*

$$i) \ a < b, b < c \Rightarrow a < c.$$

$$ii) \ a \leq b, b \leq c \Rightarrow a \leq c.$$

**PROOF.** We prove the second part. Note that  $a \leq b \Leftrightarrow a < b$  or  $a = b$ . Thus  $b - a \in P$  or  $b = a$ . And  $b \leq c \Leftrightarrow c - b \in P$  or  $b = c$ . Then we have

$$(1.45) \quad c - a = \begin{cases} (b - a) + (c - b) \in P \\ b - a \in P \\ c - b \in P \\ 0. \end{cases}$$

In all these cases  $c - a \in P$  or  $a = c$ , so  $a \leq c$ . □

**PROPOSITION 1.31. (**PROP 8**)**  $a > 0 \Rightarrow a^{-1} > 0$ .

**PROOF.** Equivalently, we want to show  $a \in P \Rightarrow a^{-1} \in P$ . Let  $a \in P$ . Then we know  $a \neq 0$  by **(P10)**. Therefore  $a^{-1}$  is well defined. By **(P10)**, either i)  $a^{-1} \in P$ , ii)  $-a^{-1} \in P$ , or iii)  $a^{-1} \in P$ . If ii) is true, then  $-a^{-1} \in P$  and  $a \in P$  which by **(P12)** tells us that  $(-a^{-1})a = -(a^{-1}a) = -1 \in P$  which is not possible. If iii), then  $a^{-1} = 0$ , so  $aa^{-1} = a \cdot 0 \Rightarrow 1 = 0$  which is a contradiction. So  $a^{-1} \in P$  and  $a^{-1} > 0$ . □

**PROPOSITION 1.32. (**PROP 9**)**

$$i) \ a < b \Rightarrow -b < -a$$

$$ii) \ a \leq b \Rightarrow -b \leq -a$$

**PROPOSITION 1.33. (**PROP 10**)**

$$i) \ - < a < b \Rightarrow 0 < b^{-1} < a^{-1}.$$

$$ii) \ 0 < a \leq b \Rightarrow 0 < b^{-1} \leq a^{-1}.$$

PROOF. By proposition 7 on the handout, which is that  $a < b$  and  $c > 0 \Rightarrow ac < bc$ . If  $a < 0 \Rightarrow a^{-1} \in P$ . If  $b > 0 \Rightarrow b^{-1} \in P$ . Then we have  $a^{-1}b^{-1} \in P$ . So we use Proposition 7 and we get

$$(1.46) \quad \begin{aligned} 0 &< a(a^{-1}b^{-1}) < b(a^{-1}b^{-1}) \\ 0 &< b^{-1} < a^{-1}. \end{aligned}$$

Part ii) follows by adding the  $a = b$  case to the above proof.  $\square$

PROPOSITION 1.34. (**PROP 11**) If  $a \geq 0, b \geq 0, n \in \mathbb{N}$ , then

- i)  $a < b \Leftrightarrow a^n < b^n$  (\*),
- ii)  $a \leq b \Leftrightarrow a^n \leq b^n$ .

PROOF. Use induction. Define

$$(1.47) \quad S = \{ n \in \mathbb{N} : (*) \text{ is satisfied for } n \}.$$

We need to prove

- i)  $1 \in S$
- ii) If  $k \in S$ , then  $k+1 \in S$ .

Then  $S = \mathbb{N}$ , by Peano's third axiom of  $\mathbb{N}$ .

**Base case:** Let  $n = 1$ . Then  $a < b \Leftrightarrow a^1 < b^1$ .

**Inductive hypothesis:** Assume  $k \in S$ , i.e.  $a < b \Rightarrow a^k < b^k$ . We want to prove that  $a < b \Rightarrow a^{k+1} < b^{k+1}$ . Note that the other direction is trivial because if  $a^n < b^n$  for every  $n$ , then it is true for  $n = 1$ . Because  $a^k < b^k$ , we may multiply on both sides by  $a$  to get  $a^k a \leq b^k a$ . Now we multiply by  $b^k$  on both sides of the inequality:  $a < b$  to get  $ab^k < b^{k+1}$ . Then we get

$$(1.48) \quad a^{k+1} = a^k a \leq b^k a = ab^k < b^{k+1}.$$

$\square$

**Some notation:**

- Let  $F$  be an ordered field,  $\forall a \in F$ .
- $\exists a \in F \dots$  (= there exists  $a \in F$ ).
- $\exists! a \in F \dots$  (= there exists a unique  $a \in F$ ).
- $\Rightarrow \Leftarrow$  = impossible = contradiction.

**Monday, August 27th**

LEMMA 1.35. The following are equivalent

$$(1.49) \quad |x - y| < a \Leftrightarrow y - a < x < y + a.$$

PROOF. **Claim:**  $|x| < a \Leftrightarrow -a < x < a$ . If we can prove that, then we just apply it for  $a = x - y$ . If  $|a| < a$ , we have  $a \in P$ . Then we have  $|s| \in P$  or  $|s| = 0$ , and  $a - |s| \in P$ . And  $a = |s| + a - |s| \in P$ .

**Case i)**  $s \in P \Rightarrow s < a$  since  $|s| < a$ . We want to prove  $-a < s$  also. Since  $s \in P, a \in P$ , then  $s + a \in P$ , therefore  $s - (-a) \in P \Rightarrow -a < s$ . And thus  $-a < s < a$ .

**Case ii)**  $s = 0$ . Then  $a > 0 \Leftrightarrow -a < 0 < a$ . Obvious.

**Case iii)**  $-s \in P$ . Then let  $t = -s$ . Then  $t \in P$ . So we have by Case i) that  $-a < t < a$ . But recall we had

$$(1.50) \quad \begin{aligned} |s| < a &\Leftrightarrow |-t| < a \\ &\Leftrightarrow |t| < a. \end{aligned}$$

**Claim 2:**  $|-t| = |t|$  for any  $t \in F$ . Then by Case i) we have

$$(1.51) \quad \begin{aligned} -a < t < a &\Leftrightarrow -a < -s < a \\ &\Leftrightarrow -a < s < a. \end{aligned}$$

Proof of Claim 2: **Case 1)** If  $t \in P \Rightarrow |t| = t$ . Since  $t \in P \Rightarrow -(-t) \in P \Rightarrow |-t| = -(-t) = t$ .

**Case 2)** If  $-t \in P \Rightarrow |-t| = -t \Rightarrow |t| = -t$ .

**Case 3)**  $t = 0 \Rightarrow -t = 0 \Rightarrow |t| = |-t| = 0$ . □

## SECTION 1.2

### NUMBERS OF VARIOUS SORTS

**REMARK 1.36. Properties of Natural Numbers:** If  $m, n, p \in \mathbb{N}$ ,

$$(1) (m + n) + p = m + (n + p)$$

$$(2) m + n = n + m$$

$$(3) m + n = m + p \Rightarrow n = p.$$

Using the 3rd Peano axiom, i.e. induction, we can prove many facts.

**EXAMPLE 1.37.** Prove that for  $n = 0$  and  $n \in \mathbb{N}$ ,  $1 + 3 + 5 = \dots + (2n + 1) = (n + 1)^2$  (\*),

**PROOF.**  $n = 0 \Rightarrow 1 = 1 \Rightarrow 1 = (0 + 1)^2$  which is (\*) for  $n = 0$ .

For  $n \in \mathbb{N}$ , we use Peano's 3rd axiom. Define

$$(1.52) \quad A = \{ n \in \mathbb{N} : (*) \text{ is valid} \}.$$

**Base case:** And we have

$$(1.53) \quad 4 = 4 \Leftrightarrow 1 = 3 = 2^2 \Leftrightarrow 1 + (2(1) + 1) = (1 + 1)^2.$$

So (\*) is valid for  $n = 1$ , and  $1 \in A$ .

Suppose  $k \in A$ ; we'll prove  $k + 1 \in A$ . Then we have

$$(1.54) \quad \begin{aligned} 1 + 3 + 5 + \dots + (2k + 1) &= (k + 1)^2 \\ &= 1 + 3 + 5 + \dots + (2k + 1) + (2k + 3) \\ &= (k + 1)^2 + (2k + 3) \\ &= k^2 + 2k + 1 + 2k + 3 \\ &= k^2 + 4k + 4 \\ &= (k + 2)^2. \end{aligned}$$

And also

$$(1.55) \quad 1 + 3 + 5 + \dots + (2(k + 1) + 1) = ((k + 1) + 1)^2.$$

So (\*) is valid for  $k + 1$ . Therefore  $k + 1 \in A$ . Then  $A = \mathbb{N}$ . □

**EXAMPLE 1.38.** Issues: If  $n, p \in \mathbb{N}$ ,  $mn = mp$  does NOT imply  $n = p$ . Take  $m = 0$ .

**REMARK 1.39. Notation:**

$$(1.56) \quad \begin{aligned} \sum_{k=0}^n (2k + 1) &= 1 + 3 + 5 + \dots + (2n + 1) \\ &= \sum_{k=1}^{n+1} (2k - 1). \end{aligned}$$

**DEFINITION 1.40.** (1) We say that  $n \in \mathbb{N}$  is **even** if there exists  $m \in \mathbb{N}$  such that  $n = m + m = 2m$ .

(2) We say  $n \in \mathbb{N}$  is **odd** if there exists  $p \in \mathbb{N}$  such that  $n = 2p - 1$ .

**EXERCISE 6.** Prove that every natural number is either even or odd.

PROOF. Let  $A = \{ n \in \mathbb{N} : n \text{ is either even or odd} \}$ .

- (1)  $1 \in A$ . Note 1 is odd, because  $1 = 2(1) - 1$ , so in the definition of odd,  $n = p = 1$ .
- (2) Assume  $k \in A$ , we want to prove that  $k + 1 \in A$ .  $k \in A \Rightarrow k$  is either even or odd. So if  $k$  is even, then by definition, there exists  $m \in \mathbb{N}$  such that  $k = 2m$ . Then

$$(1.57) \quad k + 1 = 2m + 1 = 2(m + 1) - 1,$$

thus  $k + 1$  is odd because  $m + 1 \in \mathbb{N}$ . If  $k + 1$  is even, then by definition, we have  $m \in \mathbb{N}$  such that

$$(1.58) \quad \begin{aligned} k &= 2m - 1 \\ k + 1 &= 2mk + 1 = 2m \end{aligned}$$

Then  $k + 1$  is even (in the definition with  $m \in \mathbb{N}$ ). Therefore  $m + 1$  is either even or odd which tells us  $m + 1 \in A$ , and thus  $A = \mathbb{N}$ .

□

**THEOREM 1.41 ((Complete induction)).** *Let  $A \subseteq \mathbb{N}$  be a set such that  $1 \in A$ , and if  $A$  contains all natural numbers less than  $n$ , then  $A$  contains  $n$ . Then  $A = \mathbb{N}$ .*

Conclusion is that complete induction is equivalent to Peano's 3rd axiom.

**THEOREM 1.42.** *Let  $A \subseteq \mathbb{N}$  and let  $A$  be nonempty, then there exists a lower bound for  $A$ .*

**DEFINITION 1.43.**  $A \subseteq \mathbb{N}$  has a **lower bound** if  $\exists p \in A$  such that  $p \leq q$  for all  $q \in A$ .

**Tuesday, August 28th**

We do some more simple induction proofs.

**EXERCISE 7 (Bernoulli's Inequality).** Let  $K$  be an ordered field. Let  $n \in \mathbb{N}, x \in K, x \geq -1$ . Then

$$(1.59) \quad (1 + x)^n \geq 1 + nx. (*)$$

PROOF. By induction on  $n$ . So define

$$(1.60) \quad A = \{ n \in \mathbb{N} : \text{satisfy } (*), \forall x \in K \}.$$

**Base case:** Note that  $1 \in A$ , because

$$(1.61) \quad \begin{aligned} 1 + x &\geq 1 + x \\ (1 + x)^1 &\geq 1 + 1x. \end{aligned}$$

**Induction hypothesis:** Let  $k \in A$ . **Inductive step:** Because  $k \in A$ , we know

$$(1.62) \quad (1 + x)^k \geq 1 + kx. (\alpha)$$

From the conditions on  $x$ , we know  $x \geq -1$ , so we know  $1 + x \geq 0$ . Using one of the lemmas we proved, we can multiply to each side in  $(\alpha)$ . So we get

$$(1.63) \quad \begin{aligned} (1 + x)^{k+1} &\geq (1 + kx)(1 + x) \\ (1 + x)^{k+1} &\geq 1 + (k + 1)x + kx^2. \end{aligned}$$

For any  $x \in K$ , we know  $x^2 > 0 \Rightarrow kx^2 > 0, k \in \mathbb{N}$ . So then we have

$$(1.64) \quad (1 + x)^{k+1} \geq 1 + (k + 1)x + kx^2 \geq 1 + (k + 1)x.$$

Thus  $k + 1 \in A$ , therefore  $A = \mathbb{N}$ .

□

Given an ordered field  $K$ , we have the identity element, we call it 1. But remember my field might be fractions, it might be pairs of numbers, it might be very different objects than numbers. So for today, to avoid confusion with the natural number 1, we will instead notate the multiplicative identity in  $K$  as  $\tilde{1}$ . So we have

$$(1.65) \quad a \cdot \tilde{1} = a,$$

for all  $a \in K$ .

EXAMPLE 1.44. On  $\mathbb{F} = \mathbb{Q}(i)$ , we have that  $\tilde{1} = (1, 0)$ .

From the fact that  $K$  is ordered, we know  $\tilde{1} > 0$ . Using the fact that the sum of positives is positive, we know

$$(1.66) \quad \dots > \tilde{1} + \tilde{1} + \tilde{1} + \tilde{1} > \tilde{1} + \tilde{1} + \tilde{1} > \tilde{1} + \tilde{1} > \tilde{1} > 0.$$

For every ordered field, we have a copy of  $\mathbb{N}$  as a subset. That means there exists  $\varphi : \mathbb{N} \rightarrow K$  that is injective, and that

$$(1.67) \quad \varphi(a + b) = \varphi(a) + \varphi(b).$$

We define  $\varphi(1) = \tilde{1}$ . And then

$$(1.68) \quad \varphi(s) = \tilde{1} + \tilde{1} + \dots \tilde{1},$$

where  $\tilde{1}$  is repeated  $s$  times.

EXAMPLE 1.45. Let

$$(1.69) \quad K = \left\{ \frac{p(t)}{q(t)} : p, q \text{ polynomials in } t \right\}.$$

On  $K$ , the multiplicative identity is  $1 = \frac{t}{t} = \frac{t^2}{t^2}$ . So  $\mathbb{N} \subseteq K$ .

Because (a copy of)  $\mathbb{N}$  is always included in any ordered field  $K$ , and because the negative of any  $n \in \mathbb{N}$  is also in  $K$ , we obtain (a copy of)  $\mathbb{Z}$  in  $K$ .

$$(1.70) \quad \mathbb{Z} \left\{ \begin{array}{c|c|c} & & K \\ \hline \mathbb{N} & \begin{array}{c} 3 \leftarrow \\ 2 \leftarrow \\ 1 \leftarrow \end{array} & \begin{array}{c} \tilde{1} + \tilde{1} + \tilde{1} \\ \tilde{1} + \tilde{1} \\ \tilde{1} \end{array} \\ \hline & 0 & 0 \\ \hline & \begin{array}{c} -1 \\ -2 \end{array} & \begin{array}{c} -\tilde{1} \\ -\tilde{1} - \tilde{1} \end{array} \end{array} \right\}.$$

Every element  $a \neq 0$  in  $k$  has a multiplicative inverse  $a \in \mathbb{N} \Rightarrow \varphi(a) \in K$ . So there exists  $(\varphi(a))^{-1} \in K$ . And this represents  $\frac{1}{a} \in \mathbb{Q}$ .

So we have a copy of  $\mathbb{Q}$  in  $K$ .

In other words,  $\varphi : \mathbb{Q} \rightarrow K$  such taht

$$(1.71) \quad \begin{aligned} \varphi(1) &= \tilde{1} \\ \varphi(0) &= 0 \\ \varphi(a + b) &= \varphi(a) + \varphi(b) \\ \varphi(ab) &= \varphi(a)\varphi(b). \end{aligned}$$

EXAMPLE 1.46. Let

$$(1.72) \quad K = \left\{ \frac{p(t)}{q(t)} : p, q \text{ polynomials in } t \right\}.$$

Then there exists  $\varphi : \mathbb{Q} \rightarrow K$  given by

$$(1.73) \quad x \mapsto x = \frac{a}{b} : a, b \in \mathbb{Z}, b \neq 0.$$

EXAMPLE 1.47. Consider  $K$ , the field of the last example. Let  $A \subseteq K$ ,  $A = \{1, 2, 3, 4, 5, \dots\}$ . Then there exists an element in  $K$ , call it  $x$  such that  $x > y$  for all  $y \in A$ .

Indeed  $x = t \in K$ . Note  $t = \frac{t}{1}$ , where  $t, 1$  are polynomials in  $t$ .

**Claim:**  $t - n > 0$  for every  $n \in \mathbb{N}$ .

Recall that for  $K$ , we call

$$(1.74) \quad P = \left\{ \frac{p(t)}{q(t)} : p(t)q(t) \text{ has a positive coefficient in front of the largest degree term} \right\}.$$

And clearly  $t - n \in P$ .

EXERCISE 8. Check that there exists  $\alpha \in K$ , where  $K$  is from the last example, such that

$$(1.75) \quad \alpha < n, \forall n \in \mathbb{Z}.$$

Note  $\mathbb{Q}(t)$  is not a nice field for this reason. It is not Archimedean.

THEOREM 1.48. Let  $K$  be an ordered field. The following are equivalent:

- (1)  $\mathbb{N} \subseteq K$  is not bounded from above.
- (2) Given any two  $a, b \in K, a > 0$ , there exists  $n \in \mathbb{N}$  such that  $na > b$ .
- (3) Given any  $a > 0$  in  $K$ , there exists  $n \in \mathbb{N}$  such that  $0 < \frac{1}{n} < a$ .

DEFINITION 1.49. We say that  $K$  is an **Archimedean** field if it satisfies any of the equivalent statements in the theorem above.

EXAMPLE 1.50. (1)  $\mathbb{Q}$  is an Archimedean field.

(2)  $\mathbb{R}$  is an Archimedean field.

(3)  $\mathbb{Q}(t)$  is not an Archimedean field.

### Wednesday, April 28th

Given  $F$  an ordered field, let  $X \subseteq F$ .

DEFINITION 1.51. We say  $X$  has a **least element** if there exists  $p \in X$  such that  $p \leq q$  for all  $q \in X$ . And we say  $X$  has a **greatest element** if there exists  $p \in X$  such that  $p \geq q$  for all  $q \in X$ .

DEFINITION 1.52. We say  $X$  has a **lower bound** if there exists  $p \in F$  such that  $p \leq q$  for any  $q \in X$ . And we say  $X$  has an **upper bound** if there exists  $p \in F$  such that  $p \geq q$  for all  $q \in X$ .

REMARK 1.53. • The set  $X$  might have an upper bound, but no greatest element.

EXAMPLE 1.54. Let  $X = \mathbb{N} \subseteq \mathbb{Q}(t)$ . Note  $\mathbb{N}$  does not have a greatest element, but has an upper bound (for every  $n \in \mathbb{N}$ , we have  $n \leq t \in \mathbb{Q}(t)$ , where  $\leq$  means that  $t - n = 0$  or  $t - n \in P$ , for the definition of  $P$  specific to this field).

- If  $X$  has a least element, then it is unique.

PROOF. Suppose  $p, \tilde{p}$  are both least elements of  $X$ . Then  $p \leq \tilde{p}$ , because  $p$  is a least element. And also  $\tilde{p} \leq p$ , because  $\tilde{p}$  is a least element. Thus  $p = \tilde{p}$ .  $\square$

EXERCISE 9. Prove that the greatest element is unique.

THEOREM 1.55 (**Well-ordered principle**). Let  $A \subseteq \mathbb{N}$ ,  $A \neq \emptyset$ . Then  $A$  has a least element.



PROOF. Consider  $I_n = \{ p \in \mathbb{N} : p \leq n \}$ . Then we have

$$(1.76) \quad \begin{aligned} I_1 &= \{ 1 \}, \\ I_2 &= \{ 1, 2 \}, \\ I_3 &= \{ 1, 2, 3 \}, \dots \end{aligned}$$

Let  $B = \mathbb{N} \setminus A$ . Then we know  $B \neq \mathbb{N}$  because  $A \neq \emptyset$ . Let

$$(1.77) \quad X = \{ n \in \mathbb{N} : I_n \subseteq B \}.$$

**Case 1:** Note that if  $A$  contains 1, then we are done, because 1 is the least element of  $\mathbb{N}$ , and therefore it is the least element of any subset of  $\mathbb{N}$  containing it. So suppose we had  $A = \{ 1, 3, 7 \}$ ,  $B = \{ 2, 4, 5, 6, \dots \}$ . This tells us that  $X = \emptyset$ .

**Case 2:** If  $A$  does not contain 1, then that means that  $1 \in B$ . Thus  $1 \in X$ . Note  $X \neq \mathbb{N}$  because that would make  $A$  empty.

$X$  cannot satisfy the third Peano axiom, which says that  $1 \in X$ , and  $q \in X \Rightarrow q+1 \in X$  implies  $X = \mathbb{N}$ . Since  $1 \in X$ , and  $X \neq \mathbb{N}$ , we must have that there exists  $q \in X$  such that  $q+1 \notin X$ . Note that  $q \in X$  means  $I_q \subseteq B$ , and  $q+1 \notin X$  means that  $I_{q+1} \not\subseteq B$ . Then we have

$$(1.78) \quad \begin{aligned} \{ 1, 2, 3, \dots, q \} &\subseteq B \\ \{ 1, 2, 3, \dots, q+1 \} &\not\subseteq B. \end{aligned}$$

Thus we have  $1, 2, 3, \dots, q \notin A$  and  $q+1 \in A$ . Thus  $A$  has a least element, namely  $q+1$ .  $\square$

Recall Peano's third axiom (PSI). It states that if  $X \subseteq \mathbb{N}$  such that

- (1)  $1 \in X$
- (2)  $\forall q \in X \Rightarrow q+1 \in X$

then  $X = \mathbb{N}$ .

**Complete induction (PCI):** If  $X \subseteq \mathbb{N}$  such that

- ( $\tilde{1}$ )  $1 \in X$
- ( $\tilde{2}$ )  $\forall q \in X$  such that  $1, 2, 3, \dots, q \in X \Rightarrow q+1 \in X$

then  $X = \mathbb{N}$ .

We prove that they are equivalent.

PROOF. **PCI  $\Rightarrow$  PSI:** Suppose PCI holds. Then we know that if  $X \subseteq \mathbb{N}$  such that  $1 \in X$ , and ( $\tilde{2}$ ) is true implies  $X = \mathbb{N}$ . We want to show PSI holds. So let  $Y \subseteq \mathbb{N}$  such that  $1 \in Y$ , and  $\forall q \in Y \Rightarrow q+1 \in Y$ . We want to show that  $Y = \mathbb{N}$ . But note that (2) is a stronger condition than ( $\tilde{2}$ ). Because if all numbers up to and including  $q$  are in  $Y$ , then certainly  $q$  is in  $Y$ . So then we know  $Y = \mathbb{N}$  by PCI. So PSI holds. Note we made 3 claims. We know that  $1, 2, \dots, q \in X \Rightarrow q \in X$ . And using this, we know (2)  $\Rightarrow$  ( $\tilde{2}$ ). And using this we know PCI  $\Rightarrow$  PSI.

**PSI  $\Rightarrow$  PCI** Let  $X \subseteq \mathbb{N}$  such that  $1 \in X$  and ( $\tilde{2}$ ) holds. We want to show that  $X = \mathbb{N}$ . Consider

$$(1.79) \quad Y = \{ n \in \mathbb{N} : I_n \subseteq X \}.$$

Note that  $1 \in X \Rightarrow I_1 \subseteq X \Rightarrow 1 \in Y$ . And  $I_q \subseteq X \Rightarrow I_{q+1} \subseteq X$ . Then we know that  $q \in Y \Rightarrow q+1 \in Y$ . So by PSI, we know  $Y = \mathbb{N}$ , but we wanted to show  $X = \mathbb{N}$ . But by the definition of  $Y$ , we know  $X = \mathbb{N}$ .  $\square$

PSI	PCI
$X \subseteq \mathbb{N}$ such that	$X \subseteq \mathbb{N}$ such that
1) $1 \in X$	1) $1 \in X$
2) $a \in X \Rightarrow a+1 \in X$	$\tilde{2}$ ) $1, 2, \dots, a \in X \Rightarrow a+1 \in X$
$\Rightarrow X = \mathbb{N}$	$\Rightarrow X = \mathbb{N}$ .

EXAMPLE 1.56. Let  $a_1 = 1, a_2 = 1; a_{n+1} = a_n + a_{n-1}$ . We have

$$\begin{aligned}
 a_1 &= 1 \\
 a_2 &= 1 \\
 a_3 &= 2 \\
 a_4 &= 3 \\
 a_5 &= 5 \\
 a_6 &= 8 \\
 a_7 &= 13 \\
 a_8 &= 21.
 \end{aligned}
 \tag{1.80}$$

Prove that  $a_n \geq 2n - 4$  for all  $n \geq 6$ .

PROOF. We use PSI first. Note

$$\begin{aligned}
 a_6 &= 8 \geq 2(6) - 4 = 12 - 4 = 8 \\
 a_7 &= 13 \geq 2(7) - 4 = 14 - 4 = 10.
 \end{aligned}
 \tag{1.81}$$

Now we show that  $a_n \geq 2n - 4 \Rightarrow a_{n+1} \geq 2(n+1) - 4 = 2n - 2$ . If  $a_{n-1} = 1$ , we have trouble.  $a_{n+1} = a_n + a_{n-1} \geq 2n - 3$ . This is because we cannot assume anything about  $a_{n-1}$ .

So instead we use PCI. We have

$$\begin{aligned}
 a_6 &\geq 8 \\
 a_7 &= 13 \geq 2(7) - 4 = 10 \\
 a_n &\geq 2n - 4 \\
 a_{n-1} &\geq 2(n-1) - 4
 \end{aligned}
 \tag{1.82}$$

And we get

$$a_{n+1} = a_n + a_{n-1} \geq 4n - 10.
 \tag{1.83}$$

Then our goal was to show  $a_{n-1} \geq 2(n+1) - 4 = 2n - 2$ . So from above, we know  $a_{n+1} \geq 4n - 10$ . So we claim

$$4n - 10 \geq 2n - 2.
 \tag{1.84}$$

But note

$$\begin{aligned}
 n &\geq 4 \\
 2n &\geq 8 \\
 4n - 2n &\geq 10 - 2 \\
 4n - 10 &\geq 2n - 2.
 \end{aligned}
 \tag{1.85}$$

Thus we get  $a_{n+1} \geq 2n - 2$ . □

**Thursday, August 30th**

**Logic:**

**A:** a number  $x$  is positive and an integer.

**B:** a number  $x$  is an integer.

A is stronger than B. If A is true, then B is true.  $A \Rightarrow B$ .

REMARK 1.57. PSI = 3rd Peano axiom

WOP = Every set  $A \neq \emptyset, A \subseteq \mathbb{N}$  has a least element.

PCI

$\text{PSI} \Rightarrow \text{WOP}$ . Also  $\text{PSI} \Leftrightarrow \text{PCI}$ .

REMARK 1.58. The well-ordering principle implies the principle of complete induction.

PROOF. If  $X \subseteq \mathbb{N}$ ,  $1) 1 \in X$ ,  $\tilde{2}) 1, \dots, a \in X \Rightarrow a + 1 \in X$ . Consider the set  $A = \mathbb{N} \setminus X$ ,  $A \subseteq \mathbb{N}$ . We want to prove that  $A = \emptyset$ . Suppose  $A \neq \emptyset$ . Then  $A$  has a least element by the well-ordered principle. Note  $1 \notin A$ . Let  $a > 1$  be the least element of  $A$ . Then  $1, 2, 3, \dots, a - 1 \in X$  by  $\tilde{2}) \Rightarrow a \in X \Rightarrow a \notin A$ , which is a contradiction. Therefore  $A = \emptyset$ . Then  $X = \mathbb{N}$ .  $\square$

DEFINITION 1.59. Given any ordered field  $F$ , we denote

$$\begin{aligned}
 (1.86) \quad & (a, b) = \{ x \in F : a < x < b \} \\
 & [a, b) = \{ x \in F : a \leq x < b \} \\
 & (a, b] = \{ x \in F : a < x \leq b \} \\
 & [a, b] = \{ x \in F : a \leq x \leq b \} \\
 & (a, \infty) = \{ x \in F : a < x \} \\
 & (-\infty, b) = \{ x \in F : x < b \}.
 \end{aligned}$$

LEMMA 1.60. In an ordered field

$$(1.87) \quad |x| \leq a \Leftrightarrow -a \leq x \leq a (\Leftrightarrow x \in [-a, a]).$$

$\mathbb{Q}$  is an ordered field. Consider the set

$$(1.88) \quad A = \{ x \in \mathbb{Q} : x > 0, x^2 < 2 \}.$$

$A$  is bounded by above =  $A$  has an upper bound. Because if  $x \in A \Rightarrow x^2 < 2 < 4 \Rightarrow x^2 < 4 \Rightarrow x < 2$ . Note that we can try to find a best upper bound in  $\mathbb{Q}$ , but it is impossible. The real numbers  $\mathbb{R}$  are the set which completes  $\mathbb{Q}$  so that every set has a least upper bound and greatest lower bound.

**Construction of  $\mathbb{R}$ :**

- (1) Cauchy sequences [we'll explain this through the semester].
- (2) Dedekind cuts (handouts).
- (3) Forcing the principle of best upper bound or lower bound.
- (4) Surreals and hyperreals.

**Pythagoras.** The equation  $x^2 = 2$  has no solution for  $x \in \mathbb{Q}$ .

PROOF. Suppose there exists  $p, q \in \mathbb{Z}$  such that  $x = \frac{p}{q}$ , and  $x^2 = 2$ . Assume they are coprime. Then we have

$$(1.89) \quad p^2 = 2q^2.$$

Thus  $p^2$  is even which means  $p$  is even. And then  $p = 2 \cdot r$  for some integer  $r$ . Then we get

$$\begin{aligned}
 (1.90) \quad & (2r)^2 = 2q^2 \\
 & 4r^2 = 2q^2 \\
 & 2r^2 = q^2.
 \end{aligned}$$

So  $q^2$  is even which means  $q$  is even which is impossible, since we said  $p, q$  coprime. So there exist no such  $p, q \in \mathbb{Z}$ .  $\square$

## SECTION 1 EXERCISES

11. Solve

i)  $|x - 3| = 8$

- ii)  $|x - 3| < 8$
- iii)  $|x + 4| < 2$
- iv)  $|x - 1| + |x - 2| < 1$
- v)  $|x - 1| + |x + 1| < 2$

REMARK 1.61. Note  $|a| \leq b \Leftrightarrow a \leq b$  and  $-a \leq b \Leftrightarrow -b \leq a \leq b$ .

**Solutions:**

- i) We have  $x - 3 = 8$  or  $-x + 3 = 8$ . In the first case,  $x = 11$ , and in the second case,  $x = -5$ .
- ii)  $-8 < x - 3 < 8 \Rightarrow -5 < x < 11$ .
- iii)
- iv) So consider the case where  $x < 1$  and  $x < 2$ . Then we have  $1 - x + 2 - x < 1$ . So then  $2 < 2x \Rightarrow 1 < x$ . But this is a contradiction since we said  $x < 1$  so there is no solution.
- v) *Prove the following:*

(ii) *If  $a < b$ , then  $-b < -a$ .*

PROOF. Since  $a < b$ , then we know  $b - a \in P$  by definition. We want to show that  $-b < -a$ , so by definition, we must show that  $-a - (-b) \in P$ . We show that  $-(-b) = b$ . Note that  $b + (-b) = (-b) + b = 0$  by (P3), so  $b$  is the additive inverse of  $(-b)$ . So  $-(-b) = b$ , since additive inverses are unique. Observe:

$$(1.91) \quad \begin{aligned} -a - (-b) &= -a + b \quad \text{by (P3)} \\ &= b - a \quad \text{by (P4)}. \end{aligned}$$

But we know that  $b - a \in P$ . So  $-a - (-b) \in P$ , and thus by definition,  $-b < -a$ .  $\square$

(iv) *If  $a < b$  and  $c > 0$ , then  $ac < bc$ .*

PROOF. Let  $a < b$ . Then by definition, we know  $b - a \in P$ . Since  $c > 0$ , we know  $c \in P$ , so  $c(b - a) \in P$  by (P12). Then we have

$$(1.92) \quad c(b - a) = cb - ca \quad \text{by (P9)}.$$

And so  $cb - ca \in P$  which means  $ca < cb$ . Then by (P8), we know  $ac < bc$ .  $\square$

(vi) *If  $a > 1$ , then  $a^2 > a$ .*

PROOF. Since  $1 < a$ , we know  $a - 1 \in P$ . Note that  $0 < 1$  and  $1 < a$  give us  $0 < a$  by the following:

REMARK 1.62. **Transitivity:** If  $x < y$  and  $y < z$ , then  $x < z$ .

PROOF. Let  $x < y$  and  $y < z$ . Then we know  $y - x \in P$  and  $z - y \in P$ . We want to know if  $z - x \in P$ . But by (P11), we know

$$(1.93) \quad y - x + z - y = z - x \in P.$$

Thus  $x < z$ .  $\square$

And since  $0 < a \Rightarrow a - 0 = a \in P$  by (P2),  $a \in P$ . Then we have

$$(1.94) \quad \begin{aligned} a \in P, a - 1 \in P &\Rightarrow a(a - 1) \in P \quad \text{by (P12)} \\ a(a - 1) &= a^2 - a \quad \text{by (P9)} \\ a^2 - a &= a(a - 1) \in P \Rightarrow a < a^2 \quad \text{by definition.} \end{aligned}$$

Alternatively, upon proving that  $a > 0$  you could simply apply part (iv), noting that  $1 < a$ ,  $a > 0 \Rightarrow a < a^2$  by (P6).  $\square$

viii) *Suppose that (P10)-(P12) were replaced by*

(P'10) *For any numbers  $a$  and  $b$ , one, and only one of the following holds:*

- (i)  $a = b$ ,
- (ii)  $a < b$ ,
- (iii)  $b < a$ .

(P'11) For any numbers  $a, b$ , and  $c$ , if  $a < b$  and  $b < c$ , then  $a < c$ .

(P'12) For any numbers  $a, b$ , and  $c$ , if  $a < b$ , then  $a + c < b + c$ .

(P'13) For any numbers  $a, b$ , and  $c$ , if  $a < b$  and  $0 < c$ , then  $ac < bc$ .

Show that (P10)-(P12) can then be deduced as theorems.

PROOF. We derive (P10). Applying (P'10), we define the positive numbers  $P = \{x : x > 0\}$ . Let  $a$  be a number. Following (P'10), we have

Case 1:  $a = 0$ .

Case 2:  $a > 0$ . Then by our definition of  $P$ ,  $a \in P$ .

Case 3:  $a < 0$ . Then manipulating the definition of  $<$ , we have  $0 - a > 0$ . Then by (P4),(P2), we know  $-a + 0 = -a > 0$ . Then by our definition,  $-a \in P$ . Thus we have derived (P10).

Now we will derive (P11). Let  $a, b \in P$ . Then we know  $a, b > 0$  by our definition of  $P$ . We want to show  $a + b \in P$ . So we must show  $a + b > 0$ . We show that  $-b < a$ . First we prove that  $-b < 0$ . Note that by (P'10), we know that either  $-b < 0$ ,  $-b > 0$ , or  $-b = 0$ . We cannot have  $-b = 0$ , since then  $b + -b = b + 0 = b = 0$ , by (P3). And this contradicts (P'10) because we said  $b > 0$ . Now if  $-b > 0$ , then applying (P'12) because  $0 < -b$ , we have

$$(1.95) \quad 0 + b < b + (-b) \Rightarrow b < 0 \quad \text{by (P2)}$$

which is a contradiction because we said  $b > 0$ . So we must have  $-b < 0$ . Then applying (P'11), we have  $-b < a$  since  $-b < 0$  and  $0 < a$ . Now we may apply (P'12) and get

$$(1.96) \quad -b + b < a + b \Rightarrow 0 < a + b \quad \text{by (P2)}$$

And so  $a + b \in P$ , so we have derived (P11).

Finally, we derive (P12). Let  $a, b \in P$ . Then we know by our definition of  $P$  that  $a, b > 0$ . We wish to show  $a \cdot b \in P$ . So equivalently, we must show that  $a \cdot b > 0$ . So since  $0 < a$  and  $0 < b$ , applying (P'13), we know

$$(1.97) \quad 0 \cdot c < a \cdot b \Rightarrow 0 < a \cdot b \quad \text{by (P6)}.$$

Then we know  $a \cdot b \in P$ . □

vii) Prove that if  $0 < a < b$ , then

$$(1.98) \quad a < \sqrt{ab} < \frac{a+b}{2} < b.$$

PROOF. We show that  $a < \sqrt{ab}$ . Observe:

$$(1.99) \quad \begin{aligned} a &= \sqrt{a^2} && \text{by definition of } \sqrt{\phantom{x}} \\ b - a &\in P && \text{by definition of } < \\ a < b &\Rightarrow a^2 < ab && \text{by 5(iv), since } a > 0 \\ a^2 < ab &\Rightarrow \sqrt{a^2} < \sqrt{ab} && \text{by 5(x)} \\ \sqrt{a^2} < \sqrt{ab} &\Rightarrow a < \sqrt{ab} && \text{by definition of } \sqrt{\phantom{x}}. \end{aligned}$$

Next we show that  $\sqrt{ab} < \frac{a+b}{2}$ . Let  $b - a = \epsilon > 0$ , since  $a < b$ . Observe:

$$\begin{aligned}
 (1.100) \quad & \epsilon > 0 \Rightarrow \epsilon^2 > 0 && \text{by (P12)} \\
 & \epsilon^2 > 0 \Rightarrow 2a^2 + 2a\epsilon + \epsilon^2 > 2a^2 + 2a\epsilon && \text{by (P11),(P12)} \\
 & \Rightarrow a^2 + (a + \epsilon)^2 > 2a(a + \epsilon) && \text{by (P9)} \\
 & \Rightarrow a^2 + b^2 > 2ab && \text{by definition of } \epsilon \\
 & \Rightarrow \frac{a^2 + b^2}{4} > \frac{ab}{2} && \text{by 5(iv), since } 4^{-1} > 0 \\
 & \Rightarrow \frac{a^2 + b^2}{4} + \frac{ab}{2} > \frac{ab}{2} + \frac{ab}{2} = ab && \text{by 5(i)} \\
 & \Rightarrow ab < \frac{a^2 + 2ab + b^2}{4} = \left(\frac{a+b}{2}\right)^2 && \text{by 3(ii)} \\
 & \Rightarrow \sqrt{ab} < \frac{a+b}{2} && \text{by 5(x).}
 \end{aligned}$$

Finally, we prove that  $\frac{a+b}{2} < b$ . Since  $a < b$ , we know  $\frac{1}{2}a < \frac{1}{2}b$  by 5(iv) since  $\frac{1}{2} > 0$  since  $2 > 0$ . So then we have

$$\begin{aligned}
 (1.101) \quad & \frac{a+b}{2} = \frac{1}{2}a + \frac{1}{2}b \\
 & < \frac{1}{2}b + \frac{1}{2}b \\
 & = b.
 \end{aligned}$$

Thus all together, we have  $a < \sqrt{ab} < \frac{a+b}{2} < b$ . □

xii) *Prove the following:*

(iv)  $|x - y| \leq |x| + |y|$ . (*Give a very short proof.*)

PROOF. We proved in class that  $|a + b| \leq |a| + |b|$ . Simply take  $a = x$  and  $b = -y$ . Then we have

$$(1.102) \quad |x - y| = |x + (-y)| \leq |x| + |-y| = |x| + |y|.$$

Note this proof assumes that  $|y| = |-y|$ , but this is proved below in 14(a). □

(v)  $|x| - |y| \leq |x - y|$ . (*A very short proof is possible, if you write things in the right way.*)

PROOF. If either of  $x, y$  is 0, then we have the desired result immediately, since  $|x| \leq |x|$  and  $|y| \leq |y|$ . So we assume  $x, y \neq 0$ , and we assume  $x \neq y$ , in which case we have  $0 \leq 0$ .

**Case 1:**  $x, y \in P$ . Then  $|x| = x, |y| = y$ , so  $|x| - |y| = x - y$ . Now if  $x - y \in P$ , then  $|x - y| = x - y = |x| - |y|$ . And if  $x - y \notin P$ , then  $|x - y| = y - x \in P$ . Then we have

$$(1.103) \quad |x| - |y| = x - y < 0 < y - x = |x - y|.$$

In either case,  $|x| - |y| \leq |x - y|$ .

**Case 2:**  $x, y \notin P$ . Then  $|x| = -x, |y| = -y$ , so  $|x| - |y| = y - x$ . Now if  $y - x \in P$ , then  $|x - y| = |y - x| = y - x = |x| - |y|$ , since  $|-a| = |a|$  by 14(a). And if  $y - x \notin P$ , then  $|x - y| = x - y \in P$ . Then we have

$$(1.104) \quad |x| - |y| = y - x < 0 < x - y = |x - y|.$$

In either case,  $|x| - |y| \leq |x - y|$ .

**Case 3:**  $x \in P, y \notin P$ . Then  $|x| = x, |y| = -y$ . So then

$$(1.105) \quad |x| - |y| = x + y.$$

And

$$\begin{aligned}
 (1.106) \quad |x - y| &= ||x| - (-|y|)| \\
 &= ||x| + |y|| \\
 &= |x| + |y|.
 \end{aligned}$$

But then  $x \leq |x|$  and  $y \leq |y|$  so we have

$$(1.107) \quad |x| - |y| = x + y \leq |x| + |y| = |x - y|.$$

**Case 4:**  $x \notin P, y \in P$ , then

$$(1.108) \quad |x| - |y| = -(x + y),$$

and again we have

$$(1.109) \quad |x| - |y| = -x - y \leq |x| + |y| = |x - y|.$$

since  $-x \leq |x|$  and  $-y \leq |y|$ . □

(vi)  $|(|x| - |y|)| \leq |x - y|$ . (*Why does this follow immediately from (v)?*)

PROOF. Note that by 14(a) below, we have

$$(1.110) \quad |x - y| = |y - x|.$$

So then note that

$$(1.111) \quad |(|x| - |y|)| = \begin{cases} |x| - |y| & \text{if } |x| > |y| \\ |y| - |x| & \text{if } |y| > |x| \end{cases}.$$

In the first case, then the result follows from 12(v) above, since  $|(|x| - |y|)| = |x| - |y|$ . In the second case, simply swap  $y$  and  $x$  and apply 12(v), noting that  $|y - x| = |x - y|$ . □

xiv) (a) *Prove that  $|a| = |-a|$ . (The trick is not to become confused by too many cases. First prove the statement for  $a \geq 0$ . Why is it then obvious for  $a \leq 0$ ?)*

PROOF. If  $a = 0$ , then  $a = -a = 0$ , and  $|0| = 0$ , so we have the desired result. Let  $a > 0$ . Then  $|a| = a$ , and  $|-a| = a$ , since  $-a < 0 \Rightarrow |-a| = -(-a) = a$ . Now let  $a < 0$ . Simply let  $b = -a$ . We want to show  $|a| = |-a|$ , or equivalently,  $|-b| = |b|$ , since  $-b = -(-a) = a$ . But then we know  $-b < 0 \Rightarrow b > 0$ . So we simply apply the case where  $a > 0$  to  $b$ , and we have the desired result. □

(b) *Prove that  $-b \leq a \leq b$  if and only if  $|a| \leq b$ . In particular, it follows that  $-|a| \leq a \leq |a|$ .*

PROOF. Let  $-b \leq a \leq b$ . Then we must have that  $b \geq 0$ , since otherwise  $b \leq -b$ . If  $b = 0$ , then we must have  $a = 0$ , so the result is trivial, since  $|0| = 0 \leq 0$ . And if  $a = 0$ , then  $|a| = |0| = 0 \leq b$ , since  $b \geq 0$ . So we assume  $a \neq 0, b > 0$ .

**Case 1:**  $a > 0$ . Then  $|a| = a$ . And then since  $|a| = a \leq b$ , we are done.

**Case 2:**  $a < 0$ . Then  $|a| = -a$ . Note

$$(1.112) \quad a - (-b) = a + b = b - (-a) = b - |a|.$$

Now since  $-b \leq a$ , then we know  $a - (-b) \in P$  by definition, so  $a - (-b) \geq 0 \Rightarrow b - |a| \geq 0 \Rightarrow |a| \leq b$ . □