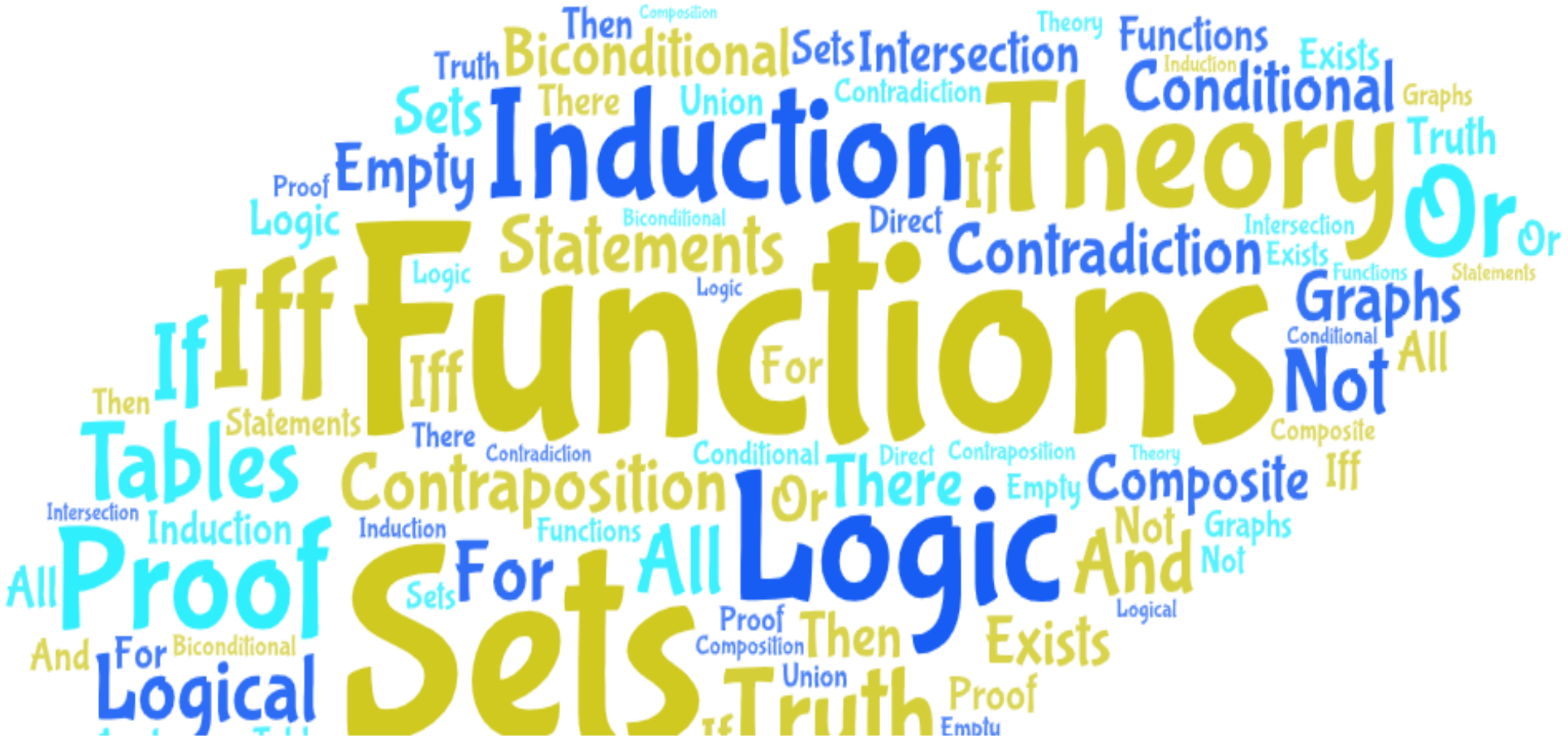
Lecture
Thursday Week 1

Discrete Mathematics and Probability 2024



Discrete Math: Covered material

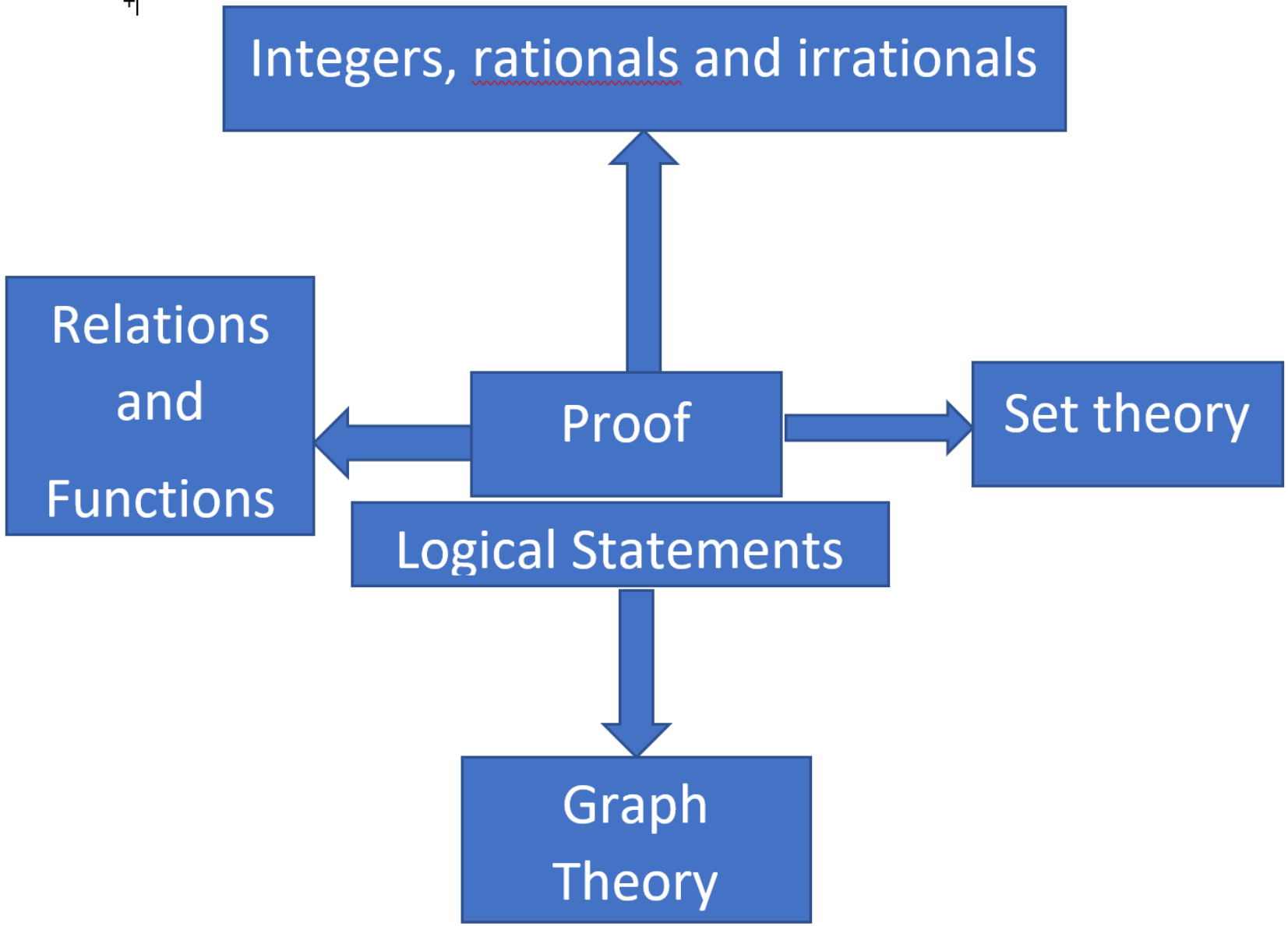
* Week 1 (Monday 16 Sept.): Epp Chapter 1: Speaking Mathematically
  - Variables
  - Language of Sets
  - Language of Relations and Functions
  - Language of Graphs

  Chapter 2: Logic of compound statements
  - 2.1 Logical Form and Logical Equivalence
  - 2.2 Conditional Statements

  Chapter 3: The logic of Quantified Statements
  - All except 3.4, which was covered in Inf1A.

* Week 2 (19 & 23 Sept): Epp Chapter 4: Elementary number theory and methods of proof.
  - Direct proof, proof by cases, by contradiction and by contraposition
  - Skip Section 4.9 and 4.10 (or 4.8 in the 4^{th} edition).

* Week 3: Epp Ch 5: Induction and Recursion
  - Skip 5.1 (you know this already), skip 5.7-5.9
* Week 4: Epp Ch 6: Set theory, without 6.4
  Epp Ch 7: Functions
* Week 5: Epp Ch 8: Relations


Integers, rationals and irrationals
Relations and Functions
Proof
Set theory
Logical Statements
Graph Theory

Appendix A

APPENDIX A

PROPERTIES OF THE REAL NUMBERS*

In this text we take the real numbers and their basic properties as our starting point. We give a core set of properties, called axioms, which the real numbers are assumed to satisfy, and we state some useful properties that can be deduced from these axioms.

We assume that there are two binary operations defined on the set of real numbers, called **addition** and **multiplication**, such that if a and b are any two real numbers, the **sum** of a and b, denoted $\boldsymbol{a+b}$, and the **product** of a and b, denoted $\boldsymbol{a \cdot b}$ or $\boldsymbol{ab}$, are also real numbers. These operations satisfy properties F1–F6, which are called the **field axioms**.

F1. *Commutative Laws* For all real numbers a and b,

$$a+b=b+a \quad \text{and} \quad ab=ba.$$

F2. *Associative Laws* For all real numbers a, b, and c,

$$(a+b)+c=a+(b+c) \quad \text{and} \quad (ab)c=a(bc).$$

F3. *Distributive Laws* For all real numbers a, b, and c,

$$a(b+c)=ab+ac \quad \text{and} \quad (b+c)a=ba+ca.$$

F4. *Existence of Identity Elements* There exist two distinct real numbers, denoted 0 and 1, such that for every real number a,

$$0+a=a+0=a \quad \text{and} \quad 1 \cdot a=a \cdot 1=a.$$

F5. *Existence of Additive Inverses* For every real number a, there is a real number, denoted $-a$ and called the **additive inverse** of a, such that

$$a+(-a)=(-a)+a=0.$$

F6. *Existence of Reciprocals* For every real number $a \neq 0$, there is a real number, denoted $1/a$ or a^{-1}, called the **reciprocal** of a, such that

$$a \cdot \left(\frac{1}{a}\right)=\left(\frac{1}{a}\right) \cdot a=1.$$

All the usual algebraic properties of the real numbers that do not involve order can be derived from the field axioms. The most important are collected as theorems T1–T16 as follows. In all these theorems the symbols a, b, c, and d represent arbitrary real numbers.

T1. *Cancellation Law for Addition* If $a+b=a+c$, then $b=c$. (In particular, this shows that the number 0 of Axiom F4 is unique.)

T2. *Possibility of Subtraction* Given a and b, there is exactly one x such that $a+x=b$. This x is denoted by $b-a$. In particular, $0-a$ is the additive inverse of a, $-a$.

*Adapted from Tom M. Apostol, *Calculus, Volume I* (New York: Blaisdell, 1961), pp. 13–19.

T3. $b - a = b + (-a)$.

T4. $-(-a) = a$.

T5. $a(b - c) = ab - ac$.

T6. $0 \cdot a = a \cdot 0 = 0$.

T7. *Cancellation Law for Multiplication* If $ab = ac$ and $a \neq 0$, then $b = c$. (In particular, this shows that the number 1 of Axiom F4 is unique.)

T8. *Possibility of Division* Given a and b with $a \neq 0$, there is exactly one x such that $ax = b$. This x is denoted by b/a and is called the **quotient** of b and a. In particular, $1/a$ is the reciprocal of a.

T9. If $a \neq 0$, then $b/a = b \cdot a^{-1}$.

T10. If $a \neq 0$, then $(a^{-1})^{-1} = a$.

T11. *Zero Product Property* If $ab = 0$, then $a = 0$ or $b = 0$.

T12. *Rule for Multiplication with Negative Signs*

$$(-a)b = a(-b) = -(ab), \qquad (-a)(-b) = ab,$$

and

$$-\frac{a}{b} = \frac{-a}{b} = \frac{a}{-b}.$$

T13. *Equivalent Fractions Property*

$$\frac{a}{b} = \frac{ac}{bc}, \quad \text{if } b \neq 0 \text{ and } c \neq 0.$$

T14. *Rule for Addition of Fractions*

$$\frac{a}{b} + \frac{c}{d} = \frac{ad + bc}{bd}, \quad \text{if } b \neq 0 \text{ and } d \neq 0.$$

T15. *Rule for Multiplication of Fractions*

$$\frac{a}{b} \cdot \frac{c}{d} = \frac{ac}{bd}, \quad \text{if } b \neq 0 \text{ and } d \neq 0.$$

T16. *Rule for Division of Fractions*

$$\frac{\frac{a}{b}}{\frac{c}{d}} = \frac{ad}{bc}, \quad \text{if } b \neq 0,\ c \neq 0, \text{ and } d \neq 0.$$

The real numbers also satisfy the following axioms, called the **order axioms**. It is assumed that among all real numbers there are certain ones, called the **positive real numbers**, that satisfy properties Ord1–Ord3.

Ord1. For any real numbers a and b, if a and b are positive, so are $a + b$ and ab.

Ord2. For every real number $a \neq 0$, either a is positive or $-a$ is positive but not both.

Ord3. The number 0 is not positive.

The symbols $<$, $>$, $\leq$, and $\geq$, and negative numbers are defined in terms of positive numbers.

Definition

Given real numbers a and b,

$a < b$ means $b + (-a)$ is positive. $b > a$ means $a < b$.
$a \leq b$ means $a < b$ or $a = b$. $b \geq a$ means $a \leq b$.
If $a < 0$, we say that a is **negative**. If $a \geq 0$, we say that a is **nonnegative**.

From the order axioms Ord1–Ord3 and the above definition, all the usual rules for calculating with inequalities can be derived. The most important are collected as theorems T17–T27 as follows. In all these theorems the symbols a, b, c, and d represent arbitrary real numbers.

T17. *Trichotomy Law* For arbitrary real numbers a and b, exactly one of the three relations $a < b$, $b < a$, or $a = b$ holds.

T18. *Transitive Law* If $a < b$ and $b < c$, then $a < c$.

T19. If $a < b$, then $a + c < b + c$.

T20. If $a < b$ and $c > 0$, then $ac < bc$.

T21. If $a \neq 0$, then $a^2 > 0$.

T22. $1 > 0$.

T23. If $a < b$ and $c < 0$, then $ac > bc$.

T24. If $a < b$, then $-a > -b$. In particular, if $a < 0$, then $-a > 0$.

T25. If $ab > 0$, then both a and b are positive or both are negative.

T26. If $a < c$ and $b < d$, then $a + b < c + d$.

T27. If $0 < a < c$ and $0 < b < d$, then $0 < ab < cd$.

One final axiom distinguishes the set of real numbers from the set of rational numbers. It is called the **least upper bound axiom**.

LUB. Any nonempty set S of real numbers that is bounded above has a least upper bound. That is, if B is the set of all real numbers x such that $x \geq s$ for every s in S and if B has at least one element, then B has a smallest element. This element is called the **least upper bound** of S.

The least upper bound axiom holds for the set of real numbers but not for the set of rational numbers. For example, the set of all rational numbers that are less than $\sqrt{2}$ has upper bounds but not a least upper bound within the set of rational numbers.

Quote any Properties you use from Epp

- Parity property: Theorem 4.5.2 used to stated that any integer is either even or odd
- Zero Product Property P184
- Additional results about even and odd integers p186-187
- Unique Factorisation of Integers Theorem (Fundamental Theorem of Arithmetic)
- Theorem 4.4.2 Divisors of 1 - See task 4
- Theorem 4.7.3 The sum of any rational number and any irrational number is irrational
- Eg Theorem 4.8.1 the square root of 2 is irrational

Properties of rational numbers

- If r and s are any two rational numbers then (r+s)/2 is rational.

Proof: Suppose r and s are any two distinct rational numbers. *[We must show that* $\frac{r+s}{2}$ *is rational.]*

By definition of rational, $r = \frac{a}{b}$ and $s = \frac{c}{d}$ for some integers a, b, c, and d with $b \neq 0$ and $d \neq 0$.

By substitution and the laws of algebra,

$$\frac{r+s}{2} = \frac{\frac{a}{b} + \frac{c}{d}}{2} = \frac{\frac{ad+bc}{bd}}{2} = \frac{ad+bc}{2bd}.$$

Now $ad + bc$ and $2bd$ are integers because a, b, c, and d are integers and products and sums of integers are integers. And $2bd \neq 0$ by the zero product property.

Hence $\frac{r+s}{2}$ is a quotient of integers with a nonzero denominator, and so $\frac{r+s}{2}$ is rational *[as was to be shown]*.

Example using properties of inequalities

- For all real numbers a and b if a<b then a < (a+b)/2 < b.

T18. *Transitive Law* If $a < b$ and $b < c$, then $a < c$.

T19. If $a < b$, then $a + c < b + c$.

T20. If $a < b$ and $c > 0$, then $ac < bc$.

T21. If $a \neq 0$, then $a^2 > 0$.

T22. $1 > 0$.

T23. If $a < b$ and $c < 0$, then $ac > bc$.

T24. If $a < b$, then $-a > -b$. In particular, if $a < 0$, then $-a > 0$.

T25. If $ab > 0$, then both a and b are positive or both are negative.

T26. If $a < c$ and $b < d$, then $a + b < c + d$.

T27. If $0 < a < c$ and $0 < b < d$, then $0 < ab < cd$.

Proof: Suppose a and b are any real numbers with $a < b$. By properties T19 and T20 in Appendix A, we may add b to both sides to obtain

$$(a + b) < 2b,$$

and we may divide both sides by 2 to obtain

$$(a + b)/2 < b.$$

Similarly, since $a < b$, we may add a to both sides, which gives

$$2a < (a + b),$$

and we may divide both sides by 2, which gives

$$a < \frac{a + b}{2}.$$

By combining the inequalities, we have

$$a < \frac{a + b}{2} < b.$$

Proof by Cases

- Prove that the fourth power of any integer has the form 8m or 8m+1 for some integer m.

Proof: Suppose n is any integer. By the quotient-remainder theorem with divisor equal to 2, $n = 2q$ or $n = 2q + 1$ for some integer q.

Case 1 ***($n = 2q$ for some integer q)***: In this case, by substitution,

$$n^4 = (2q)^4 = 16q^4 = 8(2q^4).$$

Let $m = 2q^4$. Then m is an integer because it is a product of integers. Hence $n^4 = 8m$ where m is an integer.

Case 2 ***($n = 2q + 1$ for some integer q)***: In this case, by substitution,

$$\begin{aligned}
n^4 &= (2q+1)^4 && \text{by substitution} \\
&= (2q+1)^2(2q+1)^2 \\
&= (4q^2+4q+1)(4q^2+4q+1) \\
&= 16q^4+16q^3+4q^2+16q^3+16q^2+4q+4q^2+4q+1 \\
&= 16q^4+32q^3+24q^2+8q+1 \\
&= 8(2q^4+4q^3+3q^2+q)+1 && \text{by algebra.}
\end{aligned}$$

Let $m = 2q^4 + 4q^3 + 3q^2 + q$. Then m is an integer because products and sums of integers are integers. Hence $n^4 = 8m + 1$ where m is an integer.

Conclusion: In both cases $n^4 = 8m$ or $n^4 = 8m + 1$ for some integer m.

Note: If Theorem 4.5.3 is used, it can be shown that for any integer n, $n^4 = 16m$ or $n^4 = 16m + 1$ for some integer m. See the solution to exercise 40 for a partial proof of this result.