INTRODUCTION

What is Math?

- Can't define Math since it is constantly generalizing and, through self-examination, changing in structure and foundations
- Math can be used to model internal thought and external nature
- Will survey historic high points
  Will discuss whether math and its axioms are dictated by *discovery* from physical world or *invention* by human mind.
- Math feeds on itself
  Math result often contribute to seemingly unrelated parts of math
  Mathematical triumphs in natural sciences (physics, astronomy, etc) have inspired more math
  Used to engineer the computer, which assists mathematical experiments
- themes recur in different contexts in math history
  -generalizing to infinity
  -construction vs existential arguments
- Math is a science - results judged by usefulness to other areas of math and to other sciences; not closed or perfect
  Math is unlike other sciences - knows no obsolescense, a proof is forever
  Math is also an art - judged by aesthetics which are subjective
- What do branches of math have in common? Objects and methods.
  Objects:
  - the most primative are natural numbers and points. They were taken for granted until end of 19th century when logical examination of arithmatic (Peano, Frege, Russell) and geometry (Hilbert)
  - often, math objects are inspired by physical objects
  - objects can be created: sets of objects, functions, correspondences ("transformations"), classes of functions, correspondences between functions ("operators"), classes of such correspondences, etc
  - often, objects need no definition, just what statements they satisfy
    eg Hilbert said there are 3 objects, points, lines, and planes, and gave their axioms. So can teach geometry to blind person or a computer
    eg Mach's temperature was undefined, just satisfies axiom of transitivity of thermal equilibrium (0th law of thermodynamics) and its converse

  Methods:
  - proof starts with axioms, follows logical rules to derive new statements
  - often chosen for their usefulness or beauty
- Metamathematics is the study of proof methods, their scope, and their limitations. It is itself a part of math, where objects are rules of mathematical logic

1. THE INFINITY OF PRIMES

Definition.

- *Natural numbers* are $\mathbb{N} = \{1, 2, 3, \dots\}$
- *Prime numbers* are natural numbers, excluding one, which are divisible by only one and themselves
  note: Primes are the building block; any positive integer is a product of primes

Claim. *Primes go on forever, ie there exist arbitrarily large primes; no largest prime.*

Proof. (Euclid)
By contradiction, suppose p is the largest prime
$p! + 1$ is not divisible by any prime up to p
Either there is a prime between p and $p!+1$ or $p!+1$ is prime
Contradiction □

Remark. new questions arise

Claim. *Can construct abitrarily long sequence of different integers, all of which are not prime*

Proof.
Choose n not prime
Construct sequence $n! + 2, n! + 3, \dots, n! + n, (n! + n)! + 2, \dots$
Note the first is divisible by 2, the second by 3, etc. □

Claim. *The number of primes $\pi(n)$ between 1 and n is asymptotocally $\frac{n}{\log(n)}$ i.e. $\lim_{n\to\infty} \frac{\pi(n)}{\frac{n}{\log(n)}} = 1$*

Proof. complicated
1896 Hadamard and Poussin used analytic functions
recently Erdos and Selberg used combinatorics □

Conjecture. *(Goldbach)*
every even integer is the sum of two primes

Remark.

- Every sufficiently great odd integer can be represented as a sum of 3 primes (Vinogradov)
- Generating Primes:
  1st degree polynomials $2x + 1$, $4x + 1$, and $4x+3$ each generate infinitely many primes for integer x
  More generally, every arithmetic progression $ak + b$, where $k = 1, 2, 3, \dots$ and a, b relatively prime (share no common factors except 1), generates infinitely many primes, and we know some things (see book) about the frequency of these primes
  Euler's formula $N = x^2 + x + 41$ generates primes for $x = 1, \dots, 39$
  Don't know whether there exists a polynomial in x of degree >1 that generates infinitely many primes for integer x
- Don't know whether there exist infinitely many twin primes eg (5,7), (29,31)
- Trend: Do properties of finite set of numbers generalize to infinite or total set?

2. IRRATIONALITY OF $\sqrt{2}$

Remark.
$\mathbb{N}$ is closed under addition
$\mathbb{Z}$ is closed under subtraction
$\mathbb{Q}$ is closed under division (except by 0)
$\mathbb{R}$ is closed under radicals (and more)
$\mathbb{C}$ is algebraically closed

Definition.

- *rational* ("fraction") number has decimal expansion which terminates or repeats
  note: difficult to check if repeating
- *irrational* otherwise
  two types:
  algebraic number is a root of an algebraic equations with rational coefficients (or equivalently integer coefs once denominators are cleared)
  transcendental numbers transend operations of ordinary arithmetic (eg π, e), first existence proof and construction by Liouville

Remark. the problem of deciding whether any given number is rational, algebraic, or transcendental is unsolved in general

Claim. $\sqrt{2} \notin \mathbb{Q}$

Proof. (Greeks)
By contradiction, suppose $\left(\frac{a}{b}\right)^2 = 2$ where $\frac{a}{b} \in \mathbb{Q}$ is in simplest form
Then $a^2 = 2b^2$
Then a is even and can write $a = 2a_1$
Then $4a_1^2 = 2b^2 \Rightarrow 2a_1^2 = b^2$
Then b is even
Contradiction □

Claim. *Consider $\frac{a}{b} \in \mathbb{Q} \cap (0, 1]$ in lowest form*
Let $\frac{a}{b}$ be covered by interval $[\frac{a}{b} - \frac{1}{4b^2}, \frac{a}{b} + \frac{1}{4b^2}]$
Then $\frac{\sqrt{2}}{2}$ remains uncovered $\forall \frac{a}{b}$.

Proof. Notice $\left|b^2 - 2a^2\right|$ is a positive integer, nonzero since $\sqrt{2}$ irrational. So

$$\begin{aligned}
\left|b^2 - 2a^2\right| &\geq 1 \\
\frac{\left|b^2 - 2a^2\right|}{2b^2} &\geq \frac{1}{2b^2} \\
\left|\frac{\sqrt{2}}{2} - \frac{a}{b}\right| \left(\frac{\sqrt{2}}{2} + \frac{a}{b}\right) &\geq \frac{1}{2b^2} \\
\left|\frac{\sqrt{2}}{2} - \frac{a}{b}\right| &\geq \frac{1}{2b^2} \left(\frac{1}{\frac{\sqrt{2}}{2} + \frac{a}{b}}\right) \\
&> \frac{1}{2b^2}\frac{1}{2} = \frac{1}{4b^2}
\end{aligned}$$

So distance $\left|\frac{\sqrt{2}}{2} - \frac{a}{b}\right|$ is greater than $\frac{1}{4b^2}$.
So $\frac{\sqrt{2}}{2}$ remains uncovered. □

Remark.

- can prove square root of any prime is irrational
- quadratic irrationalities (eg $\sqrt{2}$) can be constructed geometrically (with ruler and compass)
- It is impossible to geometrically construct (ruler, compass) $\sqrt[3]{2}$ (ie Delic problem of doubling the cube)
- Algebraic numbers can be enumerated wheras reals can't (Cantor) (proof in section 1.4)
- don't know whether Euler's constant $\lim_{n\to\infty} \log(n) - \sum_{k=1}^{n} \frac{1}{k} \approx .57$ is rational or not (probably not)

Definition. *continued fraction of any $x \in \mathbb{R}$ is*

$$x = a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \cfrac{1}{a_3 + \dots}}}$$

where $a_i \in \mathbb{Z}$

Remark.

- quadratic irrationalities $p + q\sqrt{r}$ where $p, q, r \in \mathbb{Q}$ eg $\sqrt{2}$
  $\Leftrightarrow$ sequence (a_i) is periodic and bounded with bound that depends on x
- don't know whether there is a single algebraic number of order > 2 (ie cubic or higher irrationality) for which (a_i) is bounded

3. APPROXIMATION BY RATIONAL NUMBERS

Example. $\pi \approx \frac{314}{100}$, $\sqrt{2} \approx \frac{14}{10}$

Remark.

- A great deal of work has been devoted to approximating irrational numbers by rationals.
- Any $x \in \mathbb{R}$ is the limit of a sequence of $\mathbb{Q}$
- Any $x \in \mathbb{R}$ is the limit of a *decimal expansion* series
- Any $x \in \mathbb{R}$ can be approximated arbitrarily well by $\frac{a}{b} \in \mathbb{Q}$ ie can make precision $\epsilon = \left|x - \frac{a}{b}\right|$ arbitrarily small. An economical approximation has b small.
- One method is choosing $\epsilon < \frac{c}{b^2}$ where c is a specific constant
  But quadratic irrationalities, eg golden ratio $\frac{\sqrt{5}-1}{2}$, difficult to approximate this way since c must be large
  Some transcendental numbers allow good approximation this way, eg Liouville transcendental numbers
- first a lemma about algebraic numbers

Lemma. *Let degree $n \geq 2$ polynomial $f(x) = a_0x^n + a_1x^{n-1} + \cdots + a_n$ with $a_i \in \mathbb{Z}$, irreducible (ie can't be factored into product of polynomials with integer coefs)*
If α is a root of $f(x)$
Then there is a positive constant γ that depends only on α and f s.t. $\forall p, q \in \mathbb{Z}$, one has $\left|\alpha - \frac{p}{q}\right| > \frac{\gamma}{q^n}$

Proof. (Liouville)
Let $\frac{p}{q} \in \mathbb{Q} \cap (\alpha - 1, \alpha + 1)$

$$\frac{1}{q^n} \leq \frac{\left|a_0p^n + a_1p^{n-1}q + \cdots\right|}{q^n} \quad \because \text{numerator} \in \mathbb{N}$$
$$= \left|f\left(\frac{p}{q}\right)\right| \quad \because f\left(\frac{p}{q}\right) \neq 0 \because \text{irreducable}$$
$$= \left|f(\alpha) - f\left(\frac{p}{q}\right)\right| \quad \because f(\alpha) = 0$$
$$= \left|\alpha - \frac{p}{q}\right| |f'(x)| \quad \because MVT$$
where $x \in (\alpha - \frac{p}{q}, \alpha + \frac{p}{q}) \subseteq (\alpha - 1, \alpha + 1)$
$$\leq M \left|\alpha - \frac{p}{q}\right|$$
where $M \geq |f'(x)|$ for $x \in (\alpha - 1, \alpha + 1)$

So $\left|\alpha - \frac{p}{q}\right| \geq \frac{1}{M}\frac{1}{q^n}$ □

Claim. *(construct Louiville's transcendental number)*
$\alpha = \frac{1}{10} + \frac{1}{10^{2!}} + \frac{1}{10^{3!}} + \cdots = 0.1100010\cdots$ *is transcendental.*

Proof.

$$0 < \alpha - \left(\frac{1}{10} + \frac{1}{10^{2!}} + \ldots + \frac{1}{10^{m!}}\right) < \frac{2}{10^{(m+1)!}}$$

Note $\exists$ sequence $(p_m) \subset \mathbb{Z}$ s.t.

$$0 < \alpha - \frac{p_m}{10^{m!}} < \frac{2}{10^{(m+1)!}}$$

Set $q_m = 10^{m!}$. Then $\exists$ sequence $\left(\frac{p_m}{qm}\right) \subset \mathbb{Q}$ s.t.

$$0 < \alpha - \frac{p_m}{q_m} < \frac{2}{q_m^{m+1}}$$

Assume by contradiction that α algebraic root of nth degree polynomial
Then $\left|\alpha - \frac{p_m}{q_m}\right| \geq \frac{\gamma}{q_m^n}$
Then $\frac{\gamma}{q_m^n} < \frac{2}{q_m^{m+1}}$
Contradiction for m large
$\therefore \alpha$ transcendental □

Remark. Dirichlet's pigeonhole principle

- if m objects are put in n holes, $m > n$, then at least one hole has ≥ 2 objects
- eg same number of hairs in NYC
  eg same initials in city of 21,000 people
- need pigeonhole principle for next proof

Theorem. *If α irrational*
Then there are infinitely many rational numbers $\frac{p}{q}$ in lowest form st $\left|\alpha - \frac{p}{q}\right| \leq \frac{1}{q^2}$

Proof. Partition $[0, 1]$ into $Q \in \mathbb{N}$ pigeonholes of size $\frac{1}{Q}$.
Let $Q + 1$ numbers $0, (\alpha), (2\alpha), \cdots, (Q\alpha)$, where parenteses mean fractional part eg $(5/3) = 2/3$, $(3) = 0$, $(\sqrt{5}) = \sqrt{5} - 2$
$Q + 1$ objects in Q pigeonholes means at least one pigeonhole has two objects or more.
Say $(q_1\alpha)$ and $(q_2\alpha)$, $q_1, q_2 \in \mathbb{N}$, $q_1 < q_2 \leq Q$, in same pigeonhole ie $|(q_2\alpha) - (q_1\alpha)| \leq \frac{1}{Q}$
Let $q = q_2 - q_1$
Then $|(q\alpha)| \leq \frac{1}{Q}$
So $\exists p \in \mathbb{N}$ st $|q\alpha - p| < \frac{1}{Q}$
So $\left|\alpha - \frac{p}{q}\right| < \frac{1}{Qq} \leq \frac{1}{q^2}$
By contradiction, assume there are finitely many $\frac{p_i}{q_i}$, $i = 1, 2, \cdots, r$, st $\left|\alpha - \frac{p_i}{q_i}\right| \leq \frac{1}{q_i^2}$
Can find Q big enough st $\left|\alpha - \frac{p_i}{q_i}\right| > \frac{1}{Q}$ $\forall i$
Repeat above to find $\frac{p}{q}$ st $\left|\alpha - \frac{p}{q}\right| < \frac{1}{Qq} \leq \frac{1}{q^2}$
But $\frac{p}{q} \neq \frac{p_i}{q_i}$ $\forall i$
Contradiction □

Remark. Using pigeonhole principle requires creativity and inventiveness, not immediatly recognizable by a computer.

4. TRANSCENDENTAL NUMBERS: CANTOR'S ARGUMENT

Remark.

- Georg Cantor precisely formulated the concept of infinity
- Trend: constructive vs existential arguments
  e.g. transcendental numbers - construcive argument in last section, existential argument in this section

Definition. *size* of a set depends on finding a one-to-one correspondence to a standardized set of that size
countable or *denumerable* set means it has one-to-one correspondence with $\mathbb{N}$, ie can be arranged in a sequence

Claim. *Exist transcendental numbers*

Proof. Cantor
the set of algebraic numbers is countable (see next 2 claims) which is smaller that the set of real numbers (see last claim) □

Claim. *Countable union of finite or countable sets is at most countable*

Claim. *the set of algebraic equations (with integer coefficients) is countable*

Proof. The set of algebraic equations of a given degree are countable since coefs are integers
Hence the set of algebraic equations of all degrees is countable □

Theorem. *$\mathbb{R}$ is uncountable*

Proof. (Cantor)
By contradiction, assume countable
Arrange all decimal expansions in a sequence where c's are digits

$$c_1.c_{11}c_{12}c_{13}\ldots$$
$$c_2.c_{21}c_{22}c_{23}\ldots$$
$$c_3.c_{31}c_{32}c_{33}\ldots$$
$$\vdots$$

Construct $d = d_0.d_1d_2d_3\ldots$ st $d_0 \neq c_1$, $d_1 \neq c_{21}, d_2 \neq c_{32}, \ldots$.
d different than all above decimal expansions
contradiction □

Remark. Controversially implies, since there is a countable number of ways to arrange a finite number of words, that some real numbers can't be defined in a finite number of words.
Poincare fought Cantorism.

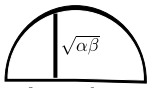
5. MORE PROOFS OF IMPOSSIBILITY

Remark. Impossibility proofs are powerful, since show our eternal limitations; other sciences dont have such finality
Will give examples.

- given cube with side a, it is impossible to construct (with straight edge and compass) a cube of side b and double volume $b^3 = 2a^3$ ie can't construct the $\sqrt[3]{2}$ of $b = a\sqrt[3]{2}$. (Delic problem of doubling the cube, from the time of Plato)
  note: similar problems are trisecting an angle and squaring a circle
- impossible to construct (with straight edge alone) the center of a given circle
- examples of geometric arrangement from combinatorial analysis

Definition. A number α is *constructable* means can construct a length α segment with a straight edge and compass
can extend to negative numbers by allowing directed segments

Claim. *The set of of constructable numbers is (i) rational numbers, and (2) given α, β constructable, then so are $\alpha \pm \beta, \alpha\beta, \frac{\alpha}{\beta}, \sqrt{\alpha\beta}$*



Remark. want to show $\sqrt[3]{2} \notin$ {construcable numbers}, but first a weaker statement

Lemma. *$\sqrt[3]{2}$ cannot be written as $\frac{a+b\sqrt{c}}{d+e\sqrt{f}}$ where $a, b, c, d, e, f \in \mathbb{Q}$ and $\sqrt{c}, \sqrt{f}$ rationally independent radicals (ie cant cant relate by rational operations $+, -, \times, /$ ie can't write $\sqrt{f}$ as $\frac{\alpha+\beta\sqrt{c}}{\gamma+\delta\sqrt{c}}$ with rationals $\alpha, \beta, \gamma, \delta$, otherwise could eliminate $\sqrt{f}$ above)*

Proof. by contradiction, suppose $\sqrt[3]{2} = \frac{a+b\sqrt{c}}{d+e\sqrt{f}}$
multiply by conjugate of denominator
$\sqrt[3]{2} = A + B\sqrt{c} + C\sqrt{f} + D\sqrt{cf}$ where $A, B, C, D \in \mathbb{Q}$ eg $A = \frac{ad}{d^2-e^2f}$ and $\sqrt{cf}$ irrational since rationally indep
rewrite
$\sqrt[3]{2} = M + N\sqrt{f}$ where $M = A + B\sqrt{c}$, $N = C + D\sqrt{c}$
cube, noting $(M \pm N\sqrt{f})^3 = M^3 + 3MN^2f \pm (3M^2N + N^3f)\sqrt{f}$
$2 = (M^3 + 3N^2Mf) + (3M^2N + N^3f)\sqrt{f}$
note: $3M^3N + N^3f = 0$ otherwise can solve for $\sqrt{f}$ in terms of $\sqrt{c}$
So eqn $x^3 - 2 = 0$ has roots $M \pm N\sqrt{f}$, with third root $-2M$ since sum of roots is zero.

So $(-2M)^3 = 2 \Rightarrow (A + B\sqrt{c})^3 = -\frac{1}{4}$
which similarly has roots $A \pm B\sqrt{c}$ and $-2A$.
So $A^3 = \frac{1}{32} \Rightarrow A = \frac{\sqrt[3]{2}}{4}$
But $\sqrt[3]{2}$ irrational by similar argument as $\sqrt{2}$
Contradiction □

Remark. notice every constructable number can be written $\frac{a_0+a_1\sqrt{P_1}+\cdots+a_k\sqrt{P_k}}{b_0+b_1\sqrt{Q_1}+\cdots+b_l\sqrt{Q_l}}$ where $a_i, b_i \in \mathbb{Q}$ and $\sqrt{P_i}, \sqrt{Q_i}$ are linear combinations (with rational coefs) of radicals

Definition.

- radical $\sqrt{P}$ has *degree* n means P is a linear combination (with rational coefs) of radicals of degree $n-1$ and lower, and if at least one of the radicals is of degree $n-1$.
  eg $\sqrt{\frac{1}{2} + 2\sqrt{\frac{1}{3} + \sqrt{2 + \frac{1}{5}\sqrt{2+\sqrt{5}}}}}$ has degree 5
  eg $\frac{1}{2}$ has degree 0
- the *degree* of a constructable number is the maximum degree of $\sqrt{P_i}, \sqrt{Q_i}$
- the *order* of a constructable number is the number of rationally independent radicals of maximum degree n
- eg $\frac{a+b\sqrt{c}}{d+e\sqrt{f}}$ above has degree 1, order 2

Claim. *$\sqrt[3]{2}$ is not constructable (Delic problem of doubling the cube)*

Proof. Assume $\sqrt[3]{2}$ constructable of degree n and order r
Use process above (?) to prove it must be of order $r-1$
Repeat until order is zero, so degree is less than n
Can eventually prove $\sqrt[3]{2}$ rational
Contradiction □

Remark. Next consider construction of center of circle by straightedge

Definition.

- *construction by straightedge* means a finite succession of steps each requiring either (i) line drawn through arbitrary two points or (ii) finding point of intersection between two lines or a line and a circle
- Let transformation ("projection") T map plane P_1 into plane P_2 st (1) points on a line in P_1 get mapped to points on a line in P_2 and (2) circumference of circle is transformed to circumference of a circle in P_2
  ie lines to lines, circles to cirlces, may distort distances, and may transform ellipses into hyperbolas
- Euclidean geometry involves straightedge and compass
  Projective geometry uses straightedge alone
  Construction by straightedge must be projection invariant

Theorem. *(Steiner)*
Cannot find the center of a given circle by straightedge alone

Proof. (Hilbert)
Can find map to $T : P_1 \to P_2$ s.t. center of circle in P_1 is not center of corresponding circle in P_2 (see book for picture)
So relationship between circle and its center is not projection invariant □

Remark. next examples from combinatorial analysis

Claim. *Consider a square subdivided into 64 equal squares with lower left and upper right corners removed*
Cannot cover the remaining 62 squares with 31 "dominoes"

Proof. Color in chessboard
both omitted corners have same color
but dominoes need one of each color
(this is obvious only once colored) □

Claim. *"squaring the square"*
can decompose square into finite number of squares of different sizes

Proof. see picture in book □

Claim. *Cannot decompose cube similarly*

Proof. By contradiction, assume can decompose.
Smallest cube on a face must not be on an edge, since otherwise bigger cubes on each side fence off inner side
Smallest cube on inside of the face is fenced off above
So must decompose into further smaller cubes
Cannot end in finite number of steps □

1.5A SPERNER'S LEMMA

Remark.

- Combinatorial topology classifies geometric objects according to properties independent of stretching and smooth distortions. eg circle and square in same class since can find continuous point-to-point correspondence
- will first prove Sperner's lemma (one of the most powerful tools in combinatorial topology), then use it to prove Brouwer's fixed point theorem (applicable to many parts of math)

Lemma. *Sperner's*
Let triangle with vertices labeled $0, 1, 2$
Divide triangle into finite number of smaller triangles simplicially (ie edges align with edges)
Label vertices arbitrarily except require only 0's and 1's on edge 01, 1's and 2's on edge 12, and 0's and 2's on edge 02
There must exist one smaller triangle whose vertices are marked with 0,1,2
In fact, there is an odd number of such triangles restated: impossibile to not find a 012 triangle

Proof. First the simple case of interval.
Decompose interval with endpoints 0,1.
Label each interior point 0 or 1
Let α be a subinterval
Let $v(\alpha) = \begin{cases} 0 & \text{if both endpoints 1} \\ 1 & \text{if endpoints 0,1} \\ 2 & \text{if both endpoints 0} \end{cases}$
Let m = number of subintervals with $v(\alpha) = 1$
$m - \sum v(\alpha) =$ even $\because m$ corresponds to $v(\alpha) = 1$
$\sum v(\alpha)$ odd $\because$ each internal 0 counted twice, plus endpoint 0.
$\therefore m$ odd.
note: induction was used
Now for the triangle case.
Let α be a subsimplex
Let $v(\alpha) = \begin{cases} 0 & \text{if no sides 01} \\ 1 & \text{if one side 01} \\ 2 & \text{if two sides 01} \end{cases}$
Let m = number of subsimplices with $v(\alpha) = 1$
$m - \sum v(\alpha) =$ even $\because m$ corresponds to $v(\alpha) = 1$
$\sum v(\alpha) =$ odd = (even since internal 01 edges counted twice) + (odd since external 01 edge using interval case).
$\therefore m$ odd.
note: can generalize to higher dimensional simplices □

Theorem. *Brouwer fixed point thm*
If an (eg 1d) interval is mapped continuously to itself by the mapping T ie $T(p), T(q)$ can be made arbitrarily close by making p, q sufficiently close
Then exists at least one point p_0 st $T(p_0) = p_0$

Proof. Subdivide interval with points
Label points 0 if transformation didn't move them left
Label points 1 if transformation didn't move them right
Sperner's lemma $\Rightarrow$ exists subinterval with endpoints 0,1
Can make subdivision arbitrarily fine
In the limit, must be at least one point whose distance from both ends has not decreased
note: can generalize to higher dimensional □

6. THE ART AND SCIENCE OF COUNTING

Remark. Want to know many different ways can one break a dollar ie how many solutions $(l_1, l_2, l_3, l_4, l_5) \in \mathbb{Z}^5$ to $100 = l_1 + 5l_2 + 10l_3 + 25l_4 + 50l_5$?
Enumerating is too cumbersome.

Example. Find number of integer solutions to $100 = l_1 + 2l_2$
Rephrase problem. Find A_{100} from

$$\begin{aligned} & A_0 + A_1 x + A_2 x^2 + \dots \\ &= (1 + x + x^2 + \cdots)(1 + x^2 + x^4 + \cdots) \\ &= \frac{1}{(1-x)(1-x^2)} \quad \because \text{geometric series} \\ &= \frac{1}{(1-x)^2(1+x)} \\ &= \frac{a}{(1-x)^2} + \frac{b}{1-x} + \frac{c}{1+x} \end{aligned}$$

solve partial fractions
$1 = a(1+x) + b(1-x)(1+x) + c(1-x)^2$
$-b + c = 0, a - 2c = 0, a + b + c = 1$
$\Rightarrow a = \frac{1}{2}, b = \frac{1}{4}, c = \frac{1}{4}$
Continue with above

$$\begin{aligned} &= \frac{1}{2}\frac{1}{(1-x)^2} + \frac{1}{4}\frac{1}{1-x} + \frac{1}{4}\frac{1}{1+x} \\ &= \frac{1}{2}(1 + 2x + 3x^2 + \dots) + \frac{1}{4}(1 + x + x^2 + \dots) \\ &\quad + \frac{1}{4}(1 - x + x^2 - \dots) \end{aligned}$$

The coefficient of x^{100} is $\frac{1}{2}101 + \frac{1}{4}1 + \frac{1}{4}1 = 51$
Or could have noted l_1 even since $100 - 2l_2$ even, and there are 51 even integers in $[0, 100]$, so 51

Example. Find number of solutions to $100 = l_1 + 5l_2 + 10l_3 + 25l_4 + 50l_5$
Rephrase problem: Find A_{100} from

$$\begin{aligned} & A_0 + A_1 x + A_2 x^2 + \dots = \\ & (1 + x + x^2 + \cdots)(1 + x^5 + x^{10} + \cdots) \\ & \quad (1 + x^{10} + x^{20} + \cdots)(1 + x^{25} + x^{50} + \cdots) \\ & \quad (1 + x^{50} + x^{100} + \cdots) \\ &= \frac{1}{(1-x)(1-x^5)(1-x^{10})(1-x^{25})(1-x^{50})} \end{aligned}$$

Rephrase problem again: Find $A_{100} = B_{100} + B_{95} + \cdots + B_5 + B_0$ where B_m is the number of ways to solve $m = k_1 5 + k_2 10 + k_3 25 + k_4 50 \Rightarrow \frac{m}{5} = k_1 + k_2 2 + k_3 5 + k_4 10$

Multiply power series

$$(1+x+x^2+\cdots)(1+x^2+x^4+\cdots)$$
$$(1+x^5+x^{10}+\cdots)(1+x^{10}+x^{20}+\cdots)$$
$$= \frac{1}{(1-x)(1-x^2)}\frac{1}{(1-x^5)(1-x^{10})}$$
$$= (1+x+2x^2+2x^3+3x^4+3x^5+\ldots)$$
$$(1+x^5+2x^{10}+2x^{15}+3x^{20}+3x^{25}+\ldots)$$

Multiply series, add coeficients of $x^0, x^1, x^2 \ldots, x^{20}$, get $A_{100} = 292$

Example. Can encounter complex numbers
Find number of solutions to $n = l_1 + 2l_2 + 3l_3$

$$(1+x+x^2+\cdots)(1+x^2+x^4+\cdots)$$
$$(1+x^3+x^6+\cdots)$$
$$= \frac{1}{(1-x)(1-x^2)(1-x^3)}$$
$$= \frac{1}{(1-x)^3(1+x)(1+x+x^2)}$$
$$= \frac{1}{(1-x)^3(1+x)(\alpha x+1)(\overline{\alpha}x+1)}$$
$$\text{where } \alpha = \frac{1}{2}+i\frac{\sqrt{2}}{2}$$
$$= \frac{a}{(1-x)^3}+\frac{b}{(1-x)^2}+\frac{c}{1-x}+\frac{d}{1+x}$$
$$+\frac{e}{1+\alpha x}+\frac{f}{1+\overline{\alpha}x}$$
$$= \frac{a}{2}(1\cdot 2+2\cdot 3x+3\cdot 4x^2+\ldots)$$
$$+b(1+2x+3x^2+\ldots)+c(1+x+x^2+\ldots)$$
$$+d(1-x+x^2-\ldots)+e(1-\alpha x+\alpha^2x^2-\ldots)$$
$$+f(1-\overline{\alpha}x+\overline{\alpha}^2x^2-\ldots)$$

Can find coefficients a, b, c, d, f, add coefs of x^n to find
$A_n = \frac{a}{2}(n+1)(n+2)+b(n+1)+c+d(-1)^n+e(-1)^n\alpha^n+f(-1)^n\overline{\alpha}^n$

Remark. While considering counting problems with integers, the complex numbers were used. Next a digression on complex numbers.

7. DIGRESSION ON THE NUMBER SYSTEM AND ON FUNCTIONS

Remark.

- Kac and Ulam build up from natural numbers to rationals by closing under operations $+, -, \times, /$ and preserving associativity, commutativity, and distributivity
- Further extension needed to include numbers like $\sqrt{2}$
- rigorous theory of reals developed in latter 19th century by Cantor and Dedekind, but reals were used freely before then
- Irrationals have nonterminating nonrepeating decimal $a_0.a_1a_2a_3$, which can be written as
  - infinite series: $a_0+\frac{a_1}{10}+\frac{a_2}{10^2}+\frac{a_3}{10^3}+\cdots$
  - nested intervals: $[a_0+\frac{a_1}{10}+\frac{a_2}{10^2}+\cdots+\frac{a_n}{10^n}, a_0+\frac{a_1}{10}+\frac{a_2}{10^2}+\cdots+\frac{a_n}{10^n}+\frac{1}{10^n}]$
- Real numbers have Dedekind property:
  If $\mathbb{R} = A \cup B$, $A, B \neq \emptyset$, $a \in A < b \in B$
  Then either A has a max or B has a min
  ie reals form a continuum
- complex numbers are algebraically closed, but strange since do not represent measurements, but very useful so finally accepted into Math in early 19th century
- now with complex numbers can study complex functions

Theorem. *Fundamental thm of Algebra*
$\exists z_1, z_2, \cdots, z_n \in \mathbb{C}$ *s.t.* $a_nz^n+a_{n-1}z^{n-1}+\cdots+a_0 = a_n(z-z_0)(z-z_1)\cdots(z-z_n)$, *where* $a_i \in \mathbb{C}$
note: this was needed for partial fractions in counting problems

Remark. This stimulated study in functions of a complex variable

- eg $f(z) = \frac{1+z}{1-z}$ maps interior of unit circle into half-plane right of y axis
  eg $f(z) = i\frac{1+z}{1-z}$ maps interior of unit circle into half-plane above x axis
- derivative of $f(z)$, if exists for in neigborhood of z, is $\lim_{\Delta z\to 0}\frac{f(z+\Delta z)-f(z)}{\Delta z}$.
  note: doesn't matter how Δz approaches zero
- Such a severe restriction allows
  $\exists$ first derivative $\Rightarrow \exists$ all orders of derivative
- differentiable implies f representable as power series around some radius of convergence
- *entire function* means power series converges everywhere
  analytic function means differentiable in some region
- the theory of analytic functions forms one of the most beautiful chapters of math
  has found applications in almost every corner of math

8. THE ART AND SCIENCE OF COUNTING (CONTINUED)

Remark. recall using power series (generating function) to find number of solutions to $n = l_1+2l_2+3l_3$

Remark. Famous problem in additive number theory: *partitio numerarum* by Euler
How many ways $p(n)$ can you split $n = l_1 + 2l_2 + 3l_3 + \cdots$ into smaller numbers $l_1, l_2, \cdots$
Rewrite as generating function
$1+p(1)x+p(2)x^2+\cdots = \frac{1}{(1-x)}\frac{1}{(1-x^2)}\cdots$

- Can't apply partial fractions since rhs is infinite product
- Hardy and Ramanujan (1917) found the asymptotic formula $p(n) \sim \frac{1}{4n\sqrt{3}}e^{\pi\sqrt{\frac{2n}{3}}}$
- Radenmacher (1934) found complicated formula for $p(n)$ extending Hardy and Ramanujan's method using complex analysis

Remark. related problem: representing integers as sums of squares

- Lagrange (Late 18th century) proved every positive integer is the sum of four squares (four square thm, one of the great math achievements)
- Jacobi determined the number of different ways a number can be written as a sum of squares
  note: $2^2+1^2 = (-2)^2+1^2 = 1^2+(-2)^2$ are different by sign and order
  Let $r(m)$ = number of ways to write m

$$1+r(1)x+r(2)x^2+\ldots$$
$$= (\ldots+x^{(-2)^2}+x^{(-1)^2}+1+x^{1^2}+x^{2^2}+\ldots)^4$$
$$= (1+2x^{1^2}+2x^{2^2}+\ldots)^4$$
$$\overset{Jacobi's}{=} 1+8\frac{x}{1-x}+8\frac{2x^2}{1-x^2}+8\frac{3x^3}{1-x^3}$$
$$+8\frac{5x^5}{1-x^5}+\ldots$$

where coefficients,powers are naturals except multiples of 4
note: $\frac{x^l}{1-x^l} = x^l+x^{2l}+x^{3l}+\cdots$
So $r(m) = 8$ times sum of divisors of m that are not multiplied by 4
Note $r(m) \geq 8\ \forall m > 0$
Note Lagrange merely states $r(m) \geq 1$

- Jacobi's identity (and many other identities) came from a class of analytic functions called elliptic functions (originally used to find circumference of ellipse and motion of pendulum) and complex integration
  Direct proofs are available, but complex analysis provides economy of thought and deeper understanding

9. ELEMENTARY PROBABILITY AND INDEPENDENCE

Remark. Historically, people counted odds of games of chance like picking cards and rolling dice But in 20th century, theory generalized, with many applications to other parts of math and to sciences

Definition. Laplaces Definition
Let Ω=finite set of all possible outcomes, and all outcomes equiprobable.
Probability of $A \subset \Omega$ is ratio of number $v(A)$ of elements in A to the total number $v(\Omega)$; Prob.$A = \frac{v(A)}{v(\Omega)}$
ie ratio of favorable outcomes to total outcomes
ie a counting problem
limitations: finite set and "equiprobable"

Example. Given equiprobable coin, find Prob.{exactly m heads in n tosses}
Ω = all words of length n with letters H and T
$v(\Omega) = 2^n$ [since bst #leaves double at each depth]
Let $C(n, m)$ = number of words of length n containing H exactly m times [more generally, # of size m subsets of a size n set]
Then $C(n+1, m)$ =[$C(n, m)$ corresponding to T at end]+[$C(n, m-1)$ corresponding to H at end],
Induction was used.
$C(n+1, m) = C(n, m) + C(n, m-1)$.
From above recursion formula,
$C(n, m) = \frac{n!}{(n-m)!m!}$
Prob.{exactly m heads in n tosses}=$\frac{C(n,m)}{2^n}$

Remark. $C(n, m)$ is also used in binomial formula $(x+y)^n = C(n,0)x^n + C(n,1)x^{n-1}y + \cdots + C(n,n)y^n$

Example. remove equiprobability
Given coin with Prob.$\{H\} = \frac{1}{6}$, Prob.$\{T\} = \frac{5}{6}$
Convert problem to equiprobable 6-sided die, ie
Prob.{exactly m 2's in n tosses}
$C(n, m)$= number of ways to arrange $H(=2)$ and $T(=1,3,4,5,6)$
5^{n-m}= number of ways to arrange 1,3,4,5,6 in remaining $n-m$ spots
Prob.{exactly m 2's in n tosses}=$\frac{C(n,m)5^{n-m}}{6^n} = \frac{n!}{(n-m)!m!}\left(\frac{1}{6}\right)^m\left(\frac{5}{6}\right)^{n-m}$
More generally, if Prob.$\{H\} = p$, $\{T\} = q$, then Prob.{exactly m heads in n tosses}=$\frac{n!}{(n-m)!m!}p^mq^{n-m}$

Remark. Mathematicians were leary of Laplace's definition due to using "equiprobability" in definition, awkwardness of irrational probability corresponding to infinite sided die, and Bertrand's paradox.

Example. Bertrand's paradox - inability to handle infinite outcomes
find Prob.{random chord of circle is longer than side of inscribed equilateral triangle}
Prob is $\frac{1}{3}$ since successes are chords from one vertex and other vertex on opposite arc
Prob is $\frac{1}{4}$ since successes are chords through concentric circle of half original's radius
This is not a logical paradox, just a warning that "random" is ambiguous

Remark. The following theorem is a triumph to Laplace's theory. Proved by Laplace.

Theorem. *DeMoivre Laplace*
Let coin, p,q=weights, n=# flips, m=# heads
$\lim_{n\to\infty}$ *Prob.*$\{np+\alpha\sqrt{2pqn} \le m \le np+\beta\sqrt{2pqn}\} = \int_\alpha^\beta \frac{1}{\sqrt{2\pi}} e^{-\frac{x^2}{2}}\,\mathrm{d}x$ *where* α,β *any consts, ie area under normal curve*
A more general thm uses normal curve $\frac{1}{\sigma\sqrt{2\pi}} e^{-\frac{(x-m)^2}{2\sigma^2}}$ *as integrand, where m=mean,* σ*=standard deviation*

Remark.

- Application motivated mathematicians were satisfied by Laplace's thm since it was already encountered in emperical contexts
- To the purist, Laplace's theorem was considered a small contribution to knowledge of binomial coefficients, and credit should go to Stirling's asymptotic formula $n! \sim \left(\frac{n}{e}\right)^n \sqrt{2\pi n}$ which was used in proof
- Purist needed more rigorous definition of probability

Definition. Purist definition of probability
Given set Ω of all possible outcomes
Set number Prob.A for all (or some) $A \subseteq \Omega$,
Can compute probabilities of more complicated events using:
(Axiom of additivity): if $E_1, E_2 \subseteq \Omega$, $E_1 \cap E_2 = \emptyset$, then Prob.$\{E_1$ or E_2 or $\cdots\}$ = Prob.E_1+ Prob.$E_2 + \cdots$
(Axiom of complimentarity): Prob.not E = Prob.Ω− Prob.E where by convention, Prob.$\Omega = 1$
note: this is compatible with Laplace's definition

Example. quantum mechanics and electron going through slits

Remark. Selecting "elementary" events and assigning probability to them may require emperical considerations. Sometimes there is correlation between events.

Example. Claude Shannon did experiments on English texts, finding emperically Prob.$\{e\}$ = 0.1309, Prob.$\{t\}$ = 0.0902, Prob.$\{a\}$ = 0.0681. Consider 27 sided die (one side "space"), loaded by the above probabilities, can make output more realistic by adding correlation that h follows t, etc.

Definition. independence
Events E (eg heads of coin) and F (eg 2 on die) are *independant* means Prob.$\{E$ and $F\}$ = Prob.E Prob.F
"rule of multiplication of probabilities"

Remark. heuristically using frequencies:
Suppose n trials, events E, F occurred $n(E), n(F)$ times, and they simultaneously occurred $n(E$ and $F)$ times.
$\frac{n(E \text{ and } F)}{n} = \frac{n(E \text{ and } F)}{n(F)} \frac{n(F)}{n}$
E, F indep $\Rightarrow \lim_{n\to\text{big}} \frac{n(E \text{ and } F)}{n(F)} = \frac{n(E)}{n}$

Example. Redo Laplace's loaded coin example using independence
Let independent tosses of coin loaded Prob.H=p, Prob.T=$q = 1-p$
Prob.$\{$any n letter word with exactly m H's$\}$ = $pp\cdots pqq\cdots q = p^m q^{n-m}$
There are $C(n,m)$ such words.
Prob.$\{m$ H's out of n independent tosses$\}$ = $C(n,m)p^m q^{n-m}$

Remark. normal curve $\frac{1}{\sqrt{2\pi}} e^{-\frac{x^2}{2}}$ is primarily a result of independence of trials, not Stirling's formula

Example. Poisson scheme
Consider differently loaded coins, Prob.$\{H\} = p_k$, Prob.$\{T\} = 1 - p_k$ for kth coin.
No simple formula for Prob.$\{$exactly m H's in n tosses$\}$
But can generalize DeMoivre Laplace Thm

Theorem. *Generalized DeMoivre Laplace*
Let n independent tosses in Poisson scheme, m = number of heads
$\lim_{n\to\infty}$ *Prob.*$\{p_1 + p_2 + \cdots + p_n + \alpha\sqrt{p_1q_1 + \cdots + p_nq_n} \le m \le p_1 + p_2 + \cdots + p_n + \beta\sqrt{p_1q_1 + \cdots + p_nq_n}\} = \frac{1}{\sqrt{2\pi}} \int_\alpha^\beta e^{-\frac{x^2}{2}}\,\mathrm{d}x$ *provided* $p_1q_1 + \cdots$ *diverges*

Remark. Is normal curve universal for indep trials? 1920s: the Laplace DeMoivre thms were subsumed into the central limit theorem

Theorem. *(Erdos-Kac)*
The number of prime divisors is distributed according to the normal law
intuitively: for random $n \in \mathbb{N}$*, the the number of distinct prime factors of n has approximately the normal distribution with mean and variance* $\log\log n$

Proof. Consider prime numbers $P_1 = 2, P_2 = 3, P_3 = 5, \cdots$
Let $E \subseteq \mathbb{Z}$
Let $K_n(E)$ =number of elements of E among first n positive integers
Let $D(E) = \lim_{n\to\infty} \frac{K_n(E)}{n}$, if exists, be the density of E
Let E_i =set of integers divisble by ith prime P_i
Then $D(E_i) = \frac{1}{P_i}$
Consider $E_1 \cap E_2 \cap \cdots \cap E_r$=set of integers divisible by the first r primes
$D(E_1 \cap E_2 \cap \cdots \cap E_r) = \frac{1}{P_1P_2\cdots P_r} = D(E_1)D(E_2)\cdots D(E_r)$
note: like law of multiplication of probabilities
let $v(n)$ =number of prime divisors of $n \in \mathbb{N}$ eg $v(2\cdot 3^2\cdot 5) = 3, v(13) = 1$
Then $D(\{n : \log\log n + \alpha\sqrt{\log\log n} < v(n) < \log\log n + \beta\sqrt{\log\log n}\}) = \frac{1}{\sqrt{2\pi}} \int_\alpha^\beta e^{-\frac{x^2}{2}}\,\mathrm{d}x$
□

Remark. So probability is actually useful

10. MEASURE

Remark.

- Many algebraic or analytic areas have origins in geometry. Measuring is one such idea.
- Euclid's axioms for areas of polygons and volumes of polyhedra:
  (1) if polygons (polyhedra) A and B are *congruent*, they have same area (volume)
  (2) If a polygon (polyhedron) A is decomposable into a finite number of disjoint polygons (polyhedra), then the area (volume) of A is the sum of the pieces
  additionally, with a unit area and unit volume, can assign numerical values for areas, volumes
- Newton's calculus provided lengths, areas, volumes of "tame" sets
- There was a need to generalize measure
- Borel and Lebesgue developed Lebesgue measure for more general sets by extending Euclid's *finitely additive measure* to more general sets by adjusting axiom to *completely additive measures* ie allow infinitely many A's.

Definition. *Measure* is a non-negative number $m(A)$ assiged to a set A with properties:
(1) If $A_1, A_2, \ldots$ are disjoint, measurable sets, then $A_1 \cup A_2 \cup \cdots$ is measurable and $m(A_1) + m(A_2) + \cdots = m(A_1 \cup A_2 \cup \cdots)$
(2) If A and B measurable and $A \subseteq B$, then $B - A$ is measureable and $m(B - A) = m(B) - m(A)$
(3) A unit set E has measure 1
(4) If two measurable sets are congruent, then their measures are equal

Remark. Limitation of Lebesgue measure

- Lebesgue measure is not complete – there are immeasureable sets, eg those constructed with axiom of choice
- Axiom of choice (Zarmelo) – given collection of mutually disjoint sets, can construct set by choosing an element from each set

Example. Vitali set - first discovered nonmeasurable set
Let circle E with $m(E) = 1$
Split whole circle into mutually disjoint equivalence classes st each class is points that differ by a rational value
eg $\sqrt{2}, (\sqrt{2} - 1)$ in same class since $\left|\sqrt{2} - (\sqrt{2} - 1)\right| = 1 \in \mathbb{Q}$
Construct Vitali set Z which is one picked element from each of these classes (used axiom of choice)
Rotate Z by angles $\alpha_1, \alpha_2, \cdots$ which are rationals in $[0, 1)$ times 2π (thus countable) to obtain countable collection of sets $Z_1, Z_2, \cdots$, each mutually disjoint, each congruent (since coincide after rotation)
Axiom of additivity implies $m(E) = 1 = \sum m(Z_i)$
What is $m(Z_i)$? Can't be zero since $\sum_{\mathbb{N}} m(Z_i) = 0$ and can't be finite since $\sum_{\mathbb{N}} m(Z_i) = \infty$.
So Vitali set not measurable.

Example. Banach Tarski paradox
Given two spheres S_1, S_2 of different radius, can divide each into finite size n dijoint sets, $S_1 = A_1 + A_2 + \cdots + A_n$, $S_2 = B_1 + B_2 + \cdots + B_n$ s.t. each A_i congruent to B_i.
So can't define measure.
This paradox impossible in the plane; Banach proved that can find a finitely additive measure for all subsets of the plane st congruent sets have equal measure

Remark.

- Lebesgue measure is a powerful tool:
  - in trig series, some convergence/divergence theorems are not valid on some uncountable set, want to show this set is negligible, ie measure zero
  - in probability, want statements valid "almost surely" ie with probability 1
  - in dynamical systems, properties are valid for "almost all" initial conditions
- With benefits of generalized measure, must live with things like unmeasurable sets and Banach-Tarski decompositions

11. PROBABILITY REVISITED

Remark.

- Probabilities are measures and probability theory is part of measure theory
- this made probability theory respectable by supplying rigorous framework
- this also increased the scope of probability theory: countable additivity axiom allows infinite sequence of trials
- Notation: replace Prob. with $p()$ so looks similar to $m()$

Example. Persons A and B alternate flipping a fair coin, starting with A, independent trials
What is probability that A tosses the first head?
For fair coin, $p(H$ on first toss$)=\frac{1}{2}$, $p(T$'s until H

on 3rd toss)=$\frac{1}{2^3}$
So p(A tosses first H)= $\frac{1}{2} + \frac{1}{2^3} + \frac{1}{2^5} + \cdots = \frac{2}{3}$

Example. Flip fair coin many times, independent trials, what is the frequency of H's?
Intuition: $\frac{1}{2}$

Theorem. *weak law of large numbers*
Let $\epsilon > 0$
$\lim_{n\to\infty} p(\left|\frac{\text{number } H\text{'s in } n \text{ trials}}{n} - \frac{1}{2}\right| > \epsilon) = 0$

Proof. (Bernoulli) Used Laplace's framework and DeMoivre Laplace theorem.
Intuition: $\forall\epsilon$ can find large but finite n ... □

Theorem. *strong law of large numbers (Borel)*
$p(\lim_{n\to\infty} \frac{\text{number } H\text{'s in first } n \text{ events}}{n} = \frac{1}{2}) = 1$

Proof. Let Ω = all infinite length two letter words
Let $A \subseteq \Omega$ = all words st $\lim_{n\to\infty} \frac{\text{number } H\text{'s in first } n \text{ letters}}{n} = \frac{1}{2}$
Is A measurable?
Construct measure on an event: p(all words with given first m letters) = $\frac{1}{2^m}$
Map each word$\in A$ to $[0,1]$ by using its binary representation
Then event mapped to $(0,1)$ is an interval of length $\frac{1}{2^m}$, and there are $2^m - 1$ such intervals
The $p() = 1$ in thm can be restated m(set of binary expansions in $(0,1)$ with asymptotically equal number of 0's and 1's)=1
which is true □

Remark.

- Strong law of large numbers was first venture beyond Laplace
- Strong law of large numbers has been generalized and extended, gave rise to new problems and stimulated new methods.
- We constructed a countably additive measure on an infinite dimensional space (since need infinite coordinates 0,1 to describe each point)
  instead of coordinates 1,0, could use elements from more general set and develop more general theory about independent trials in terms of "product measures"(?) in such infinitely dimensional spaces
- Wiener measure on a set of curves was motivated by Brownian motion.
  This measure has found applications in unrelated parts of math eg electrostatic potential

12. GROUPS AND TRANSFORMATIONS

Remark. One of the most important, fruitful, and all-embracing topics is groups.

Definition.

- *transformation* of a set S into itself is a way of assigning to each $p \in S$ a unique element $f(p) \in S$
- The *image* of p under f is $f(p)$
- *identity transformation* means $f(p) = p\ \forall p$
- *one-to-one* means $p \neq q \Rightarrow f(p) \neq f(q)$
- if 1-1, then can define *inverse transformation* f^{-1} as $f(p) = q \Rightarrow f^{-1}(q) = p$
- given transformations f and g of S into itself, *composition* is gf, where f is applied first
  note: composition is associative $(fg)h = f(gh)$
- *group* is a collection of transformations G st
  (1) $f, g \in G \Rightarrow fg, gf \in G$
  (2) identity transformation is in G
  (3) $f \in G \Rightarrow f^{-1} \in G$
- *permutation* is a one-to-one transformation of a finite set S into itself
  ie change order of elements
  note: $n!$ permutations for n elements set

Example. permutations of a set of 3 elements
$f_0 = \begin{pmatrix}1&2&3\\1&2&3\end{pmatrix}$ $f_1 = \begin{pmatrix}1&2&3\\1&3&2\end{pmatrix}$
$f_2 = \begin{pmatrix}1&2&3\\2&1&3\end{pmatrix}$ $f_3 = \begin{pmatrix}1&2&3\\2&3&1\end{pmatrix}$
$f_4 = \begin{pmatrix}1&2&3\\3&1&2\end{pmatrix}$ $f_5 = \begin{pmatrix}1&2&3\\3&2&1\end{pmatrix}$
Multiplication table:

	f_0	f_1	f_2	f_3	f_4	f_5
f_0	f_0	f_1	f_2	f_3	f_4	f_5
f_1	f_1	f_0	f_4	f_5	f_2	f_3
f_2	f_2	f_3	f_0	f_1	f_5	f_4
f_3	f_3	f_2	f_5	f_4	f_0	f_1
f_4	f_4	f_5	f_1	f_0	f_3	f_2
f_5	f_5	f_4	f_3	f_2	f_1	f_0

note: $f_1^2 = f_2^2 = f_5^2 = f_0$ ie their own inverse, $f_3f_4 = f_0, f_1f_4 = f_2, f_4f_1 = f_5$, etc

Remark. Abel and Galois first introduced permutation groups to study solvability of algebraic eqns in terms of radicals.
The following account exemplifies the spirit of algebra.

Claim. *cubic eqn* $x^3 + ax^2 + bx + c = 0$ *has three roots,* x_1, x_2, x_3 *and can express coefs in terms of roots*

$$a = -(x_1 + x_2 + x_3)$$
$$b = x_1x_2 + x_2x_3 + x_1x_3$$
$$c = -x_1x_2x_3$$

Definition. function $F(x_1, x_2, x_3)$ is *symmetric* means it is unchanged wrt permuted arguments
eg coefs of cubic eqn in terms of roots (above)
eg $\Delta = (x_1 - x_2)(x_2 - x_3)(x_2 - x_3)$ is symmetric under subgroup f_0, f_3, f_4, and changes sign under f_1, f_2, f_5
note: permutations that leave a given function unchanged form a subgroup

Theorem. *Suppose polynomial function* Ψ *is invariant under* f_0, f_3, f_4
then must be of the form $\Psi = A(x_1, x_2, x_3) + B(x_1, x_2, x_3)\Delta$ *where* A, B *are symmetric polynomial functions*

Proof.
By assumption,
$\Psi(x_1, x_2, x_3) = \Psi(x_2, x_3, x_1) = \Psi(x_3, x_1, x_2)$
Transposing x_1, x_2,
$\Psi(x_2, x_1, x_3) = \Psi(x_1, x_3, x_2) = \Psi(x_3, x_2, x_1)$
So in general, $\Psi(x_1, x_2, x_3) \neq \Psi(x_2, x_1, x_3)$, otherwise thm trivial with $B = 0$
So $\Psi(x_1, x_2, x_3) - \Psi(x_2, x_1, x_3) = 0$ only when $x_1 = x_2$
So $\Psi(x_1, x_2, x_3) - \Psi(x_2, x_1, x_3)$ divisible by $x_2 - x_1$
Similarly, divisible by $x_1 - x_3$, $x_2 - x_3$
Thus divisible by Δ
$\therefore \Psi(x_1, x_2, x_3) - \Psi(x_2, x_1, x_3) = \Psi(x_1, x_2, x_3) - \Psi(x_1, x_3, x_2) = \Psi(x_1, x_2, x_3) - \Psi(x_3, x_2, x_1) = B(x_1, x_2, x_3)\Delta$
Thus B unchanged by f_1, f_2, f_5, and also $f_3 = f_2f_1, f_4 = f_1f_2$
$\Rightarrow B$ symmetric
similarly $\Psi - B\Delta$ symmetric
$\Rightarrow A$ symmetric □

Remark. above shows that much can be learned about the structure of certain objects by merely studying their behavior under the action of certain groups

Example. physics
groups of transformations leave invariant the forces that hold atoms or molecules together; can derive behavior of their spectra

Theorem. *a cubic is solvable in terms of coefs* a, b, c *and radicals*

Proof. let $\omega = -\frac{1}{2} + \frac{\sqrt{3}}{2}$
then $\omega^2 = -\frac{1}{2} - \frac{\sqrt{3}}{2}$, $\omega^3 = 1$
Consider $\Psi = (x_1 + \omega x_2 + \omega^2 x_3)^3$
note: Ψ symetric wrt f_0, f_3, f_4, eg apply f_3

$$(x_2 + \omega x_3 + \omega^2 x_1)^3 = \omega^3(x_2 + \omega x_3 + \omega^2 x_1)^3$$
$$= (\omega x_2 + \omega^2 x_3 + x_1)^3$$

Thus $(x_1 + \omega x_2 + \omega^2 x_3)^3 = A(x_1, x_2, x_3) + B(x_1, x_2, x_3)\Delta$
Can show A, B, Δ^2 are expressable as polynomials of a, b, c
So $x_1+\omega x_2+\omega^2 x_3 = \sqrt[3]{A(x_1, x_2, x_3) + B(x_1, x_2, x_3)\Delta}$
Apply f_3 or f_4?
$x_1+\omega^2 x_2+\omega x_3 = \sqrt[3]{\overline{A}(x_1, x_2, x_3) + \overline{B}(x_1, x_2, x_3)\Delta}$
where $\overline{A}, \overline{B}$ again polynomials in the coefficients
Can solve for x_1, x_2, x_3 in terms of a, b, c, using roots. □

Remark.

- Cardono (16th century) discovered formulas for x_1, x_2, x_3, but didnt use groups of permutations
  Galois and Abel used groups of permutations, discovered underlying mechanism behind these algebraic equations, and suggested extensions to quartics.
- Every permutation of n objects can be expressed as a product of transpositions (switch two objects, leave others alone)
- Permutations can be decomposed into either an even or an odd number of permutations.
- All even permutations form the *alternating subgroup* eg f_0, f_3, f_4
- Generalize above: a function that is unchanged by the alternating subgroup is in the form $A + B\Delta$ where A, B symmetric and $\Delta = (x_1-x_2)(x_1-x_3)\cdots(x_{n-1}-x_n)$ ie product of all differences.

Claim. *For* $n = 4$ *can find a quadratic function (like* $x_1 + \omega x_2 + \omega^2 x_3$ *above) whose power is unchanged by the alternating group*

Proof. use only the properties of the group of permutations of more than four objects □

Remark. No such function for $n \geq 5$

Example. versatility of permutations and groups: Tribal mariage laws

Definition. *abstract group* G is a set of elements $f_0, f_1, f_2, \cdots$ and a binary operation $\circ : G \times G \to G$ st
(1) associative $(f_i \circ f_j) \circ f_k = f_i \circ (f_j \circ f_k)$
(2) identity $f_0 \circ f_i = f_i \circ f_0 = f_i$
(3) inverse $f_i \circ f_i^{-1} = f_i^{-1} \circ f_i = f_0$

Example. permutation of group by left multiplying each element by some element f_i is isomorphic to the original

Remark. When a mathematical framework is used repeatedly in different contexts, it becomes a theory and is studied for its own sake

Remark. Now some number theory, physics, and geometry examples

Theorem. *(Wilson)*
If p *prime*
Then $(p-1)! + 1$ *is divisible by* p

Proof. define group *residues modulo p* with elements $1, 2, \cdots, p-1$ and $i \circ j$ = remainder of dividing $i \cdot j$ by p
note: this group is commutative
Consider $(1 \circ 2 \circ \cdots \circ p-1)^2 = 1 \circ 2 \circ \cdots \circ p-1 \circ 1 \circ 2 \circ \cdots \circ p-1$
pair off inverses on rhs to make equal to 1
So lhs has property $k^2 = 1$
So $k^2 - 1 = (k+1)(k-1)$ is divisible by p
On lhs, pair off inverses, left with $p-1$
So $1 \circ 2 \circ \cdots \circ (p-1) = p-1$ □

Theorem. *Fermat (1640)*
In a finite group of n elements, every element composed with itself n times equals the identity.

Proof. apply to the group of residues $\forall k$ st $1 \le k \le p-1$, $k^{p-1} = 1$
$k^{p-1} - 1$ is divisible by p □

Example. physics

- transformations preserving distances and angles (rigid motion) form a group
- Lorentz group of special relativity: transformations of space-time leaving invariant "light-cones" $(x-x_0)^2 + (y-y_0)^2 + (z-z_0)^2 = c^2(t-t_0)^2$

Example. geometry
Klien:

- Euclidean geometry is the study of invariants of the group that consists of translations, rotations, reflections
- Projective geometry is the study of invariants of projective transformations

Remark. algebraic properties of the group of transformations that leave certain mathematical structure invariant reflect many properties of the structure itself

12a. HOMOLOGY GROUPS

Definition.

- *simplex* is a tetrahedron in 3d, triangle in 2d, line in 1d, and point in 0d
- *complex* is a collection of simplices st any two simplices are either disjoint or share a whole lower dimensional simplex
- *oriented* simplex means assigned a *definite* ordering
  two orderings are *equivalent* means they are the same after an even number of transpositions ie even permutations
  eg triangle has two orientations, since f_0, f_3, f_4 are even
  eg line has two orientations
  eg point has one orientation, but will consider two for convenience
- *induced orientation*
  -eg tetrahedron oriented 1,2,3,4, face opposite even (eg 2) is oriented negatively (eg (1 4 3)=-(1 3 4))
  -eg segment oriented (1 2) ((2 1)) induces orientation (1) (-(1)) on point
  eg two simplices with a simplex in common may induce on it either the same or opposite orientation
- *k-dimensional chain* is $a_1\sigma_1^{(k)} + a_2\sigma_2^{(k)} + \cdots + a_m\sigma_m^{(k)}$ where $a_i \in \mathbb{Z}$ and $\sigma_i^{(k)}$ is a k-dimensional simplex in complex K
- addition of two chains is adding like coefs
  note: this forms a group with chains and addition
- $\Delta(\sigma_i^{(k)}) = \sigma_{i1}^{(k-1)} + \sigma_{i2}^{(k-1)} + \cdots + \sigma_{ir}^{(k-1)}$ is the boundary of oriented k-dimensional simplex $\sigma_i^{(k)}$

Example. tetrahedron $\sigma^{(k)}$
$\Delta(\sigma^{(k)}) = -(123) - (134) + (124) + (234)$

Definition. *boundary of chain* is $\Delta(a_1\sigma_1^{(k)} + \cdots + a_m\sigma_m^{(k)}) = a_1\Delta(\sigma_1^{(k)}) + \cdots + a_m\Delta(\sigma_m^{(k)})$
note: a $k-1$ simplex in both $\sigma_i^{(k)}$ and $\sigma_j^{(k)}$ has coefficient $a_i + a_j$ if orientations agree and $a_i - a_j$ if orientations disagree

Example. Boundary of boundary of (1 2 3 4)

$$\begin{aligned}&\Delta(\Delta(1234))\\ &= -\Delta(123) - \Delta(134) + \Delta(124) + \Delta(234)\\ &= -(23) + (13) - (12) - (34) + (14) - (13)\\ &\quad + (24) - (14) + (12) + (34) - (24) + (23)\\ &= 0\end{aligned}$$

Theorem. *boundary of a boundary is zero, ie* $\Delta\Delta = 0$

Definition.

- B_r= collection of all chains that are boundaries of $(r+1)$-dimensional chains
- Z_r= collection of all chains whose boundaries are zero, ie *cycles*
  note: both are groups by addition and $B_r \subseteq Z_r$ since $\Delta(B_r) = 0$
- two chains are *equivalent* means their difference is in B_r.
  So Z_r breaks into disjoint chains of equivalent cycles
- $H^{(r)} = Z_r/B_r$= *factor* group= rth *homology* group of a complex
  note: identity is B_r

Example. 2d complex of faces of tetrahedron
$B_2 = 0$ trivially
$H^2 = Z_2$ = set of all chains $a(123) + b(124) + c(134) + d(234)$ for which $\Delta(a(123) + b(124) + c(134) + d(234)) = 0$
$= a(12) - a(12) + a(12) + b(24) - b(14) + b(12)$
$+c(23) - c(14) + c(13) + d(34) - d(24) + d(23)$
$= (a+d)(23) + (-a+c)(13) + (a+b)(12) + (b-d)(24) + (-b-c)(14) + (c+d)(34)$
$\Rightarrow b = -a, c = a, d = -a$
So Z_2 = chains of the form $a(123) - a(124) + a(134) - a(234)$
So $H^{(2)} = Z_2$ are indistinguishable from group of integers wrt to addition

Example. $B_1 = Z_1$ = group of integers wrt addition
$H^{(1)} = Z_1/B_1 = 0$ trivial

Example. Complex of 3 faces of tetrahedron
$H^{(2)} = H^{(1)} = 0$

Example. any closed convex polyhedron with triangular faces
homology group identical to those of tetrahedron

Remark.

- In topology, two geometric configurations are *identical* means there is a homeomorphism (1-1 continuous correspondence) between them
- eg tetrahedron and sphere identical
- can speak of homology groups of a configuration by approximating it with complexes
- homeomorphic confugurations have the same homology groups of all orders

Remark. Simple closed curve and figure 8 curve
Not homeomorphic since removing intersection point of figure eight makes it disconnected
Homology theory agrees:

- approximate curves with complexes
  $H^{(1)}$ of simple closed curve is the group of integers with addition
  $H^{(1)}$ of figure eight is the group of ordered pairs with addition $(a_1, b_1) + (a_2, b_2) = (a_1 + a_2, b_1 + b_2)$
  These groups differ so not homeomorphic

Remark. Homeomorphic configuration ⇒ identical homology groups
converse not true for dimension >2
Deciding if given higher dimensional configurations are homeomorphic remains unsolved

Remark. trend: algebraization of math

13. VECTORS, MATRICES, AND GEOMETRY

Remark.

- trend: unification of different parts of math
- Analytic geometry made possible by Descartes' introduction of coordinates into geometry
  eg conic sections can be expressed algebraically
  eg equations in two variables can be expressed geometrically as curves
- will see how algebraic problem of solving simultaneous linear algebraic equations is interpretted geometrically

Definition.

- *vector* is a directed line segment from a fixed origin to a point P
- *operations on vectors*:
  (a) scalar multiplication αP scales vector by α
  (b) addition $P+Q$ uses parallelogram rule
- properties of the above operations:
  (a) $P + Q = Q + P$
  (b) $(P+Q) + R = P + (Q+R)$
  (c) $\exists!$ vector 0 st $P + 0 = P\ \forall P$
  (d) $\forall P\ \exists! P'$ st $P' + P = 0$
  (e) $\alpha(P+Q) = \alpha P + \alpha Q$
  (f) $(\alpha+\beta)P = \alpha P + \beta P$
  (g) $\alpha(\beta P) = (\alpha\beta)P$
  (h) $(1)P = P$
- *linear vector space* is a set of objects $P, Q, \cdots$ which satisfy above operations and axioms

Example. Linear vector spaces

- 3d vectors
- polynomials with real coefs
- real valued continuous functions defined on an interval
- chains defined in 12a

Remark.

- above axioms allow such different linear vector spaces
- will later impose additional axioms to enrich the structure

Definition.

- *linear independence* of vectors $P_1, P_2, \cdots, P_n$ means that the linear relationship $a_1P_1 + \cdots + a_nP_n = 0$ has only trivial solution $a_1 = \cdots = a_n = 0$
- *n-dimensional* linear vector space means $\exists$ n linearly independent vectors $P_1, \cdots, P_n$ and no collection of $n+1$ linearly independent vectors
- *basis ("coordinate system")* of an n-dimensional vector space is an n-tuple of linearly independent vectors $(P_1, \cdots, P_n)$
- *coordinates* of any vector P in basis $P_1, \cdots, P_n$ is the unique n-tuple $(\alpha_1, \cdots, \alpha_n)$ st $P = \alpha_1P_1 + \cdots + \alpha_nP_n$
- *linear transformation* T of a linear vector space into itself is a mapping $P \mapsto T(P)$ st

(a) $T(P+Q) = T(P) + T(Q)$
(b) $T(\alpha P) = \alpha T(P)$

- *matrix* is a unique square array of scalars associated to each linear transformation in some basis $(P_1, \cdots, P_n)$
  $T = \begin{pmatrix} t_{11} & \cdots & t_{1n} \\ \vdots & \ddots & \\ t_{n1} & & t_{nn} \end{pmatrix}$
- *composition* of linear transformations T then S in fixed basis is linear transformation ST
  note: usally $\neq TS$
  Note: composition is mx multiplication
- *identity* transformation, regardless of base, is identity mx I st $TI = IT = T$
- *inverse* of a linear transformation T is linear transformation T^{-1} st $TT^{-1} = T^{-1}T = I$
  $\exists! \Leftrightarrow (T(P) = 0 \Rightarrow P = 0$ vector). Otherwise annihilates nonzero vector
- group: two invertable linear transformations and composition

Example. 2d real linear vector space
Set a base
Vectors are 2-tuples of reals
Linear transormations are 2×2 mxs of reals $T = \begin{pmatrix} t_{11} & t_{12} \\ t_{21} & t_{22} \end{pmatrix}$
T has inverse means only trivial solution to
$t_{11}\alpha_1 + t_{12}\alpha_2 = 0$
$t_{21}\alpha_1 + t_{22}\alpha_2 = 0$
ie $\det T = |T| = t_{11}t_{22} - t_{12}t_{21} \neq 0$
$T^{-1} = \frac{1}{\det T}\begin{pmatrix} t_{22} & -t_{12} \\ -t_{21} & t_{11} \end{pmatrix}$
check $TT^{-1} = T^{-1}T = I$

Example. n dimensional real linear vector space
Want to solve system $T\alpha = \beta$ for α_i's
Solution: $\alpha_k = \frac{\det T_k}{\det T}$
where $T_k = T$ with kth column swapped with β
and $\det A = \sum_\pi \operatorname{sign} \pi a_{1\pi(1)}a_{2\pi(2)}\cdots a_{n\pi(n)}$
where $\pi = \begin{pmatrix} 1 & 2 & \cdots & n \\ \pi(1) & \pi(2) & \cdots & \pi(n) \end{pmatrix}$ permutation
and $\operatorname{sign}(\pi) = \begin{cases} 1 & \text{even permutation} \\ -1 & \text{odd permutation} \end{cases}$

Remark. geometric point of view of determinant

- Consider bases $P_1, \cdots, P_n$ and $Q_1, \cdots, Q_n$
  Transform from one to another with matrices C and D st
  $Q_i = \sum d_{ij}P_i$
  $P_i = \sum c_{ij}Q_i$
  note: $CD = I$ ie $C = D^{-1}$ and $D = C^{-1}$
  note: D^{-1} exists $\Leftrightarrow \det D \neq 0$
- linear transformation T in basis $(P_1, \cdots, P_n)$ is the same geometric transformation as $C^{-1}TC = DTD^{-1}$ in basis $(Q_1, \cdots, Q_n)$
- determinant is invariant to basis
  ie $\det T = \det C^{-1}TC$
- want to define determinant of linear transformation A without reference to its basis
  Solve $AE_i = \lambda_i E_i$ for evals $\lambda_1, \cdots, \lambda_n$ and evecs $E_1, \cdots, E_n$
  In basis $E_1, \cdots, E_n$, transformation is diagonal mx of evals
  $\det T = \lambda_1 \cdot \lambda_2 \cdots \lambda_n$
- so we have another algebraic definition of *determinant*
- Next will add more structure to our linear vector space

Definition. recall definitions from plane geometry with basis from x, y axes

- *distance* between points $P = (x_1, y_1)$ and $Q = (x_2, y_2)$ is defined by pythagorean theorem $d(P,Q) = \sqrt{(x_2 - x_1)^2 + (y_2 - y_1)^2}$
- *angle* θ between OP and OQ is defined by the law of cosines $\cos\theta = \frac{x_1x_2 + y_1y_2}{\sqrt{x_1^2+y_1^2}\sqrt{x_2^2+y_2^2}}$
  can generalize to angle between AP and AQ
- *rigid motion* is a transformation that preserves distance and angle
  $x' = a_{11}x + a_{12}y + x_0$
  $y' = a_{21}x + a_{22}y + y_0$
  $A = \begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix}$
  st $A^T = A^{-1}$ and $\det A = 1$ (if -1, then reverses orientation, not rigid)
  so distance and angle are invariant to basis

Remark. want to match algebraic congruence to Euclid's axioms for congruence

- we also introduce axioms of continuity and order to resolve Greek's problems with irrational numbers and betweenness
- once all axioms checked, we have a complete algebraic (or analytic) model of plane Euclidean geometry
- can generalize 2d plane using linear vector space
- postulate existence of scalar product $\omega(P,Q)$ of vectors P, Q st
  (a) $w(P,Q)$ is a symmetric bilinear function of P, Q
  (b) $w(P,P) \geq 0$ and $(w(P,P) = 0 \Leftrightarrow P = 0)$

check that 2d vector space with scalar product $w(P,Q)$ can be made into a model of the Euclidean plane:

- Take linearly independent vectors P_1, P_2
- Can find linear combinations E_1, E_2 of P_2, P_2 st $w(E_1, E_1) = w(E_2, E_2) = 1$ and $w(E_1, E_2) = 0$
  note: proof uses P_1, P_2 linearly independent and Schwarz $\leq$: $w(P_1,P_1)w(P_2,P_2) - \omega^2(P_1,P_2) > 0$
- So E_1, E_2 also form a basis and
  $P = x_1E_1 + y_1E_2$
  $Q = x_2E_1 + y_2E_2$
  $\Rightarrow w(P,Q) = x_1x_2 + y_1y_2$
- define $d^2(P,Q) = w(P-Q, P-Q)$ and $\cos\theta = \frac{w(P,Q)}{\sqrt{w(P,P)}\sqrt{w(Q,Q)}}$.
  These are the same as formulas in plane analytic geometry

Definition.

- *n-dimensinal Euclidean space* is n-dimensional real vector space with scalar product $w(P,Q)$ that has properties (a),(b) above
- *rigid motions* are translations and linear transformations ("rotations") that preserve the scalar product $(w(TP,QP) = w(P,Q))$ and orientation $(\det T = 1)$

Remark.

- Euclidean geometry (in any dimension) can be studied as the properties left invariant by the "Euclidean group" of translations and rotations
- Affine geometry can be studied as the properties left invariant by the "affine group" of translations and all nonsingular linear transformations
  note: can't distinguish circle and ellipse, can distinguish hyperbola and ellipse
- Projective geometry is even more primative, studies properties left invariant by projections
  note: can't even distinguish hyperbola and ellipse

Definition. n-dimensional Euclidean geometry

- *orthonormal basis* is $E_1, \cdots, E_n$ st $w(E_i, E_i) = 1$ and $w(E_i, E_j) = 0$, ie mutually orthogonal unit vectors
- *unit cube* based on $E_1, \cdots, E_n$ is the set of vectors $P = x_1E_1 + \cdots + x_nE_n$ st $0 < x_i < 1$
  note: volume=1
- *rectangular parallelpiped* based on $E_1, \cdots, E_n$ is the set of vectors $P = x_1E_1 + \cdots + x_nE_n$ st $0 < x_i < a_i$
  note: volume=$a_1a_2\cdots a_n$

Theorem. *distortion*
measure of linearly transformed set Ω *is* $m(T(\Omega)) = |\det T|\, m(\Omega)$
eg $m(T($*unit cube*$)) = m($*skew parallelpiped*$) = |\det T|$

Proof. difficult □

Remark. geometry gives intuition to algebraic formula for determinant

Theorem. $\det(TS) = \det T \det S$

Proof. need distortion theorem □

14. SPECIAL THEORY OF RELATIVITY

Used Lorentz group

15. TRANSFORMATIONS, FLOWS, AND ERGODICITY

Remark. Ergodic properties of $T : E \to E$, 1-1 and onto, where E is Euclidean space, is the behavior of (finite or infinite) sequence of points $T^{-n}(p), T^{-n+1}(p), \cdots, p, T(p), T^2(p), \cdots$

Example. hydrodynamics
Let E be unit cube or sphere in 3-space
Let E be filled with incompressible fluid
Let steady flow (independent of time)
Let p be any position in space
$T(p)$ =position after 1 time unit
$T^n(p)$ =position after n time units
note: incompressible means $m(A) = m(T(A))$ = volume of $A \subseteq E$

Example. mechanics
Let dynamic system with n material points in 3-space
Given all initial positions and momenta vectors
Can represent full system by one point in $6n$-dimensional *phase* space (3 position, 3 momentum coordinates for each of n points)
Mathematically prescribe forces between the points, equations of dynamics
As time goes on, each representative point will move through phase space
So we have a flow in phase space
Louiville:

- conservative (constant: energy and a certain function of position and momentum) dynamic system preserves volume (incompressible) in phase space
- So representative points move on surface E of constant energy
- Incompressibility preserves a specific measure on the energy surface E, $m(A) = m(T(A))$ for $A \subseteq E$
  ie T preserves m on E

Ergodic hypothesis:

- Originally by Boltzmann, later weakened to:

- A trajectory of the representative point will pass arbitrarily close to all the points of energy surface E
- further, sequence $p, T(p), \cdots$ is uniformly dense ($\lim_{n\to\infty} \frac{1}{n}\sum_{i=1}^{n} x_A(T^i(p)) = \frac{m(A)}{m(E)}$) where x_A is characteristic function of set A

Example. T not 1-1, try change variables
$x \mapsto 4x(1-x)$ on $(0,1)$
Iterate to get higher order polynomials
The sequence of iterated images is dense in the interval
Set $x = \sin^2\theta$ then $f(x) = 4\sin^2\theta(1-\sin^2\theta) = \sin^2 2\theta$
ie $\sin^2\theta \mapsto \sin^2 2\theta$

Remark.

- Difficult to determine properties of iterates of general algebraic transformations
- Can extend ergodic theorem to not 1-1 T, but "measure preserving" means measure of the "inverse image" of a set A has the same measure as A
- can apply ergodic thearoem to continued fractions

Example. Represent $x \in (0,1) \cap \mathbb{R}$ as a continued fraction.

- $x = a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \cfrac{1}{a_3 + \cdots}}}$
  where $\frac{1}{x} = a_1 + x_1$, $\frac{1}{x_1} = a_2 + x_2$, $\cdots$
- using transformation iteration:
  $Tx = \frac{1}{x} - \left[\frac{1}{x}\right]$ where $\left[\frac{1}{x}\right]$ = integer closest to but not exceeding $\frac{1}{x}$
  $a_1(x) = \left[\frac{1}{x}\right]$
  $a_2(x) = a_1(Tx)$
  $a_3(x) = a_2(T^2x)$
  $\vdots$

Example.

- Let inverse image of interval (a,b), $0 < a < b < 1$, be the infinite union of intervals $(\frac{1}{1+b}, \frac{1}{1+a})$, $(\frac{1}{2+b}, \frac{1}{2+a})$, $(\frac{1}{3+b}, \frac{1}{3+a})$, $\cdots$
- Let measure of interval (α,β) be $\frac{1}{\log 2}\log\frac{1+\beta}{1+\alpha} = \frac{1}{\log 2}\int_\alpha^\beta \frac{dx}{1+x}$
- this measure is preserved by T
- Apply ergodic theorem:
  For almost every x, the frequency with which integer k appears in the sequence $a_1, a_2, \cdots$ is $\frac{1}{\log 2}\log\left(\frac{(k+1)^2}{k(k+2)}\right)$
  note: used $E = (0,1)$, $A = (1+\frac{1}{k+1}, 1+\frac{1}{k})$
  ie $a_1(x) = k$

16. MORE ON ITERATION AND COMPOSITION OF TRANSFORMATIONS

Example.

- Let T be *positive matrix* (all positive elements; sends positive "octant" of n-dim Euclidean space into itself)
- Let x^*= multiple of vector x which lies on the surface of unit sphere
- Define $S(x^*) = (T(x))^*$
- note: surface of unit sphere in positive octant is topologically equivalent to $n-1$ dimensional cube
  eg curve in 2d, disc in 3d, etc
- Brouwer's fixed point theorem implies S must posses a fixed point, $S(x_0^*) = x_0^*$
- So $T(x_0) = \lambda x_0$ where $\lambda = eval$, $x_0 = evec$
- Frobenius: start with any vector x, iterate $T(x), T^2(x), \cdots$, will converge in direction to unique evec

Definition. *Markov chains* generalize independent trials.
Let system randomly transition between states $s_1, s_2, \cdots$
$p_{ij} = \text{Prob}\{s_i \to s_j \text{ in one time step}\}$
Matrix $P = (p_{ij})$
$p_{ii_1}p_{i_1i_2}\cdots p_{i_{n-1}j} = \text{Prob}\{s_i \to s_{i_1} \to s_{i_2} \to \cdots \to s_{n-1} \to s_j \text{ in } n \text{ steps}\}$
note: used product since independence

Example. Two boxes I and II
Somehow distribute $2R$ numbered balls
every time step, choose number from 1 to $2R$ randomly (each has probability $\frac{1}{2R}$, independent), and move chosen ball to other box
state i of system is number of balls in box I
possible transitions are $i \to i-1$ and $i \to i+1$ (except when $i = 1$ or $2R$)
So $p_{ij} = 0$ if $j \neq 1+i, 1-i$, else $p_{i,i-1} = \frac{i}{2R}$, $p_{i,i+1} = 1 - \frac{i}{2R}$
will say more in ch 3

Example. $\text{Prob}\{s_i \to s_j \text{ in } n \text{ steps}\}$= (i,j)th entry of P^n
which equals sum over all $p_{ii_1}p_{i_1i_2}\cdots p_{i_{n-1}j}$

Remark. Consider group generated by transformations S, T and composition

Theorem. *If T, S continuous 1-1 transformations of interval into itself*
Then compositions form a dense class of transformations of interval into itself
note: can represent any transformation arbitrarily closely

Theorem. *If E= n-dimensional sphere*
Can find four homeomorphisms (1-1, continuous, onto itself) of E whose compositions allow arbitrary approximation of any homeomorphism

Remark.

- open question: is every general homeomorphism of n dim space approximable by differentiable homeomorphisms?
- drop 1-1 requirement, then yes, since Weierstrass: every continuous function on a bounded region can be approximated by polynomial functions

Theorem. *Consider E= Euclidean space*
Consider gorup of homeomorphisms obtained by composing homeomorphisms $x' = f(x,y)$, $y' = y$ or $x' = x$, $y' = g(x,y)$
Can approximate arbitrary homeomorphism given by $x' = \Phi(x,y)$, $y' = \Psi(x,y)$
open problem in 3 dim or more

Theorem. *Kalmagorov, Arnold*
Continuous functions of many variables can be represented exactly as composition of a finite number of functions of two variables
eg $f(x_1,x_2,x_3,x_4) = h_1(h_2(h_3(x,y), h_4(x,y)), h_5(x,y))$

17. PROVING THE OBVIOUS

Remark. sometimes things are intuitively obvious but difficult to prove, or even false

Theorem. *Jordan curve*
a simple closed curve divivides the Euclidean plane into 2 regions, inside and outside

Theorem. *sphere cannot be combed*

Proof. difficult
note: there will always be a whirlpool point where vectors cannot be tangent to the sphere
note: uses Brouwer's fixed point thm generalized to sphere □

Theorem. *Let 2 real valued continuous functions f_1, f_2 on sphere (eg temperature and pressure)*
Exists at least one point p_0 and its antipode p_0^* st $f_1(p_0) = f_1(p_0^*)$ and $f_2(p_0) = f_2(p_0^*)$

Theorem. *"ham sandwich"*
Given 3 solids (eg bread, ham, butter) in space,
Exists a plane that splits each solid into equal volumes

Proof. Take sphere, line through sphere, parallel plane through first solid
Let two real valued functions of volume the plane splits other two solids into
Use above thm about antipodal points

□