NOTES FOR GRE MATH SUB

ZHANG, RUI

ABSTRACT. This note covers most of the key points tested in GRE Math Sub. Notice that the test gets harder and harder and the contents in the test can go beyond this note.

Contents

Date: 2018-10-27.

Institute of Computing Technology, Chinese Academy of Sciences, z14120902@gmail.com.

1. Pre-Calculus

- A function assigns each element in the domain to one element in the range
- Injective(one-to-one): no two elements are mapped to the same element ($|\textsf{domain}| \leq |\textsf{range}|$)
- Surjective(onto): every element in the range is the image of some element in the domain ($|\textsf{domain}| \geq |\textsf{range}|$)
- Bijective: one-to-one and onto. We can define inverse function
- Factor theorem: $x = r$ is a root of polynomial $p(x) = 0 \Leftrightarrow x - k$ is a factor of $p(x)$
- Fundamental theorem of algebra: every polynomial if degree $n \geq 1$ has at least one root(real or complex)
- Every polynomial of degree n has exactly n roots: $a_n \prod (x - r_i)^{m_i}$
- For polynomial equation: $\sum r_i = -\frac{a_{n-1}}{a_n}$, $\prod r_i = (-1)^n \frac{a_0}{a_n}$
- Rational root theorem: if $p(x) = \sum_{i=0}^n a_i x^i, a_i \in \mathbb{Q}$ has rational roots. They must be $\frac{\text{a factor of } a_0}{\text{a factor of } a_n}$
- Conjugate radical root theorem: if $\sum_{i=0}^n a_i x^i = 0, a_i \in \mathbb{Q}$ has a root $a + b\sqrt{c}$, $\sqrt{c}$ is irrational, it must also has $a - b\sqrt{c}$
- Complex conjugate root theorem: if $\sum_{i=0}^n a_i x^i = 0, a_i \in \mathbb{R}$ has a root $a + bi$, it must also has $a - bi$
- $\log(ab) = \log a + \log b$, $\log(\frac{a}{b}) = \log a - \log b$
- $\csc x = \frac{1}{\sin x}$, $\sec x = \frac{1}{\cos x}$, $\cot x = \frac{1}{\tan x}$
- $\sinh x = \frac{e^x - e^{-x}}{2}$, $\cosh x = \frac{e^x + e^{-x}}{2}$
- $1 + \tan^2 x = \sec^2 x$, $1 + \cot^2 x = \csc^2 x$
- $\sin(a \pm b) = \sin a \cos b \pm \cos a \sin b$
- $\cos(a \pm b) = \cos a \cos b \mp \sin a \sin b$
- $\tan(a \pm b) = \frac{\tan a \pm \tan y}{1 \mp \tan x \tan y}$
- $\sin 2x = 2 \sin x \cos x$, $\cos 2x = \cos^2 x - \sin^2 x = 1 - 2\sin^2 x = 2\cos^2 x - 1$, $\tan 2x = \frac{2 \tan x}{1 - \tan^2 x}$
- $\tan \frac{x}{2} = \frac{\sin x}{1 + \cos x} = \frac{1 - \cos x}{\sin x} = \csc x - \cot x$
- $\forall x : f(x) \geq B$: bounded below by B
- parabola: $y^2 = 4px$: the same distance to $(p, 0)$ and to line $x = -p$
- ellipse: $\frac{x^2}{a^2} + \frac{y^2}{b^2} = 1$: sum of distances to foci$(\pm\sqrt{a^2 - b^2}, 0)$ is $2a$
- hyperbola: $\frac{x^2}{a^2} - \frac{y^2}{b^2} = 1$: differences of distances to foci$(\pm\sqrt{a^2 + b^2}, 0)$ is $2a$
- $\frac{n}{\sum_{i=1}^n \frac{1}{x_i}} \leq (\prod_{i=1}^n x_i)^{\frac{1}{n}} \leq \frac{\sum_{i=1}^n x_i}{n} \leq \sqrt{\frac{\sum_{i=1}^n x_i^2}{n}}$
- Sum of interior angle in a polygon : $180(n - 2)$
- Sum of external angle in a polygon : 360
- $x^n - 1 = (x - 1) \sum_{i=0}^{n-1} x^i$
- $a^3 + b^3 = (a + b)(a^2 - ab + b^2)$, $a^3 - b^3 = (a - b)(a^2 + ab + b^2)$
- $(x + y)^n = \sum_{i=0}^n \binom{n}{i} x^{n-i} y^i$
- $y = f(x)$, $f^{-1}(y) = x$
- angles: zero, acute, right(90), obtuse, straight(180)
- $\sum_{x=1}^n x^2 = \frac{n(n+1)(2n+1)}{6}$
- surface of sphere: $4\pi r^2$, volume is $\frac{4}{3}\pi r^3$

2. Calculus-1

- Convergent sequence:
  - Every convergent sequence is bounded
  - A monotonic and bounded sequence is convergent
- $\lim_{x\to a} f(x)$ exists $\Leftrightarrow \lim_{x\to a^+} f(x) = \lim_{x\to a^-} f(x)$ both exist
- continuous: $f(a) = \lim_{x\to a} f(x)$
- Extreme value theorem: function f is continuous in $[a,b]$, f must attain a minimum and maximum value at some point in the interval
- Intermediate value theorem: function f is continuous in $[a,b]$, m is the minimum, M is the maximum, then $\forall y \in [m,M], \exists c \in [a,b], f(c) = y$
- $f'(a) = \lim_{h\to 0} \frac{f(a+h)-f(a)}{h}$
- If function is not continuous at a, it is not differentiable at a
- derivatives
  - $(a^x)' = (\ln a)a^x$, $(\log_a x)' = \frac{1}{x\ln a}$
  - $(\tan x)' = \sec^2 x$, $(\cot x)' = -\csc^2 x$
  - $(\sec x)' = \sec x \tan x$, $(\csc x)' = -\csc x \cot x$
  - $(\sin^{-1} x)' = \frac{1}{\sqrt{1-x^2}}$, $(\cos^{-1} x)' = -\frac{1}{\sqrt{1-x^2}}$
  - $(\tan^{-1} x)' = \frac{1}{1+x^2}$, $(\cot^{-1} x)' = -\frac{1}{1+x^2}$
  - $(\sin/\cos(ax+b))^{(n)} = a^n \sin/\cos(ax+b+n\frac{\pi}{2})$
  - $(\ln(1+x))^{(n)} = (-1)^{n-1}\frac{(n-1)!}{(1+x)^n}$
  - $(u+v)^{(n)} = \sum_{i=1}^{n} \binom{n}{i} u^{(n-i)} v^{(i)}$
- $y = f(x) \to x = f^{-1}(y)$
- normal line's slope $*$ tangent line's slope $= -1$
- $f' = 0$ is a critical(stationary) point
- the points where the function has local extrema are critical points.
- inflection point is f'' changes sign
- n-th derivative test: find smallest n that $f^{(n)}(a) \neq 0$, if n is even, $f^{(n)}(a) > 0$, f has a local minimum at a, if $f^{(n)}(a) < 0$, f has a local maximum at a. If n is odd, f has no minimum nor maximum at a
- Mean-Value theorem: function f, F is continuous in $[a,b]$ and differentiable at every point in (a,b), $\forall x \in (a,b), F(x) \neq 0$ $\exists c \in (a,b), \frac{f'(c)}{F'(c)} = \frac{f(b)-f(a)}{F(b)-F(a)}$; $\exists c \in (a,b), f(b) - f(a) = f'(c)(b-a)$;
- $f(c)$ is a local extremum if it is a local minimum or maximum, $f'(c) = 0$ or does not exists
- an absolute extremum will at c that $\underline{f'(c) = 0}$ or <u>does not exists</u> or <u>at end point of the interval</u>
- integration
  - $\int x^n dx = \frac{x^{n+1}}{n+1}$, $\int a^x dx = \frac{a^x}{\ln a}$
  - $\int \tan x dx = -\ln|\cos x|$, $\int \cot x dx = \ln|\sin x|$
  - $\int \sec x dx = \int \frac{\sec x(\sec x + \tan x)}{\sec x + \tan x} dx = \int \frac{d\sec x + d\tan x}{\sec x + \tan x} = \ln|\sec x + \tan x|$
  - $\int \sec x dx = \int \frac{\cos^2\frac{x}{2} + \sin^2\frac{x}{2}}{\cos^2\frac{x}{2} - \sin^2\frac{x}{2}} dx = \int \frac{1+\tan^2\frac{x}{2}}{1-\tan^2\frac{x}{2}} dx = \int (\tan x + \frac{(1-\tan\frac{x}{2})^2}{1-\tan^2\frac{x}{2}}) dx = \int (\tan x + \frac{1-\tan\frac{x}{2}}{1+\tan\frac{x}{2}}) dx$
    $= \int (\tan x + \frac{\sin\frac{x}{2} - \cos\frac{x}{2}}{\sin\frac{x}{2} + \cos\frac{x}{2}}) dx = \int (\tan x + \frac{\sin^2\frac{x}{2} + \cos^2\frac{x}{2}}{(\sin^2\frac{x}{2} + \cos^2\frac{x}{2})^2}) dx = \int (\tan x + \frac{1}{1+\sin x}) dx = \ln|\sec x + \tan x|$
  - $\int \csc x dx = \int \frac{\csc x(\csc x + \cot x)}{\csc x + \cot x} dx = \int \frac{-d\cot x - d\csc x}{\csc x + \cot x} = -\ln|\csc x + \cot x| = \ln|\frac{\sin x}{1-\cos x}| = \ln|\tan\frac{x}{2}|$
  - $\int \csc x dx = \int \frac{\sin^2\frac{x}{2} + \cos^2\frac{x}{2}}{\sin\frac{x}{2}\cos\frac{x}{2}} d\frac{x}{2} = \int (\tan\frac{x}{2} + \cot\frac{x}{2}) d\frac{x}{2} = -\ln|\cos\frac{x}{2}| + \ln|\sin\frac{x}{2}| = \ln|\tan\frac{x}{2}|$
  - $\int \frac{dx}{x^2-a^2} = \frac{1}{2a}\ln|\frac{x-a}{x+a}|$, $\int \frac{dx}{x^2+a^2} = \frac{1}{a}\tan^{-1}\frac{x}{a}$
  - $\int \frac{dx}{\sqrt{a^2-x^2}} = \sin^{-1}\frac{x}{a}$
  - $\int \frac{dx}{\sqrt{x^2\pm a^2}} = \ln|x + \sqrt{x^2 \pm a^2}|$
  - $\int u dv = uv - \int v du$
  - $\sqrt{a^2-x^2} \to x = a\sin t$, $\sqrt{x^2+a^2} \to x = a\tan t$, $\sqrt{x^2-a^2} \to x = a\sec t$
  - $\int x\sin x dx = -\int x d(\cos x) = \int \cos x dx - x\cos x = \sin x - x\cos x$
  - $\int xe^x dx = \int x d(e^x) = xe^x - \int e^x dx = (x-1)e^x$
- Riemann sum: $\int_a^b f(x)dx = \lim_{n\to\infty} \sum_{i=1}^{n} f(a + \frac{b-a}{n}i)\frac{b-a}{n}$
- Fundamental theorem for calculus: $\int_a^b f'(x)dx = f(x)\big|_a^b$

- Leibniz's rule: $\frac{d}{dx}\int_{a(x)}^{b(x)} f(x,t)dt = f(x,b(x))b'(x) - f(x,a(x))a'(x) + \int_{a(x)}^{b(x)} \frac{\partial f(x,t)}{\partial x}dt$
- Mean-Value theorem $m(b-a) \leq \int_a^b f(x)dx = f(c)(b-a) \leq M(b-a)$
- $s = \int \sqrt{(dx)^2 + (dy)^2} = \int \sqrt{1+y'}dx$
- $e^x \sim 1 + x \to e^{\frac{1}{x}} \sim 1 + \frac{1}{x} \to e \sim (1+\frac{1}{x})^x$
- L'Hospital's rule: f, g are differentiable in interval I, $f', g' \neq 0$ exists, $\lim_{x\to a}\frac{f(a)}{g(a)} = \lim_{x\to a}\frac{f'(a)}{g'(a)}$
- test for convergence of infinite series
  - $\sum a_n$ converge $\Rightarrow \lim_{n\to\infty} a_n = 0$
  - p-series $\sum \frac{1}{n^p}$ converge for $p > 1$ and diverge for $p \leq 1$, Harmonic series for $p = 1$
  - $0 \leq a_n \leq b_n$, $\sum b_n$ converge $\Rightarrow \sum a_n$ converge, $\sum a_n$ diverge $\Rightarrow \sum b_n$ diverge
  - nonnegative series, $\lim_{n\to\infty}\frac{a_{n+1}}{a_n} < 1 \Rightarrow \sum a_n$ converge, $> 1 \Rightarrow \sum a_n$ diverge. $= 1$ no conclusion
  - nonnegative section, $\lim_{n\to\infty} a_n^{\frac{1}{n}} < 1 \Rightarrow \sum a_n$ converge, $> 1 \Rightarrow \sum a_n$ diverge. $= 1$ no conclusion
  - alternating series $\sum(-1)^{n+1}a_n, a_n \geq 0$ converge if a_n decrease monotonically with 0 as limit
  - every absolute convergent series converge
- radius of convergence for power series $\sum a_n x^n$ is $\lim_{n\to\infty}|\frac{a_n}{a_{n+1}}|$
- $\int_0^x \sum_{n=0}^{\infty} a_n x^n = \sum_{n=0}^{\infty}\frac{a_n}{n+1}x^{n+1}$
- $\frac{d}{dx}\sum_{n=0}^{\infty} a_n x^n = \sum_{n=1}^{\infty} n a_n x^{n-1}$
- Taylor series: $f(x) = \sum_{n=0}^{\infty}\frac{f^{(n)}(a)}{n!}(x-a)^n$
  - $\frac{1}{1\pm x} = \sum_{n=0}^{\infty}(\mp x)^n \quad \forall x \in (-1,1)$
  - $\ln(1+x) = \sum_{n=1}^{\infty}\frac{(-1)^{n+1}}{n}x^n \sim x - \frac{x^2}{2} \quad \forall x \in (-1,1)$: notice the starting index is 1
  - $e^x = \sum_{n=0}^{\infty}\frac{x^n}{n!} \quad \forall x \in \mathbb{R}$
  - $\sin x = \sum_{n=0}^{\infty}\frac{(-1)^n}{(2n+1)!}x^{2n+1} \sim x - \frac{x^3}{6} \quad \forall x \in \mathbb{R}$
  - $\cos x = \sum_{n=0}^{\infty}\frac{(-1)^n}{(2n)!}x^{2n} \sim 1 - \frac{x^2}{2} \quad \forall x \in \mathbb{R}$
- $\int x\ln x dx = \frac{x^2}{2}\ln x - \frac{x^2}{4}$
- $\int_0^{\infty} e^{-x^2}dx = \frac{\sqrt{\pi}}{2}$

3. Calculus-2

- x, y axes parition the plane into 4 quadrants, and x, y, z axes parition the space into 8 octants
- $a \cdot b = |a||b|\cos\theta$, $\mathsf{proj}_a b = \frac{a\cdot b}{a\cdot a}a$
- $a \times b = |a||b|\sin\theta = -b \times a = \begin{vmatrix} i & j & k \\ a_1 & a_2 & a_3 \\ b_1 & b_2 & b_3 \end{vmatrix}$: useful for calculating area
- $(a \times b)\cdot c = \begin{vmatrix} a_1 & a_2 & a_3 \\ b_1 & b_2 & b_3 \\ c_1 & c_2 & c_3 \end{vmatrix}$
- $c \cdot (a + b) = c \cdot a + c \cdot b$, $c \times (a + b) = c \times a + c \times b$
- line in 3d: $\frac{x-x_0}{v_1} = \frac{y-y_0}{v_3} = \frac{z-z_0}{v_3} = t$
- plane in 3d: $(x - x_0, y - y_0, z - z_0) \cdot (n_1, n_2, n_3) = 0$ or $n_1x + n_2y + n_3z + d = 0$
- $d = \frac{Ax_0+By_0+Cz_0+D}{\sqrt{A^2+B^2+C^2}}$
- cylindrical coordinate: $x = r\cos\theta$, $y = r\sin\theta$, $z = z$
- spherical coordinate: $x = r\sin\phi\cos\theta$, $y = r\sin\phi\sin\theta$, $z = r\cos\phi$
- $D_uf|_P = \nabla f|_P \cdot u$
- $\nabla f = \frac{\partial f}{\partial x}i + \frac{\partial f}{\partial y}j + \frac{\partial f}{\partial z}k$ points to the direction which f increases most rapidly
- $F(x, y) = 0$, $\frac{\partial F}{\partial x}dx + \frac{\partial F}{\partial y}dy = 0$ $\frac{dy}{dx} = -\frac{\frac{\partial F}{\partial x}}{\frac{\partial F}{\partial y}} = -\frac{F_x}{F_y}$
- tangent plane: $(x - x_0, y - y_0, z - z_0) \cdot (\frac{\partial f}{\partial x}, \frac{\partial f}{\partial y}, \frac{\partial f}{\partial z}) = 0$
- P is a critical point of $f(x, y)$ if $\frac{\partial f}{\partial x}\big|_P = 0$ and $\frac{\partial f}{\partial y}\big|_P = 0$
- second-derivative test: $\Delta = \begin{vmatrix} f_{xx} & f_{xy} \\ f_{yz} & f_{yy} \end{vmatrix} = f_{xx}f_{yy} - f_{xy}^2$
  - $\Delta > 0$ and $f_{xx} < 0$, local maximum
  - $\Delta > 0$ and $f_{xx} > 0$, local minimum
  - $\Delta < 0$ saddle point
  - $\Delta = 0$, no conclusion
- line integral: $\int_C f ds = \int_a^b f(x(t), y(t))\sqrt{(\frac{dx}{dt})^2 + (\frac{dy}{dt})^2}dt$
- $F(x, y) = P(x, y)i + Q(x, y)j$, $\int_C F \cdot dr = \int_C Pdx + Qdy$
- Green theorem: a simple closed curve C enclosing a region R: $\oint_C Pdx + Qdy = \iint_R(\frac{\partial Q}{\partial x} - \frac{\partial P}{\partial y})dxdy$
- Green theorem require P, Q are defined and have continuous partial derivatives both on C and throughout the region R enclosed by C
- area of R $= \frac{1}{2}\oint_C xdy - ydx = \oint_C -ydx = \oint_C xdy$
- Fundamental theorem of calculus for line integrals: $\int_{C:A\to B} \nabla f \cdot dr = f(B) - f(A)$
  line integral of a gradient field depends only on the endpoints of the path(conservative field).
- F is a gradient field $\Leftrightarrow \forall C : \oint_C Fdr = 0 \Leftrightarrow \frac{\partial Q}{\partial x} = \frac{\partial P}{\partial y} \Leftrightarrow \exists u, du = Pdx + Qdy$
- Divergence theorem $\iiint_V \nabla \cdot \vec{F}dv = \iint_S \vec{F} \cdot d\vec{s}$
- area of surface: $\iint ds = \iint \sqrt{z_x^2 + z_y^2 + 1}dxdy$

4. ODE

- Separable equation: $\int f(x)dx = \int g(y)dy$
- Homogeneous equation: $\frac{dy}{dx} = f(\frac{y}{x})$
  Let $\frac{y}{x} = t$, $\frac{dy}{dx} = t + x\frac{dt}{dx}$, $x\frac{dt}{dx} = f(t) - t$, $\int \frac{dt}{f(t)-t} = \int \frac{dx}{x}$
- exact equation: $\frac{\partial^2 f}{\partial x \partial y} = \frac{\partial^2 f}{\partial y \partial x}$
- multiplying an integrating factor transform non-exact to exact ODE
- if a non-exact equation has a solution, an integrating factor exists.
  $P(x,y)dx + Q(x,y)dy = 0$, $\frac{\partial Q}{\partial x} - \frac{\partial P}{\partial y} \neq 0$
  - $\frac{\frac{\partial P}{\partial y} - \frac{\partial Q}{\partial x}}{Q} = \phi(x)$, then $e^{\int \phi(x)dx}$ is a integrating factor.
  - $\frac{\frac{\partial P}{\partial y} - \frac{\partial Q}{\partial x}}{-P} = \Phi(y)$, then $e^{\int \Phi(y)dy}$ is a integrating factor.
- first-order linear equation: $\frac{df}{dx} + P(x)f = Q(x)$:
  - $u(x) = e^{\int P(x)dx}$
  - $u(x)\frac{df}{dx} + u(x)P(x)y = u(x)Q(x)$
  - $(uf)' = uQ$
  - $f = \frac{1}{u}\int uQdx$
- $y'' = f(x, y')$, let $y' = p$, $p' = f(x,p)$
- $y'' = f(y, y')$, let $y' = p$, $y'' = p\frac{dp}{dy}$, $p\frac{dp}{dy} = f(y,p)$
- second-order linear differential equation with constant coefficients
  $ay'' + by' + cy = d(x)$, homogeneous if $d(x) = 0$. $y = y_h + y_p$
  auxiliary polynomial equation $ax^2 + bx + c = 0$
  - 2 real roots, $y = c_1e^{r_1x} + c_2e^{r_2x}$
  - 1 root, $y = (c_1 + c_2x)e^{rx}$
  - $r_{1,2} = \alpha \pm i\beta$, $y = e^{\alpha x}(c_1 \cos \beta x + c_2 \sin \beta x)$
- n-th order ODE will have n constants

5. Linear Algebra

- each linear equation determines a hyperplane in n-dimensional space
- solution of linear system: a set of $\sum_{i=1}^{n} a_i x_i = 0$
  - homogeneous systems are always consistent(all 0 trivial solution)
  - solution set to is the null space of the corresponding matrix A
  - if $|A| \neq 0$, only 1 sol
- solution of linear system: a set of $\sum_{i=1}^{n} a_i x_i = b$
  - no sols(inconsistent): $rank(A) \neq rank([A, b])$
  - 1 sol: $rank(A) = rank([A, b]) = n$
  - infinite many sols: $rank(A) = rank([A, b]) \leq n$: $\underline{\text{if there are 2 sols, then there are } \infty}$
  - non-homogeneous systems $x = x_h + x_p$
- Gaussian elimination via elementary row operation:
  - multiply a row by a non zero const
  - interchange two rows
  - add a multiple of one row to another
- $\begin{pmatrix} a & b \\ c & d \end{pmatrix}^{-1} = \frac{1}{ad-bc} \begin{pmatrix} d & -b \\ -c & a \end{pmatrix}$
- vector space: a set closed under addition and scalar multiplication
- every vector space must contain zero vector
- the set of all linear combinations of a set of vectors is their span
- a minimal spanning set for a vector space is a basis for the space, they are linearly independent if $\sum_{i=1}^{n} a_i x_i = 0$, then $a_i = 0$
- The dimension or rank of a vector space is the size of its basis
- a subspace of $\mathbb{R}^3$ must be: $\underline{\{0\}}$, $\underline{\text{a line through origin}}$, $\underline{\text{a plane through origin}}$ or $\underline{\mathbb{R}^3}$
- every permutation can be achieved by a sequence of transposition of two elements, the sgn of a permutation σ is $+1$ is permutation is even or else -1
- $|A| = \sum_{\sigma \in S_n} \mathsf{sgn}(\sigma) \prod_{i=1}^{n} a_{i\sigma(i)}$
  - $|a_1, \dots, b_i + c_i, \dots, a_n| = |a_1, \dots, b_i, \dots, a_n| + |a_1, \dots, c_i, \dots, a_n|$
  - $|a_1, \dots, ka_i, \dots, a_n| = k|a_1, \dots, a_i, \dots, a_n|$
  - $|a_1, \dots, a_i \dots a_j, \dots, a_n| = -|a_1, \dots, a_j \dots a_i, \dots, a_n|$
  - $|a_1, \dots, a_i \dots a_j, \dots, a_n| = |a_1, \dots, a_i \dots ka_i + a_j, \dots, a_n|$
  - $|a_1, \dots, ka_i \dots la_i, \dots, a_n| = 0$
  - $|AB| = |A||B|$
- Laplace expansion: $|A| = \sum_{j=1}^{n} a_{ij} \mathsf{cof}(a_{ij}) = \sum_{j=1}^{n} a_{ij} (-1)^{i+j} (a_{ij} \mathsf{minor})$
- Crammer's rule for square linear system: $x_i = \frac{|A_i|}{|A|}$
- linear transformation is a function between two vector spaces s.t. $T(a + b) = T(a) + T(b)$, $T(ka) = kT(a)$
- If two vector spaces are isomorphic, the mapping a linear transformation
- Vector spaces are isomorphic if and only if they have the same dimension
- linear transformation maps zero vector to zero vector
- linear operator is a linear transformation map a vector spaces to itself
- every linear transformation can be represented by a matrix
- $T(x) = T(\sum_{i=1}^{n} k_i b_i) = \sum_{i=1}^{n} k_i T(b_i)$
- standard matrix for linear transformation: $T(x) = Ax$: col i is the image of e_i
- change of basis matrix: $[B][x]_B = x$
- Rank-nullity theorem: $rank(T) + nullity(T) = dim(domain)$
  - nullity is the dimension of nullspace(kernel): $ker(T) = \{x : T(x) = 0\}$
  - rank is the dimension of range: $R(T) = \{T(x) : \forall x\}$, the same as column space
  - $T(x) = Ax$, T is one-to-one and onto, $|A| \neq 0$, $rank(A) = n$, only zero vector is mapped to zero vector
- $Ax = \lambda x$, $|A - \lambda I| = 0$
- $|A| = \prod_i \lambda_i$, $tr(A) = \sum_i A_{ii} = \sum_i \lambda_i$
- Eigenspace $E_\lambda(a) = \{x : Ax = \lambda x\}$ is the nullspace of matrix $A - \lambda I$
- Cayley-Hamilton theorem: any square matrix satisfies its own characteristic equation if $p(\lambda) = \det(A - \lambda I)$ is the characteristic polynomial of matrix A, then $p(A) = 0$
- n by n matrix A is diagonalizable iff A has n linearly independent eigenvectors

6. Number theory and abstract algebra

6.1. **Number theory.**

- $\mathbb{Z}$: int, $\mathbb{Q}$: rational: reals of form $\frac{a}{b}, a, b \in \mathbb{Z}, b \neq 0$; $\mathbb{R}$: real; $\mathbb{C}$: complex
- $a \mid b$: $b = ac$, a divides b, b is divisible by a. a is a divisor or factor, b is a multiple of a
- 1 is not a prime
- an int p whose only divisors are 1 and p is a prime number, int that not prime is composite
- divisibility:
  - 2: unit digit is $0, 2, 4, 6, 8$
  - 5: unit digit is $0, 5$
  - 3: sum of digits is divisible by 3
  - 9: sum of digits is divisible by 9
  - 4: last 2 digits is divisible by 4
  - 8: last 3 digits is divisible by 8
  - 6: divisible by $2, 3$
  - 7: no
- n is divisible by primes $a \neq b$, n is divisible by ab
- relatively prime: two int have only common divisor 1
- division alg: $a = bq + r : 0 \leq r < a$, q quotient, r remainder
  $gcd(bq + r, b) = gcd(b, r)$
- $|\{p : \text{prime } p \leq x\}| \sim \frac{x}{\ln x}$
- fundamental theorem of arithmetic: every int > 1 can be expressed as unique product of primes
- great common divisor(g.c.d): $gcd(\prod_{i=1}^{n} p_i^{a_i}, \prod_{i=1}^{n} p_i^{b_i}) = \prod_{i=1}^{n} p_i^{\min(a_i, b_i)}$
- least common multiple(l.c.m): $lcm(\prod_{i=1}^{n} p_i^{a_i}, \prod_{i=1}^{n} p_i^{b_i}) = \prod_{i=1}^{n} p_i^{\max(a_i, b_i)}$
- $gcd(a, b) * lcm(a, b) = ab$
- linear Diophantine equation: $ax + by = c$ with int a, b, c
  - $gcd(a, b) \nmid c$, no int sol
  - $gcd(a, b) \mid c$, infinite int sols: $x = x_0 + \frac{b}{gcd(a,b)}t$, $y = y_0 - \frac{a}{gcd(a,b)}t$
  - we can first write gcd as linear combination of a, b: $ax_0 + by_0 = gcd(a, b)$
  - $a\frac{cx_0}{gcd(a,b)} + b\frac{cy_0}{gcd(a,b)} = gcd(a, b)\frac{c}{gcd(a,b)} = c$
  - int sol for $ax + by = c$: $a(\frac{cx_0}{gcd(a,b)} + \frac{bt}{gcd(a,b)}) + b(\frac{cy_0}{gcd(a,b)} - \frac{at}{gcd(a,b)}) = gcd(a, b)\frac{c}{gcd(a,b)} = c$
- a is congruent to b modulo n: $n \mid a - b$: $a \equiv b(mod\ n)$
  - $a \equiv b(mod\ n)$, $b \equiv c(mod\ n)$, then $a \equiv c(mod\ n)$
  - $a \equiv b(mod\ n)$, $\forall c$, $a \pm c \equiv b \pm c(mod\ n)$, $ac \equiv bc(mod\ n)$
  - $a_1 \equiv b_1(mod\ n)$, $a_2 \equiv b_2(mod\ n)$, then $a_1 \pm a_2 \equiv b_1 \pm b_2(mod\ n)$, $a_1a_2 \equiv b_1b_2(mod\ n)$
  - $a \equiv b(mod\ n)$, then $a \equiv b, b + n, \ldots, b + (c - 1)n(mod\ cn)$
  - $ab \equiv ac(mod\ n)$, $b \equiv c(mod\ \frac{n}{gcd(a,n)})$. if $gcd(a, n) = 1$, $b \equiv c(mod\ n)$
- Fermat little theorem: p is a prime, a is int, if $p \nmid a$, then $a^{p-1} \equiv 1(mod\ p)$. $\forall a : a^p \equiv a(mod\ p)$
  $\prod_{i=1}^{p-1} ai \equiv \prod_{i=1}^{p-1} i(mod\ p)$
- $ax \equiv b(mod\ n)$, $ax - nc = b$ has a sol for x, c if $gcd(a, n) \mid b$

6.2. Abstract algebra.

- $M_{m\times n}(S)$: set of all matrices with entries in S
- $M_n(S)$: set of all square matrices with entries in S
- S is a nonempty set, binary operation $f: S\times S\to S$
- Group
  - semigroup: associative binary structure $(S,*): a*(b*c)=(a*b)*c$
  - identity: $a*e=e*a=a$
  - monoid: semigroup with identity
  - inverse: $a*a^{-1}=a^{-1}*a=a$
  - group: monoid with inverse: close, assoc, id, inv: solve linear eq
  - Abelian group: commutative group: $a*b=b*a$
  - $(M_{m\times n}(S),+)$ are finite Abelian groups
  - $(GL(n,\mathbb{R}),\times)$: convertible(det $\neq 0$) $n\times n$ matrices of reals
  - $(SL(n,\mathbb{R}),\times)$: convertible(det $=1$) $n\times n$ matrices of reals
  - $(\{z:z^n=1\},\times)$: n-th root of unity under multiplication
  - $(S_n,\circ)$: permutation under composition: not Abelian $n\geq 3$, $|S_n|=n!$
  - alternating groups $|A_n|=\frac{n!}{2}$: even permutations
  - $(D_n,\circ)$: permutation of vertices of polygon P_n under composition: dihedral group: $|D_n|=2n$
    n rotations and n reflections: $D_n=\langle r,f\mid r^n=f^2=(rf)^2=1\rangle$
  - $\mathbb{Z}_n=[n-1]$, $a\oplus b=a+b(mod\ n)$
    $(\mathbb{Z}_n,\oplus)$ is a order n Abelian group: additive group of ints modulo n
  - $a\otimes b=ab(mod\ n)$, $(\mathbb{Z}_n,\otimes)$ is an Abelian monoid: not every element have inv
  - $(\mathbb{Z}_p,\otimes)$ is a order $p-1$ Abelian group: multiplicative group of ints modulo p
  - group table: every element appears once in every row and col

  - cyclic group: $\{a^n:n=0,1,\dots\}$ with generator a. They are Abelian. e.g.: $(\mathbb{Z}_n,+)$
  - Every infinite cyclic group is isomorphic to the additive group of $\mathbb{Z}$, ± 1 are generators
  - Every finite cyclic group of order n is isomorphic to the additive group of $\mathbb{Z}_n$,
    Order of generator is relatively prime to n
  - Every finite Abelian group is finitely generated
  - Every finitely generated Abelian group is isomorphic to a direct sum

$$|G|=\prod_{i=1}^{r}p_i^{k_i}: G\simeq\oplus_{i=1}^{r}\mathbb{Z}_{p_i^{k_i}}$$

  - $\mathbb{Z}_m\oplus\mathbb{Z}_n$ is cyclic $\Leftrightarrow gcd(m,n)=1$, $\mathbb{Z}_m\oplus\mathbb{Z}_n\simeq\mathbb{Z}_{mn}$
  - A finite abelian group is also finitely generated, finitely generated Abelian group need not be finite

  - generator for cyclic group does not have to be unique
  - m is a generator for $(\mathbb{Z}_n,\oplus)\Leftrightarrow m$ relatively prime to n
  - G is a cyclic group with generator a, n is smallest int s.t. $a^n=e$, then
    m is a generator for $G\Leftrightarrow m$ relatively prime to n
  - smallest non-cyclic group: Klein four-group: $K_4=\langle a,b:a^2=b^2=e,ab=ba\rangle$
  - order 4 groups: **Klein four-group** and **cyclic** 4 **group** are all Abelian
  - subgroup $(H,*)\leq(G,*)$: close, id, inv
    subgroup must contain id of the group
  - center $Z(G)=\{z\in G:\forall g\in G:zg=gz\}$ is a subgroup
  - normal subgroup: $N\trianglelefteq G$: $\forall g\in G: gNg^{-1}=N$
  - $a\in G$, the smallest subgroup contains a is cyclic subgroup $\langle a\rangle=\{a^n:n\in\mathbb{Z}\}$
    any group has a cyclic subgroup: $\langle a\rangle\leq G$
  - order of group is the number of elements in the set.
  - order of $a\in G$ is the order of $\langle a\rangle$ i.e. smallest int n s.t. $a^n=e$
  - a group that can be generated by a finite set is finitely generated
  - some theorems:
    * Lagrange theorem: if H is a subgroup of a finite group G: $|H|\mid|G|$
    * The order of any element a of a finite group divides the order of that group
    * G is a finite Abelian order n group, G has a least 1 subgroup of order of every positive divisor

        - $*$ G is a finite cyclic order n group, G has 1 subgroup of order of every positive divisor
        - $*$ Cauchy theorem: G is a finite order n group, G has a least 1 subgroup of order prime $p : p \mid n$
        - $*$ Sylow first theorem: G is a order $n = p^k m$ group, G has at least 1 subgroup of order $p^i : i \in [k]$
    - $(G_1, *_1), (G_2, *_2)$ are groups, direct product $(G_1 \times G_2, *)$: $|G_1 \times G_2| = |G_1||G_2|$
      $G_1 \times G_2 = \{(a, b) : a \in G_1, b \in G_2\}$, $(a_1, a_2) * (b_1, b_2) = (a_1 *_1 b_1, a_2 *_2 b_2)$
    - $\mathbb{Z}_m \oplus \mathbb{Z}_n$ is cyclic $\Leftrightarrow gcd(m, n) = 1$; $\mathbb{Z}_m \oplus \mathbb{Z}_n \simeq \mathbb{Z}_{mn}$
    - homomorphism: $(G_1, *_1) \simeq (G_2, *_2)$ if there's a function $f : f(a *_1 b) = f(a) *_2 f(b)$
        - $*$ $f(e_1) = e_2$
        - $*$ order of $g \in G_1$ = order of $f(g) \in G_2$
        - $*$ $f(a^{-1}) = (f(a))^{-1}$
        - $*$ $H \leq G_1$, $\{f(h) : h \in H\} = f(H) \leq G_2$
        - $*$ $H \leq G_2$, $\{f^{-1}(h) : h \in H\} = f^{-1}(H) \leq G_1$
        - $*$ $|f(G_1)| \mid |G_1|$, $|f(G_1)| \mid |G_2|$
        - $*$ zero map is always a homomorphism
        - $*$ trivial homomorphism: every elements mapped to e_2
    - monomorphism: homomorphism and injection $\Leftrightarrow ker(f) = \{g \in G : f(g) = e'\} = e$
    - epimorphism: homomorphism and surjection
    - isomorphism: homomorphism and bijection
      infinite group $(\mathbb{Z}, +)$ is isomorphic to one of its proper subgroups $(n\mathbb{Z}, +), n \geq 2, n \in \mathbb{Z}$
    - endomorphism: homomorphism to itself
    - automorphism: isomorphism to itself
    - kernel of a homomorphism is always a subgroup, thus $|ker(G)| \mid |G|$
      $f : \mathbb{Z}_p \to G$, $|ker(f)| = 1$ or p, trivial homomorphism or monomorphism
- Ring
    - $(R, +, *)$ is a ring if: $(R, +)$ is a Abelian group, $(R, *)$ is a semigroup
      Distributive property : $a * (b + c) = a * b + a * c$, $(b + c) * a = b * a + c * a$
    - if ring has ≥ 2 elements, $0 \neq 1$
    - ring with unity: ring has $*$ id. Commutative ring $2\mathbb{Z}$ does not contains 1
    - commutative ring: $(R, *)$ is commutative
    - $\begin{pmatrix} 2a & 2b \\ 2c & 2d \end{pmatrix}$ is not commutative and contains no id
    - $charR$: smallest int $n : \forall a \in R, na = 0$; sufficient to check $n * 1 = 0$
    - ring of int modulo n: $(\mathbb{Z}_n, +, *)$
    - $(M_n(\mathbb{R}), +, *)$ is a noncommutative ring with unity
    - ring of Gaussian int: $\mathbb{Z}[i] = \{a + bi : a, b \in \mathbb{Z}\}$
      commutative ring with unity, but not every nonzero element has a inv
    - real polynomials: $\mathbb{R}[x] = \{\sum_{i=0}^{n} r_i x^i : r_i \in \mathbb{R}\}$: commutative ring with unity
    - homomorphism: $(G_1, +_1, *_1) \simeq (G_2, +_2, *_2)$ if there's a function
      $f : f(a +_1 b) = f(a) +_2 f(b)$, $f(a *_1 b) = f(a) *_2 f(b)$
    - $ker(f) = \{a \in R : f(a) = 0'\}$
    - image: $f(R) = \{f(r) : r \in R\}$
    - $f(0) = 0'$
    - only 2 endomorphism for $\mathbb{Z}$: zero homomorphism, id
    - I is a subring for R, $\forall r \in R, x \in I : rx \in I, xr \in I$, I is an ideal
    - integral domain: commutative ring with unity s.t. $ab = 0 \Leftrightarrow a = 0$ or $b = 0$. Cancellation property.
    - nonzero a, b in the ring, $ab = 0$, a is left zero divisor, b is right zero divisor
    - cancellation law of integral domain: $a \neq 0, ab = ac \to b = c$
    - nonzero $m \in \mathbb{Z}$ is a zero divisor $\Leftrightarrow m$ and n are not relatively prime
    - $\mathbb{Z}_p$ is a integral domain
- Field
    - a set of elements with commutative $+, -, *, /$
    - $(F, +)$, $(F^\star, *)$ are Abelian groups
      Distributive property : $a * (b + c) = a * b + a * c$, $(b + c) * a = b * a + c * a$
    - an element in ring with unity is a unit if it is invertible (1 is always a unit)
    - m is a unit of Z_n iff m is relative prime to n

  - group of units: units of a ring with unity form a group under $*$, it never contains the element 0, is therefore not closed under addition
  - division ring: $(R^{\star}, *)$ is a group: R is a ring with unity and every nonzero element is a unit
  - a commutative division ring is a field: commutative ring with unity and every nonzero element is a unit
  - finite integral domain is a field: $\mathbb{Z}_p$ is a field $\Leftrightarrow p$ is a prime, it containing $p-1$ units
  - $\mathbb{Q} = \{\frac{a}{b} : a, b \in \mathbb{Z}, b \neq 0\}$: field of rationals
- group: $+, -$; ring: $+, -, *$; field: $+, -, *, /$
- vector spaces are Abelian groups under $+$ with a field of scalars

7. Additional

7.1. Logic.

- $\overline{A \wedge B} = \overline{A} \vee \overline{B}$
- $\overline{A \vee B} = \overline{A} \wedge \overline{B}$
- Contraposition: $A \to B \Leftrightarrow \overline{B} \to \overline{A}$
- $p \to q \equiv \overline{p} \vee q$

7.2. Set theory.

- set is a collection of elements
- $A \subseteq B, A \supseteq B \Rightarrow A = B$
- $\overline{A} = \{x \in U : x \notin A\}$
- $A \triangle B = (A \setminus B) \cup (B \setminus A) = (A \cup B) \setminus (A \cap B)$
- a set S is finite if there is a bijective function between $[n]$ and S (equivalent)
- if a set is equivalent to $\mathbb{Z}^+$, then it is countably infinite, whose cardinality is $\aleph_0$
- $\mathbb{R}$ is equivalent to the power set of $\mathbb{Z}^+$: cardinality of the continuum: $|\mathbb{R}| = 2^{\aleph_0} > \aleph_0$

7.3. Graph theory.

- a graph is a collection of vertices and edges
- the order of graph is $|V|$, the size of graph is $|E|$
- odd/even vertex: a vertex with odd/even degree
- isomorphic: graph F, G are isomorphic if there is a bijective function $f : V(F) \to V(G)$ preserving adjacencies
- connected: every pair of vertices can be connected by a path
- forest: a graph with no cycles, a connected forest is a tree
- subgraph: H is a subgraph of G if $V(H) \subseteq V(G)$, $E(H) \subseteq E(G)$, every edge in H connect 2 vertices of H
- subgraph H is a spanning subgraph of G if $V(H) = V(G)$; if H is a tree, it is called spanning tree
- Walk: Vertices may repeat. Edges may repeat (Closed or Open)
- Trail: Vertices may repeat. Edges cannot repeat (Open)
- Circuit: Vertices may repeat. Edges cannot repeat (Closed)
- Path: Vertices cannot repeat. Edges cannot repeat (Open)
- Cycle: Vertices cannot repeat. Edges cannot repeat (Closed)

7.4. Algorithms.

- no instructions can be dependent on user
- process must end with a sol after finite number of steps
- the process is deterministic

7.5. Combinatoric.

- k-permutations of n: $P(n,k) = \frac{n!}{(n-k)!}$
- k-combinations of n: $C(n,k) = \binom{n}{k} = \frac{n!}{k!(n-k)!}$
- k-permutations of n with repetition: $P(n,k)$ with repetition $= n^k$
- k-combinations of n with repetition
  - k balls into n urns: k balls add $n-1$ dividers
  - sol number of $x_1 + \cdots + x_n = k, x_i \geq 0$
  - k is total number of samples, x_i counts times of sampled i
  - $C(n,k)$ with repetition $= \binom{n+(k-1)}{k} = \binom{k+(n-1)}{n-1} = \frac{(k+n-1)!}{k!(n-1)!}$
- Pigeonhole principle: if $n = km + 1$ balls into m bins, at least 1 bin contain at least $k+1$ objects $k + 1 = \lfloor \frac{n-1}{m} \rfloor + 1 = \lceil \frac{n}{m} \rceil$

7.6. Probability and statistic.

- cards
  - face cards: jacks, queens, and kings
  - clubs, diamonds, hearts and spades
- a Boolean algebra E of sets on S is a nonempty subfamily of power set of S: $E \subseteq P(S)$ s.t.
  - $A, B \in E \to A \cap B, A \cup B \in E$
  - $A \in E \to \overline{A} \in E$
- a probability measure on E is a function $P : E \to [0,1]$, s.t.
  - $P(\varnothing) = 0$

  - $P(S) = 1$
  - $P(A \cup B) = P(A) + P(B)$ for disjoint sets $A, B \in E$
- probability space: sample space S of outcomes, event space E of events and probability measure P
- events are subsets of sample space
- $\Pr(A \cup B) = \Pr(A) + \Pr(B) - \Pr(A \cap B)$
- independent: $\Pr(A \cap B) = \Pr(A)\Pr(B)$
- exclusive: $\Pr(A \cup B) = \Pr(A) + \Pr(B)$ or $\Pr(A \cap B) = 0$
- Bernoulli trials are independent success or failure events
  $\Pr(k \text{ successes}) = \binom{n}{k} p^k (1-p)^{n-k}$
- a random variable is a function $X : S \to \mathbb{R}$ assigning outcomes to real numbers
  distribution function of X: $F_X(t) = P(\{\omega : X(\omega) \leq t\})$
  probability density function of X: $f_X(t) = \frac{d}{dt} F_X(t)$
- $\mathbf{E}X = \int xp(x)dx$, $\mathbf{Var}X = \mathbf{E}X^2 - (\mathbf{E}X)^2$, std: $\sigma(X) = \sqrt{\mathbf{Var}X}$
- Gaussian distribution: $X \sim \mathcal{N}(\mu, \sigma^2) = \frac{1}{\sqrt{2\pi\sigma^2}} e^{\frac{(x-\mu)^2}{2\sigma^2}}$
  $\Phi(-z) = 1 - \Phi(z)$
- $\Phi(0.5) = 0.69$, $\Phi(1) = 0.84$, $\Phi(1.5) = 0.93$, $\Phi(2) = 0.97$, $\Phi(2.5) = 0.99$, $\Phi(3) \sim 1$
- standard normal distribution: $Z \sim \frac{1}{\sqrt{2\pi}} e^{\frac{x^2}{2}}$; $\Phi(z) = \int_{-\infty}^{z} \frac{1}{\sqrt{2\pi}} e^{\frac{x^2}{2}} dx$
- normal approximation to binomial distribution:
  $\Pr(a \leq X \leq b) = \sum_{k=a}^{b} \binom{n}{k} p^k (1-p)^{n-k} \sim \Phi(\frac{b-np}{\sqrt{npq}}) - \Phi(\frac{a-np}{\sqrt{npq}})$
- Poisson approximation to binomial distribution: $\binom{n}{k} p^k (1-p)^{n-k} \sim e^{-np} \frac{(np)^k}{k!}$

7.7. Point Set topology.

- X is a nonempty set, a topology $T \subseteq 2^X$ on X is a set of subsets of X s.t.
  - $\varnothing, X \in T$
  - close under arbitrary union
  - close under finite intersection
- members in T are open sets (including empty set), complement of open sets are closed set
- topological space: (X, T):
  $\{\varnothing, X\}$ is trivial topological space (coarsest). power set 2^X is the discrete topology (finest)
- O is open if $\forall x \in O, \exists \epsilon > 0, \{x' : |x - x'| < \epsilon\} \subseteq O$, it doesn't contain any of its boundary points
- closed set is a set which contains all its limit points
- collection of open sets is a topology on $\mathbb{R}$
- subspace topology: given a topological space (X, T), a subset $S \subseteq 2^X$ is open in X
  if $S \supseteq U = O \cap S$, where O is open in X

  - interior $int(A)$: the largest open set contained in A, i.e. $int(A) = A \setminus bd(A)$
  - exterior $ext(A)$: union of all open sets do not intersect A, i.e. $int(\overline{A})$
  - boundary $bd(A)$: a set of all point x s.t. every open set containing x intersects A and $\overline{A}$
  - limit point of A: a point x s.t. every open set containing x also contains at least one point of A other than x
  - derived set A': the set of all limit points of A
  - closure $cl(A)$: $int(A) \cup bd(A) = A \cup A'$
  - closure $cl(A)$ is the smallest closed set containing A
  - A is closed $\Leftrightarrow$ it contains all boundary points and limit points
  - boundary points are not necessarily limit points: isolated points

$$A = (0,1) \cup (1,2)$$
$$int(A) = A, ext(A) = (-\infty, 0) \cup (2, \infty), bd(A) = [0, 1, 2], A' = [0, 2], cl(A) = [0, 2]$$
$$int(\mathbb{Z}) = \mathbb{Z}, ext(\mathbb{Z}) = \cup_{n \in \mathbb{Z}}(n-1, n), bd(\mathbb{Z}) = \mathbb{Z}, \mathbb{Z}' = \varnothing, cl(\mathbb{Z}) = \mathbb{Z}$$

  - The interior, boundary, and exterior of a set together partition the whole space
  - The interior and exterior are always open while the boundary is always closed
  - Every point of a set is either an interior point or a boundary point
  - Isolated points are always boundary points
  - $(0, 1]$ is neither close nor open because it contains only part of boundary
  - $\mathbb{Q}$ and $\mathbb{R} \setminus \mathbb{Q}$ are neither close nor open, they are dense and disjoint
    $int(\mathbb{Q}) = int(\mathbb{R} \setminus \mathbb{Q}) = \varnothing, cl(\mathbb{Q}) = cl(\mathbb{R} \setminus \mathbb{Q}) = \mathbb{R}, bd(\mathbb{Q}) = bd(\mathbb{R} \setminus \mathbb{Q}) = \mathbb{R}$
  - empty, $\mathbb{R}$ are both open and closed

- basis $\mathbf{B}$ is a collection of subsets of X s.t
  - $\forall x \in X$, $\exists B \in \mathbf{B} : x \in B$
  - $B_1, B_2 \in \mathbf{B}$, $x \in B_1 \cap B_2$, $\exists B_3 \in \mathbf{B} : x \in B_3 \subseteq B_1 \cap B_2$
- $\mathbf{B} = \{(a, b) \in \mathbb{R} : a < b\}$ of all open intervals is a basis for standard topology on $\mathbb{R}$
- $\mathbf{B} = \{[a, b) : a, b \in \mathbb{R}, a < b\}$ is a basis for low-limit topology on $\mathbb{R}$
- product topology: a topology on Cartesian product of sets: $\mathbf{B} = \{O_X \times O_Y : O_X \in T_X, O_Y \in T_Y\}$
- disconnected: there exists disjoint, nonempty open set $O_1, O_2 : O_1 \cup O_2 = X$
  - A, B are connected and intersect, union is connected
  - A is connected, $B : A \subseteq B \subseteq cl(A)$ is connected
  - Cartesian product of connected spaces is connected
  - x_1, x_2 are path-connected: $\exists$ continuous f: $[0, 1] \to X$, $f(0) = x_1$, $f(1) = x_2$
  - any path-connected space is connected
  - the intervals are the only connected subspaces of $\mathbb{R}$
- A subset A of $\mathbb{R}^n$ is said to be bounded if it is contained in some open rectangle
- a covering of X is a collection of subsets whose union is X, if subsets are open set, it is open covering
- compact space: every open covering of X contains a finite subcollection that covers X
  - $\mathbb{R}$ is not compact because no finite subcollection of $\{(n-1, n+1) : n \in \mathbb{Z}\}$ covers $\mathbb{R}$
  - trivial topology is compact
  - $(0, 1)$ is not compact: $A = \{(\frac{1}{n}, 1 - \frac{1}{n}) : n = 3, 4, \dots)\}$

  - $[0, 1]$ is compact
  - X is compact topological space, closed subset $S \subseteq X$ is compact
  - Compact subsets of Hausdorff space are closed.
  - Cartesian product of compact spaces is compact
- Heine-Borel theorem: a subset of $\mathbb{R}^n$ is compact $\Leftrightarrow$ it is closed and bounded (the norm of every point is less than certain real)
- X is nonempty set, $d : X \times X \to \mathbb{R}$ is a metric on X if
  - $d(x, y) = d(y, x)$
  - $d(x, y) \geq 0, d(x, x) = 0$
  - $d(x, y) \leq d(x, z) + d(z, y)$
- metric space (X, d)
- ε-ball: $B_d(x, \varepsilon) = \{x' \in X : d(x, x') < \varepsilon\}$
- metric topology induced by d: topology for metric space generated by collection of all ε-balls:
  $\mathbf{B} = \{B_d(x, \varepsilon) : x \in X, \varepsilon > 0\}$
- open set O is open $\Leftrightarrow \forall x \in O$, x is contained in some ε-ball contained in O, i.e.
  $\forall x \in O, \exists \varepsilon_x, B_d(x, \varepsilon_x) \subseteq O$
- (X_1, d_1), (X_2, d_2) are metric spaces, $f : X_1 \to X_2$ is continuous at x_0 if
  $\forall \varepsilon > 0, \exists \delta : d_1(x, x_0) < \varepsilon \to d_2(f(x), f(x_0)) < \delta$, i.e.
  $\forall O \subseteq X_2 : f(x_0) \in O$, inverse image $f^{-1}(O)$ is an open set containing x_0
- (X_1, T_1), (X_2, T_2) are topological spaces, $f : X_1 \to X_2$ is continuous if $\forall O \in T_2$, inverse image $f^{-1}(O) \in T_1$
- given a **continuous function** between topological spaces (X_1, T_1), (X_2, T_2)
  - $f^{-1}(C)$ is closed in X_1 for every closed subset $C \subset X_2 \Leftrightarrow f$ is continuous
  - $C \subseteq X_1$ is connected, $f(C)$ is a connected subset in X_2
  - $C \subseteq X_1$ is compact, $f(C)$ is a compact subset in X_2
- open map: image of open set is open
- homeomorphism: f is bijective, f and f^{-1} are continuous
  one-to-one correspondence between X_1 and X_2 and open sets, they are topologically identical
- Hausdorff space: every pair of distinct points $x, y \in X$, there exists disjoint open set $O_1, O_2 : x \in O_1, y \in O_2$
- Compact Hausdorff space: f is a bijective, continuous map of topological spaces, X_1 is compact and X_2 is Hausdorff, then f is homeomorphism(f^{-1} is continuous)
- Every subspace of a Hausdorff space is a Hausdorff space
- Compact sets in Hausdorff spaces are always closed

7.8. **Real analysis.**

- a lower bound of a set of reals X is a number a s.t. $\forall x \in X, a \leq x$, $\inf X$ is the greatest lower bound
- a upper bound of a set of reals X is a number a s.t. $\forall x \in X, a \geq x$, $\sup X$ is the least upper bound
- least upper bound axiom: if a set of reals has an upper bound, then there's exactly one supremum
- every sequence of reals want to converge can find a real to converge to
- a sequence of reals x_i is a Cauchy sequence if $\forall \varepsilon, \exists N \in \mathbb{Z}, \forall m, n \geq N, |x_m - x_n| < \varepsilon$
- convergent implies Cauchy, Cauchy implies convergent only if metric space is complete: every Cauchy sequence of reals converges
- a metric space in which every Cauchy sequence converges is a complete space(contains limits)
- Lebesgue measurable set: $M \subseteq \mathbb{R}$ is Lebesgue measurable $\Leftrightarrow \forall A \subseteq R : \mu^\star(A) = \mu^\star(A \cap M) + \mu^\star(\overline{A} \cap M)$, with $\mu^\star(A) = \inf\{\sum_{i=1}^{\infty}(b_i - a_i) : A \subset \cup_{i=1}^{\infty}(a_i, b_i)\}$
    - a measurable set M with $\mu(M) = 0$ is a set of measure zero, singleton set has zero measure
    - finite or countably infinite sets has measure zero: $\mu(\mathbb{Z}) = 0$, $\mu(\mathbb{Q}) = 0$ $\forall k \in \mathbb{Z}^+ : a_k \in (a_k - \frac{\varepsilon}{2^{k+1}}, a_k + \frac{\varepsilon}{2^{k+1}})$, $\mu(\{a_k\}_{k=1}^{\infty}) = \sum_{k=1}^{\infty} \frac{\varepsilon}{2^k} = \varepsilon$
    - every open, close set in $\mathbb{R}$ is measurable
    - every finite or countably infinite subset of $\mathbb{R}$ is measurable
    - complement of a measurable set is measurable
    - a finite or countably infinite union or intersection of measurable sets are measurable
    - $\mu((a, b)) = \mu((a, b]) = \mu([a, b)) = \mu([a, b]) = b - a$
    - $M_1 \subseteq M_2 \rightarrow \mu(M_1) \leq \mu(M_2)$
- Lebesgue measurable function: $\forall$ open set $O \subseteq R$, the inverse image $f^{-1}(O)$ is a Lebesgue measurable set
    - every continuous function is measurable
    - sum, difference and product of measurable functions are measurable
- characteristic function of $A \subseteq \mathbb{R}$: $\chi_A(x) = 1$ if $x \in A$, 0 if $x \notin A$ is measurable $\leftrightarrow$ A is a measurable set
- step function: a finite, linear combination (with real coefficients) of characteristic functions: $s(x) = \sum_{i=1}^{n} a_i \chi_A(x)$
- if f is measurable, there exists a sequence of step functions with limit being f
- step function $s = \sum_{i=1}^{n} a_i \chi_A$ is Lebesgue integrable if $a_i \neq 0 \rightarrow \mu(A_i) < \infty$ $\int s d\mu = \sum_{i=1}^{n} a_i \mu(A_i)$
- if every step function s, $s \geq 0$, $s \leq f$ is integrable and $\int s d\mu$ is finite f is Lebesgue integrable: $\int f d\mu = \sup_{s: s \leq f} \int s d\mu$
- arbitrary measurable function f is Lebesgue integrable if $f^+ = \frac{|f|+f}{2}$ and $f^- = \frac{|f|-f}{2}$ are Lebesgue integrable $\int f d\mu = \int f^+ d\mu - \int f^- d\mu$
- Lebesgue integral: split the domain of f into subintervals R_i and form step functions $s = \sum_i a_i \chi_{f^{-1}(R_i)}$ to approach f, $f^{-1}(R_i)$ is a measurable set
- For $f(x) = \mathbf{1}\{x \in \mathbb{Q}\}$:
    - $\{x : f(x) \neq 0\}$ has measure 0
    - Lebesgue integrable, not Riemann integrable
    - discontinuous and nondifferentiable everywhere

7.9. **Complex analysis.**

- complex numbers $\mathbb{C}$ is the set of all ordered pairs of reals (x, y) with + and × with identity $(0, 0)$ and $(1, 0)$
- $|z|^2 = z\overline{z}$
- principal argument of z: $Argz \in (-\pi, \pi)$
- $z = r(\cos\theta + i \sin\theta)$
- $(e^{ix})^n = (\cos x + i \sin x)^n = \cos nx + i \sin nx$
- n-th root of unity: $z^n = 1$: $e^{i\frac{2\pi k}{n}}$
- principal log: $Logz = \log|z| + iArgz$
- $e^{i\pi} + 1 = 0$
- principal value of z^w is e^{wLogz}
- $\cos x = \frac{e^{ix}+e^{-ix}}{2}$, $\sin x = \frac{e^{ix}-e^{-ix}}{2}$
- $\cos z$ and $\sin z$ are unbounded
- Cauchy-Riemann equations $\frac{\partial u}{\partial x} = \frac{\partial v}{\partial y}$, $\frac{\partial u}{\partial y} + \frac{\partial v}{\partial x} = 0$
- function is harmonic in some open set O if Laplace equation is satisfied $\frac{\partial^2 u}{\partial x^2} + \frac{\partial^2 v}{\partial y^2} = 0$
- if $f(z)$ is differentiable in open set O, it is harmonic in O

- if $f(z)$ is differentiable at z_0, and at every point in some open set containing z_0, it is analytic at z_0
  this means that f can be differentiable at infinite points, it is analytic nowhere
- if $f(z)$ is differentiable in open set O, it is analytic in O
- derivatives of all orders of a analytic function is analytic
- Cauchy theorem: f is analytic in a simply connected open set D, for any closed path C in D: $\oint_C f(z)dz = 0$
- Morera's theorem is the converse of Cauchy theorem
- $\oint_C \frac{dz}{z-a} = 2\pi i$, $\oint_C \frac{dz}{(z-a)^n} = 0$
- Cauchy integral formula: if f is analytic at all points within and on a simple closed path surround z_0: $f(z_0) = \frac{1}{2\pi i}\oint_C \frac{f(z)}{z-z_0}dz$, $f^{(n)}(z_0) = \frac{n!}{2\pi i}\oint_C \frac{f(z)}{(z-z_0)^{n+1}}dz$
- Liouville theorem: if $f(z)$ is an entire function (analytic everywhere in complex plane) that's bounded, f must be a constant function
- if f is analytic and not a constant in an open connected subset O, $|f|$ has no maximum in O; if O is bounded, $|f|$ achieve a maximum in cl(O).
  maximum value is attained at some boundary points
- Taylor series: z_0 is a point in disk of convergence with $R = \frac{1}{\lim_{n\to\infty}|a_n|^{\frac{1}{n}}}$ in a analytic open set O:
  $f(z) = \sum_{n=0}^{\infty} \frac{f^{(n)}(z_0)}{n!}(z-z_0)^n$
- f is analytic in a punctured open disk $0 < |z - z_0| < R$, z_0 is the isolated singularity of f
- z_0 is a pole of order n: $f(z) = \frac{g(z)}{(z-z_0)^n}$
- f is analytic in annulus: $R_1 < |z - z_0| < R_2$, then f can be expanded into Laurent series:
  $\sum_{n=1}^{\infty} a_{-n}(z-z_0)^{-n} + \sum_{n=1}^{\infty} a_n(z-z_0)^n$
  $a_n = \frac{f^{(n)}(z_0)}{n!} = \frac{1}{2\pi i}\oint_C \frac{f(z)}{(z-z_0)^{n+1}}dz$,
  singular part / Laurent coefficients $a_{-n} = \frac{1}{2\pi i}\oint_C \frac{f(z)}{(z-z_0)^{-n+1}}dz$,
  C is a simple closed positively oriented curve in annulus
- if $a_{-n} = 0$ for $n > k$, z_0 is a pole of order k, singular part contains infinite terms, essential singularity
- $a_{-1} = \frac{1}{2\pi i}\oint_C f(z)dz$ is the residue of f at z_0
- $Res(z_0, f) = \frac{1}{(k-1)!}\lim_{z\to z_0} \frac{d^{k-1}}{dz^{k-1}}[(z-z_0)^k f(z)]$
- residue theorem: $\oint_C f(z)dz = 2\pi i \sum_i Res(z_i, f)$

7.10. Numerical analysis.

- Bisection method
- Newton's method: find zeros of real-value function:
  $f(x_{n+1}) \sim f(x_n) + f'(x_n)(x_{n+1} - x_n) = 0 \to x_{n+1} = x_n - \frac{f(x_n)}{f'(x_n)}$

8. Tricks and classic problems

8.1. Combinatoric and probability.

- Two players, A and B, alternately and independently flip a coin and the first player to get a head wins. Assume player A flips first. If the coin is fair, what is the probability that A wins? $\frac{1}{2}p + \frac{1}{2}(1-p) = p$, $p = \frac{2}{3}$ A wins probability $\sum_{k=0}^{\infty} \frac{1}{2^{2k+1}} = \frac{1}{2}\frac{4}{3} = \frac{2}{3}$
- Tossing coin and drawing dice alternately, $\Pr(H$ before 5 or 6$)$?
  winning cases are H before $5, 6$: $(T, \text{not } 56)$, $(T, \text{not } 56)$, ... H. $\Pr = \frac{1}{2}\sum_{i=0}^{\infty}(\frac{1}{2}\frac{2}{3})^i = \frac{1}{2}\frac{1}{1-\frac{1}{3}} = \frac{3}{4}$
- Fair coins are tossed and when either four consecutive heads and tails appear the process will be stopped. What is the probability of two consecutive head or tail or any one of them in a row?
  Transient states are H, T, TT, TTT; Absorbing states are HH, TTTT
- Fair coins are tossed and when HHH or THH appear the process will be stopped. What is the probability that you get HHH before THH?
  Transient states are H, T, HH, TH; Absorbing states are HHH, THH
  Simple idea: for every HHH, last two HH has to appear, and it matches last two H of THH, so that the first has to be H, or else it will be THH. $\frac{1}{8}$
- Derangement: fix-point-free permutation. $D(n) = (n-1)[D(n-1) + D(n-2)]$
- n lines separate the space into $1 + \frac{n(n+1)}{2}$ parts
- sum of degree of all the vertices of a graph is even

8.2. Linear Algebra.

- A, B are subspaces of a vector space V, $A \cap B$ is a subspace of V, $A \cup B$ is not necessarily a subspace.
- number of invertible $n \times n$ matrices in $GL_n(F)$, $|F| = p$: $\prod_{i=1}^{n}(q^n - q^{n-i})$. For $n = 2$, $q^4 - q^3 - q^2 + q$
- When the vector space is finite-dimensional, the automorphism group of V is the same as the general linear group, $GL(V)$, dimension is n^2
- $tr(AB) = tr(BA) \neq tr(A)tr(B)$
- $tr(A^k) = \sum \lambda_i^k$
- Notice that $tr(A^2)$ can be negative, $A = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$, $A^2 = \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}$. $tr(A^2) \geq 0$ if the eigenvalues are real
- number of invertible $n \times n$ matrices in $GL_n(F)$, $|F| = p$: $\prod_{i=1}^{n}(q^n - q^{n-i})$. For $n = 2$, $q^4 - q^3 - q^2 + q$
- Idempotent matrix: $A^2 = A$. An idempotent matrix is always diagonalizable and its eigenvalues are either 0 or 1 a square invertible idempotent matrix is the identity matrix
- matrices can be diagonalizable but not invertible, invertible but not diagonalizable
- linear space $\{0\}$ does not have a basis, it is not a linearly independent set, it has dimension 0
- A set containing a zero vector is linearly dependent, a basis cannot contain zero vector
- product of upper/lower triangular matrix is still upper/lower triangular matrix
- $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}^n = \begin{pmatrix} 1 & n \\ 0 & 1 \end{pmatrix}$
- $A = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$, $A^2 = I$: $e^{tA} = \sum_{i=0}^{\infty} \frac{t^i A^i}{i!} = (\sum_{i=0}^{\infty} \frac{t^{2i}}{(2i)!})I + (\sum_{i=0}^{\infty} \frac{t^{2i+1}}{(2i+1)!})A$
- $rk \begin{pmatrix} 1 & 2 & 3 \\ 4 & 5 & 6 \\ 7 & 8 & 9 \end{pmatrix} = 2$
- dimension of n by n symmetric matrix is $\frac{n(n+1)}{2}$
- The set of all such polynomials of degree $\leq n$ is denoted P_n, it is a vector space, isomorphic to $\mathbb{R}^{n+1}$
- n by n matrices A and B are similar if $B = P^{-1}AP$, P is some invertible matrix. They represent the same linear operator with respect to different bases. They have the same eigenvalues, thus the same trace and det
- orthogonality $Q' = Q^{-1}$ is a more restrictive criterion than linear independence, basis are not necessarily orthogonal, determinant and eigenvalues are all $+1$
- Orthogonal matrices preserve the dot product: $u \cdot v = Qu \cdot Qv = (Qu)'Qu = u'v$
- elementary row operations are invertible, A square matrix A is invertible if and only if it can be written as the product of elementary matrices
- eigenvalues of triangular matrices are the elements of the main diagonal
- nilpotent matrix is a square matrix A such that $A^k = 0$, only eigenvalue is 0
- Every singular matrix can be written as a product of nilpotent matrices

- $(I-A)^k = 0$, A is invertible. $(I-A)x = 0x$, $(I-A-I)x = (0-1)x = -x = -Ax$, $Ax = x$

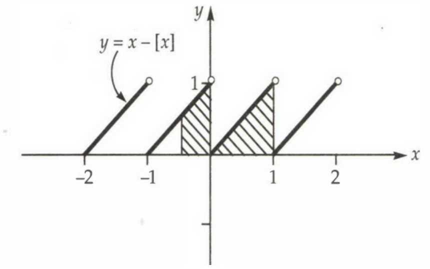
8.3. Abstract algebra and Number theory.

- some primes: 2 3 5 7 11 13 17 19 23 29
- 100! ends with how many consecutive 0?
  since $100! = c2^p5^q : p > q$, we need to count number of factor 5. $100 = 5*20 = 25*4$, $q = 24$
  More general: $k!$ will have $\sum_{i=1}^{\infty}\lfloor\frac{k}{5^i}\rfloor$ 0 at end. 400 has 99 0 at end
- $11^{100} - 1$ ends with how many consecutive 0?
  $\binom{100}{i}10^i - 1 = 100*10 + \frac{100*99}{2}*100 + \frac{100*99*98}{3*2}*1000 + \dots$ 3
- solutions of $x^{12} - x^{10} = 2$ in field $\mathbb{Z}_{11}$
  $x^{12} - x^{10} = x^{10}(x^2-1) \equiv 2(mod\ 11)$, from Fermat little theorem: $x^{10} \equiv 1(mod\ 11)$, $x^2 \equiv 3(mod\ 11)$, $x = 5, 6$
- how many non-isomorphic Abelian groups are there of order p^2q^4, $gcd(p,q) = 1$
  Since every finite Abelian group is finitely generated. Elementary divisors for p^2q^4:
  p^2: $1(p^2) + 1(p*p)$, q^4: $1(q*q*q*q) + 1(q*q*q^2) + 2(q*q^3, q^2*q^2) + 1(q^4)$. 10
- Any finite group G of even order contains an element of order 2
  $\exists a \in G : a^2 = e$. Contradiction: $\forall a \in G : a^{-1} \neq a$, cardinality of $G \setminus e$ will be even, which is false.
- All groups of prime order p are cyclic
  From the Lagrange theorem, order of subgroup has to be p, expect for $\{e\}$, thus the order of cyclic subgroup generated by any element is p, thus G can be generated by any element in the group
- There are at least two non-isomorphic groups of even order greater than 2: cyclic and dihedral
- Subgroups of $\mathbb{Z}$ are of form $n\mathbb{Z}$ for some $n \in \mathbb{Z}$
  A proper subgroup of $\mathbb{Z}$ is the set of integral multiples of some nonnegative int other than 1
- homomorphism f for a cyclic group is determined by $f(1)$
- homomorphism $f : G \to H$, $x \in G$, order of x divides order of $f(x)$
- the number of group homomorphisms $f : \mathbb{Z}_m \to \mathbb{Z}_n$ is $gcd(m,n)$
- $\forall a, b, c \in \mathbb{R} : a + b\sqrt[3]{2} + c\sqrt[3]{4}$ is a field
- A complement of subgroup is not a subgroup since it does not contain the identity.
- Irrationals are not closed under addition or multiplication. $\sqrt{2}\sqrt{2} = 2$, $(1-\sqrt{2}) + \sqrt{2} = 1$
- a, b has finite order in group G: $a^m = b^n = e$
  - $ab = ba \to ab$ has finite order: $(ab)^{mn} = a^{mn}b^{mn}$
  - ab has finite order $\to ba$ has finite order: $(ba)^{k+1} = b(ab)^k a = ba$
  - ab has finite order $\to a^{-1}b^{-1}$ has finite order: $a^{-1}b^{-1} = (ba)^{-1}$, from 2, $(ba)^k = e$, $a^{-1}b^{-1}$ has the same order
- The composition of functions is always associative, thus form a semigroup
- G is a group of exactly one non trivial proper subgroup, then G is cyclic and order is p^2
- a ring with $x^2 = x$.
  - $x + x = (x+x)^2 = 4x^2 = 2(x+x) \to x + x = 0$
  - $s + t = (s+t)^2 = s^2 + st + ts + t^2 = s + st + ts + t \to st + ts = 0 \to st = ts$
- $10^n \equiv 4(mod\ 6) : n \geq 1$
- $10^{10^{10}} \equiv 4(mod\ 7)$: $10^{6k} \equiv 1(mod\ 7)$, $10^{10} \equiv 4(mod\ 6)$, thus $10^{10^{10}}(mod\ 7) \equiv 10^4(mod\ 7)$
- product of two consecutive even numbers is always divisible by 8
- $p^2 - 1$ is divisible by 24. For $p-1, p, p+1$, they are divisible by $2, 3, 4$
- $p^4 - 1$ is divisible by 240, by Fermat, $p^4 \equiv 1(mod\ 5)$, $p^4 - 1 = (p-1)(p+1)(p^2+1)$, they are even, one of $p-1, p+1$ is divisible by 4, it is divisible by 16, $p^2 - 1$ is divisible by 3, 240
- The kernel of a homomorphism is a normal subgroup
- All groups less with order less than 6 are cyclic
  This is because 2, 3, and 5 are prime. By Lagrange's Theorem, any element that is not the identity in these groups must have an order that is the same as the group's order. This means that all groups of order 2, 3 and 5 are cyclic.
- the smallest non-Abelian group is the dihedral group of order 6
- a subgroup of a finitely generated group need not be finitely generated
- Abelian group, $gcd(|a|, |b|) = 1$, $|ab| = |a||b|$
- Subset S is a generating set of G if $\forall g \in G : g = x_1^{a_1} \dots x_n^{a_n}, x_i \in S, a_i \in \mathbb{Z}$
- G is generated by a, b, $|a| = 16$, $a^2 = b^3$, $|G| =$?
  $\forall k \in \{0, \dots, 7\} : a^n b^m = a^{(n+2k) mod\ 16} b^{(m-3k) mod\ 24}$. $\frac{16*24}{8} = 48$

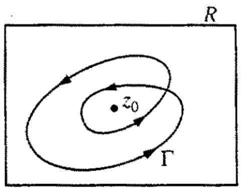
- R is a ring, additive subgroup I is a right ideal if $\forall r \in R, \forall i \in I : ir \in I$
  $\{0\}$ and R are ideals in every ring R. If R is a division ring or a field, then these are its only ideals
- Conjugacy class: two elements $a, b \in G$ are conjugate, if there exists an element $g \in G : gag^{-1} = b$, it is an equivalence relation, if $x \in G$ commute with everything, $cl_G(x) = \{x\}$, $cl_G(e) = \{e\}$
- Every element of S_n can be written as the product of disjoint cycles
- $\sigma_1, \sigma_2 \in S_n$ are conjugate iff they have the same cycle decomposition. The number of conjugacy classes in S_n equals the partition of n.
  For S_4: (4), (3)(1), (2)(2), (1)(1)(2), (1)(1)(1)(1)(1)
- The order of the product of disjoint cycles is the least common multiple of the orders of those cycles
- generator of group of units of ring Z_{17}, since 17 is a prime, elements from 1 to 16 are all units, they form a group under multiplication, the order is 16,
- P is a prime ideal for commutative ring R if $a, b \in R : ab \in P$, then $a \in P$ or $b \in P$, and P is not R

8.4. Analysis and Topology.

- $\sum_{i=2}^{\infty} \frac{1}{n \ln n}$ does not converge because $\int_2^\infty \frac{dx}{x \ln x} = \int_2^\infty \frac{d(\ln x)}{\ln x} = \ln \ln x\Big|_2^\infty = \infty$
- $f(x) = x - [x]$



- $f : [a, b] \to \mathbb{R}$, if $\forall x, y \in [a, b] : |f(x) - f(y)| \le (x - y)^2$, then f is a constant
  $|f'(x)| = \lim_{x \to y} |\frac{f(x)-f(y)}{x-y}| \le \lim_{x \to y} \frac{(x-y)^2}{|x-y|} = \lim_{x \to y} |x - y| = 0$
- $g = x^3 + x^2 + x + 1$, $f = \frac{1}{g^{-1}(x)}$, $f^{-1}(-2) =?$
  $-2 = \frac{1}{g^{-1}(x)} \to g^{-1}(x) = -\frac{1}{2} \to g(-\frac{1}{2}) = \frac{5}{8}$
- The only periodic polynomials are constants
- $x^{x^{x^{x^{\cdots}}}} = 2$, $x =?$ $2 = x^{x^{x^{x^{\cdots}}}} = x^2$, $x = \sqrt{2}$
- Independently at random choose $x, y, z \in [0, 1]$, $\Pr(x \ge yz)$?
  $\int_0^1 \int_0^1 (1 - yz) dy dx = \frac{3}{4}$
- Rademacher's theorem: every Lipschitz function is almost everywhere differentiable: undifferentiable points form a set of Lebesgue measure zero
- If two lines intersect at right angles, they are by definition perpendicular.
- $x|x|$ is differentiable everywhere!



- $Res(z_0, f) = 1$, $\int_\Gamma f(z) dz = 4\pi i$
- reals form an uncountable set, of which the rationals are a countable subset, the complementary set of irrationals is uncountable
- Harmonic series: $H_n := 1 + \frac{1}{2} + \cdots + \frac{1}{n}$, $\ln n + \frac{1}{n} < H_n < \ln n + 1$
- $\lim_{n \to \infty} \frac{1}{n} + \frac{1}{2+n} + \cdots + \frac{1}{3n} = \frac{1}{2}(H_{3n} - H_n) = \frac{1}{2} \ln \frac{3n}{n} = \frac{1}{2} \ln 3$
- $\forall x \ge 1 : \frac{f(x)}{x} = \frac{f(1)}{x} + \frac{\int_1^x f'(t) dt}{x}$
- Two points are randomly placed on a line of length 1. What is the probability that the three segments created could form a triangle?
  $(x, y, 1 - x - y)$, $x + y < 1$, $x + y < 0.5$, $x < 0.5$, $y < 0.5$, 0.25

- Uniform convergence: $\forall \varepsilon > 0 : \exists N : n \geq N, \forall x : |f_n(x) - f(x)| < \varepsilon$. N depends on ε, not x
  Pairwise convergence : $\forall x : \lim_{n\to\infty} f_n = f$, N depends on ε and x : at every point the sequence of functions has its own speed of convergence
  $f_n(x) = \frac{x}{n}$ converge pointwise but not uniformly to 0. $N \geq \frac{|x|}{\varepsilon}$
- continuity depends on ε and x, uniform continuity only depends on ε
- $a_n + \alpha a_{n-1} + \beta a_{n-2} = 0$, characteristic equation: $x^2 + \alpha x + \beta = 0$:
  2 roots : $a_n = ar_1^n + br_2^n$; 1 root: $a_n = ar^n + bnr^n$
- $\int_0^\infty \frac{\sin x}{x} dx = \frac{\pi}{2}$
- Intervals are the only connected subsets of $\mathbb{R}$ with the usual topology (topology generated by all open intervals)
- The continuous image of a connected space is connected
- A continuous function on an interval is one-to-one $\Leftrightarrow$ it is either increasing or decreasing throughout the interval, it cannot have local extreme values
- There is no continuous map $[0, 1] \to (0, 1)$, from Heine-Borel, $[0, 1]$ is compact and its image is compact
- continuous surjection $\sin^2(2\pi x)$ maps $(0, 1)$ to $[0, 1]$
- $\frac{1}{1+e^x}$ maps $\mathbb{R} \to (0, 1)$
- Every nonempty compact connected set in $\mathbb{R}$ is of the form $[a, b]$
- all metric spaces are Hausdorff
- $f : X \to Y$, $g : Y \to Z$: if $g \circ f$ is injective, f is injective. if $g \circ f$ is surjective, g is surjective
- compact but not connected : Any finite subset of $\mathbb{R}$ with 2 or more elements
- connected Hausdorff but not compact : $(0, 1)$
- compact connected not Hausdorff: $[0, 1]$
- comparison of a^b and b^a: $e^{b \ln a}$, $e^{a \ln b}$: $e^{\frac{\ln a}{a}}$, $e^{\frac{b}{b}}$, consider $\frac{\ln x}{x}$.
- two tangent balls are connected subset, but interior are not connected
- closure of a connected set is always connected
- Lipschitz continuous implies uniformly continuous
- $\sin x$ is uniformly continuous, $\sin(x^2)$ is not
- $\sqrt{x}$ is uniformly continuous on $[0, \infty)$, it is Lipschitz on $[1, \infty)$. It is not Lipschitz on $(0, 1]$, it has unbounded derivatives
- Invariance of domain: image of an open set in $\mathbb{R}$ under a continuous injection into $\mathbb{R}$ is open
- bounded derivative implies uniform continuity
- f has a vertical asymptote, it is not uniformly continuous
- $f(x) = \left\{ \begin{array}{cc} 1 & x \in \mathbb{Q} \\ e^x & x \notin \mathbb{Q} \end{array} \right.$: is discontinuous at any nonzero x, it is continuous at 0!
- Weierstrass function is continuous everywhere but differentiable nowhere
- $\sum_{i=1}^\infty \frac{k^2}{k!} = \sum_{i=1}^\infty \frac{k}{(k-1)!} = \sum_{i=1}^\infty \frac{1}{(k-1)!} + \sum_{i=2}^\infty \frac{1}{(k-2)!} = 2e$
- Schroder-Bernstein theorem: if there exist injective functions $f : A \to B$ and $g : B \to A$, then there exists a bijective function $h : A \to B$
- any path-connected space is connected
- Topologist's sine curve: $T = \left\{ \left(x, \sin \frac{1}{x}\right) : x \in (0, 1] \right\} \cup \{(0, 0)\}$ is connected but neither locally connected nor path connected, there is no way to link the function to the origin so as to make a path. Any open set that contains $(0, 0)$ must intersect with the other part of the curve, so $(0, 0)$cannot lie in a disconnected component, thus it is connected.
  $\sin(\frac{1}{x})$ is continuous for nonzero x. $\lim_{x\to 0} \sin(\frac{1}{x})$ does not exist, there is no way to extend this function by continuity on 0
- Integral of inverse functions: $\int f^{-1}(y)dy = yf^{-1}(y) - F(f^{-1}(y))$
- Rational density theorem: For any real a and b numbers such that $b > a$, there exist a rational number x such that $a < x < b$: $cl(\mathbb{Q}) = \mathbb{R}$
- $\mathbb{R} \setminus \{\pi\}$ is a open set containing all rationals.
- $\mathbb{Q} \cup (0, 1)$ is an uncountable set containing all rationals, it is not open
- $(x - y)^2$ is not a metric
- the number of functions from A to B is $|B|^{|A|}$
- $|\mathbb{N}| = |\mathbb{Z}|$, $|\mathbb{R}| = |\mathbb{R}^n| = |\mathbb{C}|$
- $|\{f : \mathbb{Z} \to \mathbb{Z}\}| = |\mathbb{Z}|^{|\mathbb{Z}|} = 2^{|\mathbb{Z}|} = |\mathbb{R}|$
- the number of the set of all finite subset of $\mathbb{R}$ is $|\mathbb{R}|$
- the number of all polynomials with coefficient in $\mathbb{R}$ is $|\mathbb{R}|$

- A countable sum of copies of $\mathbb{R}$ has the same cardinality as $\mathbb{R}$
- Every continuous real valued function on a compact set attains its minimum and maximum
- Heine-Cantor theorem: a function is continuous on a compact set is uniformly continuous on this set
- Let K be a nonempty subset of $\mathbb{R}^n$, where $n \geq 1$. If every continuous real-valued function defined on K is bounded, then K is compact
- union or finite intersection of open sets is open, infinite intersection of open sets can be closed
- intersection or finite union of closed sets is closed, infinite intersection of closed sets can be open (every subset on $\mathbb{R}$ is a infinite union of closed sets)
- $A \setminus B = A \cap B^c$, closed\open is closed, open\closed = open
- $\sin(x^2)$ is everywhere differentiable, bounded, with unbounded derivatives
- S is a subset of $[0,1] \times [0,1]$ such that x or y or both are irrationals
  S is not closed, not compact, not open, it is connected, it is path-connected
- every convergent sequence is bounded
- Bolzano-Weierstrass theorem: each bounded sequence in $\mathbb{R}^n$ has a convergent subsequence
- curvature: $\kappa = \frac{|r' \times r''|}{|r'|^3}$, for helix $r(t) = (a\cos t, a\sin t, bt)$, $\kappa = \frac{a}{a^2+b^2}$
- $\int_0^\pi \frac{\sin(100x)}{\sin x}$ let $u = x - \frac{\pi}{2}$, $\int_{-\frac{\pi}{2}}^{\frac{\pi}{2}} \frac{\sin 100u}{\cos u} du = 0$