A CONCISE INTRODUCTION TO PURE. MATHEMATICS NOTES

一. decimals.

- same real number may have two decimal expressions.

证: $0.999\cdots = \frac{9}{10}+\frac{9}{10^2}+\frac{9}{10^3}+\cdots = 9\left(\frac{\frac{1}{10}}{1-\frac{1}{10}}\right) = 1.000\cdots$

- the decimal expression for any rational number is periodical

证:考虑 $\frac{m}{n}$. at each stage of long division. we get a remainder which is one of the n integers between 0 and $n-1$, eventually we will get a remainder occured before

二. polynomial equation

- 对于 $x^3+ax^2+bx+c=0$

let $y=x+\frac{a}{3}$, $x=y-\frac{a}{3}$, 原式变为 $y^3+3hy+k=0$

when let $y=u+v$: $y^3=u^3+v^3+3uv(u+v)=u^3+v^3+3uvy$

the cubic equation. $y^3-3uvy-(u^3+v^3)=0$ has a root $u+v$

aim to: $h=-uv$, $k=-(u^3+v^3)$

$\because v^3=-\frac{h^3}{u^3}$, $u^3-\frac{h^3}{u^3}=-k$. $u^6+ku^3-h^3=0$

$\therefore u^3=\frac{-k+\sqrt{k^2+4h^3}}{2}$ $\quad v^3=\frac{-k-\sqrt{k^2+4h^3}}{2}$, $y=u+v$

since a complex number has 3 cube roots. total 9 possible values of y

$\because v=-\frac{h}{u}$ $\quad\therefore y_1=u-\frac{h}{u}$, $y_2=u\omega-\frac{h\omega^2}{u}$, $y_3=u\omega^2-\frac{h\omega}{u}$.

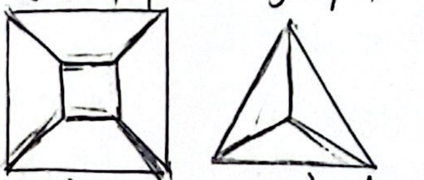
where $\omega=e^{\frac{2\pi i}{3}}$

三. EULER'S FORMULA, PLATONIC SOLIDS

- for a convex polyhedron with V vertices. E edges and F faces

$$V-E+F=2$$

证:我们先用plane graph将图画出来(3.1)



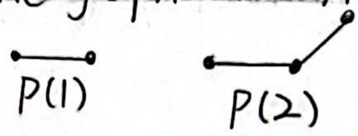
cube tetrahedron

(3.1)

plane graph: 一面为底, 其余边在底上画. no two edges crossing each other. connected (从任一点可从边上走到任意

if a connected plane graph has v vertices, e edges and f faces, then $v-e+f=1$

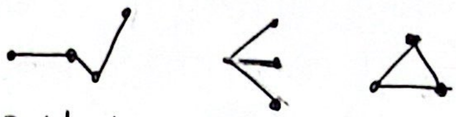
$P(n)$: every connected plane graph with n edges satisfies $v-e+f=1$



$P(1)$: True

$P(2)$: True

$P(3)$ 三种情况都 True



assume $P(k)$ is true, for $P(k+1)$:

如果 $f\neq 0$, 除去一面上的一边, $f'=f-1$, $n'=k-1$, 满足 $P(k)$

如果 $f=0$, 除去最头上一边, $v'=v-1$, $n'=k-1$, 满足 $P(k)$

所以 $P(k+1)$ True

- the only regular convex polyhedra are

	V	E	F	n	r
tetrahedron	4	6	4	3	3
cube	8	12	6	4	3
octahedron	6	12	8	3	4
icosahedron	12	30	20	3	5
dodecahedron	20	30	12	5	3

where n represents the number of sides on a face, and r represents the number of edges each vertex belongs to

证: $\because 2E=nF$, $2E=rV$, $V-E+F=2$ (物理意义)

$\therefore V=\frac{2E}{r}$, $F=\frac{2E}{n}$, $\frac{2E}{r}-E+\frac{2E}{n}=2$

$\therefore \frac{1}{r}+\frac{1}{n}=\frac{1}{2}+\frac{1}{E}$

$\because r\geq 3$, $n\geq 3$ (物理意义)

$\because$ when $r\geq 4$ and $n\geq 4$, $\frac{1}{r}+\frac{1}{n}\leq\frac{1}{2}$

$\therefore$ either $r=3$ or $n=3$

四 integer 与素数定理

- 用辗转相除法算 $hcf(a,b)$

(1) $b=q_1a+r_1$ with $0\leq r_1<a$, (a,b) convert into (a,r_1)

(2) $a=q_2r_1+r_2$ with $0\leq r_2<r_1$, (a,r_1) convert into (r_2,r_1)

(3) $r_1=q_3r_2+r_3$ with $0\leq r_3<r_2$, (r_2,r_1) convert into (r_2,r_3)

⋮

(n) $r_{n-2}=q_nr_{n-1}+0$. $gcf(a,b)=r_{n-1}$

证: let $d=gcf(a,b)$; $d\mid b-q_1a$, $d\mid r_1$; $d\mid a-q_2r_1$, $d\mid r_2$; …;

$d\mid r_n$;

$\because r_{n-1} | r_{n-2}$；$r_{n-1} | q_{n-2} r_{n-2} + r_{n-1}$，$r_{n-1} | r_{n-3}$；…；$r_{n-1} | a$，$r_{n-1} | b$
$\therefore r_{n-1} \geq d$　$\therefore r_{n-1} = d$

- 从1到n的正整数内有 $\int_2^n \frac{1}{\ln t} dt$（或 $\frac{n}{\ln n}$）个质数

证：设 $\pi(n)$ 为从1到n的正整数中质数的个数
任何大于1的正整数 $x = \prod p_i^{r_i}$，其中 p_i 为质数
但是我们会遇到两问题：① $\pi(n)$ 不一定为t；② t 不好算
为了解决①，让 $x = n!$，此时 $\pi(x) = t$
即 $n! = \prod_{i=1}^{t} p_i^{r_i}$，$r_i = [\frac{n}{p_i}] + [\frac{n}{p_i^2}] + \cdots \approx \frac{n}{p_i} + \frac{n}{p_i^2} + \cdots = \frac{n}{p_i - 1}$
因此 $n! \approx \prod_{i=1}^{t} p_i^{\frac{n}{p_i-1}}$，$\ln n! \approx n \sum_{p \leq n} \frac{\ln p}{p_i - 1}$
用斯特林公式：$n! \approx \sqrt{2\pi n} \cdot (\frac{n}{e})^n$：$\ln n! \approx n(\ln n - 1)$
所以 $\ln n - 1 = \sum_{p \leq n} \frac{\ln p}{p-1}$ $\Rightarrow$ $\ln x = \sum_{p \leq x} \frac{\ln p}{p-1} + 1$
当 $x \geq 2$，$\frac{\ln x}{x-1}$ 单调递减且恒大于0
高斯通过 by trails 发现质数的分布密度接近于自然对数的倒数
那么，我们想试试能否找到一个简单连续函数 $f(x)$，使较大的 a 与 b 有近似关系
$$\pi(b) - \pi(a) \approx \int_a^b f(t) dt$$
那也就是说，当 $p_i < p_{i+1}$，两者都很大时
$$\int_{p_i}^{p_{i+1}} f(x) dx \approx \pi(p_{i+1}) - \pi(p_i) = 1$$
所以 $\frac{\ln p_{i+1}}{p_{i+1} - 1} f(x) \leq \frac{\ln x}{x-1} f(x) \leq \frac{\ln p_i}{p_i - 1} f(x)$ for $p_i \leq x \leq p_{i+1}$
$$\frac{\ln p_{i+1}}{p_{i+1} - 1} \int_{p_i}^{p_{i+1}} f(x) dx \leq \int_{p_i}^{p_{i+1}} \frac{\ln x}{x-1} f(x) dx \leq \frac{\ln p_i}{p_i - 1} \int_{p_i}^{p_{i+1}} f(x) dx$$
$$\frac{\ln p_{i+1}}{p_{i+1} - 1} \leq \int_{p_i}^{p_{i+1}} \frac{\ln x}{x-1} f(x) dx \leq \frac{\ln p_i}{p_i - 1}$$
$$\sum_{i=1}^{t-1} \frac{\ln p_{i+1}}{p_{i+1} - 1} \leq \sum_{i=1}^{t-1} \int_{p_i}^{p_{i+1}} \frac{\ln x}{x-1} f(x) dx \leq \sum_{i=1}^{t-1} \frac{\ln p_i}{p_i - 1}$$
$$\sum_{i=1}^{t} \frac{\ln p_i}{p_i - 1} - \ln 2 \leq \int_2^{p_t} \frac{\ln x}{x-1} f(x) dx \leq \sum_{i=1}^{t} \frac{\ln p_i}{p_i - 1} - \frac{\ln p_t}{p_t - 1}$$
因为差距至多 $\ln 2$，$\int_2^{p_t} \frac{\ln x}{x-1} f(x) dx \approx \sum_{i=1}^{t} \frac{\ln p_i}{p_i - 1} =$

$\therefore \int_2^x \frac{\ln t}{t-1} f(t)\,dt \sim \sum_{p\le x} \frac{\ln p}{p-1}$

$\ln x \sim \int_2^x \frac{\ln t}{t-1} f(t)\,dt + 1$

$\frac{1}{x} \sim \frac{\ln x}{x-1} f(x)$, $f(x) \sim \frac{1}{\ln x}$. [求导]

$\therefore \pi(x) \sim \int_2^x \frac{1}{\ln t}\,dt$

[注，本题所有约等号代表"当自变量无限大，约等号两边的比值趋近于1"]

五. congruence

- $ax \equiv b \pmod m$ has a solution $x \in \mathbb{Z}$ if and only if $\gcd(a,m) \mid b$.

证： $ax = tm + b$，t is an integer $\Leftrightarrow ax - tm = b$

$\Leftrightarrow \gcd \mid b$ since $\gcd(a,m) \mid a$, $\gcd(a,m) \mid m$.

- system $\mathbb{Z}_m$ 是在module m 下的一个set，consisting of m symbo $\overline{0}, \overline{1}, \overline{2}, \ldots, \overline{m-1}$

- let p be a prime number, and let a be an integer that is no divisible by p, then

$$a^{p-1} \equiv 1 \mod p$$

证：a与p co-prime，那么 $a, 2a, \ldots, (p-1)a \bmod p$ 后得数不一样，则

$a \equiv k_1 \pmod p$，$2a \equiv k_2 \pmod p$，$\ldots$，$(p-1)a \equiv k_{p-1} \pmod p$

where $k_i \neq k_j$，$k_i \in \{1, 2, \ldots, p-1\}$

反证：若存在 $1 \le s < t < p$，使 $sa \equiv ta \pmod p$

因为 a, p co-prime，$s \equiv t \pmod p$

不可能，by contradiction

所以 $a \cdot 2a \cdot 3a \cdot \ldots \cdot (p-1)a \equiv k_1 \cdot k_2 \cdot \ldots \cdot k_{p-1} \pmod p$

$$a^{p-1}(p-1)! \equiv (p-1)! \pmod p$$

$$a^{p-1} \equiv 1 \pmod p$$

推论1：$a^p \equiv a \pmod p$ regardless of a, as long as p is prime

推论2：定理也可用来判断一个数是否为质数，仅需让其为p，任找一个co-prime的数 (2) 判断 $a^{p-1} \equiv 1 \pmod p$ 是否成立 (但不一直有效，只能说明，如果不满足一定不是prime)

推论3：let p, q be distinct prime numbers, and let a be an integer that is not divisible by p or q, then

$$a^{(p-1)(q-1)} \equiv 1 \pmod{pq}$$ [遍历所有与pq co-prime的值]

- let p be a prime, and let k be a positive integer co-prime to $(p-1)$, then
  (i) there is a positive integer s such that $sk \equiv 1 \pmod{p-1}$
  (ii) for any $b \in \mathbb{Z}$ not divisible by p, the congruence equation

  $$x^k \equiv b \pmod p$$

  has a unique solution for $\bar{x} \in \mathbb{Z}_p$, $\bar{x} \equiv b^s \pmod p$

证: (i) 因为 $(p-1)$ 与 k co-prime, 存在整数 s, t 使 $sk - t(p-1) = 1$, 所以 $sk \equiv 1 \pmod{p-1}$

(ii) 因为 p 质数且 x 与 p 互质 (因为 b 与 p 互质)

所以 $x^{p-1} \equiv 1 \pmod p$

$$x \equiv x^{1+t(p-1)} \equiv x^{sk} \equiv b^s \pmod p$$

推论1: let p, q be distinct primes, and let k be a positive integer co-pime to $(p-1)(q-1)$, then
(i) there is a positive integer s such that $sk \equiv 1 \pmod{(p-1)(q-1)}$
(ii) for any $b \in \mathbb{Z}$ not divisible by p or q, the congruence equation

$$x^k \equiv b \pmod{pq}$$

has a unique solution for $\bar{x} \in \mathbb{Z}_{pq}$, $\bar{x} \equiv b^s \pmod{pq}$

- 用 Miller test 判断 N 是否为质数

auxiliar result: let p be a prime, if a is an integer such that $a^2 \equiv 1 \pmod p$, then $a \equiv \pm 1 \pmod p$

证: $p \mid a^2 - 1$, $p \mid (a+1)(a-1)$, either $p \mid a+1$, or $p \mid a-1$

(i) 随机选 b less than N, test whether $b^{N-1} \equiv 1 \pmod N$

如果不是则 N 不是 prime, 是的话进下一步

(ii) test whether $b^{\frac{N-1}{2}} \equiv \pm 1 \pmod N$, 如果不是则 N 不是 prime, $b^{\frac{N-1}{2}} \equiv -1 \pmod N$ 则 pass test, $b^{\frac{N-1}{2}} \equiv 1 \pmod N$ 则进下一步

(iii) test whether $b^{\frac{N-1}{4}} \equiv \pm 1 \pmod N$ ……

(n) ... we always get $b^{\frac{N-1}{2^i}} \equiv 1 \pmod N$ for all i, then pass test

这个test多选几个b重复即可减少错误率.

六. set

- $A_1 \cup A_2 \cup \cdots \cup A_n = \bigcup_{i=1}^{n} A_i$. $A_1 \cap A_2 \cap \cdots \cap A_n = \bigcap_{i=1}^{n} A_i$
- let A, B be sets, the cartesian product $A \times B$, is a set, consisting of all symbols of the form (a,b) with $a \in A$, $b \in B$. such a symbol (a,b) is called an ordered pair of elements of A and B. two ordered pairs (a,b), (a',b') are deemed to be equal if and only if both $a=a'$, $b=b'$

七. equivalence relation

- let S be a set. a relation on S is defined as follows: we choose a subset R of $S \times S$. for these ordered pairs $(s,t) \in R$ we write $s \sim t$ and say "s is related to t". for $(s,t) \notin R$, $s \not\sim t$
- let S be a set, and let $\sim$ be a relation on S. then $\sim$ is an equivalence relation if the following three properties hold for all $a, b, c \in S$:
  - (i) reflexive: $a \sim a$
  - (ii) symmetric: if $a \sim b$, then $b \sim a$
  - (iii) transitive: if $a \sim b$, $b \sim c$, then $a \sim c$
- let S be a set and $\sim$ an equivalence relation on S. for $a \in S$

$$cl(a) = \{s \mid s \in S, s \sim a\}$$

thus $cl(a)$ is the set of things that are related to a. the subset $cl(a)$ is called an equivalence class of $\sim$. the equivalence classes of $\sim$ are the subsets $cl(a)$ as a ranges over the elements of S

- a partition of a set S is a collection of subsets $S_1, S_2, \ldots, S_k$ such that each element of S lies in exactly one of these subsets

let S be a set and let $\sim$ be an equivalence relation on S. then the equivalence classes of $\sim$ form a partition of S.

证: if $a \in cl(s)$, $a \in cl(t)$, then $a \sim s$, $a \sim t$, so $s \sim t$, $cl(s) = cl(t)$

推论1：我们可以把partition与equivalence classes相联系
每一种 partition / equivalence relation 对应一种 unique 的 equivalence relation / partition
number of partitions = number of collections of equivalence classes

八. function

- onto: 满射　bijection: 双射

九. permutations

- permutation: a bijection from S to S

if $f: a_1 \to f(a_1)$, $f: a_2 \to f(a_2)$, …, $f: a_n \to f(a_n)$. $f(a_i) \neq f(a_j)$ for $i \neq j$

we write permutation as $\begin{pmatrix} a_1 & a_2 & \cdots & a_n \\ f(a_1) & f(a_2) & \cdots & f(a_n) \end{pmatrix}$

if permutation is $\begin{pmatrix} a_1 & a_2 & \cdots & a_n \\ a_1 & a_2 & \cdots & a_n \end{pmatrix}$, we call it as the identity permutation ι

sometimes. $f_i \circ f_j = f_k$, where each of them represents a permutation so we use a multiplication table for set S to illustrate them.

	ι	f_1	…
ι	ι	f_1	…
f_1	f	f_1	…
⋮	⋮	⋮	⋱

- the following properties are true for the set S_n of all permutations of $\{1, 2, \ldots, n\}$

(i) if f and g are in S_n, so is fg.

(ii) for any $f, g, h \in S_n$
$$f(gh) = (fg)h$$

(iii) the identity permutation $\iota \in S_n$ satisfies
$$f\iota = \iota f = f$$
for any $f \in S_n$

(iv) every permutation $f \in S_n$ has an inverse $f^{-1} \in S_n$ such that
$$ff^{-1} = f^{-1}f = \iota$$

- for a set $S = \{a_1, a_2, \ldots, a_n\}$, the cycle $(a_1' a_2' \cdots a_r')$ is the permutation of S that sends $a_1' \to a_2'$, $a_2' \to a_3'$, …, and $a_r' \to a_1'$. the length of the cycle is r.

a collection of cycles is disjoint if no two of the cycle have a symbol in common. every permutation of S_n can be expressed as a product of disjoint cycles

$$* \begin{pmatrix} a_1 & a_2 & a_3 & \cdots & a_i & b_1 & b_2 & b_3 & \cdots & b_j & \cdots & x_1 & x_2 & x_3 & \cdots & x_k \\ a_2 & a_3 & a_4 & \cdots & a_1 & b_2 & b_3 & b_4 & \cdots & b_1 & \cdots & x_2 & x_3 & x_4 & \cdots & x_1 \end{pmatrix}$$

$$= (a_1 a_2 \cdots a_i)(b_1 b_2 \cdots b_j) \cdots (x_1 x_2 \cdots x_k)$$

this is called the cycle notation of f. this expression isn't unique

(i) each cycle can begin with any one of the symbols

(ii) the order of cycles doesn't matter.

- the cycle-shape of f is the sequence of number we get by writing down the lengths of the disjoint cycles of f in decreasing order, generally we write repeated number as power forms

we define the order of a permutation $f \in S_n$ to be the smallest positive integer r such that $f^r = \iota$

the order of a permutation in cycle notation is equal to lcm of the length of cycles.

- let $x_1, x_2, \ldots, x_n$ be variables, and take permutations in S_n to move these variables just in the same way they move the symbols $1, 2, \ldots n$ around.

$$\Delta = \prod_{1 \le i < j \le n} (x_i - x_j)$$

apply the permutation to Δ and check the result, either $+\Delta$ or $-\Delta$

$$f(\Delta) = sgn(f)\Delta, \text{ where } sgn(f) \in \{-1, +1\}$$

f is an odd permutation if $sgn(f) = -1$. it is an even permutation if $sgn(f) = +1$

- some properties of signature:

(i) $sgn(\iota) = +1$

(ii) for any $g, h \in S_n$, $sgn(gh) = sgn(g)\, sgn(h)$

(iii) for any $g \in S_n$, $sgn(g^{-1}) = sgn(g)$

(iv) the signature of any 2-cycle is -1.

证: (ii) $gh(\Delta) = g(h(\Delta)) = g(sgn(h)\Delta) = sgn(g)\, sgn(h)\Delta$

(iii) $sgn(\iota) = sgn(g^{-1}g) = sgn(g^{-1})\, sgn(g)$

(iv) let $t = (a\ b)$, $a < b$

令 x_a 被翻转为负的 $(x_a - x_{a+1})(x_a - x_{a+2}) \cdots (x_a - x_b)$.

令 x_b 被翻转为负的 $(x_{a+1} - x_b)(x_{a+2} - x_b) \cdots (x_{b-1} - x_b)$

first row $(b-a)$次, second row $(b-a-1)$次, $sgn(t)=-1$

推论1: the signature of any r-cycle is $(-1)^{r-1}$

证: $(a_1 a_2 \cdots a_r) = (a_1 a_r)(a_1 a_{r-1}) \cdots (a_1 a_2)$

推论2: if $g \in S_n$ has cycle-shape $(r_1, r_2, \cdots, r_k)$, then

$$sgn(g) = (-1)^{r_1-1}(-1)^{r_2-1}\cdots(-1)^{r_k-1}$$

推论3: for any n, exactly half of the $n!$ permutations in S_n are odd and half are even

证: 用推论2: $sgn(g) = (-1)^{n-m}$, $1 \le m \le n$

$$\sum_{i=1}^{n} (-1)^i \binom{n}{i} = 0$$

十 infinite的大小(可数无穷)

- two sets A and B are said to be equivalent to each other if there is a bijection from A to B. we write $A \sim B$ if A and B are equivalent to each other

this is an equivalence relation

- a set A is said to be countable if A is equivalent to $\mathbb{N}$. in other words, A is countable if it is an infinite set, all of whose elements can be listed as $A = \{a_1, a_2, \cdots, a_n, \cdots\}$

推论1: every infinite subset of $\mathbb{N}$ is countable

推论2: the set of rationals $\mathbb{Q}$ is countable

证

$$\begin{matrix} \frac{1}{1} & \frac{2}{1} & \frac{3}{1} & \frac{4}{1} & \cdots \\ \frac{1}{2} & \frac{2}{2} & \frac{3}{2} & \frac{4}{2} & \cdots \\ \frac{1}{3} & \frac{2}{3} & \frac{3}{3} & \frac{4}{3} & \cdots \\ \frac{1}{4} & \frac{2}{4} & \frac{3}{4} & \frac{4}{4} & \cdots \\ \vdots & \vdots & \vdots & \vdots & \ddots \end{matrix}$$

$\mathbb{Q}^+$ is countable

$\mathbb{Q} = \{0, q_1, -q_1, q_2, -q_2, \cdots\}$, $\mathbb{Q}$ is countable.

推论3: let S be an infinite set. if there is a 1-1 function $f: S \to \mathbb{N}$, then S is countable.

证: 推论1, $f(S)$ countable, 又因 S与$f(S)$ bijection, S countable

推论4: cartesian product $\mathbb{N}^n$ countable

证: $f(a, b, \cdots, n) = 2^a 3^b \cdots p_n^n$

推论5: the set $\mathbb{R}$ of all real numbers is uncountable

证: prove by contradiction

我们把list写出，$\mathbb{R}=\{r_1, r_2, r_3 \cdots, r_n, \cdots\}$

$r_1 = a_{10}.\, a_{11} a_{12} a_{13} \cdots$

$r_2 = a_{20}.\, a_{22} a_{21} a_{22} \cdots$

$\vdots$

其中 a_{i0} 为一个整数，$a_{ij} \in \{0,1,2,3,4,5,6,7,8,9\}$

设一个数 $0.\, b_1 b_2 b_3 \cdots$，其中 $b_n \neq a_{nn}$，$b_n \in \{1,2\}$.

按理，此数应在 $\mathbb{R}$ 中，但是它却不为任何数

所以说 $\mathbb{R}$ uncountable

- let A and B be sets. if A and B are equivalent to each other, we say that A and B have same cardinality, $|A|=|B|$

  if there is a 1-1 function from A to B, we write $|A| \leq |B|$

  and if there is a 1-1 function from A to B but no bijection, $|A|<|B|$, A has smaller cardinality than B.

- if S is a set. let $P(S)$ be the set consisting of all the subsets of S. then there is no bijection from S to $P(S)$. so $|S|<|P(S)|$

证：如果 there is a bijection $f: S \to P(S)$

then every subset of S is equal to $f(s)$ for some s.

define A to be the set of all elements s of S such that $s \notin f(s)$

$$A=\{s \in S \mid s \notin f(s)\}$$

since $A \subseteq P(S)$, thus $A=f(a)$ for some $a \in S$

but, 如果 $a \notin A$，那么 $a \neq f(a)$，那么根据定义 $a \in A$

同理，如果 $a \in A$，那么 $a = f(a)$，那么根据定义 $a \notin A$

contradiction

十一、limits.

- if $\lim_{n\to\infty} a_n = a$, $\lim_{n\to\infty} b_n = b$. then $\lim_{n\to\infty} a_n \cdot b_n = ab$

证. $a_n b_n - ab = (a_n - a) b_n + a(b_n - b)$

$|a_n b_n - ab| \leq |a_n - a||b_n| + |a||b_n - b|$

let $\varepsilon>0$. we want LHS $<\varepsilon$, so assume $|b_n|<K$ for all n, and for $n>N$, $|a-a_n|<\frac{\varepsilon}{2K}$, for $n>M$, $|b-b_n|<\frac{\varepsilon}{2(|a|+1)}$

when $n>\max\{N, M\}$, RHS $< \frac{\varepsilon}{2K}\cdot K + |a| \cdot \frac{\varepsilon}{2(|a|+1)} < \varepsilon$

so $|a_n b_n - ab| < \varepsilon$

- 单调有界必收敛

证：for $\varepsilon>0$, if upper boundary is l, there exists $n>N$ such that $l-\varepsilon<a_n<l$.

同理 for lower boundary

- intermedia value theorem:

let $f: \mathbb{R} \to \mathbb{R}$ be a continuous function and $a, b \in \mathbb{R}$ with $a<b$. and $f(a) \neq f(b)$. then for any γ between $f(a)$ and $f(b)$, there exists a real number c between a and b such that $f(c)=$

证：假设 $f(a)<f(b)$，所以 $f(a)<\gamma<f(b)$

define a set S of real numbers as follows:

$$S=\{x \in \mathbb{R}: x \leq b \text{ and } f(x)<\gamma\}$$

S is non-empty since $a \in S$, and S has b as an upper boundary, therefore, S has a least upper boundary, namely c

we shall prove that $\gamma=f(c)$，如此便证明了：对于任意 γ，均有 c 满足条件

by contradiction, if $f(c)<\gamma$, let $\varepsilon=\gamma-f(c)>0$

since continuous, there exists $\delta>0$ such that

$$|x-c|<\delta \Rightarrow |f(x)-f(c)|<\varepsilon=\gamma-f(c)$$

so

$$f(c+\tfrac{\delta}{2})<f(c)+\varepsilon=\gamma$$

$$(c+\delta) \in S, \text{ impossible.}$$

if $f(c)>\gamma$, let $\varepsilon=f(c)-\gamma>0$

since continuous, there exists $\delta>0$ such that

$$|x-c|<\delta \Rightarrow |f(x)-f(c)|<\varepsilon$$

for $c-\delta<x\leq c$, we have $|f(x)|>f(c)-\varepsilon=\gamma$, impossible

so $\gamma=f(c)$

十二. group.

- let G be a set, a binary operation $*$ on G is a rule which assign to any ordered pair (a,b) $(a,b \in G)$ to get $a*b \in G$

a group $(G,*)$ is a set G with a binary operation $*$, satisfying the following axioms:

(i) closure axiom: $a*b \in G$ for all $a, b \in G$

(ii) associativity axiom: $(a*b)*c=a*(b*c)$ for all $a,b,c \in G$

(iii) identity axiom: there exists an element $e \in G$ such that $a*e=e*a=a$ for all $a \in G$, here, e is an identity element

(iv) inverse axiom: for any $a \in G$ there exists an element $a' \in G$ such that $a*a'=a'*a=e$, here, a' is an inverse of a

推论1: $(G,*)$ is abelian if $a*b=b*a$ for all $a,b \in G$

推论2: (i) G only has one identity element at each stage of the division we get a remainder k which

证(i) if $e*x = x*e = x$, $f*x = x*f = x$

then $e*f = e = f$

(ii) if $a*a' = a'*a = e$. $a*a'' = a''*a = e$

then $a' = a'*(a*a'') = (a'*a)*a'' = a''$

推论3: in any group $(G,*)$, the following "cancellation laws" holds for all $a, x, y \in G$:

(i) $x*a = y*a \Rightarrow x = y$ (ii) $a*x = a*y \Rightarrow x = y$

证(i) $x*(a*a^{-1}) = y*(a*a^{-1})$

- for $(G,*)$, we define the power of a as follow:

$$a^0 = e$$
$$a^1 = a$$
$$a^2 = a*a$$
$$\vdots$$
$$a^n = a^{n-1}*a$$

	a	b	c	...
a	a^2	ab	ac	...
b	ba	b^2	bc	...
c	ca	cb	c^2	...
$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\ddots$

推论: $a^m * a^n = a^{m+n}$

同理, 可用 multiplication table 表示

- let $(G,*)$ be a group and let H be a subset of G, we say that H is a subgroup of $(G,*)$ if H is itself a group under $*$
- let G be a group, and let H be a subset of G, the H is a subgroup of G if the following three conditions hold:

(i) $e \in H$ (where e is the identity element of G)

(ii) $x, y \in H \Rightarrow xy \in H$

(iii) $x \in H \Rightarrow x^{-1} \in H$

- let G be a group, and let $a \in G$, define

$$A = \{a^n \mid n \in \mathbb{Z}\} = \{\cdots, a^{-2}, a^{-1}, a^0, a^1, a^2, \cdots\}$$

for this, we write $A = \langle a \rangle$, and call it the cyclic subgroup of G generated by a

for each element $a \in G$. there is a cyclic subgroup $\langle a \rangle$ of G

we say a group G is a cyclic group if there exists an element $a \in G$ such that $G = \langle a \rangle$. in this case we call a as a generator for G

- let G be a group and let $a \in G$, the order of a, written $o(a)$, is the smallest positive integer k such that $a^k = e$. if no such k exists, we say $o(a) = \infty$

推论1: let G be a group and let $a \in G$, the number of elements in the cyclic subgroup $\langle a \rangle$ is equal to $o(a)$

证: (i) assume $o(a)=k$, so $a^k=e$ but $a^i \neq e$ for $1 \le i \le k-1$

so $A=\{e, a, a^2, \dots, a^{k-1}\}$.

all of these elements are distinct, otherwise, for $1 \le i < j \le k-1$

$a^i = a^j \Rightarrow a^{-i}a^i = a^{-i}a^j \Rightarrow a^{j-i} = e \Rightarrow j-i \le k-1$, impossible

we now show that every element of $\langle a \rangle$ is on the list

$a^n = a^{qk+r}$, where q, r are integers, $0 \le r \le k-1$

$= a^r$

so $|A| = o(a) = k$

(ii) assume $o(a)=\infty$, meaning $a^i \neq e$ for all $i>0$.

if $a^i = a^j$ for $i<j$, $e = a^{j-i}$, impossible.

so elements of $A=\{e, a, a^2, \cdots\}$ are all distinct

$|A| = o(a) = \infty$

推论2: let G be group and let $a \in G$. suppose $a^n = e$ where n is a positive integer, then $o(a) \mid n$.

- Lagrange's Theorem.

let G be a finite group, and let H be a subgroup of G. then $|H| \mid |G|$

证 在开始之前,我们先讨论一下我们的思路

我们首先列出 element $h \in H \subseteq G$, 然后,

我们选取 $x \in G-H$, 列出 Hx …

我们要证明. (i) Hx、Hy … 均有 $|H|$ 个元素

(ii) $Hx = Hy$ or $Hx \cap Hy = \emptyset$

如此, 则 $|G| = k|H|$, 所以 $|H| \mid |G|$

H	Hx	Hy	$\cdots$
h_1	h_1x	h_1y	$\cdots$
h_2	h_2x	h_2y	$\cdots$
$\vdots$	$\vdots$	$\vdots$	
h_m	h_mx	h_my	$\cdots$

首先我们给出一个定义

for $x \in G$, define $Hx = \{hx \mid h \in H\} = \{h_1x, h_2x, \cdots, h_mx\}$

this is a subset of G, called a right coset of H in G

(i) for any $x \in G$, we have $|Hx| = |H|$.

by contradiction: if $h_ix = h_jx \Rightarrow h_i = h_j$, impossible

(ii) 只需证明 if $a \in Hx \cap Hy$, then $Hx = Hy$

thus, there exists h_i, h_j such that $a = h_ix = h_jy$.

$\Rightarrow x = h_i^{-1}h_jy \Rightarrow hx = hh_i^{-1}h_jy$ for any $h \in H$

$\Rightarrow Hx = Hy$ since $hh_i^{-1}h_j \in H$.

(iii) x lies in the right coset Hx since $e \in H$

to conclude. $G=\bigcup_{x\in G} Hx$, $Hx_i = Hx_j$ for some x_i and x_j and if right cosets $Hx_1, Hx_2, \cdots Hx_k$ form a partition, then

$$|G| = |Hx_1| + |Hx_2| + \cdots + |Hx_k| = k|H| \Rightarrow |H|\,\big|\,|G|$$

推论1: let G be a finite group and let $a\in G$. then $o(a)$ is finite and $o(a)\,|\,|G|$

证 if $A=\langle a\rangle$, $|A| = o(a)$. and A is a subgroup of G.

推论2: let G be a finite group, so $a^{|G|}=e$ for all $a\in G$

证 $a^{|G|} = a^{k\cdot o(a)} = e$

推论3: let G be a group. and suppose that $|G|$ is a prime number. then G is a cyclic group.

证 the cyclic subgroup $A=\langle a\rangle$ has size dividing p, where $a\neq e$ and $a\in G$, so $G=A=\langle a\rangle$

- $\mathbb{Z}_m^* = \mathbb{Z}_m \setminus \{\bar{0}\} = \{\bar{1}, \bar{2}, \dots, \overline{m-1}\}$

let p be a prime, then $(\mathbb{Z}_p^*, \times)$ is a group. it is abelian, and has size $p-1$

证 closure: $\bar{x}, \bar{y}\neq \bar{0}$, then $\bar{x}*\bar{y}\neq 0$ so if $\bar{x},\bar{y}\in\mathbb{Z}_p^*$, so does $\bar{x}*\bar{y}$

inverse: $hcf(p, \bar{x}*\bar{y})=1$, 辗转相除法, $\bar{x}*\bar{y}\equiv 1 \pmod p$ for some $\bar{x},\bar{y}\in\mathbb{Z}_p^*$

- 费马小定理的又一证明 ($a^{p-1}\equiv 1 \pmod p$ for prime p and co-prime a, p. a为$\bar{x}\in\mathbb{Z}_p^*$, and $\bar{x}^{|\mathbb{Z}_p^*|}\equiv 1$.

- let m be an arbitrary positive integer greater than 1, and for each x such that $1\le x\le m-1$ and $hcf(x,m)=1$. define a symbol $\bar{x}$. let $U(\mathbb{Z}_m)=\{\bar{x}\,|\,1\le x\le m-1, hcf(m,x)=1\}$. define multiplication on $U(\mathbb{Z}_m)$ by $\bar{x}\bar{y}=\bar{k}$, where $xy\equiv k \pmod m$ and $1\le k\le m-1$

$(U(\mathbb{Z}_m), \times)$ is a group. it is abelian, and has size $\phi(m)$, where ϕ is Euler's ϕ-function.

推论: let m be a positive integer, and let a be an integer which is co-prime to m. then $a^{\phi(m)}\equiv 1 \pmod m$

证: 同上方费马小定理

- if p is prime, then the period of the decimal expansion of rational $\frac{1}{p}$ divides $(p-1)$.

证 it is true for $p=2$ or 5

for other primes. they are co-prime with 10 [illegible] at each stage of the division we get a remainder x, which we regard as the element $\bar{x}$ of the group $\mathbb{Z}_p^*$

so the first remainder is $\bar{1} \in \mathbb{Z}_p^*$, the next is $\overline{10}$, the next is $\overline{10}^3$, and so on.

the decimal digits will start repeating the first time this sequence of group elements $\bar{1}, \overline{10}, \overline{10}^2 \ldots$ arrives back at $\bar{1}$

so we are going to find $o(\overline{10})$. which $o(\overline{10}) \mid p-1$.

- a prime number p is called a Mersenne prime if $p = 2^n - 1$ for some positive integer n.

suppose $2^n - 1$ is a prime, then n is a prime

证: if $n = ab$, where a, b are integers

then $2^a - 1 \mid 2^n - 1$

推论: every even perfect number is of the form $2^{p-1}(2^p - 1)$

- let p be a prime, and let $N = 2^p - 1$, suppose q is a prime divisor of N, then $q \equiv 1 \pmod p$

证: 考虑 $(\mathbb{Z}_q^*, \times)$: since $q \mid 2^p - 1$, $2^p \equiv 1 \bmod q$

so $o(\bar{2}) \mid p \Rightarrow o(\bar{2}) = 1$ or $o(\bar{2}) = p$ [p 为 prime]

if $o(\bar{2}) = 1$, then $\bar{2} = \bar{1}$, impossible

so $o(\bar{2}) = p \Rightarrow p \mid q-1$ [$|H| \mid |G|$]