我的笔记

你的名字

2025 年 8 月 3 日

目录

1 Some Conceptions **2**
1.1 binary operation 2
1.2 semigroup and group 2

2 Whatever but this is about group **2**
2.1 Hey, yo, this is GROUP 2
2.2 $\mathbb{SUBGROUP}$ 5
2.3 同态同构 15
2.4 正规子群 21
2.5 同态定理 28
2.6 有限循环群 31
2.7 置换群 34
2.8 Sylow 定理 41

3 RING! **51**
3.1 def 51
3.2 环作用(不要求) 56
3.3 环同态 59
3.4 多项式 66
3.5 商环 78
3.6 还是多项式环 80
3.7 子域 82
3.8 向量空间 87

1 Some Conceptions

1.1 binary operation

X is a set.
A binary operation on X is:
一个映射，$X \times X \to X$ (映射*在 $X \times X$ 上有定义)，且 $\forall a, b \in X$, $*(a, b) \in X$

1.2 semigroup and group

$(X, *)$
1. * is a binary operation on X.
2. $(a * b) * c = a * (b * c)$, $\forall a, b, c \in X$.
if there is a I_x, s.t. $a * I_x = I_x * a = a$, $(\forall a \in X)$
then $(X, *)$ is 幺半群，I_x is 幺元

for $(X, *)$, if $\forall a \in X$, $\exists b \in X$, s.t. $a * b = b * a = I_x$, $(X, *)$ is a group.

2 Whatever but this is about group

2.1 Hey, yo, this is GROUP

DEF:
$(X, *)$ is a group:
1. * is a binary operation on X
2. $(a * b) * c = a * (b * c)$, $\forall a, b, c \in X$.
3. $\exists I_x \in X$, $\forall a \in X$, $a * I_x = I_x * a = a$.
4. $\forall a \in X$, $\exists b \in X$, s.t. $a * b = b * a = I_x$.

examples:
$(\mathbb{Z}, +)$:
1. t
2. t
3. 0
4. $-a$

$(\mathbb{Q} \setminus \{0\}, *)$:
1. t
2. t
3. 1
4. a^{-1}

(no 0; if a semigroup, 0 is ok)

Pf: 逆元 is only one.

命题：设 $(X,*)$ 为幺半群, if $a*b=I_x$, $b*c=I_x$, then $a=c$.

$(a*b)*c=c=a$

$\implies$ if

$$a*b_1=b_1*a=I_x \tag{1}$$
$$a*b_2=b_2*a=I_x \tag{2}$$
$$\implies b_1=b_2 \tag{3}$$

$\forall a\in X$, we use a^{-1} as the inverse of a.

$a^{-1}*a=I_x$

消去律

(X,*) is a group

$a*b=a*c\Rightarrow b=c$

$b*a=c*a\Rightarrow b=c$

Pf:

1.$a^{-1}*(a*b)=a^{-1}*(a*c)\Rightarrow I_x*b=I_x*c$

2.$(b*a)*a^{-1}=(c*a)*a^{-1}$

(X, *) is a semigroup

suppose $a_1,a_2,...,a_n$ are elements of X

for $1\leqslant k\leqslant n$, 定义从a_k 乘到 a_n

$\prod_{i=k}^{n}a_i$

for $k\leqslant m\leqslant m+1$

$\prod_{i=k}^{m+1}a_i=(\prod_{i=k}^{m}a_i)*a_{m+1}$

命题： suppose $1\leqslant k\leqslant n-1$

$\prod_1^n a_i=(\prod_1^k a_i)*(\prod_{k+1}^n a_i)$

if k=n-1:

设1$\leqslant$ k $\leqslant$ n-2 ,LHS=$(\prod_{i=1}^{n-1}a_i)*a_{m+1}$

LHS = $((\prod_1^k a_i)*(\prod_{k+1}^{n-1}a_i))*a_n$=$(\prod_1^k a_i)*((\prod_{k+1}^{n-1}a_i)*a_n)$

=$(\prod_1^k a_i)*(\prod_{k+1}^n a_i)$

得证 (连乘不写( )，因为有结合律)

叉乘没有结合律，所以写x × y × z 没有意义

DEF:

* is a binary operation in X (a set)

称(X,*)满足交换律 : a*b=b*a ($\forall a, b \in X$)

if (X,*) in a group, and 满足交换律：交换群 (abel 群)、、

$GL_2(R)$(二阶可逆实矩阵) 和矩阵乘法

eg:

$$\begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix} and \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$$

无交换

{1,2,...,n}

$S_n = \{\delta | \delta : \{1, 2, ..., n\} \to \{1, 2, ..., n\}\}$ (双射) 映射的复合满足结合律

带余除法：

$a \in Z^+, b \in Z, \exists q \in Z^+, r = \{0, ..., a-1\}$, let b=qa+r (we can find a q ∈ Z , s.t. $qa \leqslant b, (q+1)a \geqslant b$)

$\{q | q \in Z, qa \leqslant b\}$,

let a,binZ ,gcd(a,b=d) → d—a , d—b

and $\exists c \in Z, c|a, c|b$→ c—d

in fact, $\exists x, y \in Z, st.(ax+by)|a, (ax+by)|b$

c—a , c—b → c—(ax+by)

Pf $\exists x, y \in Z, st.(ax+by)|a, (ax+by)|b :$

$suppose T = \{ax+by | x, y \in Z\}$

$\forall u, v \in T,$

$u \pm v \in T.$

a, b 不全为零，

$\therefore$ T 里面有正整数

取d为T里的最小正整数。

任取$\omega \in T$, 证明d —ω

$$\omega = qd + r, \quad 0 \leqslant r \leqslant d-1 \tag{4}$$
$$d \in T, \quad \therefore qd \in T \tag{5}$$
$$\therefore \omega - qd \in T \tag{6}$$
$$\therefore r \in T \tag{7}$$
$$\because r \leqslant d-1, \quad r \in T \tag{8}$$
$$\therefore r \text{ is not a positive integer} \tag{9}$$
$$\therefore r = 0 \tag{10}$$
$$\therefore d \mid \omega \tag{11}$$
$$a, b \in T \tag{12}$$
$$\therefore d \mid a, d \mid b \tag{13}$$
$$\therefore \exists x, y, d \in T \tag{14}$$
$$d = ax + by \tag{15}$$
$$\therefore ax + by \mid a, ax + by \mid b \tag{16}$$

同余：suppose n∈ Z^+ , 对Z ,a,b,∈ Z,
记$a \equiv b(modn), n \mid (b-a)$

only if a=qn+r,b=pn+s,r=s.

$$a \equiv bmodn \tag{17}$$
$$c \equiv d \tag{18}$$
$$a \pm c \equiv b \pm d \tag{19}$$
$$ac \equiv bd \tag{20}$$

(Z,+)为循环群（可以从1生成所有的正整数）

2.2 SUBGROUP

the subgroup of (Z,+)

suppose $a \in Z^+, b \in Z$,then $\exists q \in Z, r \in \{0, 1, ..., a-1\}$,
st b=qa+r,and the (q,r) is only one.
suppose $q' \in Z, r' = \{0, 1, ..., a-1\}$,b=q'a+r' ,证明 q'=q,r'=r;

$$r - r' = (q' - q)a \tag{21}$$
$$|r - r'| = |q' - q|\, a \tag{22}$$
$$0 < r, r' \leqslant a - 1 \tag{23}$$
$$\therefore |r - r'| \leqslant a - 1 < a \tag{24}$$
$$\therefore |q' - q|\, a < a \tag{25}$$
$$\therefore |q' - q| < 1 \tag{26}$$
$$\therefore |q' - q| = 0 \tag{27}$$
$$\therefore r = r', q = q' \tag{28}$$

命题： $A \in Z^+, A \neq \varnothing$,且满足：
1. $\forall a, b, \in A, a + b \in A$
2.$\forall a, b, \in A, a < b, b - a \in A$
$\exists c \in Z^+, st.A = \{cq | q \in Z\}$

Pf:
$A \neq \varnothing$,所以取$c \in A$为A 的最小值（正整数集有最小值）、、下证:$A = \{cq|q \in Z\}$(证明左右互相包含)

1.$RHS \subseteq A$
$c \in A, \therefore 2c \in A, 3c \in A$
$q \in Z^+, (q + 1)c = qc + c \in A$
得证
2.$RHS \supseteq A$
$\forall b \in A, b = qc + r(0 \leqslant r \leqslant c - 1)$
$\because c = minA$
if $r \neq 0, r = b - qc \in A, r < c$,矛盾
$\therefore r = 0$
$\therefore \forall b \in A, b = qc$
$\therefore A \subseteq$右边

得证

双射和置换：
X is a n元有限集。 $\delta : X \to X$是双射

$$y \in X \tag{29}$$
$$A = \{l | l \in Z^+, \delta^l(y) = y\} \tag{30}$$
$$\therefore y, \delta(y), \delta^2(y), ..., \delta^n(y) \in X \text{ (有n+1个元素)} \tag{31}$$
$$\therefore \exists 0 \leqslant i < j \leqslant n, st. \delta^i(y) = \delta^j(y) \tag{32}$$
$$\therefore \delta^i(y) = \delta^i(\delta^{j-i}(y)) \text{ (delta是双射，复合之后还是双射)} \tag{33}$$
$$\therefore \delta^i \text{是双射} \tag{34}$$
$$\therefore y = \delta^{j-i}, 1 \leqslant j - 1 \leqslant n, \therefore j - i \in A \tag{35}$$

we suppose $a, b \in A$,下证a+b∈ A

$$\text{if} a < b, b - a \in A \tag{36}$$
$$\delta^a(y) = \delta^b(y) = y \tag{37}$$
$$\therefore \delta^{a+b}(y) = \delta^a(\delta^b(y)) = \delta^a(y) = y \tag{38}$$
$$\delta^{b-a}(y) = \delta^{b-a}(\delta^a(y)) = \delta^b(y) = y \text{(a¡b,b-a¿0)} \tag{39}$$
$$\tag{40}$$

if c=min A
$\rightarrow A = \{cq | q \in Z^+\}$
$y, \delta(y), \delta^2(y), ..., \delta^{c-1}(y)$两两不同
δ关于y轮换

X 为有限集，$a_1, a_2, ..., a_n$is a sequence on X.
变它： $\Rightarrow a_n, a_1, ..., a_{n-1}$
$\Rightarrow a_{n-1}, a_n, ..., a_{n-2}$
重复k次, $\Rightarrow a_{n-k+1}, ...a_n, a_1, ..., a_{n-k}$
固定a1至an,
$A = \{l | l \in Z^+, (a_1, ..., a_n)$在 l 次变换后变回自身$\}$
A满足上面的两个条件
($A \in Z^+, A \neq \varnothing$,且满足：
1. $\forall a, b, \in A, a + b \in A$
2.$\forall a, b, \in A, a < b, b - a \in A$
$\exists c \in Z^+, st. A = \{cq | q \in Z\}$)
$\therefore A = \{cq | q \in Z^+, c = minA\}$
$\because n \in A, \therefore c \mid n$

$(a_1, a_2, ..., a_n) = (a_1, ..., a_c, a_1, ..., a_c, ...)$

Theroy (Z,+)'s subgroup:
1.$H \subseteq Z, H \neq \varnothing, \forall a, b \in H, a+b \in H, -a \in H$
$\therefore \exists c \in N, st.H = \{cq|q \in Z\}$
2. suppose $c \in Z, H = \{cq|q \in Z\}, \forall a, b \in H, a+b \in H, -a \in H$

Pf:
1.
1.1 prove $0 \in H$

$$
\begin{aligned}
&\because H \neq \varnothing && (41)\\
&\therefore \exists x \in H && (42)\\
&\Rightarrow -x \in H && (43)\\
&\Rightarrow 0 \in H && (44)\\
&\text{suppose} A = H \bigcap Z^+ && (45)\\
&1.1.1.A = \varnothing \text{H里面没有正整数} && (46)\\
&\Rightarrow H = \{0\}, \text{取c=0} && (47)\\
&\text{suppposе} a < 0, a \in H \Rightarrow -a \in H \bigcap Z^+, \text{but it is a varnothing} && (48)\\
&\Rightarrow \text{H里面没有负整数} \Rightarrow H = \{0\} && (49)\\
&1.1.2.A \neq \varnothing && (50)\\
&\Rightarrow \exists c \in Z^+, st.A = \{cq|q \in Z^+\} && (51)\\
&\text{in fact,} H = \{cq|q \in Z^+\} && (52)\\
&\text{下证 } H = \{cq|q \in Z^+\} && (53)\\
&\because \{cq|q \in Z^+\} \in H && (54)\\
&\forall q \in Z^+, qc \in H && (55)\\
&\therefore -qc \in H, \therefore 0 \in H && (56)\\
&\text{反之:} \forall h \in H, \text{ if} h > 0, h \in A, \rightarrow h \in RHS = H \bigcap Z^+ && (57)\\
&h = 0, ok && (58)\\
&h < 0, -h \in H \bigcap Z^+ \rightarrow h \in H \bigcap Z^+ && (59)\\
& && (60)
\end{aligned}
$$

THE DEFINITION OF SUBGROUP
(G,*) is a group,$H \subseteq G$,H is a subgroup of G, if:

$$1.H \neq \varnothing \tag{61}$$
$$2.\forall a, b \in H, a * b \in H \tag{62}$$
$$3.\forall a \in H, a^{-1} \in H \tag{63}$$
$$\iff \tag{64}$$
$$\text{(H,*)is a group} \tag{65}$$

if H is a subgroup of (G,*),then $I_G \in H$,and (H,*) is a group
pf:

$$H \neq \varnothing, \exists x \in H, \therefore x^{-1} \in H \tag{66}$$
$$\therefore x * x^{-1} \in H, \therefore I_H \in H \rightarrow \text{ H is a group} \tag{67}$$
$$\tag{68}$$

now we know there is a $I_H \in H$,但不一定是I_G
下证这个是IH:

$$\because I_H * I_H = I_H \tag{69}$$
$$\because I_H \in G \tag{70}$$
$$\therefore I_H * I_G = I_H\text{这个是在G里面讨论} \tag{71}$$
$$\therefore I_H * I_H = I_H * I_G \tag{72}$$
$$\text{由群里有消去律}I_G = I_H \in H \tag{73}$$

得证，I_G为幺元。

$$\therefore \exists b \in H, st.a * b = I_H\text{这里还没说b一定是a的逆元} \tag{74}$$
$$\text{另一方面，}a * a^{-1} = I_G = a * a^{-1} \tag{75}$$
$$\therefore b = a^{-1} \tag{76}$$
$$\tag{77}$$

子群的交集：

$$H \leqslant G\text{:H is a subgroup of G} \tag{78}$$
$$1.A \leqslant G, B \leqslant G, \Rightarrow A \bigcap B \leqslant G \tag{79}$$
$$2.\{A_i | i \in I\}\text{为一组子群} \rightarrow \bigcap A_i \leqslant G \tag{80}$$

Pf:

$$1. \tag{81}$$
$$1.I_G \in A, I_G \in B \to I_G \in A \bigcap B \tag{82}$$
$$2.\forall a \in A \bigcap B, b \in A \bigcap B, \tag{83}$$
$$\because a, b \in A, A\text{is a subgroup} \tag{84}$$
$$\therefore a * b \in A \tag{85}$$
$$\because a, b \in B, B\text{is a subgroup} \tag{86}$$
$$\therefore a * b \in B \tag{87}$$
$$\therefore a, b \in A \bigcap B \tag{88}$$
$$3.a \in A, A \leqslant G, \therefore a^{-1} \in A \tag{89}$$
$$a \in B, B \leqslant G, \therefore a^{-1} \in B \tag{90}$$
$$\therefore a^{-1} \in A \bigcap B \tag{91}$$
$$\therefore A \bigcap B \leqslant G \tag{92}$$
$$2. \tag{93}$$
$$\{x | \forall i \in I, x \in A_i\} \tag{94}$$
$$1.\forall i \in I, A_i \leqslant G \to I_G \in A_i \tag{95}$$
$$\to I_G \in \bigcap A_i \tag{96}$$
$$2.\forall a, b \in \bigcap A_i \tag{97}$$
$$a, b \in A_i \tag{98}$$
$$\therefore a * b \in A_i \tag{99}$$
$$\therefore a * b \in \bigcap A_i \tag{100}$$
$$3.a \in \bigcap A_i \tag{101}$$
$$a \in A_i \tag{102}$$
$$a^{-1} \in A_i \tag{103}$$
$$OK \tag{104}$$

考虑S生成的subgroup.任取S属于G，称$H \subseteq G$为S在G中生成的子群，指的是：

$$1.H \leqslant G, S \subseteq H \tag{105}$$
$$2.\forall K \leqslant G, S \subseteq K \Rightarrow H \subseteq K\text{最小的子群} \tag{106}$$

下证，H存在且唯一（定义里面没讲是否存在）
设S为G的子集，则S在(G,*)上生成的子群存在且唯一，记作$< S >$

$$\text{唯一性} \tag{107}$$

$$H_1, H_2\text{都是S生成的子群} \tag{108}$$

$$\text{由2，} H_1 \subseteq H_2, H_2 \subseteq H_1, \therefore H_1 = H_2 \tag{109}$$

$$\text{存在性: 把所有由S生成的子群相交一下} \tag{110}$$

$$T = \{H | H \leqslant G, S \subseteq H\} \tag{111}$$

$$\text{断言:} T \neq \varnothing and \bigcap (H \in T) H =< S > \tag{112}$$

$$Pf \tag{113}$$

$$1.G \leqslant G, S \subseteq G, \therefore T \neq \varnothing, \tag{114}$$

$$\bigcap (H \in T) H \subseteq G (\because \forall H \in T, H \leqslant G, \text{且子群对并运算封闭}) \Delta\Delta \quad S \subseteq \bigcap (H \in T) H \forall K \leqslant G, S \subseteq K, \therefore \tag{115}$$

$$\therefore \bigcap (H \in T) H \subseteq K \tag{116}$$

$$\therefore \bigcap (H \in T) H =< S > \tag{117}$$

$$S \subseteq G, \rightarrow \tag{118}$$

$$< S >= \{a_1^{c_1} * a_2^{c_2} * ... * a_n^{c_n} | n \in N, \forall 1 \leqslant i \leqslant n, a_i \in S, c_i = \pm 1\} \tag{119}$$

(线性空间有交换律，群不一定有)

(G,*),a,b,c∈G,

$$1.(a * b)^{-1} = b^{-1} * a^{-1} \tag{120}$$

$$2.(a^{-1})^{-1} = a \tag{121}$$

$$3.a * b = c \Leftrightarrow b = a^{-1} * c \Leftrightarrow a = c * b^{-1} \tag{122}$$

$$A \subseteq G, B \subseteq G \tag{123}$$

$$AB = \{a * b | a \in A, b \in B\} \tag{124}$$

$$if A = \{a\}, B \leqslant G \tag{125}$$

$$\{a\} B = \{ab | b \in B\} \tag{126}$$

$$\text{B的一个左陪集} \tag{127}$$

下面三个等价:

$$1.AB \leqslant G \tag{128}$$
$$2.\forall b \in B, \forall a \in A, b * a \in AB \subset BA \subseteq AB \tag{129}$$
$$3.AB = BA\,|AB| = \frac{|A|\,|B|}{|A \bigcap B|} \tag{130}$$

同余:

$$\text{对}a, b \in Z, n \in Z^{+}, a \equiv b(modn) \tag{131}$$
$$\Leftrightarrow n|(b-a) \tag{132}$$
$$1.a \equiv a(modn) \tag{133}$$
$$2.a \equiv b(modn) \Rightarrow b \equiv a(modn) \tag{134}$$
$$3.a \equiv b(modn), b \equiv c(modn) \Rightarrow a \equiv c(modn) \tag{135}$$
$$4.a \equiv b(modn) \Rightarrow a + c \equiv b + c(modn) \tag{136}$$
$$5.a \equiv b(modn) \Rightarrow ac \equiv bc(modn) \tag{137}$$
$$\tag{138}$$

(Z,+)的子群H,

$$\exists d \in Z^{+}, st.H = \{dq|q \in Z\} \tag{139}$$
$$\tag{140}$$

(G,*)是一个群，H是G的子群，如下定义二元关系：

$$\forall a, b \in G, a \sim b \Leftrightarrow a^{-1} * b \in H \tag{141}$$
$$\tag{142}$$

(左模)

(G,*)为(Z,+)时，$H = \{nq|q \in Z\}$,等价关系即为mod

in fact:

$$1.(G, \sim)\text{为等价关系} \tag{143}$$
$$2.\forall a, b \in G, a \sim b \Leftrightarrow \exists h \in H, st.b = a * h \tag{144}$$

pf:

$$ifa^{-1} * b \in H, a^{-1} * b = h \in H, b = a * h \tag{145}$$

$$ifb = a * h, \text{in the same way ,blablabla} \tag{146}$$

根据等价关系的自反对称传递性，可以证明前面那个弯弯是等价关系。

fact 3:

$$\text{suppose} a \in G, so, \{b|b \in G, a \sim b\} = aH = \{ah|h \in H\} \tag{147}$$

a的等价类=a关于H的左陪集。

$$G/H = \{\text{全体 下的等价类}\} = \{aH|a \in G\} \tag{148}$$

G/H：商群

H为正规子群：$g \in G, h \in H, ghg^{-1} \in h$

G/H=$\{gH|g \in G\}$

$$xH \bigcap yH \neq \varnothing \leftrightarrow xH = yH \tag{149}$$

$$\leftrightarrow x^{-1} * y \in H \leftrightarrow x \sim y \tag{150}$$

拉格朗日定理：设G有限，则$|G| = |H||G/H|$,也有$|G|/|H| = |G/H|$ 且$|G|||H|$

Pf:

$$\text{suppose (G,)是等价关系,G/H中全体成员做成G的不交并分解} \tag{151}$$
$$\text{不交并分解：不相等的话交集是空集；有交集的话必定相等} \tag{152}$$
$$(\forall g_1, g_2 \in G, if g_1 H \neq g_2 H \tag{153}$$
$$\text{Pf this :} \tag{154}$$
$$\text{if there is a } g_1 h_1 = g_2 h_2 \text{,then } g_1 = g_2 h_2 h_1^{-1}, h_2 h_1^{-1} \in H \tag{155}$$
$$\rightarrow g_1 \in g_2 H \rightarrow g_1 = g_2 h \tag{156}$$
$$\rightarrow g_1 H = g_2 h H = g_2 H, \text{矛盾，所以不相交)} \tag{157}$$
$$\tag{158}$$
$$|G| = \sum_{A \in G/H} |A| \tag{159}$$
$$\forall a \in H, \text{suppose } |aH| = |H| \tag{160}$$
$$(a * h_1 = a * h_2 \rightarrow h_1 = h_2 \therefore |aH| = |H|) \tag{161}$$
$$|G| = \sum_{A \in G/H} |H| = |H| * |G/H| \tag{162}$$

$$\forall d||G| \tag{163}$$
$$\text{G一定有d阶子群吗？12阶的G没有6阶子群} \tag{164}$$

$$\text{若G有限，设—G—为素数，那么G的子群只有两个} \tag{165}$$
$$\{I_G\}G \qquad\qquad Pf: \tag{166}$$
$$\text{H is a subgroup of G} \tag{167}$$
$$|H|||G| \tag{168}$$
$$1.|H| = 1\ I_G \in H \rightarrow H = \{I_G\} \tag{169}$$
$$2.|H| = |G| \rightarrow H = G \tag{170}$$
$$\text{这俩叫平凡子群} \tag{171}$$

如果G只有以上那两个子群，那么G有限，且个数为1或者素数。
右陪集：

$$Ha = \{h * a | h \in H\} \tag{172}$$
$$a \simeq b \leftrightarrow \exists h \in H, st.b = h * a \leftrightarrow a * b^{-1} = h \in H \tag{173}$$

元素的幂次：下面有的；
快速幂：拆成2进制表达，$O(n) = log_2(n)$

(G,*)的幺元是I_G
设$\{H_i|i \in I\}$是一组子群
交集是子群。

$$\text{suppose } S \subseteq H, \text{there always be a only one subgroup H that meets:} \tag{174}$$
$$1.S \subseteq H \tag{175}$$
$$2.\forall K \subseteq G, if S \subseteq K \Rightarrow H \subseteq K \tag{176}$$
$$\text{there,} H =< S >, \text{H is the min subgroup generated by S} \tag{177}$$
$$< S >= \{a_1^{c_1} * ... * a_n^{c_n} | n \in N, \forall a_i \in S, c_i = \pm 1\} \tag{178}$$

$$a \in G, \text{幂次：} \tag{179}$$
$$a^0 = I_G, a^1 = a \tag{180}$$
$$\forall m \in Z^+, a^{m+1} = a^m * a \tag{181}$$
$$\forall m \in N, a^{-m} = (a^{-1})^m = (a^m)^{-1} \text{两种定义方法} \tag{182}$$
$$a^{m+n} = a^m * a^n \tag{183}$$
$$(a^m)^n = a^{mn} \tag{184}$$

2.3 同态同构

一个元素生成的子群：

$$a \in G \tag{185}$$
$$\{a\} \text{generate a subgroup,write as} < a > \tag{186}$$
$$< a >= \{a^j | j \in Z\} \tag{187}$$

单独验证右边是子群：
1.封闭性
2.有逆元

有重复吗？不同整数对应的元素相同吗？

元素的阶：
设$a \in G$,$a^n = I_G$,则n为a的阶，记作o(a)

$$1.if\exists n \in Z^+, st.a^n = I_G, \text{称a为(G,*)中的有限阶元} \tag{188}$$
$$o(a) = min\{m|m \in Z^+, a^m = I_G\} \tag{189}$$
$$o(a)\text{为a的阶} \tag{190}$$
$$2.if\forall n \in Z^+, st.a^n = I_G, \text{称a为(G,*)中的无限阶元} \tag{191}$$
$$o(a) = +\infty \tag{192}$$
$$if a \in G \text{is infinite order element}, \forall i, j \in Z^+, a^i = a^j \Leftrightarrow i = j \tag{193}$$
$$Pf: \tag{194}$$
$$\forall n \in Z^+, a^n \neq I_a, a^{-n} \neq I_a \tag{195}$$
$$\text{suppose} i, j \in Z, a^i = a^j \tag{196}$$
$$\therefore a^{-i} * a^i = a^{-i} * a^j \to a^{j-i} = I_a \tag{197}$$
$$\therefore i = j \tag{198}$$

suppose $a \in G$，a 是有限阶元，记 $o(a) = m$（m is an integer）

$$1.\forall j \in Z, a^j = I_G \leftrightarrow m|j \tag{199}$$
$$2.a^i = a^j \Leftrightarrow m|(i-j) \to i \equiv j \pmod m \tag{200}$$
$$3. < a >= \{a^j|j \in \{0, 1, ..., m-1\}\}, | < a > | = m; a^i = a^j \to i = j \tag{201}$$

Pf:

$$1. \to if m|j, \text{suppose } j = ml, l \in Z, a^j = a^{ml} = (a^m)^l = I_G \tag{202}$$
$$\leftarrow \text{suppose } j = qm + r, q \in Z, r \in \{0, 1, ..., m-1\}, \tag{203}$$
$$a^j = a^{qm+r} = a^{qm} * a^r = I_G * a^r = a^r \tag{204}$$
$$\because r \in \{0, 1, ..., m-1\}, \therefore r = 0 \tag{205}$$
$$\therefore m|j \tag{206}$$
$$\text{if } H = \{i|i \in Z, a^i = I_G\}, \text{H is a subgroup of } < a > \tag{207}$$
$$\text{H is a subgroup of (Z,+)}, H = \{mq|q \in Z\} \tag{208}$$
$$2.a^i = a^j \Leftrightarrow m|(i-j) \to i \equiv j \pmod m \tag{209}$$
$$3. \because i, j \in \{0, 1, ..., m-1\} \leftrightarrow i \equiv j \pmod m \leftrightarrow i = j \tag{210}$$

the definition of cyclic group:

$$\exists a \in G, st. < a >= G, \text{称G为循环群} \tag{211}$$

the definition of 同态，同构：

$$(G,*),(H,\circ)\text{是群} \tag{212}$$
$$f:G\to H \tag{213}$$
$$\text{if}\forall a,b\in G, f(a*b)=f(a)\circ f(b), \text{称f为群G到群H的同态} \tag{214}$$
$$\text{if} f:G\to H \text{ is a bijection}, \text{称f为群G到群H的同构} \tag{215}$$
$$\tag{216}$$

example1:

$$(\{1,-1\},*)\text{and}(\{0,1\},\text{模2加法}) \tag{217}$$
$$1*1=1, 1*-1=-1, -1*1=-1, -1*-1=1 \tag{218}$$
$$0\oplus 0=0, 0\oplus 1=1, 1\oplus 0=1, 1\oplus 1=0 \tag{219}$$
$$f\{0,1\}\to\{1,-1\} \tag{220}$$
$$f(0)=1, f(1)=-1 \tag{221}$$

example2:

$$(R,+)\to(R^+,*) \tag{222}$$
$$f(x)=2^x; \tag{223}$$
$$\tag{224}$$
$$(R^+,*)\to(R,+) \tag{225}$$
$$log_2(x) \tag{226}$$
$$log_2(x)=f^{-1}(x) \tag{227}$$

example3:

$$f:R\to\text{单位圆上的点}=\{Z|Z\in C,|Z|=1\} \tag{228}$$
$$(R,+)\to(\text{单位圆上的点},\times) \tag{229}$$
$$[0,2\pi]\to\text{单位圆上的点}=\{Z|Z\in C,|Z|=1\} \tag{230}$$
$$f(\alpha+\beta)=f(\alpha)\times f(\beta) \tag{231}$$

example 4:

$$\mathbb{C} \to M_{2\times 2}(\mathbb{R}) \tag{232}$$

$$F(a+\sqrt{-1}b) = \begin{pmatrix} a & b \\ -b & a \end{pmatrix} \qquad \forall \alpha, \beta \in \mathbb{C} \tag{233}$$

$$f(\alpha+\beta) = f(\alpha) + f(\beta) \tag{234}$$

$$f(\alpha\beta) = f(\alpha)f(\beta) \tag{235}$$

$$Pf: \tag{236}$$

$$\text{suppose } \alpha = a+\sqrt{-1}b, \beta = c+\sqrt{-1}d \tag{237}$$

$$\text{then } \alpha+\beta = (a+\sqrt{-1}b) + (c+\sqrt{-1}d) = (a+c) + (\sqrt{-1}(b+d)) \tag{238}$$

$$f(\alpha) = \begin{pmatrix} a & b \\ -b & a \end{pmatrix} \tag{239}$$

$$f(\beta) = \begin{pmatrix} c & d \\ -d & c \end{pmatrix} \tag{240}$$

$$f(\alpha\beta) = \begin{pmatrix} \dots \end{pmatrix} \to \text{blablabla} \tag{241}$$

$$f(a\alpha) = af(\alpha) \tag{242}$$

$$\tag{243}$$

设 $(G,*)$ 和 $(H,\circ)$ 为群，

$$f: G \to H \tag{244}$$

$$\text{if} \forall a, b \in G, f(a*b) = f(a)\circ f(b), \text{称f为群G到群H的同态} \tag{245}$$

$$\text{if} f: G \to H \text{ is a bijection, 称f为群G到群H的同构} \tag{246}$$

$$\tag{247}$$

群同态的性质：

$$1.f(I_G) = I_H \tag{248}$$

$$2.f(a^{-1}) = (f(a))^{-1}\text{第一个指G下的逆元，第二个是H下的逆元} \tag{249}$$

$$3.f(a^m) = (f(a))^m \tag{250}$$

Pf:

$$1.f(I_G) = f(I_G * I_G) = f(I_G) \circ f(I_G) \tag{251}$$
$$\rightarrow \text{由于消去律}, f(I_G) = I_H \tag{252}$$
$$2f(a * a^{-1}) = f(a^{-1}) \circ f(a) \tag{253}$$
$$RHS = f(I_G) = I_H \tag{254}$$
$$ok \quad 3.\text{suppose} a \in G, f(a^2) = f \tag{255}$$
$$\dots \tag{256}$$
$$\text{归纳} \tag{257}$$
$$k \in Z+ \Leftrightarrow f(a^k) = f(a)^k \tag{258}$$
$$\therefore f(a^{k+1}) = f(a^k * a) = ... \tag{259}$$
$$f(a^{-m}) = f((a^m))^{-1} = (f(a^m))^{-1}, \text{由整数时的情况}, = (f(a)^m)^{-1} = f(a)^{-m} \tag{260}$$

example1

$$M_(n * n)(\mathbb{R}) \rightarrow \mathbb{R} \tag{261}$$
$$f(A) = det(A) \tag{262}$$
$$det(AB) = det(A) * det(B) \tag{263}$$
$$|A| \neq 0 \Leftrightarrow A\text{可逆} \tag{264}$$

example2

$$Gl_n(\mathbb{R}) \rightarrow \text{R上的n阶可逆矩阵} Gl_(n+1)(\mathbb{R}) \tag{265}$$
$$f(A) = \begin{pmatrix} A & O \\ O & det(A)^{-1} \end{pmatrix} \tag{266}$$
$$det(f(A)) = det(A) * det(A)^{-1} = 1 \tag{267}$$

凯莱定理：概念循环群：

$$\text{a set X} \tag{268}$$
$$\text{映射：} M(X) : \{f : X \rightarrow X\} \tag{269}$$
$$M(X) \text{ is a monoid(幺元是恒等映射)} \tag{270}$$
$$Sym(X) = \{f : X \rightarrow X | f\text{是双射}\} \tag{271}$$
$$(Sym(X), \circ) \text{ is a group} \tag{272}$$

$$(G,*)\text{is a semigroup} \tag{273}$$
$$a \in G, \text{诱导G -¿ G 上的映射} L_a \tag{274}$$
$$\forall b \in G, L_a(b) = a * b \tag{275}$$
$$L_a \in M(G) \tag{276}$$

凯莱定理：

$$(G,*)\text{is a semigroup} \tag{277}$$
$$\forall a \in G, L_a : G \to G \tag{278}$$
$$\text{定义f:} G \to M(G) \tag{279}$$
$$f(a) = L_a \tag{280}$$
$$\text{then:} \tag{281}$$
$$1.\forall u, v \in G, L_{u*v} = L_u \circ L_v \tag{282}$$
$$\therefore f \text{为} (G,*) \text{到} (,\circ) \text{的同态} \tag{283}$$
$$2.(G,*)\text{is a monoid} \tag{284}$$
$$f(I_G) = L_{I_G} = idx, \text{f is a 单射} \tag{285}$$
$$3.(G,*)\text{is a group}, L_a\text{is a 双射} \tag{286}$$
$$\therefore f \text{为} (G,*) \text{到} (G,*) \text{的同态} \tag{287}$$

Pf:

$$1.\forall u, v \in G, L_{u*v} = L_u \circ L_v \quad (288)$$
$$\forall b \in G, L_{u*v}(b) = (u * v) * b \quad (289)$$
$$(L_u \circ L_v)(b) = L_u(L_v(b)) = L_u(v * b) = u * (v * b) \quad (290)$$
$$ok \quad (291)$$
$$2.\forall b \in G, L_{I_G}(b) = b \quad (292)$$
$$L_{I_G} = idx \quad (293)$$
$$\text{suppose} u, v \in G, f(u) = f(v) \quad (294)$$
$$L_u = L_v \quad (295)$$
$$\therefore L_u(I_G) = L_v(I_G) \quad (296)$$
$$\therefore u = v \quad (297)$$
$$3.\text{证单射：} u, v \in G, L_a(u) = L_a(v) \quad (298)$$
$$a * u = a * v \to u = v \quad (299)$$
$$\text{证满射(每个b都有对应的u)} \quad (300)$$
$$\forall b \in G, L_a(a^1 * b) = b \quad (301)$$

$$|G| = n, |Sym(G)| = n! \quad (302)$$

2.4 正规子群

DEF:

$$(G, *) \text{ is a group} \quad (303)$$
$$H\text{is a subgroup of } (G, *)\text{,H is a normal subgroup of } (G, *) \text{ if} \quad (304)$$
$$\forall g \in G, \forall h \in H, ghg^{-1} \in H \quad (305)$$
$$H \lhd g \quad (306)$$
$$\text{ if G is a 交换群, H 全都是正规子群(因为可以交换)} \quad (307)$$

example1:

$$GL_n(R)\text{所有 n×n 的实数可逆方阵构成的集合} \tag{308}$$
$$SL_n(R) = \{A|A \in GLn(R), det(A) = 1\} \tag{309}$$
$$SL_n(R) \text{ is a subgroup of } GL_n(R) \tag{310}$$
$$SL_n(R) \text{ is a normal subgroup of } GL_n(R) \tag{311}$$
$$Pf: \quad \forall A \in SL_n(R), \forall C \in GL_n(R), \tag{312}$$
$$det(C^{-1}AC) = det(C^{-1}) * det(A) * det(C) = 1 * 1 * 1 = 1 \tag{313}$$
$$\therefore SL_n(R) \lhd GL_n(R) \tag{314}$$

对于平凡子群:

$$\{I_G\}, G \text{ is normal subgroups of } G \tag{315}$$
$$\text{单群: 除了这俩没有其他正规子群(素数群：除了这俩没有其他子群和正规子群)} \tag{316}$$

命题：

$$(G, *), (H, \triangle) \text{ is a group} \tag{317}$$
$$\text{f 是同态} \tag{318}$$
$$\text{记}ker(f) = \{a \in G|f(a) = I_G = I_H\} \tag{319}$$
$$ker(f) \lhd G \tag{320}$$
$$Pf: \tag{321}$$
$$f(I_G) = I_H\text{所以ker不是空集} \tag{322}$$
$$a, b \in ker(f), f(a) = f(b) = I_H \tag{323}$$
$$f(a * b) = f(a)\triangle f(b) = I_H * I_H = I_H \tag{324}$$
$$f(a^{-1}) = (f(a))^{-1} = I_H \tag{325}$$
$$\text{ if } a * b \in ker(f), \therefore a^{-1} \in ker(f) \tag{326}$$
$$\text{suppose } g \in G, a \in ker(f), \tag{327}$$
$$f(g * a * g^{-1}) = f(g)\triangle f(a)\triangle f(g^{-1}) = f(g) * f(g^{-1}) = f(g) * (f(g))^{-1} = I_H \tag{328}$$

$$g * a * g^{-1} : \text{a关于g的共轭元素，类似相似矩阵什么的} \tag{329}$$

正规子群和等价关系：

$$\text{fact}: a, c, d \in G, c \sim d \to a * c \sim a * d \tag{330}$$
$$\because c \sim d, \exists h \in H, st.d = h * c \tag{331}$$
$$a * d = a * (c * d) = (a * c) * h \to a * c \sim a * d \tag{332}$$

下面两个等价：

$$1.H \lhd G \tag{333}$$
$$2.\forall a, b, c, d \in G, a \sim b, c \sim d \to a * c \sim b * d \tag{334}$$
$$Pf: \tag{335}$$
$$1 \rightleftarrows 2 \qquad a \sim b, \exists u \in H, st.b = a * u \tag{336}$$
$$c \sim d, \exists v \in H, st.d = c * v \tag{337}$$
$$b * d = a * u * c * v = a * (c * c^{-1}) * u * c * v = (a * c) * (c^{-1} * u * c) * v \tag{338}$$
$$u \in H, H \lhd G, \therefore c^{-1} * u * c \in H, v \in H, \therefore a * c \sim b * d \tag{339}$$

in fact:

$$H \lhd G \text{ if} \tag{340}$$
$$H\text{is a subgroup of } G \tag{341}$$
$$\forall g \in G, \forall a \in H, g * a * g^{-1} \in H \text{ or } g^{-1} * a * g \in H \tag{342}$$
$$Pf: \tag{343}$$
$$\to \text{suppose} g \in H, a \in H, g^{-1} \in G, H \lhd G \tag{344}$$
$$(g^{-1})^{-1} = g \tag{345}$$
$$\therefore g^{-1} * a * g \in H\text{两个形式都可以} \qquad \leftarrow g \in H, a \in H, \text{for } g^{-1} \in H, (g^{-1})^{-1} * a * g^{-1} \in H \tag{346}$$
$$\therefore H \lhd G \tag{347}$$

another example:

$$n \in Z^+, Z_n = \{0, 1, ..., n-1\} \tag{348}$$
$$(Z_n, \oplus)(a \oplus b = (a+b) \mod n) \tag{349}$$
$$a \equiv a\%n(modn) \tag{350}$$
$$\text{结合律}:(a \oplus b) \oplus c = a \oplus (b \oplus c) \equiv a+b+c \mod n \tag{351}$$
$$\text{幺元 } 0 \tag{352}$$
$$\forall a \in Z_n \tag{353}$$
$$a \oplus 0 = a \oplus 0 \equiv a \mod n \tag{354}$$
$$\text{逆元}:0 \sim 0; n \sim n-a(1 \leqslant a \leqslant n-1) \tag{355}$$
$$\text{交换率}:a \oplus b = b \oplus a \tag{356}$$
$$a_1 \oplus a_2 \oplus ... \oplus a_n = \sum a_i(modn) = \sum a_i\%n \tag{357}$$

$$R \leftrightarrow Z \tag{358}$$
$$H \leftrightarrow \{nq|q \in Z\} \tag{359}$$
$$? \leftrightarrow \{0, 1, ..., n-1\}? \tag{360}$$
$$\tag{361}$$
$$1.a, b \in Z_n, a \equiv b \to a = b \tag{362}$$
$$2.\forall k \in Z, \exists r \in Z_n, st.k \equiv r \mod n \tag{363}$$
$$(G, \sim), T \subset G, \text{满足} \tag{364}$$
$$1.\forall a, b \in T, a \sim b \to a = b \tag{365}$$
$$2.\forall g \in G, \exists a \in T, st.g \sim a\text{这里T不一定为群} \tag{366}$$
$$example: \tag{367}$$
$$G = \{1, 2, 3, 4\}, \text{以奇偶性为等价类} \tag{368}$$
$$T = \{1, 2\}or\{3, 4\}or\{1, 4\}or\{2, 3\} \tag{369}$$

$$\text{在T上定义二元运算}(T,\circledast) \qquad \forall a,b\in T, a*b\in G \tag{370}$$
$$\text{由以上的1和2，}\exists\text{唯一}c\in T, st.a*b\sim c \tag{371}$$
$$\text{在这里定义符合以上条件的}, a\circledast b=c \tag{372}$$
$$(\text{对于}\forall a,b\in Z_n, a\oplus b=(a+b) \mod n) \tag{373}$$
$$\circledast \text{ is a binary operation on } T \tag{374}$$
$$\text{now we prove } (T,\circledast) \text{ is a group} \tag{375}$$
$$1.c=a\circledast b\sim a*b \tag{376}$$
$$(a\circledast b)*c\sim(a*b)*c \tag{377}$$
$$\therefore(a\circledast b)\circledast c\sim(a\circledast b)*c\sim(a*b)*c \tag{378}$$
$$\therefore(a\circledast b)\circledast c\sim a*b*c \tag{379}$$
$$\text{同理，}a\circledast(b\circledast c)\sim a*(b\circledast c)\sim a*(b*c)\sim(a*b)*c \tag{380}$$
$$\therefore(a\circledast b)\circledast c\sim a\circledast(b\circledast c) \tag{381}$$
$$\text{由定义}, (a\circledast b)\circledast c=a\circledast(b\circledast c) \tag{382}$$
$$2.\text{由1,2 }\exists\text{唯一}w\in T, st.I_G\sim w \tag{383}$$
$$\forall a\in T, I_G\sim w, \therefore a*I_G\sim a*w \tag{384}$$
$$a\sim a*w \tag{385}$$
$$\because a\in T, \therefore a\circledast w=a \tag{386}$$
$$w*a\sim I_G*a=a, w\circledast a=a \tag{387}$$
$$\text{w是幺元} \tag{388}$$
$$3.\text{逆元} \tag{389}$$
$$\forall a\in T, \text{a在G中有逆元}\to a^{-1}*a=I_G \tag{390}$$
$$\exists\text{唯一}b\in T, st.b\sim a^{-1} \tag{391}$$
$$a\circledast b=b\circledast a=w \tag{392}$$
$$Pf: \tag{393}$$
$$b\sim a^{-1}\to a*b\sim I_G\sim w; b*a\sim I_G\sim w \tag{394}$$
$$\therefore b\circledast a=a\circledast b=w \tag{395}$$
$$\to T\text{is a group} \tag{396}$$

SUMMARY:

$$(G,*), H \triangleleft G \tag{397}$$
$$(T,\circledast) \tag{398}$$
$$\text{考虑f:}G \to T \tag{399}$$
$$\forall g \in G, \exists a \in T, st.g \sim a \tag{400}$$
$$\text{令}f(g) = a(f(g) \sim g) \tag{401}$$
$$\text{则}f\text{为}(G,*)\text{到}(T,\circledast)\text{的同态} \tag{402}$$
$$\text{且}ker(f) = H; (\{g|g \in G, f(g) = I_T = w\}) \tag{403}$$
$$\text{suppose } u, v \in G, Pf : f(u*v) = f(u) \circledast f(v) \tag{404}$$
$$def : f(u*v) \sim u*v, f(u) \sim u, f(v) \sim v \tag{405}$$
$$\therefore f(u*v) \sim u*v \sim f(u)*f(v) \sim f(u) \circledast f(v) \tag{406}$$
$$\therefore f(u)*f(v) = f(u*v), f(u)*f(v) = f(u) \circledast f(v) \tag{407}$$
$$\therefore OK \tag{408}$$
$$\tag{409}$$
$$Pf : ker(f) = H \tag{410}$$
$$\forall g \in G, g \in ker(f) \to f(g) = I_T = w \tag{411}$$
$$\leftrightarrow g \sim w(\text{the definition of f}) \tag{412}$$
$$\leftrightarrow g \sim I_T(w \sim I_G) \tag{413}$$
$$g * I_T^{-1} = g \in H(\text{the definition of } \sim) \tag{414}$$
$$\tag{415}$$

example: G/H:全体左陪集

$$(G/H,\circledast)(\text{子集之间的乘法}) \tag{416}$$
$$\text{幺元}H,\text{逆元}a^{-1}H \tag{417}$$
$$f : G \to G/H \tag{418}$$
$$f(a) = aH, \text{suppose } a \in G \tag{419}$$
$$\text{f是群G到群G/H的同态}, ker(f) = H \tag{420}$$
$$\tag{421}$$

$$G = (Z, +), n \in Z^+ \tag{422}$$
$$H = \{nq|q \in Z\} \tag{423}$$
$$a \sim b \leftrightarrow a \equiv b(modn) \tag{424}$$
$$T = \{0, 1, ..., n-1\} \tag{425}$$
$$a \circledast b = (a+b) \mod n \tag{426}$$
$$\tag{427}$$

$$A, B \subseteq G \tag{428}$$
$$AB = \{ab|a \in A, b \in B\} \tag{429}$$
$$AB \subseteq G \tag{430}$$
$$\tag{431}$$

$$G \text{ is a group}, H \lhd G \tag{432}$$
$$\text{then } (G/H, *) \text{ is a group}, *\text{is the multiply between subsets} \tag{433}$$
$$\text{and} \tag{434}$$
$$1.\forall a, b \in G, (aH) * (bH) = abH(\text{这个是运算结果}) \tag{435}$$
$$2.H\text{是幺元} \tag{436}$$
$$\forall a \in H, aH * H = H * aH = aH \tag{437}$$
$$3.\forall a \in G, \exists a^{-1} \in G, st.a * a^{-1} = I_G \tag{438}$$
$$(aH)(a^{-1}H) = (a^{-1}H)aH = H \tag{439}$$
$$\tag{440}$$
$$4.\text{def}\pi_H : G \to G/H \tag{441}$$
$$\text{suppose } a \in G, \pi_H(a) = aH \tag{442}$$
$$\pi_H\text{是同态} \tag{443}$$
$$ker(\pi_H) = H, ran(\pi_H) = G/H \tag{444}$$
$$\tag{445}$$

$$G, H \leqslant G, HH = H \tag{446}$$
$$H \lhd G, \forall a \in G, aH = Ha, \qquad \forall A \subseteq G, AH = HA \tag{447}$$
$$\tag{448}$$

$$Pf: \tag{449}$$
$$1.HH = \{ab|a \in H, b \in H\} \subseteq H \tag{450}$$
$$I_G \in H, H = \{I_G h|h \in H\} \subseteq HH \tag{451}$$
$$OK \tag{452}$$
$$2.\text{对于} aH, \forall h \in H, ah = (aha^{-1})a \in Ha \tag{453}$$
$$\therefore aH \subseteq Ha \tag{454}$$
$$Ha : \forall h \in H, ha = a(a^{-1}ha) \in aH \tag{455}$$
$$OK \tag{456}$$

Pf一些命题:

$$1.(aH)(bH) = a(Hb)H = a(bH)H = (ab)H \tag{457}$$
$$2.HaH = aHH = aH \tag{458}$$
$$3.aH(a^{-1}H) = H \tag{459}$$
$$4.\forall a, b \in G, \pi_H(ab) = \pi_H(a)\pi_H(b) \tag{460}$$
$$\pi_H(ab) = aHbH = a(bH)H = a(bH)H = (ab)H = \pi_H(ab) \tag{461}$$
$$\forall a \in G, a \in ker(\pi_H) \leftrightarrow \pi_H(a) = H \leftrightarrow aH = H \leftrightarrow a \in H \tag{462}$$
$$\therefore ker(\pi_H) = H \tag{463}$$

2.5 同态定理

$$G, L \text{are groups} \tag{464}$$
$$f : G \to L \tag{465}$$
$$\text{if } f(a * b) = f(a) * f(b), \text{称f为群G到群L的同态} \tag{466}$$
$$ker(f) = \{a|a \in G, f(a) = I_L\} \tag{467}$$
$$ker(f) \lhd G \tag{468}$$

同态定理：

$$G, L \text{ are groups} \tag{469}$$

$$f : G \to Ltext\text{fi˘} f\text{:}G0L\text{fi}\Delta \tag{470}$$

$$ker(f) = \{a|a \in G, f(a) = I_L\} \tag{471}$$

$$1.\forall a, b \in G, aH = bH \leftrightarrow f(a) = f(b) \tag{472}$$

$$2.\text{def } \varphi : G/H \to L \tag{473}$$

$$\forall a \in G, \varphi(aH) = f(a) \tag{474}$$

$$\therefore \varphi \text{ is a 同态和单射} \tag{475}$$

$$ran(\varphi) = ran(f) \tag{476}$$

$$\varphi : G/H \to ran(f)\text{的群同构} \tag{477}$$

$$\text{记作} G/H \overset{\varphi}{\cong} \tag{478}$$

$$\text{if 同态f是双射，f同构，记作} G \overset{f}{\cong} L \tag{479}$$

$$f : G \to L\text{的同态} \tag{480}$$

$$1.A \leqslant G \to f([A]) = \{f(a)|a \in A\} \leqslant L \tag{481}$$

$$2.B \leqslant G \to f^{-1}([B] = \{f(a)|a \in B\} \leqslant G \tag{482}$$

证明同态定理

$$1. \Rightarrow aH = bH \leftrightarrow \exists h \in H, st.b = ah \tag{483}$$
$$\because h \in ker(f), \therefore f(h) = I_L \tag{484}$$
$$f(b) = f(ah) = f(a)f(h) = f(a)I_L = f(a) \tag{485}$$
$$\Leftarrow f(a) = f(b) \tag{486}$$
$$I_L = f(a)^{-1}f(a) = f(a)^{-1}f(b) = f(a^{-1})f(b) = f(b^{-1})f(b) = f(a^{-1}b) \tag{487}$$
$$\therefore a^{-1}b \in H.OK \tag{488}$$
$$(\text{ if } a_1H = a_2H \to \varphi(a_1H) = \varphi(a_2H)) \tag{489}$$
$$2. \tag{490}$$
$$1.\text{先说明}\varphi\text{是合理定义的} \tag{491}$$
$$\text{if } a, b \in G, aH = bH \to f(a) = f(b) \tag{492}$$
$$\to aH = bH \to \varphi(aH) = \varphi(bH) \tag{493}$$
$$\varphi\text{是同态，下面证明}\varphi(aH)\varphi(bH) = \varphi((aH)(bH)) \tag{494}$$
$$RHS = \varphi(abH) = f(ab) = f(a)f(b) = LHS \tag{495}$$
$$\text{证明是单射} \tag{496}$$
$$\varphi(aH) = \varphi(bH), \to f(a) = f(b) \to a = b, \therefore aH = bH \tag{497}$$
$$ran(\varphi) = ran(f), \text{suppose } a \in G \tag{498}$$
$$\tag{499}$$

$$\begin{tikzcd}
 & G/H \arrow[dr, "\varphi"] & \\
G \arrow[ur, "\pi_H"] \arrow[rr, "f"'] & & L
\end{tikzcd}$$

$\varphi \circ \pi_H = f$

example:

$$(Z, +), n \in Z^+ \tag{500}$$
$$f : Z \to Z_n \tag{501}$$
$$\forall a \in Z, f(a) = a \mod n, \text{这个是同态} \tag{502}$$
$$f : (Z, +) \to (Z_n, \oplus)\text{的同态} \tag{503}$$
$$ran(f) = Z_n, \text{suppose } a \in Z \tag{504}$$
$$ker(f) = \{a|a \in Z, f(a) = 0\} = \{nq|q \in Z\} \tag{505}$$
$$G/H \overset{\varphi}{\to} Z_n \tag{506}$$
$$\varphi(aH) = a\%n, \text{是同构} \tag{507}$$

2.6 有限循环群

G是有限的循环群

$$\exists g \in G, st.G =< g >= \{g^i | i \in Z\} \tag{508}$$
$$o(g) = n(g^n = I_G) \tag{509}$$
$$\forall i \in \{1, 2, ..., n-1\}, g^i \neq I_G \tag{510}$$
$$\therefore G = \{i | i \in \{1, 2, ..., n-1\}\} \tag{511}$$

Pf:

$$1.\text{suppose} d \in Z^+, d|n, H =< g^d >, \tag{512}$$
$$\rightarrow H \leqslant G, |H| = \frac{n}{d} H = \{y | y \in G, y^{\frac{n}{d}} = I_G\} \tag{513}$$
$$2.H \leqslant G, \exists d \in Z^+, H =< g^d >, d|n, st.H =< g^d > \tag{514}$$

有限循环群的子群，置换群

$$G, H \leqslant G, \text{定义等价关系} \sim \tag{515}$$
$$\forall a, b \in G, a \sim b \leftrightarrow a^{-1} b \in H \leftrightarrow \exists h \in H, b = ah \tag{516}$$
$$1.(G, \sim)\text{为等价关系。用H为子群的特点} \tag{517}$$
$$2.a \in G, \{b | b \in G, a \sim b\} = \{a * h | h \in H\} = aH \tag{518}$$
$$3.a \sim b \rightarrow \forall g \in G, ga \sim gb \tag{519}$$

从陪集定义出发:

$$aH = \{a * h | h \in H\} \tag{520}$$
$$I_H \in H \tag{521}$$
$$\therefore a \in aH \tag{522}$$
$$a, b \in G\text{下面几个等价} \tag{523}$$
$$1.a^{-1} b \in H \tag{524}$$
$$2.h \in aH \tag{525}$$
$$3.\exists a, h, b = ah \tag{526}$$
$$4.aH \cap bH \neq \varnothing \tag{527}$$
$$5.aH = bH \tag{528}$$

Pf:

$$2 \leftrightarrow 1 \leftrightarrow 3 \tag{529}$$
$$b \in aH \to b = a * h, h \in aH \tag{530}$$
$$\leftrightarrow \exists h \in H, st.a^{-1}b = h \in H \tag{531}$$
$$2 \leftrightarrow 4 \tag{532}$$
$$b \in aH, b \in bH, \therefore aH \cap bH \neq \varnothing \tag{533}$$
$$4 \to 3 \tag{534}$$
$$x \in aH \cap bH, \tag{535}$$
$$\because x \in aH, \exists h_1 \in H, st.x = a * h_1 \tag{536}$$
$$\because x \in bH, \exists h_2 \in H, st.x = b * h_2 \tag{537}$$
$$\therefore ah_1 = b * h_2 \tag{538}$$
$$\therefore a * h_1 * h_2^{-1} = b \in aH \tag{539}$$
$$3 \to 5 \tag{540}$$
$$b = ah, h \in H, \text{Pf:} bH \subseteq aH \tag{541}$$
$$\forall x \in H, bx = ahx = a(hx) \tag{542}$$
$$\because H \leqslant G, h, x \in H, \therefore hx \in H \tag{543}$$
$$\therefore bx \in bH, bH \subseteq aH \tag{544}$$
$$\text{Pf:} aH \subseteq bH \tag{545}$$
$$b = ah, a = bh^{-1}, h \in H \to h^{-1} \in H \tag{546}$$
$$\forall x \in H, ax = bh^{-1}x = b(h^{-1}x) \in bH \tag{547}$$
$$\therefore aH \subseteq bH \tag{548}$$
$$\therefore aH = bH \tag{549}$$

G为循环群，$|G|$=n,设$G =< a >$,则

$$1.\text{suppose} d \in Z^+, d|n, H =< a^d > \tag{550}$$
$$\to H \leqslant G, |H| = \frac{n}{d}, H = \{y | y \in G, y^{\frac{n}{d}} = I_G\} \tag{551}$$
$$2.\text{suppose} H \leqslant G, \exists d \in Z^+, st.H =< a^d > \tag{552}$$
$$\{H | H \leqslant G\} \leftrightarrow \{d | d \in Z^+, d|n\}\text{一一对应} \tag{553}$$

有几个子群：写出因子列出来。

$$eg.n = 6 \tag{554}$$
$$< a^d > \rightleftarrows d \tag{555}$$
$$a, a^2, a^3, a^6 = \{I_G\} \tag{556}$$

阶数的定义和性质：

$$1.\forall m \in Z^+, \exists m_0 \in Z^+, a^{m_0} = I_G \tag{557}$$
$$n = min\{m|a^m = I_G, m \in Z^+\} \tag{558}$$
$$\text{记}o(a) = n \tag{559}$$
$$a^i = I_G \leftrightarrow i|n \tag{560}$$
$$a^i = a^j \leftrightarrow i \equiv j \mod n \tag{561}$$
$$< a >= \{a^j|j = 0, 1, ..., n-1\} \tag{562}$$
$$| < a > | = n = o(a) \tag{563}$$

Pf:

$$1.o(a) = n; \text{断言}o(a^d) = \frac{n}{d} \tag{564}$$
$$(a^d)^{\frac{n}{d}} = I_G \tag{565}$$
$$Pf \tag{566}$$
$$i \in \{1, 2, ..., n-1\}, \forall (a^d)^i = I_G \tag{567}$$
$$\leftrightarrow a^{id} = I_G \tag{568}$$
$$\leftrightarrow n|di \tag{569}$$
$$\leftrightarrow \frac{n}{d}|i \tag{570}$$
$$| < a^d > | = o(a^d) = \frac{n}{d} \tag{571}$$
$$2.H\text{也是一个循环群} \tag{572}$$
$$\exists b \in G, b = a^d, H =< b >=< a^d > \tag{573}$$
$$\tag{574}$$
$$\forall h \in H, h \in< a^d >, \exists i \in Z^+, st.h = (a^d)^i = a^{di} \tag{575}$$
$$h^{\frac{n}{d}} = a^{ni} = I_G \tag{576}$$
$$\therefore \forall y \in G, \exists d, s.t.y^{\frac{n}{d}} = I_G, \exists i \in Z^+, st.y = (a^d)^i = a^{di} \tag{577}$$
$$\because y \in< a >, \exists j \in Z, st.y = a^j \tag{578}$$
$$I_G = y^{\frac{n}{d}} = a^{j*\frac{n}{d}} \therefore n|j * \frac{n}{d} \tag{579}$$
$$\therefore d|j \tag{580}$$
$$y = a^j, H =< a^d >, \therefore y = (a^d)^{\frac{j}{d}} \in H \tag{581}$$

$$\forall k \in Z, o(a^k) = \frac{n}{gcd(n,k)} \tag{582}$$
$$< a^k >=< a^{\frac{n}{gcd(n,k)}} > \tag{583}$$

2.7 置换群

设X是一个集合，

$$Sym(X) = \{\sigma | \sigma X \to X, \sigma\text{是双射（置换）}\} \tag{584}$$
$$(Sym(X), \circ) \text{ is a group} \tag{585}$$
$$I_X : idx \qquad \sigma \in Sym(X), \sigma^{-1} \in Sym(x) \tag{586}$$
$$(\sigma \circ \sigma^{-1} = \sigma^{-1} \circ \sigma = idx) \tag{587}$$
$$Sym(x)\text{是X上的对称群} \tag{588}$$
$$H \leqslant Sym(X), H\text{也是X上的置换群} \tag{589}$$
$$I_X \in H, \forall \sigma_1, \sigma_2 \in H, \sigma_1\sigma_2 \in H, \sigma_1^{-1} \in H \tag{590}$$
$$\forall a \in G, \text{def } L_a \in Sym(G), (\text{是双射}) \tag{591}$$
$$\forall b \in G, L_a(b) = a * b\text{左乘} \tag{592}$$
$$f : G \to Sym(G) \tag{593}$$
$$f(a) = L_a, f(ab) = L_a \circ L_b\text{f是单射，同态} \tag{594}$$

置换群的例子：

$$X = \{1, 2, ..., n | n \in Z^+\} \tag{595}$$
$$Sym(X) = S_n \tag{596}$$
$$|S_n| = n! \tag{597}$$
$$eg.n = 3 \tag{598}$$
$$S_3 = \{(1,2,3), (1,3,2), (2,1,3), (2,3,1), (3,1,2), (3,2,1)\} \tag{599}$$
$$\{\sigma | \sigma(i) \neq i \forall 1 \leqslant i \leqslant n\} = C_n \tag{600}$$
$$\frac{|C_n|}{n!} = \Sigma_{i=0,n} \frac{(-1)^n}{i!} \tag{601}$$

$$Sym(X)\text{对换i,j}, i \in X, j \in X, i \neq j, \sigma(i) = j, \sigma(j) = i \tag{602}$$
$$\text{三轮换} \tag{603}$$

计算题

$$S_5, \tag{604}$$

$$\alpha = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 3 & 1 & 5 & 4 \end{pmatrix} \tag{605}$$

$$\beta = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 3 & 4 & 5 & 2 \end{pmatrix} \tag{606}$$

$$\alpha \circ \beta = \alpha(\beta) = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 1 & 5 & 4 & 3 \end{pmatrix} \tag{607}$$

$$\beta \circ \alpha = \beta(\alpha) = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 4 & 1 & 2 & 5 \end{pmatrix} \tag{608}$$

$$\alpha^{-1} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 1 & 2 & 5 & 4 \end{pmatrix} \tag{609}$$

$$\tag{610}$$

三次对称群

$$Sym(X) = \{\sigma|\sigma : X \to X\text{双射}\} \tag{611}$$
$$S_3 = \{(1,2,3),(1,3,2),(2,1,3),(2,3,1),(3,1,2),(3,2,1)\} \tag{612}$$
$$\text{第一个非交换群。一个六阶非交换群同构于}S_3 \tag{613}$$
$$\text{一阶ok；二阶e,a,三阶循环群，四阶循环或者klein，五阶素数循环群} \tag{614}$$
$$\sigma = (a_1, a_2, a_3, ..., a_m) : \sigma(a_1) = a_2, ..., \sigma(a_m) = a_1 \tag{615}$$
$$\text{幺元：}\begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix} \tag{616}$$
$$\text{令}\tau(1,2,3) \tag{617}$$
$$\tau^2 = (1,3,2) \tag{618}$$
$$\tau^3 = I_{S_3} \tag{619}$$
$$\tag{620}$$
$$H =< \tau >= \{(1,2,3),(1,3,2), idx\} \lhd S_3 \tag{621}$$
$$\eta = (1,2) \tag{622}$$
$$\eta\tau\eta^{-1} = \tau^2 \tag{623}$$
$$S_3 =< \{\eta, \tau\} > \tag{624}$$
$$|H| = 3(\tau^i) \tag{625}$$
$$|\eta H| = 3(\eta\tau^i)(\eta \notin H) \tag{626}$$
$$\therefore H \cup \eta H = S_3 \tag{627}$$
$$\text{计算题：} \qquad \eta\tau \neq \tau\eta \tag{628}$$
$$\eta\tau\eta^{-1} = \tau^2 \tag{629}$$
$$\tau\eta\tau\eta^{-1}\tau^2 = \tau\tau\tau^2 = \tau \tag{630}$$
$$S_3\text{'s subgroup :} \tag{631}$$
$$1.\{id\} \tag{632}$$
$$2.\{id,(1,2)\},\{id,(2,3)\},\{id,(1,3)\} \tag{633}$$
$$3.\{id,(1,2,3),(1,3,2)\}\text{only one} \tag{634}$$
$$6.S_3 \tag{635}$$

$$(a_1,...,a_m),(b_1,...,b_k),a_i \neq b_j, \text{两个轮换不相交，没有公共变动元素} \tag{636}$$
$$\rightarrow (a_1,...,a_m)(b_1,...,b_k)=(b_1,...,b_k)(a_1,...,a_m) \tag{637}$$
$$eg.S_7: \tag{638}$$
$$(1,2,3)=\begin{pmatrix}1&2&3&4&5&6&7\\2&3&1&5&4&6&7\end{pmatrix} \tag{639}$$
$$(4,5,6)=\begin{pmatrix}1&2&3&4&5&6&7\\1&2&3&5&6&4&7\end{pmatrix} \tag{640}$$
$$(1,2,3)(4,5,6)=\begin{pmatrix}1&2&3&4&5&6&7\\2&3&1&5&6&4&7\end{pmatrix}=(4,5,6)(1,2,3) \tag{641}$$
$$\forall\sigma\in Sym(X),M(\sigma)=\{x|x\in X,\sigma(x)\neq x\} \tag{642}$$
$$\sigma_1,\sigma_2\in Sym(X),if.M(\sigma_1)\cap M(\sigma_2)=\varnothing \tag{643}$$
$$\sigma_1\sigma_2=\sigma_2\sigma_1 \tag{644}$$

Thm:Sn中任何一个置换可以写成两两不相交的轮换的乘积（复合），且在不计次序的情况下分解唯一(不考证明)

$$Sym(X),\sigma\in Sym(X),\forall x\in X, \text{x所在的轮换} \tag{645}$$
$$\exists only.k\in Z^+,st.\sigma(x)^k=x,\forall i\in\{1,2,...,k-1\},\sigma(x)^i\neq x \tag{646}$$
$$\text{这个轮换写成：（也是分解式之一）}(x,\sigma(x),\sigma(\sigma(x)),...,(\sigma^{k-1}(x))) \tag{647}$$

def:

$$\sigma\in Sym(X) \tag{648}$$
$$def:(X,\sim) \tag{649}$$
$$i\sim j\leftrightarrow\exists l\in Z,st.j=\sigma^l(i) \tag{650}$$
$$\rightarrow \text{ 每个轮换元素在一个等价类里面} \tag{651}$$
$$\text{(轮换ok，不相交的对换不一定，可以相交的对换ok)} \tag{652}$$

eg:

$$(1,2,3)=(1,2)(2,3) \tag{653}$$
$$(a_1,...,a_m)=(a_1,a_2)(a_2,a_3)...(a_{m-1},a_m) \tag{654}$$
$$\text{置换可以写成对换的乘积} \tag{655}$$
$$S_n\text{中有}C_n^2=\frac{‘\Phi n-1}{2}\text{个轮换} \tag{656}$$
$$\text{命题}S_n\text{can be produced by:} \tag{657}$$
$$(1,2),(2,3),(3,4),...,(n-1,n) \tag{658}$$
$$eg.(1,3)=(1,2)(2,3)(1,2) \tag{659}$$
$$(1,4)=(1,3)(3,4)(1,3)=(1,2)(2,3)(1,2)(3,4)(1,2)(2,3)(1,2) \tag{660}$$
$$(i,j)(j,k)(i,j)=(i,k) \tag{661}$$
$$\text{Statement:Sn can be produced by two elements} \tag{662}$$
$$(1,2)(1,2,..,n) \tag{663}$$
$$(1,2,...,n)(i-1,i)(1,...,n)^{-1}=(i,i+1)\text{min} \tag{664}$$
$$\text{奇/偶数置换} \tag{665}$$
$$S_n:\{1,2,...,n\}\text{的所有置换} \tag{666}$$
$$\sigma=(a_1,b_1)...(a_m,b_m)=(c_1,d_1)...(c_k,d_k) \tag{667}$$
$$\therefore m\equiv k \mod 2 \tag{668}$$

下面证明以上命题

$$I_n = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \tag{669}$$

$$\text{三阶单位阵有六种变换形式，对应三阶置换群的6个元素}\Delta\Delta \quad \sigma \in S_n, \text{如下定义n阶矩阵}A \tag{670}$$

$$A_{ij} = \begin{cases} 1 \text{ if i=}\sigma(j) \\ 0 \text{ if i} \neq \sigma(j) \end{cases} \tag{671}$$

$$1.\forall\sigma, A(\sigma(i), j) = 1 \tag{672}$$

$$2.\forall 1 \leqslant i, j \leqslant n, i \neq \sigma(j), A(i, j) = 0 \tag{673}$$

$$\text{in fact:define a f}, S_n \to M_n, \text{由}f(\sigma) = \sigma\text{确定的置换矩阵} \tag{674}$$

$$\text{f是同态} \tag{675}$$

$$f(\sigma\tau) = f(\sigma) * f(\tau)\text{矩阵乘法(不考证明)} \tag{676}$$

$$Pf: \tag{677}$$

$$A = f(\sigma), B = f(\tau), C = f(\sigma * \tau) \tag{678}$$

$$C(i, j) = \begin{cases} 1 \text{ if i} = \sigma \circ \tau(j) = \sigma(\tau(j)) \\ 0 \text{ if i} \neq \sigma(\tau(j)) \end{cases} \tag{679}$$

$$\text{we want to prove C=AB} \tag{680}$$

$$AB(i, j) = \Sigma_{k=1}^{n} A(i, k) * B(k, j) \tag{681}$$

$$i = \sigma(k), k = \tau(j) \to i = \sigma(\tau(j)) \tag{682}$$

$$AB(i, j) = \Sigma_{k=1}^{n} A(i, \tau(j)) * B(\tau(j), j) \tag{683}$$

$$\text{在}i = \sigma(\tau(j))\text{才等于1.C同理} \tag{684}$$

$$\text{suppose}\sigma = (a_1, b_1)...(a_m, b_m) \tag{685}$$

$$f(\sigma) = f((a_1, b_1))...f(a_m, b_m)) \tag{686}$$

$$det(f(\sigma)) = det(f((a_1, b_1))...f((a_m, b_m))) \tag{687}$$

$$\text{一个对换的行列式是-1} \tag{688}$$

$$(-1)^m = (-1)^k, ok \tag{689}$$

逆序对

$$\sigma \in S_n \quad (690)$$
$$T(\sigma) = \{(i,j)|1 \leqslant i < j \leqslant n, \sigma(i) > \sigma(j)\} \quad (691)$$
$$= \sigma\text{的全部逆序对} \quad (692)$$
$$|T(\sigma \circ \tau)| = |T(\sigma)| + |T(\tau)|(mod2) \quad (693)$$
$$(2|m+k) \quad (694)$$
$$(695)$$
$$\text{suppose } A_n = \{\sigma|\sigma \in S_n, \sigma\text{是偶置换}\} \quad (696)$$
$$(A_n) \qquad (i,j)(i,j) = id \quad (697)$$
$$\forall \sigma \in A_n, (1,2)\sigma\text{是奇置换} \quad (698)$$
$$\tau \in S_n - A_n, (1,2)\tau\text{是偶置换} \quad (699)$$
$$S_n = A_n \cup (1,2)A_n \quad (700)$$
$$\therefore |A_n| = \frac{n!}{2} \quad (701)$$
$$\sigma\text{可写为不相交的轮换的乘积} \quad (702)$$
$$\sigma = \tau_1\tau_2...\tau_k, \text{阶数为} d_1,...,d_k \quad (703)$$
$$o(\sigma) = lcm(d_1,...,d_k) \quad (704)$$
$$Pf: \quad (705)$$
$$\tau_1\tau_2 = \tau_2\tau_1 \quad (706)$$
$$\sigma^m = \tau_1^m\tau_2^m...\tau_k^m \quad (707)$$
$$\sigma^m = id \leftrightarrow \forall i, \tau_i^m = id \quad (708)$$
$$\leftrightarrow \forall i, d_i|m \quad (709)$$
$$\leftrightarrow lcm(d_1,...,d_k)|m \quad (710)$$
$$\text{考察题型：求置换的乘积；不相交轮换分解；置换的阶} \quad (711)$$

（如果 $\sigma^m = id$，则 σ 的 m 次幂必须将每个元素映射回它自身。由于 σ 是不相交轮换 $\tau_1, \tau_2, \ldots, \tau_k$ 的乘积，每个 τ_i 也必须将每个元素映射回它自身，即 $\tau_i^m = id$。）

2.8 Sylow 定理

$$G\text{是有限的群} \tag{712}$$
$$H \leqslant G, H\text{是G的子群} \tag{713}$$
$$d||G| \tag{714}$$
$$\text{有d阶子群吗？} \tag{715}$$
$$A_4\text{没有六阶子群} \tag{716}$$

群论学家：
伽罗瓦
阿贝尔
Sylow
Burnside
Frobenius
Kurosh
Wielandt
Huppet
段学复
张远达

DEF:

$$G\text{是有限群} \tag{717}$$
$$|G| = n, p \text{ is prime} \tag{718}$$
$$\text{suppose} p^k|n, p^{k+1} \nmid n \tag{719}$$
$$\text{1.if } |H|\text{是p的幂次，H是G的p-子群} \tag{720}$$
$$2.if.|H| = p^k, H\text{是G的Sylow-p子群} \tag{721}$$
$$|H|\text{是p-子群，}|H| = p^l, \therefore l \leqslant k \tag{722}$$
$$\tag{723}$$
$$G, A \subseteq G, gAg^{-1} = \{gag^{-1}|\forall a \in A\} \qquad def : f : G \to G \tag{724}$$
$$\forall a \in G, f(a) = gag^{-1} \tag{725}$$
$$\text{f是G到自身的群同构(双射+同态)}, f^{-1} = g^{-1}ag \tag{726}$$
$$f : \text{由g诱导的内自同构（可能会考）} \tag{727}$$

Sylow定理

$$G\text{是有限群}, |G| = n, p.prime \tag{728}$$
$$\therefore \tag{729}$$
$$1.G\text{有Sylow-p子群} \tag{730}$$
$$|\{H|H\text{是Sylow-p子群}\}| \equiv 1(modp) \tag{731}$$
$$2.H, K\text{are two Sylow-p子群} \tag{732}$$
$$\to \exists g \in G, K = gHg^{-1} \tag{733}$$
$$3.A\text{是G的p-子群}, \exists H\text{是G的Sylow-p子群}, st.A \subseteq H \tag{734}$$

Stronger:

$$1' : p^l|n, \to \tag{735}$$
$$|\{A|A \leqslant G, |A| = p^l\}| \equiv 1(modp) \tag{736}$$
$$\text{证明大致思路：分成等价类，每个等价类里面要么没有子群要么只有一个} \tag{737}$$

Statement:

$$\text{G是偶数阶群} \tag{738}$$
$$\therefore |\{a|a \in G, a^2 = I_G\}| \equiv 0(mod2) \tag{739}$$
$$= \{I_G\} \cup \{\text{G中二阶元}\} \tag{740}$$
$$\to \text{二阶子群的个数是奇数} \tag{741}$$

$$\text{定义等价关系} \tag{742}$$
$$\forall a,b\in G, a\sim b \leftrightarrow a=b/a=b^{-1}a \tag{743}$$
$$\forall a\in G, \text{a在}\sim\text{下的等价类}:\{b|b\in G, a\sim b\}=\{a,a^{-1}\} \tag{744}$$
$$|\{a,a^-1\}|=\begin{cases}1, a^2=I_G\\ 2, a^2\neq I_G\end{cases} \tag{745}$$
$$\text{记T是G在}\sim\text{下的等价类的集合} \tag{746}$$
$$|G|=\Sigma_{A\in T}|A|=\Sigma_{A\in T,|A|=1}|A|+2\Sigma_{A\in T,|A|=2}|A| \tag{747}$$
$$=|\{a|a^2=I_G\}|+2|\{a|a^2\neq I_G\}| \tag{748}$$
$$\text{G是偶数阶群} \tag{749}$$
$$\therefore |\{a|a^2=I_G\}|\equiv 0(mod2) \tag{750}$$
$$\text{这一段也可以像下面这么写:} \tag{751}$$
$$\text{记}A_1,...,A_m\text{是全体等价类} \tag{752}$$
$$|A_1|=...=|A_l|=1, |A_{l+1}|=...=|A_m|=2 \tag{753}$$
$$|G|=l+2(m-l) \tag{754}$$
$$ok \tag{755}$$

$$\text{G为n阶群},d|n\text{，考察G中有无d阶子群} \tag{756}$$
$$\text{记T}=\{A|A\subseteq G, |A|=d\} \tag{757}$$
$$\text{定义等价关系} \tag{758}$$
$$A\sim B\leftrightarrow \exists g\in G, st.B=gA=\{ga|a\in A\} \tag{759}$$
$$\forall A\subseteq G, |A|=d, \text{A所在的等价类}:\{B|B\subseteq G, |B|=d, A\sim B\}=\{gA|g\in G\}(\text{这里不要求子群}) \tag{760}$$
$$\tag{761}$$
$$G/H=\{gH|g\in G\}, H\leqslant G \tag{762}$$
$$for.A\leqslant G, \text{记}[A]=\{gA|g\in G\}, \rightarrow \tag{763}$$
$$1.if[A]\text{中有子群，则有且只有一个，}, |[A]|=\frac{n}{d} \tag{764}$$
$$2.if_not_|[A]|=\frac{n}{d}*w, w\geqslant 2, w|d \tag{765}$$
$$\text{记}L_1,...,L_m\text{是全体等价类} \tag{766}$$
$$L_1,...,L_k\text{have subgroup}, L_{k+1},...,L_m\text{have no subgroup} \tag{767}$$
$$\rightarrow \text{have k d阶subgroups} \tag{768}$$

$$\text{G is a finite group, } d \mid n, \text{ and } H \leq G, \tag{769}$$

$$\text{ we want to determine whether } , p^l||G|, \tag{770}$$

$$\text{the number of the subgroups of order } p^l \tag{771}$$

$$\text{ is odd.(考试只需证明有就可以，不要求证明奇数)} \tag{772}$$

$$Statement: \tag{773}$$

$$\text{G is a finite group,}, d \mid n, d \geqslant 2, \text{the number of the subgroups of order d is k} \tag{774}$$

$$①\exists d, \text{有一些d的因子} \geqslant 2, (w_i|d), st. \tag{775}$$

$$((n-1), d-1) = k + w_1 + w_2 + ... + w_s \tag{776}$$

$$②\text{p is a prime number}, d = p^l \to k \geqslant 1 \tag{777}$$

$$③.for②, k \equiv 1(modp) \tag{778}$$

$$Pf: \tag{779}$$

$$① \to ②, ③ \tag{780}$$

$$\text{代入} d = p^l, \therefore ((n-1), p^l - 1) = k + w_1 + w_2 + ... + w_s \tag{781}$$

$$\forall 1 \leqslant i \leqslant s, w_i|p^l \tag{782}$$

$$\therefore w_i = p^t(t \leqslant l, t \neq 0) \tag{783}$$

$$\therefore p|w_i \tag{784}$$

$$\therefore ((n-1), p^l - 1) \equiv k(modp)\text{(考试考到这里)} \tag{785}$$

$$\text{p is a prime number}, p^l|n, \therefore ((n-1), p^l - 1) \equiv 1 \equiv k(modp) \tag{786}$$

Pf刚刚的几个命题：

$$T = \{A|A \leqslant G, |A| = d\}, \sim: \tag{787}$$
$$A \sim B \leftrightarrow \exists g \in G, st.B = gA = \{ga|a \in A\} \tag{788}$$
$$\forall A \subseteq G, |A| = d, \text{A所在的等价类}: [A] = \{gA|g \in G\} \tag{789}$$
$$\text{and } 1.if_[A]\text{中有子群，则有且只有一个，}, |[A]| = \frac{n}{d} \tag{790}$$
$$2.if_not_|[A]| = \frac{n}{d} * w, w \geqslant 2, w|d \tag{791}$$
$$\text{这里还没证明，证明见后面} \tag{792}$$
$$\text{记}L_1, ..., L_m\text{是全体等价类} \tag{793}$$
$$\text{G中d阶子群个数为k，分布在k个等价类里面，不妨设是}L_1, ..., L_k \tag{794}$$
$$\therefore |L_1| = ... = |L_k| = \frac{n}{d} \tag{795}$$
$$\forall k+1 \leqslant j \leqslant m, |L_j| = \frac{n}{d} * w_j, w_j \geqslant 2, w_j|d \tag{796}$$
$$|T| = \frac{n}{d} * k + \Sigma_{j=k+1}^{m} \frac{n}{d} * w_j \tag{797}$$
$$|T| = C_n^d = \frac{n}{d} C_{n-1}^{d-1}, \therefore ok \tag{798}$$

作用：定义：幺半群在集合上的作用

$$\forall g \in X, g \to X = \to (g, X) \tag{799}$$
$$1.\forall g, h \in G, x \in H, (gh) \to x = g \to (h \to x) \tag{800}$$
$$2.\forall x \in H, I_G \to x = x \tag{801}$$
$$\text{称X是幺半群G上的作用} \tag{802}$$
$$\tag{803}$$
$$A \sim B : \exists g \in G, st.B = gA = \{ga|a \in A\}, \text{群在子集上的作用} \tag{804}$$
$$\text{定义：} g \to A = gA. \tag{805}$$
$$I_G \to A = A \tag{806}$$
$$(gh) \to A = (gh)A \tag{807}$$
$$eg. \tag{808}$$
$$\text{X is a set,G=Sym(X) }, \sigma \to x = \sigma(x) \tag{809}$$
$$id \to x = x \tag{810}$$
$$(\sigma \circ \tau) \to x = \sigma(\tau(x)) \tag{811}$$

共轭作用

$$g \to X = gXg^{-1} \tag{812}$$
$$1.I_G \to X = X \tag{813}$$
$$2.(gh) \to X = (gh)X(g^{-1}h^{-1}) = g \to (h \to x) \tag{814}$$
$$类比 : G, X = 2^G.H \leqslant G, and_H \lhd G \rightleftarrows \forall g \in G, gHg^{-1} = H \leftrightarrow \forall g \in G, g \to H = H \tag{815}$$
$$eg.GL_2(R) = \{\begin{pmatrix} a & b \\ c & d \end{pmatrix} |a, b, c, d \in R, 矩阵可逆\} \tag{816}$$
$$X是2元列向量 \tag{817}$$
$$defA \to \beta = A\beta \tag{818}$$
$$\alpha, \beta \in X, \alpha, \beta \neq 0; \tag{819}$$
$$\exists A \in G, st.\beta = A\alpha. \tag{820}$$
$$\alpha = (1, 0)^T, \beta = (c, d)^T, \tag{821}$$
$$令A = \begin{pmatrix} c & * \\ d & * \end{pmatrix} \tag{822}$$
$$(\text{(**)和(c,d)线性无关即可。这样A可逆)} \tag{823}$$
$$\to A\alpha = \beta \tag{824}$$

群作用和等价关系：

$$x \sim y \leftrightarrow \exists g \in G, st.y = g \to x \tag{825}$$
$$自反I_G \to x = x, x \sim x \tag{826}$$
$$对称x \sim y \leftrightarrow y = g \to x \leftrightarrow x = g^{-1} \to y \tag{827}$$
$$传递x \sim y, y \sim z \to y = g \to x, z = h \to y \Rightarrow z = (hg) \to x \to x \sim z \tag{828}$$

群作用的轨道公式：

$$\text{if X is finite,suppose } U_1, ..., U_m是(X, \sim)的两两不同的等价类 \tag{829}$$
$$\therefore |U_1| + ... + |U_m| = |X| \tag{830}$$
$$\forall x \in X, \text{x所在的等价类} : \{y|y \in X, x \sim y\} = g \to x|g \in G是\text{X上的一个轨道} \tag{831}$$
$$记为G_x/orbit(x)/G(x), 称为\text{x在G作用下的轨道} \tag{832}$$
$$stab(x) = \{g|g \in G, g \to x = x\}\text{作用在G上不变，稳定化子} \tag{833}$$

Statement:

$$G\text{依作用}\to\text{作用在X上，}x \in X \tag{834}$$
$$\text{记}G_x = \{g \to x|g \in G\}, H = stab(x) = \{g|g \in G, g \to x = x\} \tag{835}$$
$$\to: \tag{836}$$
$$1.H \leqslant G \tag{837}$$
$$2.\forall a, b \in G, a \to x = b \to x \leftrightarrow a^{-1}b \in H \leftrightarrow aH = bH \tag{838}$$
$$3.\phi : G/H \to G_x \tag{839}$$
$$def : \forall a \in G, \phi(aH) = a \to x \tag{840}$$
$$\text{那么这个是合理定义的（如果aH=bH,但是作用下的结果不相同，就不合理）} \tag{841}$$
$$4.\text{如果G，X是有限的,} |G_x| = \frac{|G|}{|H|} = |G/H| \tag{842}$$
$$Pf : \tag{843}$$
$$1.I_G \to x = x, \therefore I_G \in H \tag{844}$$
$$a, b \in H, a \to x = b \to x = x, (ab) \to x = x, \therefore ab \in H \tag{845}$$
$$a^{-1} \to x = a^{-1} \to (a \to x) = x \to a^{-1} \in H \tag{846}$$
$$ok. \tag{847}$$
$$2.if.a \to x = b \to x \tag{848}$$
$$(a^{-1}b) \to x = a \to (a \to x) = x. \tag{849}$$
$$if.(a^{-1}b) \to x = x, \to a \to x = a \to ((a^{-1}b) \to x) = b \to x \tag{850}$$
$$\therefore a \to x = b \to x \leftrightarrow a^{-1}b \in H \leftrightarrow aH = bH(\text{这个是陪集的定义}) \tag{851}$$
$$3.\phi : G/H \to G_x \tag{852}$$
$$\text{由2，}aH = bH \to a \to x = b \to x \tag{853}$$
$$\therefore \phi(aH) = \phi(bH) \to a \to x = b \to x \to aH = bH\text{所以是单射} \tag{854}$$
$$ran(\phi) = G_x, \forall a \in G, a \to x = \phi(aH) \in ran(\phi) \tag{855}$$
$$(\phi' : G \to G_x) \tag{856}$$
$$(\phi'(a) = a \to x) \tag{857}$$
$$4.G_x, G/H\text{一一对应（由于phi）} \tag{858}$$

Statement:

$$有限群G按照\rightarrow作用在有限集X上，U_1,...,U_m两两不同的轨道 \quad (859)$$

$$记U_i = G_{x_i}. \quad \rightarrow |X| = \Sigma_{i=1}^{m}\frac{|G|}{|stab(X_i)|} \quad (860)$$

$$Pf: \quad (861)$$

$$\forall i, U_i = G_{x_i} \quad (862)$$

$$|U_i| = |G_{x_i}| = \frac{|G|}{|stab(x_i)|}从上面那个结论推出来的 \quad (863)$$

不动点定理

$$g \rightarrow x = x : \text{x是不动点} \quad (864)$$

$$\leftrightarrow G_x = \{x\} \leftrightarrow stab(x) = G \quad (865)$$

$$\text{G共轭作用在G上，} : g \rightarrow x = gxg^{-1} \quad (866)$$

$$x \in G, \text{x是共轭作用下的不动点} \leftrightarrow \forall g \in G, g \rightarrow x = x \leftrightarrow \forall g \in G, gxg^{-1} = x \leftrightarrow gx = xg \quad (867)$$

$$Z(G) = \{x|x \in G, \forall g \in G, gx = xg\} : \text{G的中心} \quad (868)$$

$$eg.\text{对二阶可逆实矩阵}, Z(G) = \{\begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix}|a \neq 0\} \quad (869)$$

$$\text{n阶：} aI_n \quad (870)$$

Statement:

$$\text{p是素数，}|G| = p^k \tag{871}$$
$$G, \rightarrow, Y: \text{全体不动点} \tag{872}$$
$$\rightarrow |X| = |Y|(mod p) \tag{873}$$
$$if.p \nmid |X|, \text{则有不动点} \tag{874}$$
$$Pf: \tag{875}$$
$$U_1, ..., U_m \text{all orbits} \tag{876}$$
$$U_i = G_{x_i} \tag{877}$$
$$\text{不妨设前k个有一个元素，其他的至少两个} \tag{878}$$
$$i = 1 \sim k: |U_i| = \frac{|G|}{|stab(x_i)|} = 1 \tag{879}$$
$$i = k+1 \sim n: |U_i| = \frac{|G|}{|stab(x_i)|} \geqslant 2 \tag{880}$$
$$|stab(x_i)|||G|\text{根据前面那个除法式子} \tag{881}$$
$$\because |U_i|\text{是p的幂次}, |U_i| \geqslant 2 \tag{882}$$
$$\therefore p||U_i| \tag{883}$$
$$\therefore |X| \equiv k(mod p) \tag{884}$$
$$\therefore |Y| = k\text{设 Y 是 X 中的全体不动点，那么 Y 中的元素对应的轨道大小都是 1} \tag{885}$$

Statement:

$$\text{G is finite,p is prime}, |A| = p^k, H \leqslant G, p \nmid \frac{|G|}{|H|}, \tag{886}$$
$$\therefore \exists g \in G, st.A \subseteq gHg^{-1} \tag{887}$$
$$Pf: \tag{888}$$
$$\text{考虑}G/H, A\text{依左乘作用在G/H上}\forall a \in A, \forall g \in G, a \rightarrow (gH) = agH \tag{889}$$
$$|A|\text{是p的幂次}, p \nmid |G/H|\text{(根据上一个命题构造的A)} \tag{890}$$
$$\rightarrow \text{有不动点} \tag{891}$$
$$\text{取}g \in G, st, gH\text{是不动点}, \forall a \in A, a \rightarrow (gH) = gH, \tag{892}$$
$$agH = gH \rightarrow ag \in gH \rightarrow a \in gHg^{-1} \rightarrow ok. \tag{893}$$

Sylow定理第二部分：

$$\text{G is finite.p is prime.}, p^k||G|, p^{k+1} \nmid |G| \tag{894}$$

$$(p^k\text{是 G 的阶数中 p 的最高幂次因子}, |H| = p^k) \tag{895}$$

$$\therefore \tag{896}$$

$$1.H, K\text{are two Sylow-p子群}, \exists g \in G, K = gHg^{-1} \tag{897}$$

$$2.\text{A is a p-subgroup}, \exists \text{a Sylow-p subgroup H }, st.A \subseteq H. \tag{898}$$

$$Pf: \tag{899}$$

$$1.K\text{is p-subgroup}, p \nmid |G|/|H| \tag{900}$$

$$(\text{根据前面讨论的不动点定理，H 在 G 的共轭作用下存在不动点}) \tag{901}$$

$$\exists g \in G, st.K \subseteq gHg^{-1} \tag{902}$$

$$\text{但是}|K| = p^k, |H| = |gHg^{-1}| = p^k, \therefore ok. \tag{903}$$

$$2.\text{取一个G的Sylow子群L}, a\text{is a p-subgroup}, p \nmid |G|/|L| \tag{904}$$

$$\therefore \exists g \in G, st.A \subseteq gLg^{-1} = H \tag{905}$$

$$\text{另外：第一部分里面有一个}C_{n-1}^{p^l-1} \equiv 1(modp): \tag{906}$$

$$C_n^m, \text{p进制下}, n = n_k, ..., n_0; m = m_k, ..., m_0 \tag{907}$$

$$C_n^m = \Pi C_{n_i}^{m_i}(modp) \tag{908}$$

$$p^l: 1\text{后面l个零} \tag{909}$$

$$p^l - 1: \text{l个(p-1)} \tag{910}$$

$$n - 1: n_k, ..., n_1(n_0 - 1) \tag{911}$$

$$C_{n_i}^{p-1}, \text{在ni大于等于p-1的时候才不等于零}, n_i = p - 1, = 1 \tag{912}$$

$$n = k * p^l, \therefore n - 1: (k-1)(p-1)...(p-1) \tag{913}$$

$$C_{n-1}^{p^l-1} = C_{k-1}^0 * 1 * ...1 \equiv 1(modp) \tag{914}$$

3 RING!

3.1 def

$$(R,+,*)\text{is a ring} \tag{915}$$
$$1.(R,+)\text{是交换群,幺元记为0} \tag{916}$$
$$2.(R,*)\text{is a monoid，幺元记为}I_R \tag{917}$$
$$3.\forall a,b,c \in R, a(b+c)=ab+ac,(a+b)c=ac+bc \tag{918}$$
$$if.ab=ba,\text{是交换环} \tag{919}$$

example:

$$1.(M_n(R),+,*) \tag{920}$$
$$2.n \in Z^+,(\{0,1,...,n-1\},\oplus,\otimes) \tag{921}$$
$$3.\text{实数序列}(a_0,a_1,...,a_n,...) \tag{922}$$
$$(a_0,a_1,...,a_n,...)+(b_0,b_1,...,b_n,...)=(a_0+b_0,a_1+b_1,...,a_n) \tag{923}$$
$$textmultiply: \tag{924}$$
$$c_0=a_0b_0 \tag{925}$$
$$c_1=a_0b_1+a_1b_0 \tag{926}$$
$$c_2=a_0b_2+a_1b_1+a_2b_0 \tag{927}$$
$$... \tag{928}$$
$$c_n=a_0b_n+a_1b_{n-1}+...+a_{n-1}b_1+a_nb_0 \tag{929}$$
$$(\Sigma a_ix^2)+(\Sigma b_ix^2)=(\Sigma(a_i+b_i)x^2) \tag{930}$$
$$(\Sigma a_ix^2)*(\Sigma b_ix^2)(\Sigma\Sigma_{i+j=n}a_i+b_jx^n) \tag{931}$$
$$4.Z_2^n=\{0,1\}^n,\text{长度为n的0,1序列} \tag{932}$$
$$(Z_2^n,\oplus),(0,0,...,0) \tag{933}$$
$$(Z_2^n,\otimes),(1,1,..,1) \tag{934}$$
$$5.\text{集合X和环的关系:} \tag{935}$$
$$\text{ for two sets,A and B} \tag{936}$$
$$A\oplus B=(A-B)\cup(B-A)=A\cup B-A\cap B \tag{937}$$
$$P(X)=\{A|A\subseteq X\}, \tag{938}$$
$$(P(X),\oplus,\cap)\text{is a ring} \tag{939}$$
$$\text{序列}(a_1,...,a_n)\to A=\{i|1\leqslant i\leqslant n,a_i=1\}\in P(X) \tag{940}$$
$$\phi:Z_2^n\to P(X) \tag{941}$$
$$\phi(a_1,...,a_n)=\{i|1\leqslant i\leqslant n,a_i=1\} \tag{942}$$
$$\phi(\alpha)=A,\phi(\beta)=B \tag{943}$$
$$\phi(\alpha\oplus\beta)=A\oplus B \tag{944}$$
$$\phi(\alpha\beta)=A\cap B \tag{945}$$
$$ \tag{946}$$

群环：

$$\text{G is a finite group,C is complex} \tag{947}$$
$$C^G : f : G \to C \tag{948}$$
$$(C^G, +, *) : \tag{949}$$
$$f, g \in C^G, (f+g)(a) = f(a) + g(a), \tag{950}$$
$$* f * g(a) = \Sigma_{b \in G} f(b) g(b^{-1}a) \tag{951}$$
$$= \Sigma_{(b,c) \in G*G, bc=a} f(b) g(c) \tag{952}$$
$$\tag{953}$$

四元数环

$$R = \{ \begin{pmatrix} \alpha & \beta \\ -\beta & \alpha \end{pmatrix} | \alpha, \beta \in C \} \tag{954}$$
$$\tag{955}$$
$$I_2 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \tag{956}$$
$$i = \begin{pmatrix} \sqrt{-1} & 0 \\ 0 & \sqrt{-1} \end{pmatrix} \tag{957}$$
$$j = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \tag{958}$$
$$k = \begin{pmatrix} 0 & \sqrt{-1} \\ -\sqrt{-1} & 0 \end{pmatrix} \tag{959}$$
$$i^2 = j^2 = k^2 = I_2, ij = k, ji = -k \tag{960}$$
$$a + bi + cj + dk \tag{961}$$

mod剩余类环:

$$\{ Z_n, \oplus, \otimes \} \tag{962}$$

$$\text{if } (R, +, *) \text{ is a ring} \tag{963}$$
$$1.a0 = 0a = 0 \tag{964}$$
$$2. -(ab) = (-a)b = a(-b) \tag{965}$$
$$Pf: \tag{966}$$
$$1.a0 = a(0+0) = a0 + a0 \to a0 = 0, \tag{967}$$
$$0a = (0+a)0 = a0 + a0 \to 0a = 0 \tag{968}$$
$$2.0 = a0 = a(b + (-b)) \to ok \tag{969}$$

$$(R, +, *)\text{is a ring} \tag{970}$$
$$(R, +)\text{是交换群} \tag{971}$$
$$(R, *)\text{is a semigroup,if 有幺元，记作}I_R \tag{972}$$
$$\text{if ab=ba,是交换环} \tag{973}$$

$$(F, +, *)\text{是域：} \tag{974}$$
$$1.(F, +, *)\text{是交换环,有乘法幺元}I_F \tag{975}$$
$$2.\forall a, b \in F, a, b \neq 0, ab^{-1} \in F \tag{976}$$
$$\text{另外一种写法：} \tag{977}$$
$$1.(F, +)\text{是交换群,幺元是0} \tag{978}$$
$$2.(F, *)\text{是交换幺半群，或者：}(F - 0, *)\text{是群} \tag{979}$$
$$3.\text{分配律}a(b+c) = ab + ac \tag{980}$$

$$\text{field:}Q, R, C.\text{Z is not a field} \tag{981}$$
$$\text{other examples:} \tag{982}$$
$$K = \{a + b\sqrt{2}|a, b \in Q\} \tag{983}$$
$$(K, +, *) \tag{984}$$
$$1.\text{交换环:} \tag{985}$$
$$a.\text{(K,+)是交换群} \tag{986}$$
$$\text{封闭，结合，有幺元，有逆元} \tag{987}$$
$$\text{逆元}: -a - b\sqrt{2} \tag{988}$$
$$\text{交换群:}(a + b\sqrt{2}) + (c + d\sqrt{2}) = (c + d\sqrt{2}) + (a + b\sqrt{2}) \tag{989}$$
$$b.(K, *)\text{是半群或者幺半群都可以} \tag{990}$$
$$\text{封闭，结合(幺元是1)} \tag{991}$$
$$c.\text{分配律} \tag{992}$$
$$a(b + c) = ab + ac \tag{993}$$
$$(a + b)c = ac + bc \tag{994}$$
$$\text{交换环} \tag{995}$$
$$(a + b\sqrt{2})(c + d\sqrt{2}) = (c + d\sqrt{2})(a + b\sqrt{2}) \tag{996}$$
$$\tag{997}$$
$$I_K = 1 \tag{998}$$
$$\forall a + b\sqrt{2} \in K, \text{有逆元}\frac{a}{a^2 - 2b^2} - \frac{b}{a^2 - 2b^2} * \sqrt{2} \tag{999}$$

$$L = \{a + b\sqrt[3]{2} + d\sqrt[3]{4}|a, b, c \in Q\}\text{类似} \tag{1000}$$
$$a + b\pi\text{是环不是域} \tag{1001}$$
$$\{\{0, 1, ..., n - 1\}, \oplus, \otimes\}\text{是交换环不是域} \tag{1002}$$
$$Z_6 : 2 \otimes 3 = 0 \tag{1003}$$
$$if 2 \otimes x = 0 \to 2x \equiv 1(mod 6), no 3\text{也没有乘法逆元} \tag{1004}$$
$$Z_5\text{is a field} \tag{1005}$$

Statement:

$$(Z_n, \oplus, \otimes)\text{is a field} \leftrightarrow \text{n is a prime} \tag{1006}$$

$$\text{分式域:} \tag{1007}$$
$$R_{[x]} = \{a_0 + ... + a_n x^n | n \in N, \forall a_i \in R\} \tag{1008}$$
$$\text{乘法幺元是1,逆元没有，所以:} \quad R(x) = \{\frac{f}{g} | f, g \in R_{[x]}, g \neq 0\} \tag{1009}$$
$$\text{这样有逆元了} \tag{1010}$$

3.2 环作用(不要求)

$$\text{凯莱定理:半群也可以} \tag{1011}$$
$$R^n : \text{R上的向量空间} \tag{1012}$$
$$1.(\alpha + \beta) + \gamma = \alpha + (\beta + \gamma) \tag{1013}$$
$$2.\vec{0} \in R^n, \vec{a} + \vec{0} = \vec{0} + \vec{a} = \vec{a} \tag{1014}$$
$$3.\forall \alpha \in R^n, \alpha + (-\alpha) = \vec{0} \tag{1015}$$
$$4.\alpha + \beta = \beta + \alpha \tag{1016}$$
$$5.(ab)\alpha = a(b\alpha) \tag{1017}$$
$$6.1 * \alpha = \alpha \tag{1018}$$
$$7.(a + b)\alpha = a\alpha + b\alpha \tag{1019}$$
$$8.a(\alpha + \beta) = a\alpha + a\beta \tag{1020}$$
$$\text{一到四是加法作用下的交换群，5，6是作用，7,8是分配律} \tag{1021}$$

$$(R, +, *)\text{is a ring,有幺元,} (M, +) \text{ is a Abel group} \tag{1022}$$
$$\rightarrow: \forall a \in R, x \in M, a \rightarrow x = ax \tag{1023}$$
$$if : 1.\forall a, b \in R, \forall x \in M, a \rightarrow (b \rightarrow x) = (ab) \rightarrow x \tag{1024}$$
$$2.\forall x \in, I_R \rightarrow x = x \tag{1025}$$
$$3.\forall a \in R, x, y \in M, a \rightarrow (x + y) = a \rightarrow x + a \rightarrow y \tag{1026}$$
$$4.\forall a, b \in R, x \in M, (a + b) \rightarrow x = a \rightarrow x + b \rightarrow y \tag{1027}$$
$$\text{(M,+)在} \rightarrow \text{下做成左R模} \tag{1028}$$

$$M(R)\text{环}, (R^2, +) \tag{1029}$$

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} x & y \end{pmatrix} = \begin{pmatrix} ax+by \\ cx+dy \end{pmatrix} \tag{1030}$$

$$(M, +)\text{is a Abel group} \tag{1031}$$

$$R = \{f | f : M \to M\text{群同态}\} \tag{1032}$$

$$f, g \in R, \text{def:} f + g : \tag{1033}$$

$$\forall x \in M, (f+g)(x) = f(x) + g(x) \tag{1034}$$

$$* : \text{复合映射} \tag{1035}$$

$$(R, +, \circ) \tag{1036}$$

$$f + g : \tag{1037}$$

$$\forall x \in M, (f+g)(x+y) = (f+g)(x) + (f+g)(y)\text{f+g也是同态} \tag{1038}$$

$$Pf : \tag{1039}$$

$$LHS = f(x) + f(y) + g(x) + g(y) = f(x) + g(x) + f(y) + g(y) = RHS\text{因为是交换群} \tag{1040}$$

$$g \circ f : \tag{1041}$$

$$\forall x, y \in M, (g \circ f)(x+y) = g(f(x+y)) = g(f(x) + f(y)) = g \circ f(x) + g \circ f(y) \tag{1042}$$

$$\text{分别用了f和g为同态，最后得出复合也是同态} \tag{1043}$$

$$\tag{1044}$$

$$1.(R, +)\text{是交换群} \tag{1045}$$

$$\forall x \in M, (f+g)(x) = f(x) + g(x) = g(x) + f(x) = (g+f)(x) \tag{1046}$$

$$\text{幺元是0，逆元是-f(x)} \tag{1047}$$

$$2.(R, \circ)\text{is a monoid} \tag{1048}$$

$$idM : \text{恒等映射} \tag{1049}$$

$$3.(f+g) \circ h = f \circ h + g \circ h \tag{1050}$$

$$4.f \circ (g+h) = f \circ g + f \circ h \tag{1051}$$

$$\text{3和4要验证} \tag{1052}$$

$$Pf_3 : \tag{1053}$$

$$\forall x \in M, ((f+g) \circ h)(x) = (f+g)(h(x)) = f(h(x)) + g(h(x)) \tag{1054}$$

$$= (f \circ h)(x) + (g \circ h)(x) = RHS \text{ f+g的定义} \tag{1055}$$

$$Pf_4 : \tag{1056}$$

$$(f \circ (g+h))(x) = f((g+h)(x)) = f(g(x) + h(x)) = f(g(x)) + f(h(x)) = (f \circ g + f \circ h)(x) \tag{1057}$$

$$(R,+,\circ),(M,+) \tag{1058}$$
$$(g\circ f)(x)=g(f(x)) \tag{1059}$$
$$idM(x)=x \tag{1060}$$
$$f(x+y)=f(x)+f(y) \tag{1061}$$

设$(A,+,\circ)$是环 (1062)

$(A,+)$是半群 (1063)

$a\in A, L_a$: (A,+)到自身的同态 (1064)

$i.\forall x\in A, L_a(x)=ax$ (1065)

$L_a(x+y)=a(x+y)=ax+ay=L_a(x)+L_a(y)$ (1066)

$ii.a,b\in A, L_{a+b}=L_a+L_b$ (1067)

$L_{a+b}(x)=(a+b)x=L_a(x)+L_b(x)=(L_a+L_b)(x)$ (1068)

$iii.a,b\in A, L_{ab}=L_a\circ L_b$ (1069)

$(L_{ab})(x)=(ab)x=a(bx)=L_a(L_b(x))=(L_a\circ L_b)(x)$ (1070)

$iv.$如果$(A,+,\circ)$有乘法幺元，则A到L是单射, $L_{I_A}=idA$ (1071)

$Pf:$ (1072)

$L_a=L_b\leftrightarrow L_a(I_X)=L_b(I_X)\leftrightarrow a=b$ (1073)

La是A到A的同态 (1074)

1.$L_{a+b}=L_a+L_b$ (1075)

2.$L_{ab}=L_a\circ L_b$ (1076)

3.有乘法幺元，从A到L的映射是单射,$L_{I_A}=idA$类似于凯莱定理 (1077)

(1078)

3.3 环同态

$$\text{以下是要求的} \tag{1079}$$

$$(R, +, \circ), (S, +, \circ) \tag{1080}$$

$$f : R \to S \tag{1081}$$

$$\forall a, b \in R, f(a+b) = f(a) + f(b), f(ab) = f(a)f(b)\text{不保证幺元到幺元，可能都没有幺元} \tag{1082}$$

$$\text{若f是双射，则为环同构} \tag{1083}$$

$$\text{R上的向量空间U}, f: U \to U \tag{1084}$$

$$f(x+y) = f(x) + f(y)\text{fi}f(ax) = af(x) \tag{1085}$$

$$A = \{f | f: R^2 \to R^2\}\text{(线性映射)} \tag{1086}$$

$$M_2(R), \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in M_2(R) \tag{1087}$$

$$\text{def:} f(\begin{pmatrix} x \\ y \end{pmatrix}) = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} ax+by \\ cx+dy \end{pmatrix} \tag{1088}$$

$$\text{f是线性映射} \tag{1089}$$

$$f_{\beta_1+\beta_2} = f_{\beta_1} + f_{\beta_2} \tag{1090}$$

$$f(\beta_1+\beta_2)\begin{pmatrix} x \\ y \end{pmatrix} = f\beta_1 \begin{pmatrix} x \\ y \end{pmatrix} + f\beta_2 \begin{pmatrix} x \\ y \end{pmatrix} \tag{1091}$$

$$f_{\beta_1\beta_2} = f_{\beta_1} f_{\beta_2} \tag{1092}$$

$$f_{\beta_1\beta_2} \begin{pmatrix} x \\ y \end{pmatrix} = (\beta_1\beta_2) \begin{pmatrix} x \\ y \end{pmatrix} = \beta_1(\beta_2 \begin{pmatrix} x \\ y \end{pmatrix}) \tag{1093}$$

$$= f_{\beta_1}(f_{\beta_2} \begin{pmatrix} x \\ y \end{pmatrix}) = (f_{\beta_1} \circ f_{\beta_2}) \begin{pmatrix} x \\ y \end{pmatrix} \tag{1094}$$

$$\text{证明单射} \tag{1095}$$

$$\beta_1 = \begin{pmatrix} a_1 & b_1 \\ c_1 & d_1 \end{pmatrix}, \beta_2 = \begin{pmatrix} a_2 & b_2 \\ c_2 & d_2 \end{pmatrix} \tag{1096}$$

$$\forall \begin{pmatrix} x \\ y \end{pmatrix} \in R^2, \tag{1097}$$

$$\beta_1 \begin{pmatrix} x \\ y \end{pmatrix} = \beta_2 \begin{pmatrix} x \\ y \end{pmatrix} \tag{1098}$$

$$\text{取} \begin{pmatrix} 1 \\ 0 \end{pmatrix}, \to \begin{pmatrix} a_1 \\ c_1 \end{pmatrix} = \begin{pmatrix} a_2 \\ c_2 \end{pmatrix} \tag{1099}$$

$$\text{取} \begin{pmatrix} 0 \\ 1 \end{pmatrix}, \to \begin{pmatrix} b_1 \\ d_1 \end{pmatrix} = \begin{pmatrix} b_2 \\ d_2 \end{pmatrix} \tag{1100}$$

$$\to \text{单射} \tag{1101}$$

$$\tag{1102}$$

$$\text{任取}\delta, R^2 \to R^2\text{的线性映射} \tag{1103}$$

$$\text{记}\delta(\begin{pmatrix} 1 \\ 0 \end{pmatrix}) = \begin{pmatrix} a \\ c \end{pmatrix} \tag{1104}$$

$$\text{记}\delta(\begin{pmatrix} 0 \\ 1 \end{pmatrix}) = \begin{pmatrix} b \\ d \end{pmatrix} \tag{1105}$$

$$\beta = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \tag{1106}$$

$$\forall \begin{pmatrix} x \\ y \end{pmatrix} \in R^2, \tag{1107}$$

$$\begin{pmatrix} x \\ y \end{pmatrix} = x \begin{pmatrix} 1 \\ 0 \end{pmatrix} + y \begin{pmatrix} 0 \\ 1 \end{pmatrix} \tag{1108}$$

$$\delta(\begin{pmatrix} x \\ y \end{pmatrix}) = \delta(x \begin{pmatrix} 1 \\ 0 \end{pmatrix}) + \delta(y \begin{pmatrix} 0 \\ 1 \end{pmatrix}) \tag{1109}$$

$$= x\delta(\begin{pmatrix} 1 \\ 0 \end{pmatrix}) + y\delta(\begin{pmatrix} 0 \\ 1 \end{pmatrix}) \tag{1110}$$

$$= x \begin{pmatrix} a \\ c \end{pmatrix} + y \begin{pmatrix} b \\ d \end{pmatrix} \tag{1111}$$

$$= \begin{pmatrix} ax + by \\ cx + dy \end{pmatrix} = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix} \tag{1112}$$

$$\text{delta是由矩阵确定的线性映射} \tag{1113}$$

$$\text{f是R到S的环同态} \tag{1114}$$

$$\text{f是R到S的环同态} \tag{1115}$$
$$ker(f) = \{x|x \in R, f(x) = 0\} \tag{1116}$$
$$ker(f) \leqslant (R, +) \tag{1117}$$
$$1.f(x+y) = f(x) + f(y) = 0, \therefore x + y \in ker(f) \tag{1118}$$
$$f(-x) = -f(x) = 0, \therefore -x \in ker(f) \tag{1119}$$
$$2.\forall a \in ker(f), b \in R, f(ab) = f(a)f(b) = 0, f(ba) = f(b)f(a) = 0, \therefore ab, ba \in ker(f) \tag{1120}$$
$$(R, +, \circ)\text{is a ring}, I \subseteq R, \tag{1121}$$
$$\text{if: } I \leqslant (R, +), \forall a \in I, b \in R, ab, ba \in I \tag{1122}$$
$$\text{I是(R,+)的一个理想} \tag{1123}$$

$$G, H, G/H; \tag{1124}$$
$$R \text{ 的子群 } I\text{，Abel 群的子群是正规子群} \tag{1125}$$
$$R/I = \{u + I|u \in R\}(\text{用 + 表示运算}) \tag{1126}$$
$$u + I = \{u + a|a \in I\} \tag{1127}$$

$(G,*)$	$(R,+)$
ab	$a+b$
a^{-1}	$-a$
a^k	ka
$AB = \{ab \| a \in A, b \in B\}$	$A + B = \{a + b \| a \in A, b \in B\}$
aH	$u+I$
$ah, h \in H$	$u+b, b \in I$

$$(u + I) + (v + I) = (u + v) + I \tag{1128}$$
$$(u + I)(v + I) = (uv) + I \tag{1129}$$
$$\text{if } u + I = x + I, v + I = y + I \tag{1130}$$
$$(u + I)(v + I) = (uv) + I = xy + I \tag{1131}$$
$$\tag{1132}$$

如果I是理想，I是(R,+)的子群

$$a, b \in I \rightarrow ab, ba \in I \tag{1133}$$

$$\text{example} : (Z, +, *), \{bq|b \in Z\} \leqslant (Z, +) \tag{1134}$$

$$\text{I是(R,+)的一个理想}, (u+I)+(v+I)=(u+v)+I, (u+I)*(v+I)=uv+I \tag{1135}$$

$$u, v, x, y \in R, u+I=x+I, v+I=y+I \tag{1136}$$

$$\rightarrow uv+I=xy+I \tag{1137}$$

$$Pf: \tag{1138}$$

$$x+I=u+I \rightarrow x \in u+I \rightarrow \exists a \in I, st.x=u+a \tag{1139}$$

$$y+I=v+I \rightarrow y \in v+I \rightarrow \exists b \in I, st.y=v+b \tag{1140}$$

$$xy=(u+a)(v+b)=uv+ub+a(v+b), ub \in I, a(v+b) \in I(a \in R, b \in I, ab, ba \in I) \tag{1141}$$

$$\therefore ub+a(v+b) \in I \tag{1142}$$

$$\therefore \exists c \in I, st.xy=uv+c \tag{1143}$$

$$\therefore xy+I=uv+I \tag{1144}$$

$$\text{如果*合理定义，那么I确实是理想} \tag{1145}$$

$$\tag{1146}$$

$$Statement: \tag{1147}$$

$$\text{R是一个环，I是(R,+)的一个理想，在R/I上定义二元运算+，*} \tag{1148}$$

$$\forall u, v \in R, (u+I)+(v+I)=(u+v)+I, (u+I)*(v+I)=uv+I \tag{1149}$$

$$\text{则(R/I,+,*)是一个环，且R有乘法幺元IR时，IR+I是这个环的幺元} \tag{1150}$$

$$Pf: \tag{1151}$$

$$\text{证明是环} \tag{1152}$$

$$\text{结合律} \tag{1153}$$

$$((u+I)*(v+I))*(w+I)=(uv)w+I=u(vw)+I=(u+I)*((v+I)*(w+I)) \tag{1154}$$

$$\text{分配} \tag{1155}$$

$$(u+I)*((v+I)+(w+I))=(u+I)*(v+I)+(u+I)*(w+I) \tag{1156}$$

$$((u+I)+(v+I))*(w+I)=(u+v)w+I=(u+I)*(w+I)+(v+I)*(w+I) \tag{1157}$$

$$\text{如果R有乘法幺元:} \tag{1158}$$

$$(I_R+I)*(u+I)=u+I \tag{1159}$$

$$(u+I)*(I_R+I)=u+I \tag{1160}$$

$$\tag{1161}$$

$$Statement: \quad (1162)$$
$$\text{R是环，I是理想，} f : R \to R/I \quad (1163)$$
$$\forall u \in R, f(u) = u + I \quad (1164)$$
$$\text{则f是一个环同态} \quad (1165)$$
$$ker(f) = I, Im(f) = R/I \quad (1166)$$
$$Pf : \forall u, v \in R, f(u + v) = (u + v) + I = f(u) + f(v) \quad (1167)$$
$$f(uv) = (uv) + I = f(u) * f(v) \quad (1168)$$
$$f(I_R) = I_R + I \quad (1169)$$
$$I\text{是(R/I,+)的幺元}, ker(f) = \{u|u \in R, f(u) = I\} \quad (1170)$$
$$= \{u|u \in R, u + I = I\} = I \quad (1171)$$
$$Im(f) = \{u + I|u \in R\} = R/I \quad (1172)$$
$$(1173)$$

定理：

$$\text{R,S是环，} \phi : R \to S, \phi\text{是环同态}, I = ker(\phi) \quad (1174)$$
$$\therefore \quad (1175)$$
$$1.I \text{ is a n ideal of R} \quad (1176)$$
$$2.\text{定义g}, R/I \to S, \forall u \in R \quad (1177)$$
$$\text{则g是合理定义的，g是单射，且g是环同态} \quad (1178)$$
$$Pf : \quad (1179)$$
$$1.ker(\phi) = \{u|u \in R, \phi(u) = 0_S\} \quad (1180)$$
$$\forall u, v \in I, \phi(u) = 0 = \phi(v) \to \phi(u + v) = 0 \quad (1181)$$
$$\therefore u + v \in I \quad (1182)$$
$$\phi(u) = -\phi(u) = 0, \therefore -u \in I \quad (1183)$$
$$\forall a \in I, b \in R, \phi(ab) = \phi(a)\phi(b) = 0 \quad (1184)$$
$$2. \text{ assert: } \forall u, v \in R, u + I = v + I \leftrightarrow \phi(u) = \phi(v) \quad (1185)$$
$$Pf : \quad (1186)$$
$$u + I = v + I \to v \in u + I \to \exists b \in I, st.v = u + b \quad (1187)$$
$$\to: b \in I, \therefore \phi(b) = 0, \therefore \phi(v) = \phi(u) + \phi(b) = \phi(u) \quad (1188)$$
$$\leftarrow: \phi(u) = \phi(v) \to \phi(v - u) = 0 \to v - u \in I \to v + I = u + I \quad (1189)$$
$$(1190)$$

g合理定义：如果自变量相同，因变量也相同
g单射：像相同，原像相同

环同态：

$$1. + \text{保持} \tag{1191}$$

$$g((u+I)+(v+I)) = g((u+v)+I) = \phi(u+v) = \phi(u)+\phi(v) = g(u+I)+g(v+I) \tag{1192}$$

$$* : g((u+I)*(v+I)) = g((uv)+I) = \phi(uv) = \phi(u)\phi(v) = g(u+I)g(v+I) \tag{1193}$$

$$\tag{1194}$$

$$\text{和群相比多的部分:1.}\forall a \in I, b \in R, \phi(ab) = \phi(a)\phi(b) = 0 \tag{1195}$$

$$2.* : g((u+I)*(v+I)) = g((uv)+I) = \phi(uv) = \phi(u)\phi(v) = g(u+I)g(v+I) \tag{1196}$$

$$corollary : \tag{1197}$$

$$\text{R,S是环，}\phi\text{是环同态}, Im(\phi) = S, \text{则R/ker(f)和S 同构} \tag{1198}$$

$$Pf : \tag{1199}$$

$$g : R/ker(\phi) \to S \tag{1200}$$

$$\forall u \in R/ker(\phi), g(u+ker(f)) = \phi(u) \tag{1201}$$

$$\text{g是环同态，单射，且}Im(\phi) = S = Im(g)\text{，所以是同构} \tag{1202}$$

$$\text{记作}R/ker(\phi) \cong S \tag{1203}$$

example:

$$n \in Z^+, Z_n = \{0, 1, ..., n-1\}, \oplus, \otimes \tag{1204}$$

$$f : Z \to Z_n, \forall a \in Z, f(a) = a \mod n \tag{1205}$$

$$ker(f) = nZ = \{nq | q \in Z\} \tag{1206}$$

$$Z/nZ \cong Z_n \tag{1207}$$

3.4 多项式

$$\text{f是多项式:}R[x], f = a_0 + a_1x + ... + a_nx^n, a_i \in R \tag{1208}$$
$$\text{f是R上的一个多项式} \tag{1209}$$
$$f = a_0 + a_1x + ... + a_nx^n \tag{1210}$$
$$g = b_0 + b_1x + ... + b_nx^n \tag{1211}$$
$$f + g = (a_0 + b_0) + (a_1 + b_1)x + ... + (a_n + b_n)x^n \tag{1212}$$
$$f * g : c_0 = a_0 * b_0, \tag{1213}$$
$$c_1 = a_0 * b_1 + a_1 * b_0, \tag{1214}$$
$$c_2 = a_0 * b_2 + a_1 * b_1 + a_2 * b_0, \tag{1215}$$
$$... \tag{1216}$$
$$c_n = a_0 * b_n + a_1 * b_{n-1} + ... + a_n * b_0 \tag{1217}$$
$$x^4 + 2x^3 + 5x + 1 : \tag{1218}$$
$$textx/*C\text{fi}4/!p\text{fi}yp1 \tag{1219}$$
$$f = a_0 + a_1x + ... + a_nx^n, \text{至多n个根，在复数上有n个根} \tag{1220}$$
$$\text{取}c \in F, |F| = q >> n, \text{求}f(c), \text{ if } f(c) = 0, \text{f大概率是零多项式} \tag{1221}$$
$$\text{恰好找到根的概率很小} \tag{1222}$$

以下开始是要求的。

$$\text{两个n位正整数相乘，位数不超过}n^2 \tag{1223}$$
$$\text{R是有乘法幺元的环，记}T = \{(a_0, ..., a_n, ...)|a_i \in R\} \tag{1224}$$
$$T_1 = \{(a_0, ..., a_n, ...)|a_i \in R\text{至多有有限个i，使得}a_i \neq 0\} \tag{1225}$$
$$(T, +, *) \tag{1226}$$
$$\alpha = \{a_0, a_1, ...\} \tag{1227}$$
$$\beta = \{b_0, b_1, ...\} \tag{1228}$$
$$\alpha + \beta = \{a_0 + b_0, a_1 + b_1, ...\} \tag{1229}$$
$$\alpha * \beta = \{c_0, c_1, ...\} \tag{1230}$$
$$c_i = \sum_{j=0}^{n} a_j b_{n-j} \tag{1231}$$
$$\tag{1232}$$

$$(T,+,*)\text{是一个环。} \tag{1233}$$
$$\text{加法幺元}(0,0,...) \tag{1234}$$
$$\text{逆元}-(a_0,a_1,...)=(-a_0,-a_1,...) \tag{1235}$$
$$\text{乘法幺元}(I_R,0,0,...) \tag{1236}$$
$$x=(0,I_R,0,0,...) \tag{1237}$$
$$\forall n\in N, x^n=(0,0,...,0,I_R,0,0,...)\text{第n个分量是幺元} \tag{1238}$$
$$\alpha=(a_0,a_1,...,a_n,...) \tag{1239}$$
$$\to\alpha=a_0+a_1x+...+a_nx^n \tag{1240}$$
$$\text{这里的多项式是推出来的不是直接定义的} \tag{1241}$$

$$(T_1,+,*)\text{是一个环。} \tag{1242}$$
$$\text{R上的多项式环，记作}R[x] \tag{1243}$$
$$\alpha=(a_0,a_1,...)\in R[x] \tag{1244}$$
$$1.\alpha=0, deg(\alpha)=-\infty \tag{1245}$$
$$2.\alpha\neq 0\text{仅有有限个i，使得}a_i\neq 0,\text{所以deg(x)有意义},=max\{i\in N, a_i\neq 0\} \tag{1246}$$
$$\tag{1247}$$

$$(F,+,*)\text{域，有乘法幺元的交换环} \tag{1248}$$
$$\forall a\in F, a\neq 0, \exists b\in F, st.a*b=I_F \tag{1249}$$
$$Statement: \tag{1250}$$
$$\text{域的理想仅有0和F} \tag{1251}$$
$$Pf: \tag{1252}$$
$$I\text{ is an ideal of F}, I\neq 0 \tag{1253}$$
$$\text{取}a\in I, a\neq 0, \because F\text{ is a field}, \tag{1254}$$
$$\therefore\exists b\in F, st.a*b=I_F \tag{1255}$$
$$a\in I, ab\in I, I_F\in I. \tag{1256}$$
$$\therefore\forall c\in F, I_F\in I, \therefore cI_F=c\in I. \tag{1257}$$
$$\therefore I=F\qquad\text{(R是有幺元的交换环，且理想只有0和R，则R是域。)} \tag{1258}$$
$$\tag{1259}$$

$$\text{关于多项式次数的命题} \tag{1260}$$
$$f, g \in F[x], \tag{1261}$$
$$\therefore \tag{1262}$$
$$1.deg(f+g) \leqslant max\{deg(f), deg(g)\} \tag{1263}$$
$$2.\forall a \in F, a \neq 0, deg(af) = deg(f) \tag{1264}$$
$$3.deg(f * g) = deg(f) + deg(g) \tag{1265}$$
$$4.f \neq 0, g \neq 0 \to fg \neq 0 \tag{1266}$$
$$Pf: \tag{1267}$$
$$1.\text{设}deg(f) \leqslant n, f = \Sigma_{i=0}^{n} a_i x^i, deg(g) \leqslant n, g = \Sigma_{i=0}^{n} b_i x^i \tag{1268}$$
$$\text{可以有}0 \tag{1269}$$
$$f + g = \Sigma_{i=0}^{n}(a_i + b_i)x^i \tag{1270}$$
$$deg(f+g) \leqslant n. \tag{1271}$$
$$(\text{如果次数相同，有可能可以取等}) \tag{1272}$$
$$2.f = b_0 + b_1 x + ... + b_n x^n \tag{1273}$$
$$af = ab_0 + ab_1 x + ... + ab_n x^n \tag{1274}$$
$$\text{ if } u, v \in F, u, v \neq 0, \therefore uv \neq 0. \tag{1275}$$
$$(\text{if uv=0}, (uv)v^-1 = 0 \to u = 0.) \tag{1276}$$
$$\text{if } f = 0, af = 0. \tag{1277}$$
$$\text{if } f \neq 0, a, b_n \neq 0, \therefore ab_n \neq 0, \therefore deg(af) = n \tag{1278}$$
$$3.4. \tag{1279}$$
$$f = 0/g = 0 \to ok. \tag{1280}$$
$$\text{设均不等于}0. \tag{1281}$$
$$deg(f) = m, deg(g) = n, \tag{1282}$$
$$f * g = \Sigma_{i=0}^{m} + n(\Sigma_{i+j=k} a_i b_j x^k) \tag{1283}$$
$$x^{m+n} : a_m, b_n \neq 0, \therefore a_m b_n \neq 0 \tag{1284}$$
$$deg(f * g) = m + n. \tag{1285}$$
$$\tag{1286}$$

带余除法

$$Thm : f, g \in F[x], g \neq 0 \tag{1287}$$
$$\exists q, r \in F[x], st.f = qg + r, deg(r) < deg(g) \tag{1288}$$
存在性和唯一性分开证明，用构造证明存在性，用其他方法证明唯一性 (1289)
1.唯一性 (1290)
$$f = q_1g + r_1 = q_2g + r_2 \tag{1291}$$
$$r_1 - r_2 = q_1g - q_2g = (q_1 - q_2)g \tag{1292}$$
$$deg(r_1 - r_2) \leqslant max\{deg(r_2), -deg(r_1)\} = max\{deg(r_2), deg(r_1)\} < deg(g) \tag{1293}$$
$$\therefore deg((q_1 - q_2)g) = deg(q_1 - q_2) + deg(g) \geqslant deg(g) \tag{1294}$$
$$\therefore q_1 - q_2 = 0 \tag{1295}$$
$\therefore q_1 = q_2, r_1 = r_2, \therefore$ 唯一 (1296)
2.存在性 (1297)
用归纳。 (1298)
记$g = b_0 + b_1x + ... + b_mx^m$ (1299)
$$deg(g) = m, deg(f) = n \tag{1300}$$
$1.n < m, q = 0, r = f$ (1301)
$2.n \geqslant m.h = a_nb_mx^n - m, \phi = f - gh \to deg(\phi) = deg(f) - 1$ (1302)
由归纳$, \exists q_1, r \in F(x), \phi = q_1g + r$ (1303)
令$q = h + q_1, r = \phi$ (1304)
$$\therefore f = qg + r. \tag{1305}$$

$$def : \tag{1306}$$
$$f, g \in F[x], g|f : st.q \in F[x], f = qg.(r = 0) \tag{1307}$$
$$a, b \in Z, \exists x, y \in Z, st.(ax + by)|x, (ax + by)|y \to gcd. \tag{1308}$$

Statement:

$$f,g \in F[x], \exists u,v \in F[x], (uf+vg)|f, (ug+vf)|g \quad (1309)$$

$$\text{if } g=0, u=I_F. \quad (1310)$$

$$g \neq 0, \text{suppose } deg(f) \geqslant deg(g), \quad (1311)$$

$$f = qg + r, deg(r) < deg(g) \quad (1312)$$

$$deg(r) < deg(g) \leqslant deg(f). \quad (1313)$$

$$\text{由归纳假设}, \exists u_1, v_1 \in F[x], (u_1 f + v_1 g)|r, (u_1 g + v_1 f)|g \quad (1314)$$

$$u_1 g + v_1 r = u_1 g +_1 (f - qg) = v_1 f + (u_1 - v_1 q)g = uf + vg \quad (1315)$$

$$\to (uf+vg)|r, (ug+vf)|g, \quad (1316)$$

$$(uf+vg)|f - qg \to (uf+vg)|f \quad (1317)$$

$$def: \quad (1318)$$

$$f,g \in F[x]. \quad (1319)$$

$$1.h \in F[x], h|f, h|g \to \text{h为f,g的公因子} \quad (1320)$$

$$2.f = g = 0, 0\text{是最大公因式} \quad (1321)$$

$$3.\text{不全为零，存在唯一}d \in F[x], \quad (1322)$$

$$a.\text{d是公因式}, \quad (1323)$$

$$b.\forall h \in F[x], \text{h是公因式}, h|d \quad (1324)$$

$$c.\text{(唯一性)d的首项系数是}I_F \quad (1325)$$

$$\to d = gcd(f,g) \quad (1326)$$

$$G\text{is a monoid}, a \in G, \tag{1327}$$
$$\text{a为G的可逆元是指：}\exists b \in G, st.ab = ba = I_G \tag{1328}$$
$$(Z, *), \text{if a是可逆元}, \exists b \in Z, st.ab = ba = 1 \tag{1329}$$
$$\to a = \pm 1 \tag{1330}$$
$$\text{F is a field,F[x]多项式} \tag{1331}$$
$$a \in F, a \neq 0, \exists a^{-1} \in F, st.aa^{-1} = a^{-1}a = I_F(\text{可逆元}) \tag{1332}$$
$$f \in F[x], \text{f是可逆元是指：} \tag{1333}$$
$$\exists g \in F[x], st.fg = I_F \tag{1334}$$
$$0 = deg(fg) = deg(f) + deg(g), deg(f) \in N, deg(g) \in N, \tag{1335}$$
$$\therefore deg(f) = 0.(\therefore f \in F, f \neq 0) \tag{1336}$$
$$\therefore \text{F[x]中可逆元全体:}F - \{0\}, = \{f | f \in F[x], deg(f) = 0\} \tag{1337}$$

整除和多项式的相似性质的对比。

$$a \mid b \leftrightarrow \exists q \in Z, st.b = qa \tag{1338}$$
$$\text{Some facts:} \tag{1339}$$
$$1.c \mid 0, \text{ and if } 0 \mid c \to c = 0 \tag{1340}$$
$$2.a \mid a \tag{1341}$$
$$3.a \mid b, b \mid a \to b = \pm a \tag{1342}$$
$$4.a \mid b, b \mid c \to a \mid c \tag{1343}$$
$$5.a \mid b, a \mid c \to a \mid (b \pm c) \tag{1344}$$
$$Pf: \tag{1345}$$
$$1.0 = 0c. \tag{1346}$$
$$0 \mid c: \exists q \in Z, st.c = q0 = 0 \tag{1347}$$
$$2.a = 1 * a \tag{1348}$$
$$3.\exists q_1 \in Z, st.b = q_1 a \tag{1349}$$
$$\exists q_2 \in Z, st.a = q_2 b \tag{1350}$$
$$\therefore a = q_1 q_2 a. \tag{1351}$$
$$i.a = 0.ok \tag{1352}$$
$$ii.q_1 q_2 = 1 \to b = \pm a. \tag{1353}$$
$$\tag{1354}$$

$$4.\exists q \in Z, st.b = qa \quad (1355)$$
$$\exists p \in Z, st.c = pb \quad (1356)$$
$$\therefore c = qab = qa(pb) = q(ab) \quad (1357)$$
$$5.\exists q \in Z, st.b = qa \quad (1358)$$
$$\exists p \in Z, st.c = pa \quad (1359)$$
$$\therefore b \pm c = (q \pm p)a \quad (1360)$$

多项式 (1361)

$$def : f, g \in F[x], f \mid g : \exists h \in F[x], st.g = hf \quad (1362)$$

Some facts: (1363)

$$1.f \mid 0, \text{ and if } 0 \mid f \to f = 0 \quad (1364)$$
$$2.f \mid f \quad (1365)$$
$$3.f \mid g, g \mid f \leftrightarrow \exists a \in F, a \neq 0, g = af \quad (1366)$$
$$4.f \mid g, g \mid h \to f \mid h \quad (1367)$$
$$5.f \mid g, f \mid h \to f \mid (g \pm f) \quad (1368)$$
$$Pf_3 : \quad (1369)$$
$$f \mid g, \exists h_1 \in F[x], st.g = h_1 f \quad (1370)$$
$$g \mid f, \exists h_2 \in F[x], st.f = h_2 g \quad (1371)$$
$$f = h_2 h_1 f. \quad (1372)$$
$$i.f = 0.ok \quad (1373)$$
$$ii.(I_F - h_2 h_1)f = 0 \to I_F - h_2 h_1 = 0 \to h_2 h_1 = I_F \to \exists a \in F - \{0\}, h_1 = a \quad (1374)$$
(1375)

可能会考求多项式的商和余数
次数是一个很好的性质。
最大公因数/最大公因式

对最大公因数 (1376)

$a, b \in Z$, gcd(a,b)=d存在且唯一，且$\exists u, v \in Z, d = au + bv$ (1377)

对最大公因式 (1378)

$f, g \in F[x]$, gcd(f,g)=d存在且唯一，且$\exists u, v \in F[x], d = fu + gv$ (1379)

(1380)

$Pf_1:$ (1381)

$d_1, d_2 = gcd(a,b), \therefore d_1 \mid d_2, d_2 \mid d_1 \therefore \exists a, d_1 = ad_2$ (1382)

因为首项是$I_F, \therefore d_1 = d_2$唯一性 (1383)

存在性： (1384)

$\exists u_1, v_1 \in F[x], st. fu_1 + gv_1$为f,g的公因式 (1385)

$d_1 = fu_1 + gv_1$ (1386)

h是f,g的公因式$, h \mid f, h \mid g$ (1387)

$\therefore h \mid d_1,$ (1388)

设d1首项系数是a$, a^{-1} \in F, d = a^{-1}d_1 = fa^{-1}u_1 + ga^{-1}v_1$ (1389)

(1390)

互素 (1391)

$a, b \in Z,$ gcd(a,b)=1 (1392)

多项式的互素：公因式只有零次多项式 (1393)

$f = a(a^{-1}f)$ (1394)

(F是域，每个元素a都有逆元$, \therefore a \mid f$) (1395)

fact:f, g互素 $\leftrightarrow \exists u, v \in F[X], fu + gv = I_F$ (1396)

$\Leftarrow$: (1397)

$u, v \in F[x], fu + gv = I_F$ (1398)

$\forall h \in F[x], f \mid f, h \mid g \rightarrow h \mid fu + gv = I_F$ (1399)

$\therefore \exists q \in F[x], I_F = qh \rightarrow deg(h) = 0$ (1400)

$\rightarrow \exists a \in F, a \neq 0, h = a.$ (1401)

$\Rightarrow$: (1402)

因为互素，所以f,g不全为0$gcd(f,g) = I_F,$ (1403)

$\therefore \exists u, v \in F[x], st. fu + gv = I_F$(前面有一个的证明fu+gv=最大公因式的) (1404)

$$\text{fact:} \tag{1405}$$
$$1.(a,b)=1, a \mid bc \to a \mid c \tag{1406}$$
$$2.(a,b)=1, a \mid c, b \mid c \to ab \mid c. \tag{1407}$$
$$\text{多项式} \tag{1408}$$
$$f,g,h \in F[x], f,g\text{互素}, \tag{1409}$$
$$1.f \mid gh, \to f \mid h \tag{1410}$$
$$2.f \mid h, g \mid h \to fg \mid h \tag{1411}$$

$$Pf: \tag{1412}$$
$$1.\exists u,v \in F[x], fu+gv=I_F \tag{1413}$$
$$hfu+hgv=h \tag{1414}$$
$$f \mid gh, \to f \mid hgv \tag{1415}$$
$$\text{又因为} f \mid hfu, \to f \mid h. \qquad 2.fu+gv=I_F.f \mid h, g \mid h \tag{1416}$$
$$\therefore \exists a \in F[x], h=af \tag{1417}$$
$$\therefore \exists b \in F[x], h=bg \tag{1418}$$
$$hfu+hgv=h \to bgfu+afgv=h=gf(bu+av) \tag{1419}$$
$$\therefore fg \mid h \tag{1420}$$

fact:

$$H \leqslant (Z,+) \leftrightarrow \exists d \in N, st.H=\{dq|q \in Z\}, \text{也是(Z,+)的全体理想} \tag{1421}$$
$$\text{R is a ring}, I \subseteq R \text{ is an ideal of R} \tag{1422}$$
$$1.I \leqslant (R,+) \tag{1423}$$
$$2.\forall u \in I, \forall r \in R, ru, ur \tag{1424}$$

$$\text{THM} \tag{1425}$$
$$I \subseteq F[x], I \text{ is an ideal of } F[x] \tag{1426}$$
$$\leftrightarrow \exists d \in F[x], st. I = \{du|u \in F[x]\} = \{f|f \in F[x], d|f\} \tag{1427}$$
$$Pf: \tag{1428}$$
$$\leftarrow: \tag{1429}$$
$$d \in F[x], I = \{du|u \in F[x]\} \qquad du + dv = d(u+v) \in I \tag{1430}$$
$$\forall f \in F[x], f(du) = (du)f = d(uf) \tag{1431}$$
$$\therefore \text{ I is an ideal of F[x]} \tag{1432}$$
$$\rightarrow: \tag{1433}$$
$$\text{I is an ideal of F[x]} \tag{1434}$$
$$1.I = 0.Ok \tag{1435}$$
$$\text{2.I里面有非零多项式，记d是I-0中次数最小的多项式。} \tag{1436}$$
$$\text{下证} I = \{du|u \in F[x]\} \tag{1437}$$
$$\forall u \in F[x], d \in I, I \text{ is an ideal of F[x]}, \rightarrow du \in I \tag{1438}$$
$$\forall g \in I, \text{做带余除法}, \exists q, r \in [x], st. g = qd + r \tag{1439}$$
$$deg(r) < deg(d), \because d \in I, qd \in I, g \in I \tag{1440}$$
$$\therefore r \in I, deg(r) < deg(d). \tag{1441}$$
$$\therefore r = 0. \therefore g = qd. \tag{1442}$$

Z和域上的多项式环

$$\text{Z,prime}, m \in Z^+, m \geqslant 2, if \text{只有1和m为正因子} \tag{1443}$$
$$\forall a \in \{1, 2, ..., m-1\}, a \nmid m. \tag{1444}$$
$$\text{多项式} \tag{1445}$$
$$g \in F[x], deg(g) \geqslant 1, \text{因式只有g和ag}, a \in F, a \neq 0. \tag{1446}$$
$$\text{g是F上不可约的多项式。} \tag{1447}$$
$$\forall f \in F[x], 1 < deg(f) \leqslant deg(g) - 1, f \nmid g \tag{1448}$$
$$\forall a \in F, a \neq 0, a^{-1} \in F, g = a(a^{-1}g) = a^{-1}(ag) \tag{1449}$$
$$\text{在R[x]上的不可约多项式在C[x]上可以可约。} x^2 + 1. \tag{1450}$$

facts

$$p \text{ is a prime}.a \in Z. \tag{1451}$$
$$\text{下面两个之一成立} \tag{1452}$$
$$1.p \mid a \tag{1453}$$
$$2.p \nmid a, (p,a) = 1 \to \exists u, v \in Z, st.pu + va = 1 \tag{1454}$$
$$\text{多项式} \tag{1455}$$
$$g \in F[x]\text{上不可约多项式。}, h \in F[x] \tag{1456}$$
$$1.g \mid h \tag{1457}$$
$$2.g \nmid h, (g,h) = I_F, \to \exists u, v \in F[x], st.gu + hv = I_F \tag{1458}$$
$$\tag{1459}$$

Pf:

$$gcd(g,h) = d, d \mid g, g \in F[x]\text{不可约}, \tag{1460}$$
$$1.d = ag, d \mid h, ag \mid h, \therefore g \mid h \tag{1461}$$
$$2.d = a, \because \text{首项是}I_F, \therefore aI_F = d, \therefore gcd(g,h) = I_F \tag{1462}$$
$$\tag{1463}$$

fact:

$$p \text{ is a prime}, a, b \in Z, p \mid ab \to p \mid a\text{或}p \mid b. \tag{1464}$$
$$g\text{不可约}, f, h \in F[x], g \mid fh \to g \mid f\text{或}g \mid h. \qquad Pf: \tag{1465}$$
$$\text{设}g \nmid h, \text{证明}g \mid f. \tag{1466}$$
$$(g,h) = I_F, \therefore \exists u, v \in F[x], st.gu + hv = I_F \tag{1467}$$
$$\therefore gfu + hfv = f \tag{1468}$$
$$g \mid fh, \to g \mid f. \tag{1469}$$

算数基本定理

$$m \in Z^+, \therefore \exists p_1, ..., p_s(\text{prime}), \tag{1470}$$
$$p_1 \leqslant ... \leqslant p_m, st.m = p_1...p_s. \tag{1471}$$
$$\text{if there are} q_1, ..., q_t, q_1 \leqslant ... \leqslant q_t, \tag{1472}$$
$$\text{st.}m = q_1...q_t, \tag{1473}$$
$$\text{then } s = t, p_i = q_i. \tag{1474}$$

Thm:

$$h \in F[x], h \neq 0, h\text{首项系数是}a, \tag{1475}$$
$$\exists g_1, ..., g_s \in F[x], \text{为F上不可约多项式，首项系数为}I_F, st.h = ag_1...g_s, \tag{1476}$$
$$\text{if 还有}b, f_1, ..., f_t, h = bf_1...f_t, \tag{1477}$$
$$\text{则调整顺序后}, s = t, f_i = g_i. \tag{1478}$$
$$Pf: \tag{1479}$$
$$\text{1.证明存在性} \tag{1480}$$
$$i.h\text{不可约}, ok \tag{1481}$$
$$ii.h\text{在F可约}, \exists f \in F[x], 1 \leqslant deg(f) \leqslant deg(h) - 1, f \mid h \tag{1482}$$
$$h = qf. \tag{1483}$$
$$1 \leqslant deg(q) = deg(h) - deg(f) < deg(f). \tag{1484}$$
$$\text{用归纳法，q、f可以写成多项式的积，h=qf也可以写。} \qquad \text{2.证明唯一性} \tag{1485}$$
$$g_1g_2...g_s = f_1f_2...f_t \tag{1486}$$
$$\therefore g_s \mid f_1...f_t. \tag{1487}$$
$$\exists 1 \leqslant j \leqslant t, st, g_s \mid f_j \tag{1488}$$
$$\text{设}g_s \mid f_t. \tag{1489}$$
$$\text{因为ft不可约}, \rightarrow g_s = a\text{或}g_s = af_t \tag{1490}$$
$$deg(g_s) \geqslant 1, \therefore g_s = af_t. \tag{1491}$$
$$\text{因为首项系数为IF}, \therefore g_s = f_t. \tag{1492}$$
$$\rightarrow g_1...g_{s-1} = f_1...f_{t-1}, \text{归纳法可证} \tag{1493}$$

3.5 商环

$$F[x], \text{I is an ideal of F[x]} \tag{1494}$$
$$\exists g \in F[x], st.I = \{g * f | f \in F[x]\} = \{h | h \in F[x], g \mid h\} \tag{1495}$$
$$F[x]/I \tag{1496}$$
$$1.g = 0, I = \{0\}, F[x]/\{0\} = F[x] \tag{1497}$$
$$2.g = a \in F, a \neq 0, I = F[x], F[x]/I = \{I\} \tag{1498}$$
$$\text{(以上这两个不关心。)} \tag{1499}$$
$$3.deg(g) \geqslant 1.F[x]/I = \{f + I | f \in F[x]\} \tag{1500}$$
$$fact.\forall f \in F[x], \exists\text{唯一} r \in F[x], deg(r) \geqslant deg(g) - 1, \tag{1501}$$
$$st.f + I = r + I \qquad\qquad Pf: \tag{1502}$$
$$\text{f对g带余除法}, f = qg + r, \therefore f - r \in I, \therefore f + I = r + I \tag{1503}$$
$$\text{若}\exists r_1, f + I = r_1 + I, \therefore \exists q_1 \in F[x], f = q_1 g + r_1 \tag{1504}$$
$$\therefore r = r_1. \tag{1505}$$

Statement:

$$g \in F[x], \deg(g) \geqslant 1, I = \{qg | q \in F[x]\}, H = \{r | r \in F[x], deg(r) \leqslant deg(g) - 1\} \tag{1506}$$
$$1.F[x]/I = \{r + I | r \in H\}, \text{且}\forall r_1, r_2 \in H, r_1 + I = r_2 + I \to r_1 = r_2 \tag{1507}$$
$$2.\forall r_1, r_2 \in H, (r_1 + I) + (r_2 + I) = (r_1 + r_2) + I \tag{1508}$$
$$3.r_1 r_2 = qg + \phi, (\phi \in H), r_1 r_2 + I = \phi + I \tag{1509}$$
$$4.\text{幺元：} I_F + I \tag{1510}$$
$$5.if.\text{g在F不可约，} F/I\text{是域} \tag{1511}$$
$$6.if.\text{g在F可约，} F/I, \text{存在两个非零元的乘积是0，这个不是域。} \tag{1512}$$
$$(a, b \in F, ab = 0 \to a = 0/b = 0.\text{(因为有逆元)}) \tag{1513}$$
$$7.\delta : F \to F[x]/I. \tag{1514}$$
$$\forall a \in F, \delta(a) = a + I. \to \delta\text{是单射，环同态} \tag{1515}$$
$$\tag{1516}$$

$$Pf: \tag{1517}$$
$$1.h_1 + I = h_2 + I, \therefore h_1 - h_2 \in I \rightarrow g \mid (h_1 - h_2) \tag{1518}$$
$$deg(h_1), deg(h_2) \leqslant deg(g) - 1, \therefore deg(h_2 - h_1) \leqslant deg(g) - 1 \tag{1519}$$
$$\therefore h_2 - h_1 = 0. \tag{1520}$$
$$2.3.\text{用定义，3加一个带余除法} \tag{1521}$$
$$4.\text{商环的幺元是大环的幺元的陪集，交换环上的多项式，商环也是交换环。} \tag{1522}$$
$$5.F[x]/I\text{的非零元有乘法逆元，}\forall f \in F[x], f + I \neq I. \tag{1523}$$
$$\text{如果g在F不可约，下面两种情况成立其一:} \tag{1524}$$
$$i.g \mid f, f \notin I, \therefore g \nmid f \tag{1525}$$
$$ii.\exists u, v \in F[x], st.gu + hv = I_F. \tag{1526}$$
$$assert: \text{v+I是所求的逆元。} \tag{1527}$$
$$(f + I)(v + I) = fv + I = (I_F - gu) + I = I_F + I. \tag{1528}$$
$$6.g\text{在F上可约}, \exists h_1, h_2 \in F[x], st.g = h_1 h_2, \tag{1529}$$
$$1 \leqslant deg(h_1), deg(h_2) \leqslant deg(g) - 1, \tag{1530}$$
$$(h_1 + I)(h_2 + I) = I. \therefore \text{不是域。} \tag{1531}$$

$$H = \{h | h \in F[x], deg(h) \leqslant deg(g) - 1\} \tag{1532}$$
$$(H, \oplus, \otimes), \oplus: \text{多项式加法}, \otimes: \text{对g做带余除法} \tag{1533}$$
$$(H, \oplus, \otimes)\text{是交换环，IF是幺元} \tag{1534}$$
$$H \simeq F[x]/I, \phi(h) = h + I, \forall h \in F[x] \tag{1535}$$
$$example: \tag{1536}$$
$$F = R, g = x^2 + 1, H = \{ax + b | a, b \in R\} \tag{1537}$$
$$I = \{(x^2 + 1)q | q \in R[x]\} \tag{1538}$$
$$R[x]/I = \{ax + b + I | a, b \in R\} \tag{1539}$$
$$(x + I)(x + I) = x^2 + I = -1 + (x^2 + 1) + I = -1 + I \tag{1540}$$
$$-1 = a^2 \rightarrow \text{复数} \tag{1541}$$
$$(a + bx) + I, (c + dx) + I, \text{加法和乘法都和复数一样} \tag{1542}$$
$$\phi(a + b\sqrt{-1}) = a + bx + I, \text{同构映射} \tag{1543}$$

$$另一种构造: \tag{1544}$$
$$(H,+,\otimes). \tag{1545}$$
$$a+bx, c+dx \tag{1546}$$
$$\phi(a+bx)=a+b\sqrt{-1} \tag{1547}$$

$$(F_2,\oplus,\otimes) \tag{1548}$$
$$H=\{0,1,x,1+x\} \tag{1549}$$
$$\tag{1550}$$
$$H=\{0,1,x,1+x,x^2,x^2+1,x^2+x,x^2+x+1\},(H,\oplus,\otimes)\text{is a field} \tag{1551}$$
$$|H|=8.(模x^3+x+1,模x^3+x^2+1也一样是八个，同构) \tag{1552}$$

3.6 还是多项式环

$$\text{R是有乘法幺元的交换环，R[x]是R上的全体一元多项式。} \tag{1553}$$
$$f\in R[x], f=a_0+a_1x+...+a_nx^n, a_i\in R \tag{1554}$$
$$\forall u\in R, f(u)=a_0u+a_1u^2+...+a_nu^n \tag{1555}$$
$$f(u)=0\text{u是f在R中的一个根或者零点} \tag{1556}$$
$$Statement: \tag{1557}$$
$$u\in R,\forall f,g\in R[x], \tag{1558}$$
$$(f+g)(u)=f(u)+g(u) \tag{1559}$$
$$(fg)(u)=f(u)g(u) \tag{1560}$$
$$Pf: \tag{1561}$$
$$1.f=\Sigma_{i=0}^n a_ix^i, g=\Sigma_{i=0}^n b_ix^i \tag{1562}$$
$$(f+g)(u)=\Sigma_{i=0}^n(a_i+b_i)x^i \tag{1563}$$
$$f(u)+g(u)=\Sigma_{i=0}^n a_iu^i+\Sigma_{i=0}^n b_iu^i \tag{1564}$$
$$\tag{1565}$$
$$f=\Sigma_{i=0}^n a_ix^i, g=\Sigma_{i=0}^m b_ix^i \tag{1566}$$
$$(fg)(u)=\Sigma_{i=0}^m+n\Sigma_{j=0}^k a_ib_{k-i}u^k \tag{1567}$$
$$f(u)g(u)=(\Sigma_{i=0}^n a_iu^i)(\Sigma_{j=0}^m b_iu^j) \tag{1568}$$

$$= \Sigma_{i=0}^{m}\Sigma_{j=0}^{n}a_iu^ib_ju^j(\text{加交换环}) \quad (1569)$$
$$= \Sigma_{i=0}^{m}\Sigma_{j=0}^{n}a_ib_ju^{i+j} \quad (1570)$$
$$= \Sigma_{k=0}^{m+n}\Sigma_{i+j=k}^{n}(a_ib_j)u^k = ...ok \quad (1571)$$
$$(1572)$$

$\forall u \in R, f(u) = g(u) \leftrightarrow f = g$ (1573)

$R = F_2, f = x + 1, g = x^2 + 1,$ 不成立。域太小了。F4中不是全相等了 (1574)

无限域上都相等，可以说相等，优先于不一定 (1575)

余式定理 (1576)

F is a field,$f \in F[x], a \in F, \exists q \in F[x], f = q(x - a) + f(a)$ (1577)

if $(x - a)|f \to f(a) = 0$ (1578)

f对x-a做带余除法，$f = q(x - a) + r, f(a) = q(a)(x - a) + r(a),$ (1579)

$(x - a)|f \leftrightarrow r(a) = 0.$ (1580)

推论:f is a field, $f \in F[x],$ 在F上不可约, $deg(f) \geqslant 2,$ (1581)

$\therefore \forall u \in F, f(u) \neq 0.$ (1582)

$Pf : f(u) = 0 \to (x - u)|f, deg(f) \geqslant 2,$ 矛盾 (1583)

推论$f \in F[x], deg(f) = n \geqslant 0, \to$ 至多n个零点 (1584)

$Pf :$ (1585)

对n归纳 (1586)

$1.n = 0, f = a \in F - \{0\}, ok$ (1587)

$2.n \geqslant 1,$ suppose $\exists v \in F, st/f(v) = 0,$ (1588)

$(x - v)|f, \exists q \in F[x], f = q(x - v)$ (1589)

$assert : u \in F, f(u) = 0, u \neq v \to q(u) = 0.$ (1590)

$0 = f(u) = q(u)(x - u).$ (1591)

由归纳，q在F上至多n-1个根, $+assert \to ok$ (1592)

$$R, S\text{are rings}, R * S = \{(r,s)|r \in R, s \in S\} \quad (1593)$$
$$(R * S, +, *)\text{is a ring} \quad (1594)$$
$$\text{乘法幺元是}(I_R, I_S) \quad (1595)$$
$$\text{加法幺元是}(0,0) \quad (1596)$$
$$(a,b) + (c,d) = (a+c, b+d) \quad (1597)$$
$$(a,b) * (c,d) = (ac, bd) \quad (1598)$$

$$\text{F is a field}, g \in F[x], \text{不可约}, F[x]/I, I = \{qg|q \in F[x]\} \quad (1599)$$
$$C, Q \quad (1600)$$
$$\text{取}\alpha \in C\text{加入Q} \to \text{包含Q，a的最小子域}Q(\alpha) \quad (1601)$$
$$Q(\sqrt{-1}) = \{a + b\sqrt{-1}|a, b \in Q\}, ok \quad (1602)$$
$$Q(e) = \{a + be\}\text{不行}, = \{\frac{f(e)}{g(e)}|f, g \in Q[x], g \neq 0\}, ok. \quad (1603)$$
$$\text{C是不可列集，(N到C没有满射)Q，Q[x]是可列集} \quad (1604)$$
$$\text{代数数(可列)}\{\alpha|\alpha \in C, \exists 0 \neq f \in Q[x], f(\alpha) = 0\} \quad (1605)$$
$$\text{上面是复数里面的一小部分} \quad (1606)$$

3.7 子域

$$(K, +, *)\text{是域,F是子域:}F \subseteq K, (F, +, *)\text{is a field} \quad (1607)$$
$$fact: \quad (1608)$$
$$F\text{是K的子域} \leftrightarrow \quad (1609)$$
$$1.0 \in F, I_K \in F \quad (1610)$$
$$\forall a, b \in F, a + b, -a, ab \in F \quad (1611)$$
$$\forall a \in F, a \neq 0, a^{-1} \in F. \quad (1612)$$

$$\text{定义代数元，超越元,K is a field,F is a subfield of K} \quad (1613)$$
$$\forall \alpha \in K, \quad (1614)$$
$$\text{1.if } \exists f \in F[x], f(\alpha) = 0, \alpha\text{是F上的代数元} \quad (1615)$$
$$\text{2.if } \forall f \in F[x], f(\alpha) \neq 0, \alpha\text{是F上的超越元} \quad (1616)$$

$$K = C, F = Q : \sqrt{2}, \sqrt{3}, \sqrt{-1}\text{是代数元}, e, \pi\text{是超越元} \quad (1617)$$

$$\quad (1618)$$

$$F \subseteq K, F\text{is a subfield of K}, u \in K \quad (1619)$$

K中含有F并上u的最小子域，记为F(u)(证明:类似群里面的) (1620)

$$Pf : \quad (1621)$$

$$def : \forall K_i\text{是子域}, F \cup u \subseteq K_i \to K \subseteq K_i. \quad (1622)$$

1.suppose K1,K2都是, $\to K_1 \subseteq K_2, K_2 \subseteq K_1 \to K_1 = K_2$ (1623)

2.$T = \{K|K\text{是符合条件的子域}\}$, assert $T \neq \varnothing, \cap_{K \in T} K = F(u)$ (1624)

$$Pf : \quad (1625)$$

非空：K就是一个 (1626)

子域的交集还是子域。所以可以。 (1627)

$$1.\forall f \in F[x], f(u) \in F(u) : \quad (1628)$$

$$Pf : \quad (1629)$$

$$f = a_0 + a_1 x + ... + a_n x^n, a_i \in F \quad (1630)$$

$$f(u) = a_0 u + a_1 u^2 + ... + a_n u^n \quad (1631)$$

$$a_0 \in F(u) \quad (1632)$$

$$a_1, u \in F(u), \to a_1 u \in F(u) \quad (1633)$$

$$a_2, u^2 \in F(u), \to a_2 u^2 \in F(u) \quad (1634)$$

$$... \quad (1635)$$

$$\to f(u) \in F(u) \quad (1636)$$

$$2.\forall g \in F[x], g(u) \neq 0, g(u)^{-1} \in F(u) \quad (1637)$$

$$\forall f \in F[x], g \in F[x], g(u) \neq 0, f(u)g(u)^{-1} \in F(u) \quad (1638)$$

Statement:

$$K\text{中含有F并上u的最小子域F(u)}:\{f(u)g(u)^{-1}|f,g\in F[x],g(u)\neq 0\} \tag{1639}$$
$$\text{记}L=\text{上述式子} \tag{1640}$$
$$1.\text{取}f=a,g=I_K,a=f(u)g(u)^{-1} \tag{1641}$$
$$\text{取}f=x,g=I_K,u=f(u)g(u)^{-1} \tag{1642}$$
$$2.\forall K\text{的任意子域L'},if.F\cup\{u\}\subseteq L',\text{有}L\subseteq L' \tag{1643}$$
$$(f(u),g(u)\in L',f(u)g(u)^{-1}\in L') \tag{1644}$$
$$3.Pf\text{L is a subfield} \tag{1645}$$
$$i.F\subseteq L,\therefore I_k,0\in F\subseteq L \tag{1646}$$
$$ii.\forall f_1,g_1\in F[x],g_1(u)\neq 0, \tag{1647}$$
$$\forall f_2,g_2\in F[x],g_2(u)\neq 0, \tag{1648}$$
$$a=f_1(u)g_1(u)^{-1},b=f_2(u)g_2(u)^{-1},\text{证明a+b,-a,ab}\in L \tag{1649}$$
$$a+b=f_1(u)g_1(u)^{-1}+f_2(u)g_2(u)^{-1}=(f_1g_2+f_2g_1)(u)(g_1g_2)^{-1}(u)\in L \tag{1650}$$
$$-a=(f_1)(u)(-g_1)^{-1}(u)\in L \tag{1651}$$
$$ab=(f_1f_2)(u)(g_1g_2)^{-1}(u)\in L \tag{1652}$$
$$a\neq 0,a^{-1}=g_1(u)f_1^{-1}(u)\in L \tag{1653}$$
$$f(u)g(u):\text{u是超越元，不能化简了，代数元的话可以。比如复数表示为a+bi} \tag{1654}$$

$$\text{进一步}f_1,f_2,g_1,g_2\in F[x],g_1(u)\neq 0,g_2(u)\neq 0 \tag{1655}$$
$$f_1(u)g_1(u)^{-1}=f_2(u)g_2(u)^{-1}\to f_1g_2=f_2g_1 \tag{1656}$$
$$Pf: \tag{1657}$$
$$(f_1g_2-f_2g_1)(u)=0,\to f_1g_2-f_2g_1\in F[x]\to f_1g_2-f_2g_1=0 \tag{1658}$$
$$\tag{1659}$$

极小多项式：

$$F\subseteq K,u\in K\text{是代数元},f\in F[x],f\neq 0,and \tag{1660}$$
$$1.f(u),\text{f首项系数是}I_K \tag{1661}$$
$$2.\forall h\in F[x],h\neq 0,if.h(u)=0\to deg(h)\leq deg(f) \tag{1662}$$
$$\to\text{f是u在F上的极小多项式} \tag{1663}$$
$$eg.x^2+1\sim\sqrt{-1}. \tag{1664}$$
$$\exists\{h|h\in F[x],h\neq 0,h(u)=0\}\text{取其中次数最小的多项式，乘一个适当的非零元使其首项系数是}I_F \tag{1665}$$

Statement:

$$f\text{是u在F上的极小多项式},\therefore deg(f) \geqslant 1, and \tag{1666}$$
$$1.\forall h \in F[x], if.h(u) = 0, f \mid h \tag{1667}$$
$$2.f\text{是F上的不可约多项式} \tag{1668}$$
$$Pf: \tag{1669}$$
$$1.h \in F[x], h = qf + r.h(u) = 0, f(u) = 0 \to r(u) = 0. \tag{1670}$$
$$r \in F[x], deg(r) < deg(f), \therefore r = 0, ok \tag{1671}$$
$$2.\text{反证，设f可约}, f = g_1 g_2. \tag{1672}$$
$$1 \leqslant deg(g_1), deg(g_2) \leqslant deg(f). \tag{1673}$$
$$\text{设}g_1(u) = 0,\text{则与f是极小多项式矛盾。} \tag{1674}$$

$$\text{推论：}F \subseteq K, u \in K\text{是代数元,则u在F上的极小多项式唯一} \tag{1675}$$
$$I = \{h | h \in F[x], h(u) = 0\}\text{做成F[x]上的理想，}, \exists f \in F[x], I = \{qf | q \in F[x]\} \tag{1676}$$
$$f\text{首项系数为1，f是u在F上的极小多项式} \tag{1677}$$
$$\tag{1678}$$

Statement:

$$F(u) = \{r(u) | r \in F[x], deg(r) < deg(f)\}, \tag{1679}$$
$$r_1, r_2 \in F[x], if.deg(r_1), deg(r_2) \leqslant deg(f), \tag{1680}$$
$$r_1(u) = r_2(u) \to r_1 = r_2.((r_1 - r_2)(u) = 0, ...) \tag{1681}$$

$$L \subseteq F(u) = \{f(u)g(u)^{-1} | g, h \in F[x], g(u) \neq 0\} \tag{1682}$$
$$\forall g \in F[x], g(u) \neq 0,\text{来说明}\exists \phi \in F[x], \phi(u) = g(u)^{-1} \tag{1683}$$
$$f\text{是F上的不可约多项式，下面两种情况成立其一:} \tag{1684}$$
$$i.f \mid g \tag{1685}$$
$$ii.\exists v_1, v_2 \in F[x], st.fv_1 + gv_2 = I_F. \tag{1686}$$
$$f(u) = 0, g(u) \neq 0, \therefore f \nmid g. \tag{1687}$$
$$I_K = f(u)v_1(u) + g(u)v_2(u) = g(u)v_2(u) \to v_2(u) = g(u)^{-1} \tag{1688}$$
$$\therefore F(u) = \{h(u) | h \in F[x]\}(h(u) = f(u)v_2(u)) \tag{1689}$$
$$\text{用带余除法消去次数} \tag{1690}$$

$$F[x], f\text{不可约}, I = \{qf|q \in F[x]\} \tag{1691}$$
$$F[x]/I\text{is a field} \tag{1692}$$
$$\phi : F[x] \to F(u), h \to h(u), \text{是环同态} \tag{1693}$$
$$ker(\phi) = I \tag{1694}$$
$$\to F[x]/I \cong F(u) \tag{1695}$$
$$Statement : \tag{1696}$$
$$F \subseteq K, u \in K\text{是代数元} \tag{1697}$$
$$f \in F[x], \text{是u在F上的极小多项式} \tag{1698}$$
$$\phi : F[x] \to F(u) \tag{1699}$$
$$\forall h \in F[x], \phi(h) = h(u) \tag{1700}$$
$$1.\phi\text{是环同态} \tag{1701}$$
$$2.ker(\phi) = \{h|h \in F[x], f|h\}, \text{有域同构}F[x]/I \cong F(u) \tag{1702}$$
$$Pf : 1.\forall g, h \in F[x], \phi(g + h) = (g + h)(u) = g(u) + h(u) = \phi(g)(u) + \phi(h)(u) \tag{1703}$$
$$\phi(gh) = (gh)(u) = g(u)h(u) = \phi(g)(u)\phi(h)(u) \tag{1704}$$
$$2.Pf : ran(\phi) = F(u) \tag{1705}$$
$$ran(\phi) = \{h(u)|h \in F[x]\} \subseteq F(u) \qquad \because \text{u是代数元}, \therefore F(u) \subseteq \tag{1706}$$
$$(\leftrightarrow \forall x \in F(u), \exists y \in F[x](\text{因为F(u)里的元素可以写成是u的多项式}) \tag{1707}$$
$$, y(u) = x, \therefore \phi(y) = x) \tag{1708}$$
$$ker(\phi) : \tag{1709}$$
$$\forall h \in F[x], h \in ker(\phi) \leftrightarrow \phi(h) = h(u) = 0 \to f|h \tag{1710}$$
$$\text{由环同态定理}, F[x]/I \cong F(u)\text{R 除以核的商环与 σ 的像同构} \tag{1711}$$
$$\text{(找到了f，可以用F[x]/I,有更大的与可以用F(u))} \tag{1712}$$

$$Thm : \tag{1713}$$
$$F \subseteq K, F\text{is a subfield of K} \tag{1714}$$
$$1 \leftrightarrow 2 \tag{1715}$$
$$1.\exists u \in K, \text{u是F上的代数元}, st.K = F(u) \tag{1716}$$
$$2.\text{K中包含的子域只有有限个} \tag{1717}$$

Pf:

$$\text{已知2，设F是无限的域。} \tag{1718}$$
$$T = \{F(z)|z \in K\}, \text{T是有限的，T在包含关系下有极大元} \tag{1719}$$
$$u \in K, F(u)\text{是T在包含关系下的极大元} \tag{1720}$$
$$\forall z \in K, F(u) \subseteq F(z) \to F(u) = F(z)(\text{因为是极大元}) \tag{1721}$$
$$\text{只需说明}\forall z \in K, z \in F(u) \tag{1722}$$
$$T' = \{F(az+u)|a \in F\} \tag{1723}$$
$$\text{T'有限，F无限} \tag{1724}$$
$$\exists a, b \in F, st.a \neq b, F(az+u) = F(bz+u) = E(\text{抽屉定理}) \tag{1725}$$
$$\therefore az+u, bz+u \in E, \therefore (b-a)z \in E \tag{1726}$$
$$b-a \in F \subseteq E \to (b-a)^{-1} \in F \subseteq E \tag{1727}$$
$$\to z \in R. \tag{1728}$$
$$\because az+u \in E, z \in E \to u \in E \tag{1729}$$
$$\therefore F(u) \subseteq E.(F \in E, u \in E, ...) \tag{1730}$$
$$\therefore E = F(u), z \in E = F(u) \tag{1731}$$

3.8 向量空间

$$K\text{is a field}, K^2 = \{(a,b)|a, b \in K\} = ae_1 + be_2 \tag{1732}$$
$$e_1 = (I_K, 0), e_2 = (0, I_K) \tag{1733}$$
$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} = A, ad - bc = det(A), if \neq 0, A\text{可逆} \tag{1734}$$
$$A^{-1} = \frac{1}{ad-bc}\begin{pmatrix} d & -b \\ -c & a \end{pmatrix} \tag{1735}$$
$$\text{K上面也是一样的，K上面也有矩阵乘法一样的，但是正定之类的性质就不一定有了} \tag{1736}$$

$$\text{K is a field,(X,+)is an Abel group,} \tag{1737}$$
$$\text{数乘}\cdot\forall a\in K, x\in X, a\cdot x\in X \tag{1738}$$
$$\text{数乘满足：} \tag{1739}$$
$$1.\forall a,b\in K, x\in X, a(bx)=(ab)x \tag{1740}$$
$$2.\forall x\in X, I_K x=x \tag{1741}$$
$$3.\forall a,b\in K, x,y\in X, a(x+y)=ax+ay,(a+b)x=ax+bx \tag{1742}$$
$$\text{称(X,+)在数乘下做成K上的向量空间} \tag{1743}$$

$$K^n=\{(a_1,...,a_n)|a_i\in K\} \tag{1744}$$
$$(K^n,+):(a_1+b_1,...,a_n+b_n)=(a_1,...,a_n)+(b_1,...,b_n) \tag{1745}$$
$$\cdot:\lambda(a_1,...,a_n)=(\lambda a_1,...,\lambda a_n) \tag{1746}$$
$$(K^n,+)\text{是K上的向量空间,} \tag{1747}$$
$$e_k=(0,...,I_K,0,...)(\text{第k个}) \tag{1748}$$
$$(a_1,...,a_n)=a_1e_1+...+a_ne_n \tag{1749}$$
$$e_1\sim e_n\text{向量空间的一组基} \tag{1750}$$

$$F_2=\{0,1\} \tag{1751}$$
$$(F_2)^4=\{(a_1,...,a_4)|a_i\in F_2\} \tag{1752}$$
$$(K,+,\cdot),\text{F是子域,u是代数元，f是u在F上的极小多项式} \tag{1753}$$
$$F(u)=\{r(u)|r\in F[x],deg(r)<deg(f)\} \tag{1754}$$
$$\text{F是F(u)子域，F(u)用域的乘法做成F上的向量空间} \tag{1755}$$
$$I_K,u,...,u^{n-1}\text{是F(u)的一组基} \tag{1756}$$
$$\text{可以生成:}\forall y\in F(u),\exists r\in F[x],deg(r)\leqslant deg(f)-1,r(y)=0 \tag{1757}$$
$$n-1,st.y=r(u) \tag{1758}$$
$$r=a_0+...+a_{n-1}x^{n-1},a_i\in F, \tag{1759}$$
$$y=r(u)=a_0u+...+a_{n-1}u^{n-1} \tag{1760}$$
$$\text{证明基线性无关：} \tag{1761}$$
$$\forall a_i,a_0I_K+...+a_{n-1}u^{n-1}=0, \tag{1762}$$
$$r(u)=0,\text{因为f是u在F上的极小多项式},deg(r)<deg(f) \tag{1763}$$
$$\rightarrow r=0\rightarrow a_i=0\rightarrow\text{线性无关} \tag{1764}$$
$$\text{空间的维数为n=deg(f)} \tag{1765}$$

$$\text{X是域K上的向量空间，} U \subseteq X, if. \tag{1766}$$
$$1.U \neq 0 \tag{1767}$$
$$2.\forall x, y \in U, x + y \in U \tag{1768}$$
$$3.\forall a \in K, \forall x \in U, ax \in U \tag{1769}$$
$$\text{U是X的一个K-子空间} \tag{1770}$$

$$\text{F is a field,X is a vector space} \tag{1771}$$
$$v_1 \sim v_n \in X. \tag{1772}$$
$$1.\text{线性无关} \tag{1773}$$
$$\forall a_1, ..., a_n \in F, st.a_1v_1 + ... + a_nv_n = 0 \tag{1774}$$
$$\to a_1 = ... = a_n = 0 \tag{1775}$$
$$2.\forall \omega \in X, \exists a_1, ..., a_n \in F, st.\omega = a_1v_1 + ... + a_nv_n \tag{1776}$$
$$\text{如果v1,...,vn线性无关,X由它们生成，称这些是}\ {}_FX\text{的一组基} \tag{1777}$$
$$3.(a_1, ..., a_n) + (b_1, ..., b_n) = (a_1 + b_1, ..., a_n + b_n) \tag{1778}$$
$$\lambda(a_1, ..., a_n) = (\lambda a_1, ..., \lambda a_n) \tag{1779}$$
$$e_1 = (I_F, 0, ..., 0), e_2 = (0, I_F, ..., 0), ..., e_n = (0, ..., 0, I_F) \tag{1780}$$
$$4.v_1, ..., v_n\text{是X的一组基，} \to dim({}_FX) = n \tag{1781}$$

$$Statement: \tag{1782}$$
$$\text{如果X中的w1,...,wn都可以用v1,...,vn表示，那么它们线性相关} \tag{1783}$$
$$\text{如果存在a1,...,an不全为零,a1v1+...+anvn=0,则v1,...,vn线性相关} \tag{1784}$$
$$\text{R在Q上的向量空间是无限维的，R不可列，Q可列,} Q^2, Q^3, ..., Q^n\text{都是可列的} \tag{1785}$$

$$\text{K is a field,F is a sub-field,}\alpha \in K \tag{1786}$$
$$F(\alpha)\text{, 则a是F上的代数元} \leftrightarrow F(\alpha)\text{作为向量空间是有限维的} \tag{1787}$$
$$f \in F[x], f \neq 0\text{是a在F上的极小多项式} \tag{1788}$$
$$deg(f) = n \to dim_F(F(\alpha)) = n \tag{1789}$$
$$\text{基是} I_F, \alpha, ..., \alpha^{n-1} \tag{1790}$$
$$(I_F, ..., \alpha^n\text{有n个元素,} f(\alpha = 0, \text{多的可以由少的表示，线性相关，所以代数元})) \tag{1791}$$

$$Statement: \tag{1792}$$
$$dim_F(X)=n,\text{U是X的一个F-子空间}(\forall x_1,x_2\in U,x_1+x_2,\lambda x_1\in U, \tag{1793}$$
$$\rightarrow \text{U是F上的向量空间，有限维，}dim_F(U)\leqslant n \tag{1794}$$
$$\text{if}dim_F(U)=n,U=X. \tag{1795}$$
$$eg.n=1 \tag{1796}$$
$$X=av_1|a\in F \tag{1797}$$
$$U\text{是X的子空间}:b\in F,b\neq 0,bv_1\in U. \tag{1798}$$
$$\forall a\in F,(ab^{-1})(bv_1)inU\rightarrow av_1\in U \tag{1799}$$
$$\tag{1800}$$

Statement:

$$\text{设K是域。E是K的子域},dim_E(K)=n \tag{1801}$$
$$\text{F是E的子域},dim_F(E)=m \tag{1802}$$
$$\rightarrow dim_F(K)\geqslant mn(F\subseteq E\subseteq K) \tag{1803}$$
$$Pf: \tag{1804}$$
$$dim_E(K)=n,\exists v_1,...,v_n\text{是K在E上的一组基} \tag{1805}$$
$$dim_F(E)=m,\exists u_1,...,u_m\text{是E在F上的一组基} \tag{1806}$$
$$assert:v_iu_j\text{是K作为F上的向量空间的一组基} \tag{1807}$$
$$1.\forall y\in K,\exists b_1,...,b_n\in E,st.y=v_1b_1+...+v_nb_n \tag{1808}$$
$$\forall b_j\in E,\exists a_{1j},...,a_{Mj}\in F,st.b_j=u_1a_{1j}+...+u_ma_{mj} \tag{1809}$$
$$y=v_1b_1+...+v_nb_n=\Sigma_{j=1}^n(\Sigma_{i=1}^m(a_{ij}u_i)v_i) \tag{1810}$$
$$=\Sigma_{i=1}^m\Sigma_{j=1}^n(a_{ij}u_iv_j) \tag{1811}$$
$$\text{2.证明线性无关} \tag{1812}$$
$$\Sigma_{i=1}^m\Sigma_{j=1}^n(a_{ij}u_iv_j)=0,\text{因为vi线性无关，所以} \tag{1813}$$
$$\forall 1\leqslant j\leqslant n,\Sigma_{i=1}^m(a_{ij}u_i)=0 \tag{1814}$$
$$\text{ui线性无关},a_{ij}=0. \tag{1815}$$

$$F_2\text{上的可逆矩阵} \tag{1816}$$
$$M_n(R).A\in M_n(R),\text{可逆:} \tag{1817}$$
$$\exists B\in M_n(R),st.AB=BA=I_n\text{或者}det(A)\neq 0\text{或者 A的n行/列在R上线性无关} \tag{1818}$$
$$\tag{1819}$$

$$F_2\text{上的可逆矩阵} \tag{1820}$$
$$M_n(F_2) = \{A|A\text{是F2上的n阶方阵}\} \tag{1821}$$
$$|M_n(F_2)| = 2^{(n^2)} \tag{1822}$$
$$GL_n(F_2) = \{A|A\text{是F2上的n阶方阵，且A可逆}\} \tag{1823}$$
$$2\text{阶，第一行不全为零，有}2^n - 1\text{种} \tag{1824}$$
$$\text{第二行，不全为零，不是第一行}, 2^n - 2\text{种} \tag{1825}$$
$$\to (2^2 - 1)(2^2 - 2) \tag{1826}$$
$$GL_n(F_2)\text{和}S_3\text{同构} \tag{1827}$$
$$\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix} \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix} \tag{1828}$$
$$\text{三阶：第一行第二行一样，第三行：0,a1,a2,a1+a2不行} \tag{1829}$$
$$(2^3 - 1)(2^3 - 2)(2^3 - 2^2) \tag{1830}$$
$$\text{四阶：}(2^4 - 1)(2^4 - 2)(2^4 - 2^2)(2^4 - 2^3) \tag{1831}$$