代数数 $Q(\alpha)=\{\alpha\in\mathbb{C}: \exists f\in\mathbb{Z}[x], f(\alpha)=0\}$

整系数多项式的复数根

No.

Date L2

均唯一，故而 $ax=ay\Rightarrow x=y$, $xa=ya\Rightarrow x=y$

(默认要求运算封闭)

group: ① Association ② identity ③ inverse ; Abilian group: $a*b=b*a$

field: ① $(F,+)$ abelian ② $(F\backslash\{0\},\times)$ abelian. ③ Distribution

ring: ① $(R,+)$ abelian ② Association ③ Distribution

field一定是ring 但ring不一定是field

例: $Q(\sqrt{2})=\{a+b\sqrt{2}\mid a,b\in Q\}\subseteq\mathbb{R}$ a field with $(+,\times)$

$Q(2^{1/3})=\{a+b\cdot2^{\frac{1}{3}}+c\cdot2^{2/3}\mid a,b,c\in Q\}\subseteq\mathbb{R}$, $Q(2^{\frac{1}{n}})$ … 同上

$\mathbb{Z}(i)=\{a+bi\mid a,b\in\mathbb{Z}, i=\sqrt{-1}\}$ gaussian ring

$M_{m\times n}(K)$ 构成群, general linear group: K上n阶可逆矩阵构成 $GL_n(K)$

special linear group: $GL_n(K)$中行列式=1的元素 $SL_n(K)$

def: $H\neq\phi$ is subset of group G, H在G的运算定义下构成群, 则 H is subgroup 记为 $H\leq G$ (和subspace的定义类似)

例: $SL_n(K)\leq GL_n(K)$, $*=+$ 或 $*=\times$

pro: $H\neq\phi$ is subset of group G, 则: (1) $H\leq G$ $\Leftrightarrow$ (2) $\Leftrightarrow$ (3)

(2): $\forall a,b\in H$, $ab\in H$, $a^{-1}\in H$, $b^{-1}\in H$

(3): $\forall a,b\in H$, $ab^{-1}\in H$, $ba^{-1}\in H$

(1)→(2): 由于 G is group $a,b\in H\subseteq G$, ①② 自动成立, ③ $\Rightarrow a^{-1}\in H, b^{-1}\in H$.

(3)→(1): $H\neq\phi$ ∴ $\exists a\in H$. let $a=b$ $ab^{-1}=a\cdot a^{-1}=e$ … ②

let $b=e$, $e\cdot a^{-1}=a^{-1}\in H$ … ③, ①是自动成立的 $\Rightarrow H\leq G$

(当 $|H|$ finite 也行)

pro: $H\neq\phi$ is subset of group G, 且 $|G|$ finite, $\Leftrightarrow xy\in H$ $\forall x,y\in H$

"$\Leftarrow$": $H=\{h_1,h_2,\cdots h_n\}$ $G=\{g_1,g_2\cdots g_m\}$ $g_1=e$, $g_2^{-1}\cdots g_m^{-1}\in G$

则 $G=\{e,g_2,g_2^{-1},g_3,g_3^{-1},\cdots g_t,g_t^{-1}\}$

$x=g_2$, $y_1=g_2^{-1}$ 可以, $y_2=g_3$ 则 $g_2^{i}g_3=e$, $g_2\cdot g_3^{j}=e$ some i,j since finite

∴ h 与 h^{-1} 要同时出现在H中, 且 $e=h\cdot h^{-1}\in H$

No. $C_G(P)=\{x: xP=Px\}$

Date $N_G(P)=\{x: x^{-1}Px=P\}$

def: 群G的中心(center)和G中所有元素可交换: $Z(G)=\{z\in G \mid gz=zg\ \forall g\in G\}$

例: $C=\{\begin{bmatrix}a & \\ & \ddots \\ & & a\end{bmatrix}: 0\neq a\in F\}\subseteq SL_n(F)$ 是 $SL_n(F)$ 的中心; $C=Z(SL_n(F))$

$z_1\in Z(G), z_2\in Z(G)$ 则 for $\forall g\in G$, $z_1z_2g=z_1gz_2=gz_1z_2$ $\therefore z_1z_2\in Z(G)$

$eg=ge$ $\therefore e\in Z(G)$ (y^{-1}在G中存在)

for $y\in C$ $yg=gy \Rightarrow gy^{-1}=y^{-1}g$; $Z(G)$定为subgroup.

def: $HK=\{h\cdot k \mid h\in H, k\in K\}$; $H^{-1}=\{h^{-1}: h\in H\}$; $H^n=\{h_1h_2\cdots h_n: h_i\in H, \forall i\}$

$Hg=\{h\cdot g: h\in H\}$ $g\in G$, 记: right coset

$gH=\{g\cdot h: h\in H\}$ $g\in G$, 记: left coset; 在coset和H之间存在双射 $gH\to g$

pro: G is group, $H\neq\emptyset$, $H\subseteq G$, 则 (1) $H\leq G \Leftrightarrow$ (2) $H^2\subseteq H$, 且 $H^{-1}\subseteq H \Leftrightarrow$

(3): $HH^{-1}\subseteq H$, $H^{-1}H\subseteq H$

显然任何G均有subgroup G $\{e\}$; $\{e\}$称为ordinary subgroup

pro: $g_1,g_2\in G$, $Hg_1\cap Hg_2\neq\emptyset \Leftrightarrow Hg_1=Hg_2$ (与Affine set类似)

设 $\exists h_1,h_2\in H$. $h_1g_1=h_2g_2\in Hg_1\cap Hg_2$

$Hg_1=H\cdot h_1g_1=H\cdot h_2g_2=Hg_2$

$\{hh_1g: h\in H\}=\{h'\cdot h_1^{-1}\cdot h_1g: h'\in H\}=\{h'g: h'\in H\}$ since: 群中元素有逆元

Lagrange: $H<G$, 则 $|H| \mid |G|$ if $|G|$ is finite

$|G:H|$ gH的个数

the coset $\{Hg: g\in G\}$ is finite; 记为 $Hg_1, Hg_2\cdots Hg_m$

取 $Hg_1,\cdots Hg_m$ s.t. $Hg_i\cap Hg_j=\emptyset$, 则 $G=Hg_1\cup Hg_2\cup\cdots Hg_m$

$|G|=|Hg_1|+|Hg_2|+\cdots|Hg_m|=m|H|$

接下来说明: 可以取出有限个disjoint coset, 使 $\cup Hg_i=G$

① $\forall g\in G$. $g, g^2\cdots g^m\cdots$ finite. 即 $\exists m$ s.t. $g^{m+1}\in\{g,g^2,\cdots,g^m\}$

$\therefore g^{m+1}=g^i$ some 个 $i\in[1,m]$, 则逆元 $g^{-1}=g^{m-i}$#, $e=g^{m+1-i}$

逆命题不成立 最小群 A_4

∴ $\langle g\rangle=\{g,g^2,\dots g^{m+1-1}\}$ forms a subgroup

② Lemma: $H\le G$, $g\in G$ 则 gH 为 H 的 left coset, 由于coset为等价类, ∴ G 可以分解为coset的无交并, $G=\dot{\bigcup}_{g\in G} gH$

g和gh之间有双射

例如: g_1H 和 g_2H 无交集

⇔ $\forall h_1\in H$, $g_1h_1\ne g_2h_2$ $\forall h_2\in H$, $\Rightarrow \forall h_1$, $g_2^{-1}g_1h_1\notin H$, $\forall h_2$ $g_1^{-1}g_2h_2\notin H$

只要 g_i 满足 $g_i^{-1}g_j\notin H$

在本定理中 找 subgroup $G'\le G$, $G'\cap H\ne\phi$, $g\in G'$ 则 $\langle g\rangle=\{g,g^2\dots g^{m+1-1}\}\le G'$

则 $Hg, Hg^2\dots Hg^{m+1-1}$ 无交集,

✓ $H\le G$. define: $a\overset{L}{\sim}b$, $\exists h\in H$ s.t $a=bh$; "$\overset{L}{\sim}$" 满足 reflective, sym., transtive

这个等价关系下, G 之元 g 的等价类为 gH; since: $g\overset{L}{\sim}b$, $\exists h$ s.t $g=bh$ ∴ $b=g\cdot h^{-1}$

等价类 $\{b\}=\{g\cdot h^{-1}: h\in H\}=\{g\cdot h: h\in H\}=gH$

✓ pro: R是A集合上的等价关系: ①: $[x]_R\ne\phi$ $\forall x$ 每个元素的等价类非空

②: $xRy \Rightarrow [x]_R=[y]_R$ 等价类若有交集,则相等 $\neg xRy\Rightarrow [x]_R\cap[y]_R=\phi$

③: $\bigcup\{[x]_R\mid x\in A\}=A$. 所有等价类的并集为原集合

$\forall a\in A$ $a\in[x]_R$ for some x; or a start a new class

$\Rightarrow A=\dot{\bigcup}[x]_R$ by ③, disjoint union by ②

在平板里写了(这个不好)

☆ Fermat: p 为素数; $a\in\{1,2\dots p-1\}$, $a^{p-1}\equiv 1 \pmod p$

let $G=(\mathbb{Z}_p\setminus\{0\},\otimes)$, $\mathbb{Z}_p$ 为mod p的等价类, $\otimes$: $i\times j \pmod n$; $|G|\overset{?}{=}p-1$

for $a\in G$, $|\langle a\rangle|\mid|G|=k$; $\langle a\rangle=m$

∴ $a^{p-1}=a^{km}=(a^m)^k\equiv 1 \pmod p$ since $a^m\equiv 1 \pmod p$

Rmk: $\mathbb{Z}_p$ 仍为 group $\{0,1,\dots p-1\}$ under addition module p

a构成循环群: (仅由一个元素生成的群)

对于G中任意 a, 称 $\langle a\rangle$ 的阶为元素 a 的阶, $o(a)=|\langle a\rangle|$; $o(a)=\arg\min a^n=e$

n正整~

No.

Date G/N：设G群运算为*，G/N为：$(g_1N)\cdot(g_2N)=(g_1*g_2)N$
我觉的这么写更严谨

def: $H\le G$. H is normal subgroup of G if：$g^{-1}hg\in H$ $\forall h\in H, g\in H$，记为 $H\trianglelefteq G$

G is group. $S\le G$. S^c 是否是 group (∵不定，封闭性不清楚)
Associate 自动成立，$s\in S$ $\exists s^{-1}\in S$，$s*s^{-1}=e\in S$；*为G的群运算
S中的e和G中的e是同一个 $\forall S\le G$ (那这样看起来 $e\in S$ ∴ $e\notin S^c$ } ?为什么 $S^c\cap S\ne\varnothing$
$x\notin S$ $x\in S^c$；$x^{-1}\notin S$ $x^{-1}\in S^c$ ∴ $x*x^{-1}=e\in S^c$

class 2.1. 9.19
$H\le G$. $H\trianglelefteq G$ $\Leftrightarrow g^{-1}Hg\subseteq H$，$\Leftrightarrow g^{-1}hg\in H$，$\forall h\in H$；$gH=Hg$；$\forall g$
对象
$g^{-1}Hg=\{g^{-1}hg:h\in H\}$ 满足 closed. inv. ind，是 subgroup
例：$SL_n(F)\trianglelefteq GL_n(F)$
well-defined 用
||
def: $N\trianglelefteq G$；let $G/N=\{gN:g\in G\}=[G:N]$ 记为 quotient / factor group (G module N)
1. 定义群运算(·)：$(g_1N)\cdot(g_2N)=(g_1\cdot g_2)N$ ；it's well-defined
$((g_1N)(g_2N))\cdot(g_3N)=(g_1N)\cdot((g_2N)\cdot(g_3N))$
N is identity，$(gN)^{-1}=g^{-1}N$ is inverse
∴在(·)下，$(G/N,\cdot)$ is group

↓与自变量的写法无关
let $g_1N=g_1hN$，$h\in N$
$\cdots=(g_1h\cdot g_2)N$
$=(g_1g_2\cdot g_2^{-1}h\cdot g_2)N$
$=(g_1\cdot g_2)N$

例：$|GL_n(F_p)/SL_n(F_p)|=p-1$ (HW2写得好一点)
$\left\{ g\in GL_n(F_p) \right.$ $g=g_1h$ for some $h\in SL_n(F_p)$，$g_1\in GL_n(F_p)$ (学会讨论元!)
$\det h=1$，$g_1=\begin{pmatrix}a&&\\&1&\\&&\ddots\\&&&1\end{pmatrix}$；$a=\det(g)\ne0$

$\Rightarrow$ 把对 $\{g\cdot SL_n(F_p):g\ldots\}$ 转化为 $\{g_1\cdot SL_n(F_p):g_1\in\ldots\}$

∴ $GL_n(F_p)/SL_n(F_p)=\{g\cdot SL_n(F_p):g\in GL_n(F_p)\}$
$=\{g_1h\cdot SL_n(F_p):g_1=\begin{pmatrix}a&&\\&\ddots&\\&&1\end{pmatrix},a\ne0\}$
$=\{g_1SL_n(F_p):g_1=\begin{pmatrix}a&&\\&\ddots&\\&&1\end{pmatrix},a\ne0\}$

$(\mathbb{Z}_p)^\times$ finite with order $p-1$，$\langle a_1\rangle$ 为其中一个生成元 $\langle g_1\rangle=\langle a_1\rangle=p-1$