1.1.1 验证以下域的性质：

(1) $a\cdot c=b\cdot c$ 且 $c\neq 0_K \Rightarrow a=b$

$(a\cdot c)c^{-1}=(b\cdot c)c^{-1} \Rightarrow a\cdot(c\cdot c^{-1})=b(c\cdot c^{-1}) \Rightarrow a=b$

(2) $\forall a,b\in K$ 若 $a\cdot b=0_K$ 则 $a=0_K$ 或 $b=0_K$

$a\cdot b=b\cdot a=0$ $b\neq 0$, $a=1\cdot a=(b^{-1}b)a=\cdots=b^{-1}\cdot(b\cdot a)=0$ $a\neq 0$ 类似

$a=b=0$ 显然.

(3) $(a^{-1})^{-1}=a$ ($\forall a\in K, a\neq 0$)

$(a^{-1})^{-1}=(a\cdot a^{-1})(a^{-1})^{-1}=a\cdot[a^{-1}(a^{-1})^{-1}]=a$

(4) $(a\cdot b)^{-1}=a^{-1}b^{-1}$

$(a\cdot b)^{-1}(a\cdot b)=1$ $(a^{-1}b^{-1})(a\cdot b)=(a^{-1}b^{-1})(b\cdot a)=1 \Rightarrow (a\cdot b)^{-1}$ 和 $a^{-1}b^{-1}$ 均为 ab 的逆元. 由逆元唯一性 $(a\cdot b)^{-1}=a^{-1}b^{-1}$

(5) $(-a)^{-1}=-a^{-1}$ ($\forall a\neq 0_K$);

$(-a)^{-1}=[(-1)\cdot a]^{-1}=(-1)^{-1}\cdot a^{-1}$ 而 $(-1)\cdot(-1)=1 \Rightarrow (-1)^{-1}=-1$ $(-1)^{-1}a^{-1}=(-1)a^{-1}$

$=-a^{-1}$

(6) $\forall a\neq 0_K$, $m,n\in\mathbb{Z}$, 则 $a^{m+n}=a^m\cdot a^n$ $a^{mn}=(a^m)^n$

运用归纳法 $a^m\cdot a^0=a^m\cdot 1_K=a^m=a^{m+0}$ $a^m\cdot a^{n+1}=a^m\cdot a^n\cdot a=(a^m\cdot a^n)\cdot a$

$=a^{m+n}\cdot a=a^{(m+n)+1}$ □ $a^{m(n+1)}=a^{mn+m}=a^{mn}\cdot a^m=(a^m)^n\cdot a^m=(a^m)^{n+1}$ □

1.1.2 证明非空个域 K 的任意一组子域的交集(可无限)仍是子域.

(2) 若 $K_i\subset K$ ($i\in\mathbb{N}$) 是满足 $K_i\subseteq K_{i+1}$ 的子域，则它们的并仍是子域.

(1) 归纳法 $n=2$ 时 $\forall\alpha_1,\alpha_2\in K_1\cap K_2$ 由于 $\alpha_1,\alpha_2\in K_1$ $\alpha_1+\alpha_2\in K_1$

$\alpha_1,\alpha_2\in K_2$ $\alpha_1+\alpha_2\in K_2 \Rightarrow \alpha_1+\alpha_2\in K_1\cap K_2$ $\alpha_1\alpha_2$ 类似

$\forall\alpha\in K_1\cap K_2$ 由于 $\alpha\in K_1$ $\exists -\alpha\in K_1$ $\alpha\in K_2$ $\exists -\alpha\in K_2$ 而由负元唯一性

$-\alpha\in K_1\cap K_2$ α^{-1} 类似

$n=k+1$ 时成立 $n=k$ 时由于 $n=k+1$ 时成立 回到2元情形 D

(2) 归纳法 $n=2$ 时 $K_1\subseteq K_2$ $K_1\cup K_2=K_2 \Rightarrow K_2$ 为子域

$n=k+1$ 时成立 $n=k$ 时由于 $n=k+1$ 时成立 回到2元情形 D

1.1.3 令 $K[\sqrt{2},\sqrt{3}]$ 表示 K 中含 $K,\sqrt{2},\sqrt{3}$ 的最小子域，证明 $K[\sqrt{2},\sqrt{3}]=K[\sqrt{2}+\sqrt{3}]$

proof: $K[\sqrt{2},\sqrt{3}]=\{a+b\sqrt{2}+c\sqrt{3}+d\sqrt{6} \mid a,b,c,d\in K\}$

记 $r=\sqrt{2}+\sqrt{3}$ $K[\sqrt{2}+\sqrt{3}]=\{a'+b'r+c'r^2+d'r^3 \mid a',b',c',d'\in K\}$

$K[\sqrt{2}+\sqrt{3}]\subseteq K[\sqrt{2},\sqrt{3}]$ 直接验证即可.

下证 $K[\sqrt{2}+\sqrt{3}]\supseteq K[\sqrt{2},\sqrt{3}]$ 由于 $\sqrt{2}+\sqrt{3}$ 是代数元由例1.1.2 $K[r]=K(r)$

注意到 $(\sqrt{2}+\sqrt{3})^{-1}=\sqrt{3}-\sqrt{2} \Rightarrow \sqrt{3}-\sqrt{2}\in K[\sqrt{2}+\sqrt{3}]$

$\Rightarrow \sqrt{2}+\sqrt{3}+\sqrt{3}-\sqrt{2}\in K[\sqrt{2}+\sqrt{3}] \Rightarrow \sqrt{3}\in K[\sqrt{2}+\sqrt{3}]$ 同理 $\sqrt{2}\in K[\sqrt{2}+\sqrt{3}]$

$\Rightarrow K[\sqrt{2}+\sqrt{3}]\supseteq K[\sqrt{2},\sqrt{3}]$ □

1.1.5 证明域的定义中交换律可去.

$(1+1)(a+b)=a+(a+b)+b=a+(b+a)+b \Rightarrow a+b=b+a$

1.1.4 $f:\mathbb{N}\to K$ $f^{-1}:K\to\mathbb{N}$ 利用有理数加和乘定义 $\forall n,m\in\mathbb{N}$

$n\oplus m=f^{-1}(f(n)+f(m))$, $n*m=f^{-1}(f(n)f(m))$, $\mathbb{N}$ 不包

证明：$\mathbb{N}=(\mathbb{N},\oplus,*)$ 是域，并求 0元 和单位元.

Proof: ① 结合律

$f^{-1}(f(n)+f(m\oplus p))=f^{-1}(f(n)+f(m)+f(p))=f^{-1}(f(n\oplus m)+f(p))$

② 交换律 $m\oplus n=f^{-1}(f(m)+f(n))=f^{-1}(f(n)+f(m))=n\oplus m$

③ 零元 $n\oplus 0_{\mathbb{N}}=f^{-1}(f(n)+f(0_{\mathbb{N}}))=f^{-1}(f(n))=n$ $\overset{f\text{双射}}{\Rightarrow} 0_{\mathbb{N}}=f^{-1}(0)$

④ 负元 $n\oplus(-n)_{\mathbb{N}}=f^{-1}(f(n)+f(-n)_{\mathbb{N}})=f^{-1}(0)$ $\overset{f\text{双射}}{\Rightarrow} f(n)+f(-n)_{\mathbb{N}}=0$

$\Rightarrow f(-n)_{\mathbb{N}}=-f(n) \Rightarrow -n_{\mathbb{N}}=f^{-1}(-f(n))$

⑤ $*$结合律类① ⑥ 乘交换律类②

⑦ $1_{\mathbb{N}}*n=f^{-1}(f(1_{\mathbb{N}})\cdot f(n))=f^{-1}(f(n))=n$ $\overset{f\text{双射}}{\Rightarrow} 1_{\mathbb{N}}=f^{-1}(1)$

⑧ $\forall n\neq 0_{\mathbb{N}}$ $n*(n^{-1}_{\mathbb{N}})=f^{-1}(f(n)\cdot f(n^{-1}_{\mathbb{N}}))=f^{-1}(1)$

$\overset{f\text{双射}}{\Rightarrow} n^{-1}_{\mathbb{N}}=f^{-1}(\frac{1}{f(n)})$

⑨ $n*(m\oplus p)=f^{-1}(f(n)(f(m)+f(p)))=f^{-1}(f(n)f(m)+f(n)f(p))$

$=(n*m)\oplus(n*p)$ □

1.1.6 设 $p>2$ 是素数，$\mathbb{F}_p=\{\bar{0},\bar{1},\bar{2},\cdots,\overline{p-1}\}$ 是 $\mathbb{Z}$ 的模 p 剩余类域

计算：(1) $\bar{2}$ 在 $\mathbb{F}_p$ 中逆元；(2) $\overline{p-1}\cdot\overline{p-2}$；(3) $\overline{p-2}$ 在 $\mathbb{F}_p$ 中逆元

(1) $\bar{2}\cdot\overline{(\frac{1}{2}(p+1))}=\bar{1}=\overline{p+1}$ 令 $\bar{2}^{-1}=\overline{\frac{1}{2}(p+1)}$ (2) $\overline{p-1}\cdot\overline{p-2}=\bar{-1}\cdot\bar{-2}=\overline{(-1)(-2)}=2$

(3) $\overline{p-2}=\bar{-2}=\bar{-1}\cdot\bar{2}$ $\overline{p-2}^{-1}=\bar{-2}^{-1}=(\bar{-1})^{-1}\bar{2}^{-1}=\bar{-1}\cdot\bar{2}^{-1}=\bar{-1}\cdot\overline{\frac{1}{2}(p+1)}=\overline{\frac{1}{2}(p-1)}$

1.1.7 证环的交换律可去

$(1+1)(a+b)=a+(a+b)+b=a+(b+a)+b \Rightarrow a+b=b+a$

1.2.3 设 X 是集合，$P(X)$ 表示 X 所有子集组成的集合，在 $P(X)$ 上定义“加法”和“乘法”：$A+B=A\cup B-A\cap B$，$A\cdot B=A\cap B$

证：上述定义中 $P(X)$ 是环且 $2A=0$ ($\forall A\in P(X)$)

① 结合 $(A+B)+C=(A\cup B-A\cap B)\cup C-(A\cup B-A\cap B)\cap C=(A\cup B)\cup C-(A\cap B)\cup C$

$-(A\cup B)\cap C+(A\cap B)\cap C=A\cup(B\cup C)-A\cup(B\cap C)-A\cap(B\cup C)+A\cap(B\cap C)=$

$A+(B\cup C-B\cap C)=A+(B+C)$

② 交换显然 ③ 零元 $A+\phi=\phi+A=A$

④ 负元 $A+A=0$ (自身为负元) $\Rightarrow 2A=0$

⑤ 结合显然 ⑥ 单位元 $A\cdot A=A\cap A=A$ (自身为单位元)

⑦ 分配律 $A\cdot(B+C)=A\cap(B\cup C)-A\cap(B\cap C)=$

$(A\cap B)\cup(A\cap C)-(A\cap B)\cap(A\cap C)=A\cap B+A\cap C=A\cdot B+A\cdot C$

$(A+B)\cdot C=(A\cup B-A\cap B)\cdot C=(A\cup B)\cap C-A\cap B\cap C=AC+B\cdot C$

1.2.4 R 是一个环，$S\subset R$ 是一个非空子集合，证：

$C(S)=\{a\in R\mid ax=xa,\ \forall x\in S\}$ 是 R 的子环.

proof: ① $\forall a,b\in C(S)$ $a,b\in R \Rightarrow a+b\in R$ $a\cdot b\in R$

② $1\cdot x=x\cdot 1 \Rightarrow 1\in C(S)$

③ $1\cdot x=x\cdot 1 \Rightarrow -(1\cdot x)=(1\cdot x)\cdot(-1) \Rightarrow (-1)x=1\cdot(x\cdot(-1))=x(-1)$

$(-a)x=-(a\cdot x)=a\cdot x(-1)=x\cdot a(-1)=x\cdot(-a) \Rightarrow (-a)\in C(S)$ □

1.2.6 $\forall x \in R, x^2 = x$ 证 R 是交换环

Proof: $(x+x) = (x+x)^2 = x^2+x^2+x^2+x^2 = x+x+x+x \Rightarrow x+x=0 \quad x=-x$ ①

$(x+y) = (x+y)^2 = x^2+xy+yx+y^2 = x+y+xy+yx \Rightarrow xy+yx=0$

$\Rightarrow xy+(xy+yx) = xy$ 由于 R 中至少 2 个元 $\Rightarrow xy+yx=0 \overset{①}{\Rightarrow} xy=yx$

1.2.9 "$\Leftarrow$"

$\forall \bar{a} \in \mathbb{F}_p$ 且 $\bar{a} \neq \bar{0} \Rightarrow p \nmid a \Rightarrow (p,a)=1 \Rightarrow \exists u,v \in \mathbb{Z}$ s.t.

$1 = up+va \Rightarrow \bar{1} = \overline{u \cdot p + v \cdot a} = \bar{u} \cdot \bar{p} + \bar{v}\bar{a} = \bar{u} \cdot \bar{0} + \bar{v} \cdot \bar{a} = \bar{v} \cdot \bar{a}$

从而 $\forall \bar{0} \neq \bar{a} \in \mathbb{F}_p \quad \exists \bar{v} \in \mathbb{F}_p$ s.t. $\bar{a} \cdot \bar{v} = \bar{1}$

"$\Rightarrow$" $\bar{v}a + \bar{u}m = \bar{1} \quad \bar{v} \cdot \bar{a} = \bar{1} \Rightarrow \bar{u}m = 0 \Rightarrow m = p \Rightarrow (m,a)=1$

1.2.13 (1) 由 $2^b=2$, $3^b=3 \Rightarrow 64=2$, $729=3 \Rightarrow 62=0, 726=0$

由 Bezout 定理 $gcd2=(j,k)=nj+mk=0$ ⇒ 得到 $2=0$ 的环

⇒ $x^6+6x^5+15x^4+20x^3+15x^2+6x+1=x+1$ ⇒ 消去偶项 $x^6+x^4+x^2+1=x+1$

由 $2=0$ 又有 $1=-1 \Rightarrow x^2=-x^2$ 而 $x^6=x$ 可得 $x^4+x^2=0$ 或 $x^4=x^2$

⇒ $x^4\cdot x^2=x^2\cdot x^2 \Rightarrow x^6=x^4 \Rightarrow x^6=x^2$ 又由 $x^6=x \Rightarrow x^2=x$ □

或 $f(x)=x^6-x=0=f(x+1)$ $gcd[f(x),f(x+1)]=x^2-x$ 由 Bezout $x^2-x=0$ □

(2) $(x+x)=(x+x)^2=x^2+x^2+x^2+x^2=x+x+x+x \Rightarrow x+x=0$ $x=-x$ ①

$(x+y)=(x+y)^2=x^2+xy+yx+y^2=x+y+xy+yx \Rightarrow xy+yx=0$

⇒ $xy+(xy+yx)=xy$ 由于 R 中至少 2 个元 ⇒ $xy+yx=0 \overset{②}{\Rightarrow} xy=yx$ □

1.3.1 $(ab)^n=e$ $a^{-1}(ab)^n a=e=(ba)^n \Rightarrow ab$ 与 ba 同阶

1.3.3 $e=(ab)^2=a^2=b^2 \Rightarrow ba=ba\cdot(ab)^2 \Rightarrow ba=ba^2bab \Rightarrow ba=ab$

1.3.8 "⇒" 由逆元的唯一性, $x=a^{-1}b$ $y=ba^{-1}$ 是唯一解

"⇐" 取 $a=b$ 则设 $ea=a$, 则 e 为所有元素的左单位元因为 $\forall b$ $ax=b \Rightarrow eb=eax=ax=b$ 同理若 e' 为某一元素的右单位元, 则 e' 为所有元素的右单位元. 若 l 是一左单位元, r 是一右单位元

则 $lr=l=r \Rightarrow l=r$ 故单位元仅有一个记为 e, 又由左右单位元的唯一性单位元唯一. 下证存在唯一逆元 若 $xa=ya=e$ 令 $az=e$

⇒ $x=xe=xaz=yaz=ye=y$ 其 $z=ez=xaz=xe=x$

⇒ 存在唯一逆元 □

1.3.10 将 G 中各元素与其逆元一一对应, 则仅有 e 没有元素与之对应因为 $e^{-1}=e$. 由于 G 为偶数阶, $\exists a\in G$ $a\neq e$ s.t. $a=a^{-1}$

$a^2=e \Rightarrow$ G 中有二阶元

1.3.11 $x^4=I_2$ $y^3=I_2$ 而 $xy=-\begin{pmatrix}1&1\\0&1\end{pmatrix} \Rightarrow (xy)^k=(-1)^k\begin{pmatrix}1&k\\0&1\end{pmatrix}$

⇒ xy 是无限阶元.

1.4.3 (1) $x_1,x_2\in\ker\varphi$ $\varphi(x_1+x_2)=\varphi(x_1)+\varphi(x_2)=0 \Rightarrow x_1+x_2\in\ker\varphi$

$\forall x\in\ker\varphi$ $\varphi(-x)=\varphi(0)-\varphi(x)=0$

(2) $\varphi(ax)=\varphi(a)\varphi(x)=\varphi(a)\cdot 0_R=0$ $\varphi(xa)$ 同理

1.4.5 由于 exp 单调 $\exp: \mathbb{R}\to\mathbb{R}^\times$ 为单同态.

$\forall y\in\mathbb{R}^\times$, $\log y\in\mathbb{R}$ $e^{\log y}=y \Rightarrow \exp$ 为满同态

⇒ $\exp: \mathbb{R}\to\mathbb{R}^\times$ 为同态. 其逆映射 $\log: \mathbb{R}^\times\to\mathbb{R}$

$\forall x,y\in\mathbb{R}^\times$ $\log(xy)=\log x+\log y$. □

1.4.8 设 $F_1=\Phi[\sqrt{d}]$ $F_2=\Phi[\sqrt{d'}]$ 下证若 $F_1\cong F_2$, 则 $d=d'$, 该命题逆否命题即所需结论.

若 $(x+y\sqrt{d'})^2=d \Rightarrow x^2+d'y^2+2xy\sqrt{d'}=d \Rightarrow 2xy=0 \Rightarrow$

$x^2+d'y^2=d$ 若 $x=0$ 则 $d=d'y^2$ 消去分母 $da^2=d'b^2$ 而 $gcd(a,b)=1$

1.2.13 如果环R满足条件：$x^6=x$ $(\forall x\in R)$ 证明：

(1) $x^2=x$ $(\forall x\in R)$.

(2) R是一个交换环.

解：(1) $\forall x\in R$. 有 $2x\in R$, $3x\in R$.

进而有 $(2x)^6=2x \Rightarrow 64x^6=2x \Rightarrow 64x=2x \Rightarrow 62x=0$

$(3x)^6=3x \Rightarrow 729x^6=3x \Rightarrow 729x=3x \Rightarrow 726x=0$

从而由 726, 62的最大公因数为2. 知 $\exists q,p\in\mathbb{Z}$

有 $q(62x)+p(726x)=2x=0$.

考虑多项式：$x^6-x=(x^2-x)(x^4+x^3+x^2+x+1)$.

$g(x)=(x^2-x)((x+1)^4+(x+1)^3+(x+1)^2+(x+1)+1)$

(此x为单纯的未知变量，且不一定属于环R).

显然地，x^6-x 与 $g(x)$ 的最大公因式为 (x^2-x).

从而 $\exists u(x), v(x)$.

s.t $u(x)(x^6-x)+v(x)g(x)=x^2-x$. (且不难验证 $u(x), v(x)$ 的系数均为整数).

代入到环R中，即有 $\forall x\in R$.

有 $u(x)(x^6-x)+v(x)g(x)=x^2-x$.

又 $2x=0$. 即得 $x^2-x=x^2+x$.

故有 $g(x)=(x^2-x)[(x+1)^4+(x+1)^3+(x+1)^2+(x+1)+1]$

$=(x^2+x)[(x+1)^4+(x+1)^3+(x+1)^2+(x+1)+1]$

$=(x+1)^6-(x+1)$.

从而 $u(x)(x^6-x)+v(x)[(x+1)^6-(x+1)]=x^2-x=0$.

即有 $x^2=x$.

(2). 由 $x^2=x$.

有 $2(x+x)^2=(2x)^2=2x$.

又 $(2x)^2=4x^2=4x$.

从而 $4x=2x \Rightarrow x=-x$.

$\forall x,y\in R$

由 $(x+y)^2=x^2+y^2+xy+yx=x+y$

又 $x^2+y^2+xy+yx=x+y+xy+yx$.

从而 $xy+yx=0 \Rightarrow xy=-yx=yx$.

从而R为一个交换环.

3.1 设G是一个群，对 $\forall a,b\in G$. 证明 ab 的阶与 ba 的阶相等.

证明：设 ab 的阶为 n.

则 $(ab)^n=e$. 即 $a(ba)^{n-1}b=e$. 从而 $(ba)^{n-1}b=a^{-1}$. 得 $(ba)^{n-1}ba=e$.

即 $(ba)^n=e$.

同样地，可说明 $(ba)^n=e$ 时，有 $(ab)^n=e$. 故 ab 的阶与 ba 的阶相等

1.3.3 证明：除3单位元之外所有元素的阶都是2的群一定是交换群.

证明：设这样的群为 R.

从而 $\forall x \in R$. 有 $x^2 = e$.

故 $\forall a, b \in R$. 有 $(ab)^2 = abab = e$.

故 $ba = ba \cdot e = baabab = b(a^2)bab = (b^2)ab = ab$.

故 R 必为交换群.

1.3.8. 证明：半群 G 是群的充要条件为：$\forall a, b \in G$，$ax = b$ 和 $ya = b$ 都有唯一解.

证明：先说明必要性

若 G 是群，则 $\forall a, b \in G$. 有 $a^{-1}, b^{-1} \in G$.

故 $ax = b \iff b^{-1}ax = e$.

得 $x = (b^{-1}a)^{-1}$，由 $b^{-1}a \in G$ 且其逆元唯一.

故有 $x \in G$，x 唯一. 即 $ax = b$ 有唯一解.

同样地，$ya = b \iff yab^{-1} = e \iff y = (ab^{-1})^{-1}$. 亦得 $ya = b$ 有唯一解.

再说明充分性.

由条件. $a_0 x = a_0$ 有唯一解. 设其为 I_r.

$\forall a \in G$. 由有：$ya_0 = a$ 有唯一解.

从而 $aI_r = ya_0 \cdot I_r = y(a_0 \cdot I_r) = ya_0 = a$.

从而 G 含有右单位元 I_r.

由条件. $\forall a \in G$. $ax = I_r$ 有唯一解. 故 G 中每个元素 a 有右逆.

由 1.3.7 知 半群 G 为群.

下去征一下.

1.3.10. 证明：偶数阶有限群中必有二阶元

证明：设 G 为任意一个偶数阶群. 即 G 中元素的个数为 $2n$ $(n \in \mathbb{Z}_+)$.

下面考虑 G 中各类阶的元素的个数.

i 若 $a \in G$，$|\langle a \rangle| = 1$. 则 a 必为 e.

ii 若 $a \in G$，$|\langle a \rangle| > 2$. 则有 $a^2 \neq e$，即 $a \neq a^{-1}$ 且 $a \neq e$.

从而有 $a^{-1} \neq e$，$(a^{-1})^2 \neq e$. 从而有 $|\langle a^{-1} \rangle| > 2$.

故阶大于2的元素必成对出现.

结合 i，ii 且 G 中不存在零阶元素. 若 G 中不存在二阶元. 则 G 中元素的个数为奇数.

故 G 中必存在二阶元，且为奇数个.

1.3.11. 由 $x = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$，$x^2 = \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}$，$x^3 = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$，$x^4 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$.

$y = \begin{pmatrix} 0 & 1 \\ -1 & -1 \end{pmatrix}$，$y^2 = \begin{pmatrix} -1 & -1 \\ 1 & 0 \end{pmatrix}$，$y^3 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$.

从而 $|\langle x \rangle| = 4$，$|\langle y \rangle| = 3$.

因 $xy=\begin{pmatrix}-1,&-1\\0,&-1\end{pmatrix}$, $(xy)^2=\begin{pmatrix}1,&2\\0,&1\end{pmatrix}$, $(xy)^3=\begin{pmatrix}-1,&-3\\0,&-1\end{pmatrix}$

下面用数学归纳法说明 $(xy)^n=(-1)^n\begin{pmatrix}1&n\\0&1\end{pmatrix}$.

① $n=1,2,3$ 时结论成立.

② $n\geq 2$ 时. 下面说明 $n+1$ 时结论亦成立.

$$(xy)^{n+1}=(xy)^n\cdot(xy)=(-1)^n\begin{pmatrix}1&n\\0&1\end{pmatrix}\begin{pmatrix}-1,&-1\\0,&-1\end{pmatrix}=(-1)^n\begin{pmatrix}-1,&-(n+1)\\0,&-1\end{pmatrix}=(-1)^{n+1}\begin{pmatrix}1,&\\0,&\end{pmatrix}$$

故由归纳. 结论成立.

从而 $\forall n\in\mathbb{Z}_+$. 有 $(xy)^n\neq E\begin{pmatrix}1&0\\0&1\end{pmatrix}$.

故 xy 为无限阶元.

1.4.3 设 $R\xrightarrow{\varphi}R'$ 是环同态. 证明集合 $\ker(\varphi)=\{x\in R\mid\varphi(x)=0_{R'}\}$ 满足:

(1) $\ker(\varphi)$ 是 $(R,+)$ 的子群.

(2). $\forall a\in\ker(\varphi)$, $x\in R$ 有 $ax\in\ker(\varphi)$, $xa\in\ker(\varphi)$.

证明: (1). 群 $(R,+)$ 的单位元 $e=0_R$.

$\forall a,b\in\ker(\varphi)$.

则 $\varphi(a+b)=\varphi(a)+\varphi(b)=0_{R'}+0_{R'}=0_{R'}$.

故 $a+b\in\ker(\varphi)$.

$\because\varphi(0_R)=\varphi(0_R)+\varphi(0_R)\Rightarrow\varphi(0_R)=0_{R'}$.

故 $0_R\in\ker(\varphi)$.

$\forall a\in\ker(\varphi)$., 有 $a^{-1}=-a$.

由 $\varphi(a+(-a))=\varphi(a)+\varphi(-a)=\varphi(0_R)=0_{R'}$.

从而 $\varphi(-a)+0_{R'}=0_{R'}\Rightarrow\varphi(-a)=0_{R'}$.

即有 $a^{-1}=-a\in\ker(\varphi)$.

综上 $\ker(\varphi)$ 是 $(R,+)$ 的子群.

(2). ~~$\varphi(ax)=$~~

$\forall a\in\ker(\varphi)$, $x\in R$.

有 $\varphi(ax)=\varphi(a)\cdot\varphi(x)=0_{R'}\cdot\varphi(x)=(0_{R'}+0_{R'})\cdot\varphi(x)$.

故得 $0_{R'}\cdot\varphi(x)=0_{R'}$. 便有 $\varphi(ax)=0_{R'}\Rightarrow ax\in\ker(\varphi)$.

$\varphi(xa)=\varphi(x)\cdot\varphi(a)=\varphi(x)\cdot 0_{R'}=\varphi(x)(0_{R'}+0_{R'})$.

得 $\varphi(x)\cdot 0_{R'}=0_{R'}$ 便有 $\varphi(xa)=0_{R'}\Rightarrow xa\in\ker(\varphi)$.

1.4.5. 证明实数域 R 的加法群 $(R,+)$ 和正实数域的乘法群 $(R_{>0},\cdot)$ 同构.

证明: 定义映射 $\varphi: R\to R_{>0}$.

$$x\longmapsto e^x$$

$\forall a,b\in R$. 有 $\varphi(a+b)=e^{a+b}=\varphi(a)\cdot\varphi(b)$.

又 φ 为双射. 从而 R 与 $R_{>0}$ 同构. 即 $R\simeq R_{>0}$.

1.4.8 证明：$\mathbb{Q}[\sqrt{2}]=\{a+b\sqrt{2}\mid a,b\in\mathbb{Q}\}$ $\mathbb{Q}[\sqrt{5}]=\{a+b\sqrt{5}\mid a,b\in\mathbb{Q}\}$ 都是 $\mathbb{R}$ 的子域，它们是同构的域吗？

证明：先说明 $\mathbb{Q}[\sqrt{2}]$ 和 $\mathbb{Q}[\sqrt{5}]$ 是 $\mathbb{R}$ 的子域.

令 $f(x)=x^2-2\in\mathbb{Q}[x]$, $g(x)=x^2-5\in\mathbb{Q}[x]$.

由 $f(\sqrt{2})=0$, $g(\sqrt{5})=0$ 知 $\mathbb{Q}[\sqrt{2}]=\mathbb{Q}(\sqrt{2})$, $\mathbb{Q}[\sqrt{5}]=\mathbb{Q}(\sqrt{5})$.

从而 $\mathbb{Q}[\sqrt{2}]$ 和 $\mathbb{Q}[\sqrt{5}]$ 都是 $\mathbb{R}$ 的子域.

假设存在 $\varphi:\mathbb{Q}[\sqrt{2}]\longrightarrow\mathbb{Q}[\sqrt{5}]$

至少满足：① φ 为双射. ② $\forall a,b\in\mathbb{Q}[\sqrt{2}]$, $\varphi(ab)=\varphi(a)\varphi(b)$

假设存在同构 $\varphi:\mathbb{Q}[\sqrt{2}]\to\mathbb{Q}[\sqrt{5}]$.

则 $\forall a\in\mathbb{Q}[\sqrt{2}]$.

$\varphi(a)=\varphi(1\cdot a)=\varphi(1)\cdot\varphi(a)$

从而必有 $\varphi(1)=1$.

又 $\varphi(2)=\varphi(1+1)=\varphi(1)+\varphi(1)=2$.

故 $\varphi(2)=\varphi(\sqrt{2}\cdot\sqrt{2})=\varphi(\sqrt{2})\cdot\varphi(\sqrt{2})$.

记 $\varphi(\sqrt{2})=a+b\sqrt{5}$. 则 $a^2+5b^2+2ab\sqrt{5}=2$. $(a,b\in\mathbb{R})$.

故 $\begin{cases}a=\sqrt{2}\\ b=0\end{cases}$ 或 $\begin{cases}b=\frac{\sqrt{2}}{5}\\ a=0\end{cases}$ ×. $\varphi(\sqrt{2})=\pm\sqrt{2}$.

从而 $\varphi(\sqrt{2})=\sqrt{2}$ 或 ~~$\varphi(\sqrt{2})=-\sqrt{2}$~~ $\notin\mathbb{Q}[\sqrt{5}]$.

假设不成立. 故二个域不同构.

1.4.13 设 $V=(V,+)$ 是一个加法群，$\mathrm{Hom}(V)$ 表示其自同态环. 对任意域 K. 若存在运算 $K\times V\to V$. $(\lambda,v)\mapsto\lambda\cdot v$ 使得加法群 $V=(V,+)$ 成为一个 K 线性空间，则称该数乘运算是加法群 $V=(V,+)$ 上的一个 K-线性空间结构. 试证明：

(1) 如果存在一个环同态 $\varphi:K\to\mathrm{Hom}(V)$. 则数乘运算

$$K\times V\to V,\ (\lambda,v)\mapsto\lambda\cdot v:=\varphi(\lambda)(v).$$

是 V 上的一个 K-线性空间结构.

(2) 如果存在 K-线性空间结构 $\phi:K\times V\to V$. 则映射

$$\varphi:K\to\mathrm{Hom}(V),\ \lambda\mapsto\phi(\lambda,\cdot)$$

是一个环同态，其中 $\phi(\lambda,\cdot):V\to V$ 定义为 $v\mapsto\phi(\lambda,v):=\lambda\cdot v$;

(3) 对任意域 K，整数加法群 $\mathbb{Z}=(\mathbb{Z},+)$ 上不存在 K-线性空间结构.

证明：(1) 因 $\varphi(\lambda)\in\mathrm{Hom}(V)$.

从而有 $\varphi(\lambda)(a+b)=\varphi(\lambda)(a)+\varphi(\lambda)(b)$. $(\forall a,b\in V)$.

$\varphi(\lambda)(\overset{0}{\lambda\cdot a})=\varphi(\lambda)(0)+\varphi(\lambda)(0)\Rightarrow\varphi(\lambda)(0)=0$. (0为加法群中的单位元)

$\varphi(\lambda)(na)=\varphi(\lambda)(\underbrace{a+\cdots+a}_{n\text{个}})=n\varphi(\lambda)(a)$. $(n\in\mathbb{Z}_+)$.

$\varphi(\lambda)(-na)=-\varphi(\lambda)(na)=-n\varphi(\lambda)(a)$ $(n\in\mathbb{Z}_+)$.

从而下面验证 $K\times V\to V$ 是 V 上的一个 K-线性空间结构. (八条定义)

$\forall \lambda,u\in K,\ \forall x,y\in V.$

$\begin{cases} 1_K\cdot x=\varphi(1_K)\cdot x=x. \\ \lambda\cdot u\cdot x=\varphi(\lambda\cdot u)\cdot x=\varphi(\lambda)\varphi(u)x=\lambda(ux). \end{cases}$

则 $\lambda\cdot(x+y)=\varphi(\lambda)(x+y)=\varphi(\lambda)(x)+\varphi(\lambda)(y)=\lambda\cdot x+\lambda\cdot y.$

$(\lambda+u)\cdot x=\varphi(\lambda+u)(x)=(\varphi(\lambda)+\varphi(u))(x)=\varphi(\lambda)(x)+\varphi(u)(x)$

$=\lambda x+ux.$

2). $\forall \lambda,u\in K.\ \forall v\in V.$

(i) $\varphi(\lambda+u)=\phi(\lambda+u,v)=(\lambda+u)\cdot v=\lambda v+uv=\phi(\lambda,v)+\phi(u,v)$

$=\varphi(\lambda)+\varphi(u).$

$\varphi(\lambda\cdot u)=\phi(\lambda\cdot u,v)=(\lambda\cdot u)v=\lambda(uv)=\varphi(\lambda)\varphi(u).$

(ii) $\varphi(1_K)=\phi(1_K,v)=1_V\cdot v=v\Rightarrow$ $\varphi(1_K)$ 为恒等映射. 即 $\mathrm{Hom}(V)$ 中的单位元.

从而 $\varphi:K\to \mathrm{Hom}(V)$ 是一个环同态.

3). 若整数加法群上存在 K-线性空间结构.

则必存在一个环同态 $\varphi: K\to \mathrm{Hom}(\mathbb{Z})$.

又 $\mathrm{Hom}(\mathbb{Z})\cong\mathbb{Z}$

则必存在一个环同态 $\varphi: K\to\mathbb{Z}$.

下面用环同态的相关性质导出矛盾.

$\forall a,b\in K.$

$\varphi(a\cdot b)=\varphi(a)\cdot\varphi(b).$

$\varphi(a+b)=\varphi(a)+\varphi(b).$

$\varphi(1_K)=1.$

对于 $\forall a\neq 0_K$. 有 $\varphi(a\cdot a^{-1})=\varphi(a)\cdot\varphi(a^{-1})=\varphi(1_K)=1.$

又 $\varphi(a),\varphi(a^{-1})\in\mathbb{Z}$. 则 $\varphi(a)=\pm 1.$

由 a 的任意性. 得 $\varphi(2a)=\pm 1.$

又 $\varphi(2a)=\varphi(a)+\varphi(a)=\pm 2$. 故矛盾.

则整数加法群上不存在 K-线性空间结构.

A^+.

1. (2.1.1)
R是交换环，I⊂R是理想，证：

$\sqrt{I}=\{r\in R \mid \exists m\in\mathbb{Z} \text{ s.t. } r^m\in I\}$

也是理想：

$\forall a\in R,\ b\in\sqrt{I}$ 设 $b^m\in I$

要证 $ab\in\sqrt{I}$，$ba\in\sqrt{I}$

由于 $(ab)^m=a^mb^m\in I\Rightarrow ab\in\sqrt{I}$

$(ba)^m=b^ma^m\in I\Rightarrow ba\in\sqrt{I}$

下证 $\sqrt{I}$ 为 $(R,+)$ 子群

$\forall a,b\in\sqrt{I}$ 设 $a^m\in I$，$b^n\in I$

$(a+b)^{m+n}=\sum_{k=0}^{m+n}C_{m+n}^{k}a^kb^{m+n-k}\in I$

因为 $k\geq m$ 和 $m+n-k\geq n$ 必有一个成立

$\Rightarrow a+b\in\sqrt{I}$

由于 $\sqrt{I}\in I$，可得结合律

下证逆元

$\forall x\in R$ $ax=xa$ $(ax)^m=a^mx^m\in I$

故 $ax,xa\in\sqrt{I}$ 令 $x=-1\Rightarrow -a\in\sqrt{I}$

□

2、(2.1.3)
证仅有有限个元素的整环是域

整环内除零外元素构成乘法满足消去律的半群，而有限半群构成群，故有限整环为域

3、(2.1.4)
证有有限个理想的整环是域

$\forall u\in R$ $u\neq 0$ 考虑由 u 生成的理想

降链 $(u)\subseteq(u^2)\subseteq(u^3)\subseteq\cdots\subseteq(u)^m$

由于仅有有限个理想，$\exists m$ s.t.

$(u)^m=(u)^{m+1}\Rightarrow\exists v\in R$ s.t.

$u^m=vu^{m+1}\Rightarrow 1=uv$

整环有消去律 □

4、(2.1.5)
理想 $P\subset R$ 称为素理想，如果 $ab\in P\Rightarrow a\in P$ 或 $b\in P$。试证明：$P\subset R$ 是素理想当且仅当 R/P 没有零因子。

证明：(反证)

"⇒"

若 $P\subset R$ 是素理想，设 R/P 有零因子，则 $\exists\bar{a}\cdot\bar{b}\neq\bar{0}$，$\bar{a}\cdot\bar{b}=\bar{0}$

从等价类 $\bar{a}$ 中取出 a，等价类 $\bar{b}$ 中取出 b。$\exists c\in P$ s.t. $ab=c$ 即 $ab\in P$

$\Rightarrow a\in P$ or $b\in P\Rightarrow\bar{a}=\bar{0}$ 或 $\bar{b}=\bar{0}$

矛盾

"⇐" 若 R/P 无零因子，设 P 非素理想，即 $\exists a\notin P$，$b\notin P$，$ab\in P$

考虑环同态 $R\xrightarrow{\varphi}R/P$

$\varphi(a)=\bar{a}$ $\varphi(b)=\bar{b}$ 则 $\bar{a},\bar{b}\neq 0$

但 $\bar{a}\cdot\bar{b}=0$ 这与无零因子矛盾

5 (2.1.6) 理想 $m\subset R$ 称为极大理想，若 R 中不存在真包含 m 的非平凡理想

(引：若 $I\supsetneq m$ 是 R 的理想，则必有 $I=R$)

证：R 是交换环时，$m\subset R$ 是极大理想，当且仅当 R/m 是一个域。特别，交换环中极大理想必为素理想。

证："⇒"

若 m 是 R 的极大理想，R/m 是环，从而仅验证：

(1) $\bar{a}\cdot\bar{b}=\bar{b}\cdot\bar{a}\in R/m$

(2) $\forall\bar{a}\in R/m$ $\bar{a}\neq 0$ $\exists\bar{a}^{-1}\in R/m$ $\bar{a}\cdot\bar{a}^{-1}=\bar{1}$

(1) 由 R 是交换环易得

(1) 先证 x 与 m 能生成 R

由于 m 是极大理想.

$\forall \bar{x} \in R/m$，若 x 与 m 不能生成 R

而 $x \in R \Rightarrow \exists y_0, y_0 \neq ax+n$

其中 $n \in m$，$a \in R$

(其存在意是 $\forall y$，$y = ax+n$ 由 m 是极大理想保证，因为下会证 $\{ax+n\}$ 是理想，如不成立则与极大理想矛盾)

考虑集合 $I = \{ax+n \mid a \in R, n \in m\}$

显然它是加法子群，并且有

$\forall y \in R \quad y(ax+n) = xay + ny \in I$

故其是一个理想.

从而 I 为包括 m 的理想，因为

有 $x \in I$，$x \notin m$ 矛盾.

从而 x 与 m 可生成 R.

而考虑 $R \xrightarrow{\varphi} R/m$

设 $1 = ax+n$

$\varphi(1) = \varphi(ax+n) = \varphi(a)\varphi(x) + \varphi(n)$

$= \varphi(a)\varphi(x)$

$\Rightarrow \bar{a}\cdot\bar{x} = 1 \Rightarrow \bar{x}$ 有逆 $\bar{a}$

$\Rightarrow R/m$ 是域.

("$\Leftarrow$")

若 R/m 是域，则反设 m 不是极大理想.

$\Rightarrow \exists\, m \subsetneq I$，$I$ 为一个理想.

$\Rightarrow \exists a \in I$，$a \notin m$

而 R/m 是域 $\Rightarrow \exists b$ s.t. $1 = \bar{a}\bar{b}$

$\Rightarrow ab - 1 \in m \Rightarrow ab \in I$

又 $m \subsetneq I \Rightarrow ab - 1 \in I$

$\Rightarrow 1 \in I \Rightarrow \forall x \in R \quad x\cdot 1 = x \in I$

$\Rightarrow I = R$. 故 m 为极大理想.

6. (2.1.11)

设 R 是一个环，子环

$C(R) = \{a \in R \mid ab = ba \ \forall b \in R\}$ 称为 R 的中心. 证:

(1) 若 R 是一个除环，$C(R)$ 是一个域

(2) 令 $\mathbb{H}$ 表示 Hamilton 四元数环，则 $C(\mathbb{H}) = \mathbb{R}$.

$$\mathbb{H} = \left\{ \begin{pmatrix} z & -w \\ \bar{w} & \bar{z} \end{pmatrix} \mid z, w \in \mathbb{C} \right\} \subset M_2(\mathbb{C})$$

(1) R 为除环，即其非零元集合 R^* 关于 R 的乘法成为一个群(非零元可逆) 又由 $C(R)$ 满足交换律

故 $\square$.

(2)

差 2.1.5

去年期中用态.定理的应用

设 $R \xrightarrow{f} R'$ 是一个环同态，令 $I = \ker(f)$，则 $\exists$ 唯一单同态 $R/I \xrightarrow{\bar{f}} R'$ 使 $f = \bar{f}\cdot\varphi$，其中 $\varphi: R \to R/I$ 是商同态.

$$\begin{array}{ccc} R & \xrightarrow{f} & R' \\ \varphi \downarrow & \nearrow \bar{f} & \\ R/I & & \end{array}$$

2.1.15 加法部分成立.

关于乘法:

$$\begin{pmatrix} a & b \\ -b & a \end{pmatrix}\begin{pmatrix} c & d \\ -d & c \end{pmatrix}=\begin{pmatrix} ac-bd & ad+bc \\ -bc-ad & ac-bd \end{pmatrix} \in \mathbb{F}_{3^2}$$

交换律由上式可得.

结合律由矩阵乘法给出.

单位元: $\begin{pmatrix} a & b \\ -b & a \end{pmatrix}\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}=\begin{pmatrix} a & b \\ -b & a \end{pmatrix}$

逆元: 对于 $\begin{pmatrix} a & b \\ -b & a \end{pmatrix}$ 希望: $\begin{cases} ac-bd=1 \\ ad+bc=0 \end{cases}$ (a,b不同时为0).

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

$\begin{pmatrix} 1 & 1 \\ -1 & 1 \end{pmatrix}\begin{pmatrix} 2 & 1 \\ -1 & 2 \end{pmatrix}=\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$

$\begin{pmatrix} 1 & 2 \\ -2 & 1 \end{pmatrix}\begin{pmatrix} 2 & -2 \\ -2 & 2 \end{pmatrix}=\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$

$\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}\begin{pmatrix} 0 & 2 \\ -2 & 0 \end{pmatrix}=\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$

$\begin{pmatrix} 2 & 0 \\ 0 & 2 \end{pmatrix}\begin{pmatrix} 2 & 0 \\ 0 & 2 \end{pmatrix}=\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$

从而 $\forall \begin{pmatrix} a & b \\ -b & a \end{pmatrix} \neq \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$ 存在逆元.

分配律亦由矩阵环给出.

换为 $\mathbb{F}_5$ 后, 上述集合是25元域

只用验证逆元. 即 $\forall a,b$ 不全为0, $\begin{pmatrix} a & b \\ -b & a \end{pmatrix}$ 有逆元.

即 $\begin{cases} ax-by\equiv 1 \pmod 5 \\ ay+bx\equiv 0 \pmod 5 \end{cases}$ 有解. $\Rightarrow \begin{cases} y\equiv \frac{-b}{a^2+b^2} \pmod 5 \\ x\equiv \frac{a}{a^2+b^2} \pmod 5 \end{cases}$

由于 a,b 不全为0, $\Rightarrow a^2+b^2\neq 0 \pmod 5 \Rightarrow \frac{1}{a^2+b^2}$ 有意义

$\Rightarrow y,x$ 存在.

从而其有逆元. 从而是25元域.

2.2.2 由于 $P=(p)R$ 是素理想, $\forall R\setminus (p)R$ 无零因子.

~~若p可逆 $\Rightarrow p^{-1}p\in(p)R \Rightarrow 1_R\in(p)R \Rightarrow R\subset(p)R$.~~

~~$\Rightarrow (p)\cap R=R=\{ap \mid a\in\mathbb{Z}\}$.~~ (这种情况反例)

~~下面我们说明. p一定可逆.~~ 考虑. mod p 剩余类域 R.

~~若p可约~~

~~考虑. R的子环 $R_0=\{a\cdot 1_R \mid a\in\mathbb{Z}\}\subset\{a\cdot p \mid a\in\mathbb{Z}\}$.~~

由1生成的理想为R.

可逆并且 $1=a\cdot a^{-1}$

可约)

由 $p^2\in R$. 设 $p^2=a\cdot p$. $a\in\mathbb{Z}$. $\Rightarrow p(p-a\cdot 1_R)=0$

$\Rightarrow p=a\cdot 1_R$.

又 $1_R\in R \Rightarrow 1_R=b\cdot p \Rightarrow p=ab\cdot p \Rightarrow (ab-1)p=0$.

~~若p不可逆~~. 假设p可约, $p=a\cdot b$. $a,b\in R$. a,b为不可逆元.

考虑 由于 $p\in P$, $\Rightarrow a\cdot b\in P$. 而P为素理想. $\Rightarrow$ a不妨 $a\in P$.

设 $a=mp$, $m\in\mathbb{Z}$. $m\neq\pm 1$. $p=mp\cdot b \Rightarrow (mb-1)p=0$.

$\Rightarrow mb-1=0$, 即 $mb=1$. $\Rightarrow m\cdot 1_R\cdot b=1_R$. 即b可逆.

这与p可约矛盾

~~若p可逆. 则 $p^{-1}\cdot p\in R \Rightarrow 1\in R \Rightarrow R\in(p)R \Rightarrow R=\{ap \mid a\in\mathbb{Z}\}$~~

~~设p可约 $\Rightarrow$ 存在不可逆元 $a=mp$, $b=np$, $m,n\in\mathbb{Z}$.~~

~~$p=mp\cdot np \Rightarrow mnp=1$, 即 $mp\cdot n1=1$. $\Rightarrow$ a可逆. 矛盾!~~

2.2.3 反证法，假设有无穷多个理想，包含 r. ~~记为~~

其可列子集为 $\{I_1, I_2, \cdots\}$. $r \in I_j$, I_j 为 R 的理想.

进而 I_j 为主理想. ~~$\Rightarrow r \in I_j$~~ $\Rightarrow$ 设 $I_j = (a_j)$

由 $r \in I_j \Rightarrow \exists b_j \in R$, 使 $a_j b_j = r$

而由 R 是主理想整环，进而是不可分解整环，从而 r 有唯一~~不可约~~分解.

而考虑集合 $\{a_j, b_j\}_{j=1}^{\infty}$，其中每个元均为 r 的因子.

由 r 有唯一不可约分解. 故必存在 a_i, a_j 使 $a_i = u \cdot a_j$ (r 不同因子有限).

其中 u 为可逆元. 而由 I_i 与 I_j 为不同的理想. 矛盾!

(因 $\forall x \in I_i$, $x = ma_i$, 有 $m \in R$, 有 $x = (m \cdot u) \cdot u \cdot a_j = (m \cdot u) a_j \in I_j$

$\forall y \in I_j$, $y = na_j$, $n \in R$ 有 $y = (n \cdot u^{-1}) u a_j = (nau^{-1}) a_i \in I_i$

$\Rightarrow I_i = I_j$)

2.2.5 (1) $\forall a + b\sqrt{5}i \in R$. 若其可逆. ~~若 $b \neq 0$~~

$(a+b\sqrt{5}i)(c+d\sqrt{5}i) = 1$, $a, b, c, d \in \mathbb{Z}$.

$\Rightarrow \begin{cases} ac - 5bd = 1 \\ bc + ad = 0 \end{cases}$, 模5知 a, c 不为0.

$\Rightarrow (ac, bd) = 1$, ~~而 $\Rightarrow (a, bd) \neq 1 \Rightarrow (ac, d) = 1$~~

~~而 $a \mid bc \Rightarrow$~~ $d \mid bc \Rightarrow d \mid b$ ~~设 $b = xd$~~

若 $d = 0 \Rightarrow ac = 1 \Rightarrow a = \pm 1$, 由 $bc = 0 \Rightarrow b = 0$. 即 $a + b\sqrt{5}i = \pm 1$

若 $d \neq 0 \Rightarrow b \neq 0$

$\Rightarrow (ac, bd) = 1$, 而 由 $bc = -ad$

~~设 $b = xd$,~~ $\Rightarrow d \mid bc \Rightarrow d \mid b$

由 $b \mid ad \Rightarrow b \mid d$. 即 $b = \pm d$, $a = \pm c$.

若 $b = d \Rightarrow a = -c \Rightarrow -a^2 - 5b^2 = 1$. 无解.

若 $b = -d$, $\Rightarrow a = c \Rightarrow a^2 + 5b^2 = 1$. 无解.

综上，只有 ± 1 有逆. $\Rightarrow U(R) = \{1, -1\}$.

(2) 注意到，对 R 中元素 $m = a + b\sqrt{5}i$，若其可约，即存在不可逆元

$n = c + di$, $r = e + fi$, 使 $m = n \cdot r$.

而 注意到若 n, r 不可逆，则 $N(r) \neq 1$，即 $N(r) > 1$.

且 $N(m) = N(n) \cdot N(r)$. 即

反证法，假设 $m = a + bi$ 无不可约分解，则 m 必为可约元.

$m = n_1 \cdot r_1$, n_1, r_1

先证：m 必有不可约因子

反证法. 则 m 必为可约元.

设 $m = n_1 \cdot r_1$, n_1, r_1 为可约元.

$n_1 = n_2 \cdot r_2$, $\cdots$

依此类推，得到无穷序列. 但

$a^2 + b^2 = N(m) = \prod_{k=1}^{n} N(r_k) \cdot N(n_n)$

$\geq 2^{n+1}$, n 可趋于 ∞. 矛盾.

故 m 有不可约因子 p_1. $m = p_1 \cdot m_1$, $1 < N(m_1) < N(m)$.

m_1 有不可约因子 p_2, $m_1 = p_2 \cdot m_2$.

依此类推，$m = p_1 \cdots p_s m_s$

由于 $N(m_s)$ 严格递减. 必有一个时刻不能递减

此时 m_s 为不可约元. 否则 $N(m_s)$ 可约.

从而得到 m 的不可约分解.

(3) ~~反证~~. 先证：m 不可约的充要条件为 $N(m)$ 不可约 (在 $\mathbb{Z}$ 中).

只用注意到：若 $m = n \cdot r$. $N(m) = N(n) \cdot N(r)$

反证，若 m 可约 $\Rightarrow N(m)$ 可约. 矛盾.

对于原题：由 $N(3) = 3$, $N(2+\sqrt{5}) = 7$. $N(2-\sqrt{5}) = 7$

均不可约 $\Rightarrow 3$. $2+\sqrt{5}$, $2-\sqrt{5}$ 都是不可约元

2.3.3 反证法.

"⇐". 由于假设$(f(x),g(x))=d(x)$

$d(x)\in K[x]\subset F[x]$.

$\Rightarrow d(x)=1$. 从而互素.

"⇒" 反证法, 假设$(f(x),g(x))=d(x)\neq 1$, $d(x)\in F[x]$.

但$(f(x),g(x))=1$.

由Bezout定理, 存在$u(x),v(x)\in K[x]$.

$$u(x)f(x)+v(x)g(x)=1. \quad (*)$$

而$(*)$在$F[x]$上也成立 $\Rightarrow$ $f(x),g(x)$在$F[x]$上互素.

2.3.4 "⇒"若$f(x)$无一次因子. 则$f(\bar{0})\neq 0$, $f(\bar{1})\neq 0$.

$\Rightarrow a_n\neq 0$, $1+\sum_{i=1}^{n}a_i\neq 0$ $\Rightarrow a_n(1+\sum_{i=1}^{n}a_i)\neq 0$

"⇐" 若$a_n(1+\sum_{i=1}^{n}a_i)\neq 0$.

则 $\Rightarrow a_n\neq 0$, $1+\sum_{i=1}^{n}a_i\neq 0$

若其有一次因式, 则必有根. 即$f(\bar{0})=0$与$f(\bar{1})=0$之一成立.

矛盾. 从而$f(x)$无一次因式.

2.3.4. ~~反设~~ 由 $\deg f'(x) < \deg f(x)$.

而 $f(x)$ 不可约. 若 $(f'(x), f(x)) \neq 1$

$\Rightarrow f(x) \mid f'(x)$. 矛盾. (因 $\mathrm{char}(K)=0 \Rightarrow f'(x) \neq 0$).

2.3.6 证明: (1) ~~$\phi_p(f(x)+g(x))$~~

设 $f(x)=\sum_{i=0}^{\infty} a_i x^i$, $g(x)=\sum_{i=0}^{\infty} b_i x^i$

$$\phi_p(f(x)+g(x)) = \sum_{i=0}^{\infty} \overline{a_i+b_i}\, x^i$$

而 $\overline{a_i+b_i} = \overline{a_i}+\overline{b_i}$. $\Rightarrow \phi_p(f(x)+g(x)) = \phi_p(f(x))+\phi_p(g(x))$

$$\phi_p(f(x)g(x)) = \sum_{i=0}^{\infty} \overline{c_i}\, x^i$$

$$\overline{c_i} = \overline{a_0 b_i + \cdots + a_i b_0} = \overline{a_0}\,\overline{b_i} + \cdots + \overline{a_i}\,\overline{b_0}$$

$$\Rightarrow \sum_{i=0}^{\infty} \overline{c_i}\, x^i = \left(\sum_{i=0}^{\infty} \overline{a_i} x^i\right)\left(\sum_{i=0}^{\infty} \overline{b_i} x^i\right) = \phi_p(f(x))\,\phi_p(g(x))$$

$\phi_p(1_R) = \bar{1}$. 从而 ϕ_p 是环同态.

(2) 反证法, 假设 $f(x)$ 在 $\mathbb{Z}[x]$ 中可约. 则设

$f(x) = g(x)h(x)$. $g(x)$ 与 $h(x)$ 均首一.

而 ① $\bar{f}(x) = \phi_p(f(x)) = \phi_p(g(x))\,\phi_p(h(x))$

$= \bar{g}(x)\,\bar{h}(x)$

由 $\bar{f}(x)$ 不可约. ~~知道~~ 不妨 $\bar{g}(x)$ 为常数. 但 $g(x)$ 为首一多项式.

~~$\bar{g}(x)$ 首项次数仍为 $g(x)$~~ $\Rightarrow \deg(\bar{g}(x)) = \deg(g(x))$. 矛盾!

2.3.8. 设存在 $g(x) \in R[x]$. $f(x)g(x)=0$, $g(x) \neq 0$

设 $f(x) = a_n x^n + \cdots + a_0$. $g(x) = \sum_{k=0}^{m} b_k x^k$. $a_n, b_m \neq 0$

~~用归纳法说明: $a_0, \cdots, a_n$ 均为零因子.~~

~~由 $a_0 b_0 = 0 \Rightarrow a_0$ 零因子.~~

~~下设 ② 对 $t<s$, a_t 是零因子.~~

令 $g(x)$ 是所有满足 $f(x)g(x)=0$ 中次数最小的多项式.

则 $f(x)g(x)=0 \Rightarrow a_n b_m = 0$

$\Rightarrow$

~~由 $a_nb_m=0 \Rightarrow a_n$是零因子~~

$$\Rightarrow a_n f(x)g(x)=0$$

$$\Rightarrow f(x)(a_nb_mx^m+\cdots+a_nb_0)=0$$

$$\Rightarrow \begin{cases} a_nb_m=0 \\ \vdots \\ a_nb_0=0. \end{cases}$$

$$\Rightarrow (a_{n-1}x^{n-1}+\cdots+a_0)(b_mx^m+\cdots+b_0)=0$$

$$\Rightarrow a_{n-1}b_m=0$$

同理 $\Rightarrow \begin{cases} a_{n-1}b_m=0 \\ \vdots \\ a_{n-1}b_0=0. \end{cases}$ 展开.

依此类推:

$$a_0(b_mx^m+\cdots+b_0)=0$$

$$\Rightarrow \begin{cases} a_0b_m=0 \\ \vdots \\ a_0b_0=0 \end{cases}$$

$\Rightarrow b_m(a_nx^n+\cdots+a_0)=0.$ 即证.

2.4.3 "$\Rightarrow$" 设由 a 是 $f(x)\in F[x]$ 的重根.

故在 $f(x)\in K[x]$ 上有 $(x-a)^2 \mid f(x)$.

设 $f(x)=(x-a)^2 p(x)$. $p(x)\in K[x]$.

$f'(x)=2(x-a)p(x)+(x-a)^2 p'(x)$

$\Rightarrow f'(a)=0$.

"$\Leftarrow$" 由 $f(a)=0$. 设 $f(x)=(x-a)q(x)\in K[x]$.

$f'(x)=q(x)+(x-a)q'(x)$

由 $f'(a)=0 \Rightarrow q(a)=0 \Rightarrow (x-a)\mid q(x)$

令 $q(x)=(x-a)p(x)$. $f(x)=(x-a)^2 p(x)\in K[x]$. 即证.

2.4.4 采用归纳法. $n=1$ 时, $f(x)\in F[x]$ 非零.

~~设 $\deg(f)=m$. 则 f 至多 m 个根~~

设 $f(x)=a_m x^m+\cdots+a_0$, $a_m\neq 0$.

由于 F 为域, 故 $f(x)$ 在 F 上至多 m 个根. 而 F 无限域, 知存在 $a\in F$,

$f(a)\neq 0$.

设 $n-1$ 时成立，n 时，$f(x_1,\cdots,x_n)\triangleq g(x_n)\in F[x_1,\cdots,x_{n-1}][x_n]$.

由 F 为域知 $F[x_1,\cdots,x_n]$ 必为整环.

设 $g(x_n)=b_t x_n^t+\cdots+b_0$，$b_i\in F[x_1,\cdots,x_{n-1}]$. $b_t\neq 0$（由归纳假设保证）.

设 $g(c_1)=0$，$c_1\in F\subset F[x_1,\cdots,x_{n-1}]$

$\Rightarrow (x_n-c_1)\mid g(x_n)$，依此类推，可知 $g(x_n)$ 在 F 上至多 t 个根.

$g(x_n)=(x_n-c_1)g_1(x_n)$

从而 $\exists\, a_n$，使 $g(a_n)\neq 0 \Rightarrow \exists\, a_1,\cdots,a_n$，$f(a_1,\cdots,a_n)\neq 0$.

2.4.7 问题的关键在于说明：存在 $f(x)=g(x)\in R[x]$，但

$$\psi_u(f(x))=f(u)\neq g(u)=\psi_u(g(x))$$

由于 R 非交换环，知存在 $a,u\in R$，$a\cdot u\neq u\cdot a$.

考虑 $f(x)=x^2-ax=\cancel{(x-a)x}\ x(x-a)$

$$f(u)=u^2-au\neq u\cdot(u-a)=u^2-ua.$$

扫描全能王 创建

3.3.1 由于 $u_1 \in K[u_1]$, $a \in K[u_1]$

$\Rightarrow -a-u_1 \in K[u_1]$.

而 $(-a-u_1)^2 + a(-a-u_1)+b$

$= a^2+2au_1+u_1^2-a^2-au_1+b$

$= u_1^2+au_1+b=0$

故 $-a-u_1$ 是 $f(x)=0$ 的根

若 $u_1=-a-u_1 \Rightarrow 2u_1=-a$

$\Rightarrow x^2+ax+b=(x-u_1)^2$. 有两个重根.

综上, E 必包含 $f(x)=0$ 的另一根.

3.3.2 由于 $\mathbb{Q}[u_1] \subset \mathbb{R}$. 而 $f(x)=0$ 另两根为复数, 不在 $\mathbb{R}$ 中.

故其余两根不在 $\mathbb{Q}[u_1]$ 中.

3.3.3 设 $f(x)=(x-\alpha_1)\cdots(x-\alpha_n)$

则分裂域 $L=K[\alpha_1,\cdots,\alpha_n]$.

而 $[L:K]=\prod_{k=1}^{n}[K[\alpha_1,\cdots,\alpha_k]:K[\alpha_1,\cdots,\alpha_{k-1}]]$ (*)

而 $f(x)\in K[x]$. $(x-\alpha_1)\cdots(x-\alpha_{k-1})\in K[\alpha_1,\cdots,\alpha_{k-1}]$.

$\Rightarrow \dfrac{f(x)}{(x-\alpha_1)\cdots(x-\alpha_{k-1})}=(x-\alpha_k)\cdots(x-\alpha_n)\in K[\alpha_1,\cdots,\alpha_{k-1}]$.

$\Rightarrow [K[\alpha_1,\cdots,\alpha_k]:K[\alpha_1,\cdots,\alpha_{k-1}]]\le n-k+1$

$\Rightarrow (*)\le \prod_{k=1}^{n}(n-k+1)=n!$ 即证.

3.3.4 ~~$L=K[\alpha]$. $\alpha=\sqrt[5]{2}\cdot(\cos\frac{2\pi}{5}+i\sin\frac{2\pi}{5})$.~~

$L=\mathbb{Q}[\sqrt[5]{2},\ (\cos\frac{2\pi}{5}+i\sin\frac{2\pi}{5})]$.

~~另外~~ 由 ~~$\frac{\sqrt[5]{2}(\cos\frac{2\pi}{5}+i\sin\frac{2\pi}{5})}{\sqrt[5]{2}}$~~ $\cos\frac{2\pi}{5}+i\sin\frac{2\pi}{5}\in L$

$\Rightarrow e^{\frac{4\pi}{5}i},\ e^{\frac{6\pi}{5}i},\ e^{\frac{8\pi}{5}i}\in L$

$\Rightarrow \sqrt[5]{2}e^{\frac{4\pi}{5}i},\ \sqrt[5]{2}e^{\frac{6\pi}{5}i},\ \sqrt[5]{2}e^{\frac{8\pi}{5}i}\in L$. $\Rightarrow L$ 即为 $x^5-2\in\mathbb{Q}[x]$ 分裂域

$[L:\mathbb{Q}]=[L:\mathbb{Q}[\sqrt[5]{2}]]\cdot[\mathbb{Q}[\sqrt[5]{2}]:\mathbb{Q}]$ ~~$\Rightarrow 5\mid[L:\mathbb{Q}]$~~

$\Rightarrow 5\mid[L:\mathbb{Q}]$.

$\cos\frac{2\pi}{5}+i\sin\frac{2\pi}{5}\in L$.

$e^{\frac{2\pi}{5}i},\ e^{\frac{4\pi}{5}i},\ e^{\frac{6\pi}{5}i},\ e^{\frac{8\pi}{5}i}\in L$. (*)

一方面，对于 L 中元素 α，必定可写成 $f(e^{\frac{2\pi}{5}i},\sqrt[5]{2})$. $f(x)\in K[\sqrt[5]{2}][x]$.

故 α 可由 (*) 线性表出.

另一方面，设 $\lambda_1+\lambda_2e^{\frac{2\pi}{5}i}+\lambda_3e^{\frac{4\pi}{5}i}+\lambda_4e^{\frac{6\pi}{5}i}+\lambda_5e^{\frac{8\pi}{5}i}=0$

而 $[L:\mathbb{Q}]=[L:\mathbb{Q}[e^{\frac{2\pi}{5}i}]]\cdot[\mathbb{Q}[e^{\frac{2\pi}{5}i}]:\mathbb{Q}]$

$\Rightarrow 4\mid[L:\mathbb{Q}]\Rightarrow 20\mid[L:\mathbb{Q}]$.

而注意到 ~~$[L:\mathbb{Q}[\sqrt[5]{2}]]$~~

$$\begin{array}{l} e^{\frac{2\pi}{5}i},\ e^{\frac{4\pi}{5}i},\ e^{\frac{6\pi}{5}i},\ e^{\frac{8\pi}{5}i} \\ \sqrt[5]{2}e^{\frac{2\pi}{5}i},\ \cdots \\ \vdots \\ \sqrt[5]{2^4}e^{\frac{2\pi}{5}i},\ \cdots \end{array} \quad (*)$$

共20个数. $\forall\alpha\in L$, $\alpha=f(\sqrt[5]{2},\ e^{\frac{2\pi}{5}i})$, ~~$f(x)\in$~~ $f(x,y)\in\mathbb{Q}[x,y]$.

而 $\sqrt[5]{2}^m\cdot e^{\frac{2\pi}{5}i\cdot n}$ 均可被 (*) 中表出.

$\Rightarrow [L:\mathbb{Q}]\le 20\Rightarrow[L:\mathbb{Q}]=20$.

3.3.7 (1) 关于加法结合律交换律 单位元 逆元平凡.

乘法交换律、结合律 单位元平凡. 分配律平凡.

以上均由商同态给出.

关于逆元、~~由~~ 若 $(x^2-2)\mid f(x)$. 则 $f(u_1)=0$.

若 $(x^2-2)\nmid f(x) \Rightarrow (f(x), x^2-2)=1$

$\Rightarrow \exists u(x), v(x)$. $u(x)f(x)+v(x)(x^2-2)=1$

$\Rightarrow$ ~~$v(u_1)$~~ $u(u_1)f(u_1)=1$. $\Rightarrow f(u_1)$ 逆元即为 $v(u_1)$、故逆元存在

$\Rightarrow K$ 是一个域.

即证: $[\mathbb{Q}[\sqrt{2},\sqrt{3}]:\mathbb{Q}[\sqrt{2}]]=2$.

否则 $\sqrt{3}=q_1+q_2\sqrt{2}$, $q_1,q_2\in\mathbb{Q}$

$\Rightarrow 3=q_1^2+2q_2^2+2q_1q_2\sqrt{2} \Rightarrow q_1q_2=0$. $\Rightarrow q_1=0$ 或 $q_2=0$. 两种情况均矛盾.

(2) 由于 $[L:\mathbb{Q}]=[L:\mathbb{Q}[\sqrt{2}]]\cdot[\mathbb{Q}[\sqrt{2}]:\mathbb{Q}]=2\times2=4$.

3.3.9. 反证法. 设 $\alpha+\beta\in\mathbb{Q}$.

~~设 $f(x)$ 分裂域为 L. $f(x)$ 根 $x_1,\cdots,x_n$, n 为奇数. (由 $f(x)$ 不可约知 x_i 互不相同).~~

~~$L=\mathbb{Q}[x_1,\cdots,x_n]$~~

~~由于 α,β 不同,~~

设 $\alpha+\beta=q\in\mathbb{Q}$.

$f(x)=x^n+\cdots+a_0$. 为 α,β 极小多项式

而 $f(q-x)$ 也有根 α,β,

$f(q-x)=(q-x)^n+\cdots+a_0$. 对比系数 x^n

$\Rightarrow f(x)+f(q-x)=0$

$\Rightarrow a_0=0$, 这与极小多项式矛盾!

若 $\alpha\beta\in\mathbb{Q}$. ~~设 $\alpha\beta=q$~~

由于 $\forall x_i$，存在 $\varphi\in Gal(L/\mathbb{Q})$，使 $\varphi(\alpha)=x_i$.

~~$\varphi(\beta)$~~ 由 $\varphi(\beta)=x_j$. $\varphi(\alpha\beta)\in\mathbb{Q}$

$\Rightarrow x_ix_j\in\mathbb{Q}$

这说明：$\forall x_i, \exists x_j$，使 $x_ix_j\in\mathbb{Q}$

由于有奇数个根，故必有一个 α 对应两个根.

即 $\exists i,j$，$x_i=qx_j$.

由 $f(x_i)=f(qx_j)=f(x_j)=0$

$f(x)=x^n+a_{n-1}x^{n-1}+\cdots+a_0$.

$f(qx_j)=q^nx_j^n+\cdots+a_0$

$=q^n\left(x_j^n+\frac{a_{n-1}}{q}x_j^{n-1}+\cdots+\frac{a_0}{q^n}\right)$

由极小多项式唯一性，~~$q=1$ 或 $=1$~~. $\Rightarrow x_i=x_j$（矛盾）~~或 $x_i+x_j=0$~~.

$q^n=1\Rightarrow q=1$

即证.

扫描全能王 创建

3.4.1 考虑 $\mathbb{Q}[\alpha] \longrightarrow \mathbb{Q}[\alpha]$ 的自同构 φ.

我们说明: $\varphi(\mathbb{Q}) \subseteq \mathbb{Q}$.

由于 φ 是域自同构 $\Rightarrow \varphi(0)=0, \varphi(1)=1$.

$\Rightarrow \varphi(n)=n, \varphi(-n)=-n. \Rightarrow \varphi(\frac{p}{q})=\frac{\varphi(p)}{\varphi(q)}=\frac{p}{q}$.

$\Rightarrow \varphi(q)=q, \forall q \in \mathbb{Q}$.

从而 $\varphi \in Gal(\mathbb{Q}[\alpha]/\mathbb{Q})$ (因 $\mathbb{Q}[\alpha]$ 为 $f(x)$ 分裂域)

即 自同构群 $\subset Gal(\mathbb{Q}[\alpha]/\mathbb{Q}) \subset$ 自 $Aut(\mathbb{Q}[\alpha])$.

而 $\Rightarrow Gal(\mathbb{Q}[\alpha]/\mathbb{Q}) = Aut(\mathbb{Q}[\alpha])$.

而 $Gal(\mathbb{Q}[\alpha]/\mathbb{Q})$ 中元素会将 $f(x)$ 根映到 $f(x)$ 根.

而 $f(x)$ 根为 $\{\alpha, \alpha^2, \cdots, \alpha^{p-1}\}$

故 $Gal(\mathbb{Q}[\alpha]/\mathbb{Q}) = \{\varphi_1, \cdots, \varphi_{p-1}\}$. $\varphi_i(\alpha)=\alpha^i$

注意到 $\varphi_i^2(\alpha) = \varphi_{2i}(\alpha)$

取 p 的原根 g, 则 $Gal(\mathbb{Q}[\alpha]/\mathbb{Q}) = \{\varphi_g\}$, 即为 $p-1$ 阶循环群.

3.4.2 注意到, $\forall \varphi \in Gal(L/K)$. ~~设 $\varphi(\sqrt[3]{2}) = a+b\sqrt[3]{2}+c\sqrt[3]{4}$. $a,b,c \in$ 根 $\mathbb{Q}$~~

$2=\varphi(2)=\varphi(\sqrt[3]{2})^3$. $\Rightarrow \varphi(\sqrt[3]{2})$ 是 $x^3=2$ 的根.

由 $\varphi(\sqrt[3]{2}) \in \mathbb{R} \Rightarrow \varphi(\sqrt[3]{2})=\sqrt[3]{2}$.

故 φ 必为恒等映射, $\Rightarrow Gal(L/K)=\{1\}$.

$\bar{L}=K[\sqrt[3]{2}, \sqrt{-3}]$, 考虑 $f(x)=x^3-2=0$ 根, 为 $\sqrt[3]{2}, \sqrt[3]{2}\frac{-1+\sqrt{3}i}{2}, \sqrt[3]{2}\frac{-1-\sqrt{3}i}{2} = x_1, x_2, x_3$.

故 $f(x)$ 分裂域 $\subset \bar{L}$. 而 $\bar{L} \subset f(x)$ 分裂域.

故 $\bar{L}$ 即为 $f(x)$ 分裂域.

$|Gal(\bar{L}/K)| = [\bar{L}:K]$

$= [\bar{L}:L] \cdot [L:K]$.

由 $\sqrt{-3} \notin L$, 知 $[\bar{L}:L]=2$. $[L:K]=3$

$\Rightarrow |Gal(\bar{L}/K)|=6$.

另一方面, $|Gal(\bar{L}/K)| \leq 3! = 6$. $\Rightarrow$ 取等.

即每个 $\varphi \in Gal(\bar{L}/K)$. 对应 S_3 中一个元: $\begin{pmatrix} x_1 & x_2 & x_3 \\ x_{\pi(1)} & x_{\pi(2)} & x_{\pi(3)} \end{pmatrix}$.

$\Rightarrow Gal(\bar{L}/K) \cong S_3$.

$H = Gal(\bar{L}/K[\sqrt{-3}])$

$\bar{L} = K[\sqrt{-3}][\sqrt[3]{2}]$, $x^3-2=0$ 在 $K[\sqrt{-3}]$ 中不可约

$\Rightarrow |Gal(\bar{L}/K[\sqrt{-3}])| = \deg f(x) = 3$.

注意到, $\varphi(\sqrt[3]{2})$ 可确定 φ.

故 $Gal(\bar{L}/K\sqrt{3}) = \{\varphi_1, \varphi_2, \varphi_3\}$.

$\varphi_i(\sqrt[3]{2}) = x_i$

4.1.1 "$\Leftarrow$", 同态: $\varphi(xy) = y^{-1}x^{-1} = x^{-1}y^{-1} = \varphi(x)\varphi(y)$.

单射: 若 $\varphi(x)=\varphi(y) \Rightarrow x^{-1}=y^{-1} \Rightarrow x=y$

满射: $\forall x \in G$, $\varphi(x^{-1}) = x$.

"$\Rightarrow$" 由于 φ 是同构 $\Rightarrow \varphi(x^{-1}y^{-1}) = \varphi(x^{-1})\varphi(y^{-1})$

$\Rightarrow yx = xy$, 即 G 为 Abel 群.

4.1.2. "$\Rightarrow$" 由 $\forall x$, $xH=Hx$.

故 $\forall h \in H$, ~~xhx^{-1}~~ $ghg^{-1} = gh = h'g$

$\Rightarrow ghg^{-1} = h'gg^{-1} = h' \in H$

$\Rightarrow gHg^{-1} \subset H$.

"$\Leftarrow$" 由 $\forall g$, $gHg^{-1} \subset H$, 知 $gH \subset Hg$.

同样的取 g^{-1}, $\Rightarrow g^{-1}Hg \subset H \Rightarrow H \subset gHg^{-1}$

$\Rightarrow gH = Hg$. 即证.

1. (1) $E=\mathbb{Q}[\sqrt[4]{2},i]=\mathbb{Q}[\sqrt[4]{2},\sqrt[4]{2}i,-\sqrt[4]{2},-\sqrt[4]{2}i]$

则对于 $\varphi\in Gal(E/\mathbb{Q})$ 只用确定 $\varphi(\sqrt[4]{2})$ 与 $\varphi(i)$ 即可确定 φ.

由 $\varphi(i)^2=\varphi(-1)=-1 \Rightarrow \varphi(i)=\pm i$

$\varphi(\sqrt[4]{2})$ 为 $x^4-2=0$ 的根. ，这样确定的 φ 互不相同共8个.

且 $[E:\mathbb{Q}]=[E:\mathbb{Q}[\sqrt[4]{2}]]\cdot[\mathbb{Q}[\sqrt[4]{2}]:\mathbb{Q}]=2\times4=8$.

由 $\mathbb{Q}\subset E$ 是有限扩张，所以是单扩张.

设 $E=\mathbb{Q}[\alpha]$. $\deg\mu_\alpha(x)=[E:\mathbb{Q}]=8$.

$Gal(E/\mathbb{Q})=\{\varphi_1,\cdots,\varphi_8\}$ φ_i 把 α 映到第i个根 α_i

所以 $Gal(E/\mathbb{Q})$ 即为 $\begin{cases}\varphi(i)=\pm i\\ \varphi(\sqrt[4]{2})=\sqrt[4]{2},\sqrt[4]{2}i,\sqrt[4]{2},\sqrt[4]{2}i\end{cases}$ 确定的8个映射.

现在考虑 $Gal(E/\mathbb{Q})$ 的非平凡子群.

记 α: $\alpha(i)=i$, $\alpha(\sqrt[4]{2})=\sqrt[4]{2}i$ β: $\beta(i)=-i$, $\beta(\sqrt[4]{2})=\sqrt[4]{2}$.

则 $Gal(E/\mathbb{Q})=\{id,\alpha,\alpha^2,\alpha^3,\beta,\beta\alpha,\beta\alpha^2,\beta\alpha^3\}$

由Lagrange定理: $|H|\,\big|\,Gal(E/\mathbb{Q})$ $\Rightarrow |H|=2$ 或4

① $|H|=2$ 时, $H=\{id,\gamma\}$. 要求 $\gamma^2=id$.

	id	α	α^2	α^3	β	$\beta\alpha$	$\beta\alpha^2$	$\beta\alpha^3$
$\sqrt[4]{2}$	$\sqrt[4]{2}$	$\sqrt[4]{2}i$	$-\sqrt[4]{2}$	$-\sqrt[4]{2}i$	$\sqrt[4]{2}$	$-\sqrt[4]{2}i$	$-\sqrt[4]{2}$	$\sqrt[4]{2}i$
i	i	i	i	i	$-i$	$-i$	$-i$	

$\Rightarrow \gamma=\alpha^2,\beta,\beta\alpha,\beta\alpha^2,\beta\alpha^3$

对应的中间域为 E^H

$\mathbb{Q}[\sqrt{2},i]$, $\mathbb{Q}[\sqrt[4]{2}]$, $\mathbb{Q}[\sqrt[4]{2}i]$, $\mathbb{Q}[\sqrt[4]{2}(1+i)]$, $\mathbb{Q}[\sqrt[4]{2}(1-i)]$

② $|H|=4$ 时, $H=\{id,\alpha,\alpha^2,\alpha^3\}$ (若包含 α 或 α^3)

$=\{id,\beta,\alpha^2,\beta\alpha^2\}$ (若包含 β 和 α^2)

$=\{id,\beta\alpha,\beta\alpha^3,\alpha^2\}$

1

对应的中间域为 $\mathbb{Q}[i]$, $\mathbb{Q}[\sqrt{2}]$, $\mathbb{Q}[\sqrt{2}i]$.

综上,全部中间域为:

$\mathbb{Q}[\sqrt{2},i]$, $\mathbb{Q}[\sqrt[4]{2}]$, $\mathbb{Q}[\sqrt[4]{2}(1+i)]$, $\mathbb{Q}[\sqrt[4]{2}(1-i)]$, $\mathbb{Q}[\sqrt[4]{2}i]$

$\mathbb{Q}[i]$, $\mathbb{Q}[\sqrt{2}]$, $\mathbb{Q}[\sqrt{2}i]$.

(2) 考虑 $Gal(E/\mathbb{Q})$ 的正规子群 H.

首先,由 $\mathbb{Q}[\sqrt{2},i]$ 是 $(x^2-2)(x^2+1)$ 的分裂域

$\mathbb{Q}[i]$ 是 x^2+1 的分裂域

$\mathbb{Q}[\sqrt{2}]$ 是 x^2-2 的分裂域

$\mathbb{Q}[\sqrt{2}i]$ 是 x^2+2 的分裂域. $\Rightarrow$ 它们是 $\mathbb{Q}$ 的伽罗瓦扩张.

$\mathbb{Q}[\sqrt[4]{2}]$: $\{id,\beta\}$. 由 $\alpha\beta\notin\{id,\beta\}\alpha$ $\Rightarrow$ 不是正规子群.

$\mathbb{Q}[\sqrt[4]{2}(1+i)]$: $\{id,\beta\alpha^3\}$ $\alpha^{-1}\beta\alpha^3\alpha=\alpha^{-1}\beta=\alpha^3\beta\notin\{id,\beta\alpha^3\}$ $\Rightarrow$ 不是正规子群.

$\mathbb{Q}[\sqrt[4]{2}(1-i)]$: $\{id,\beta\alpha\}$. $\alpha\beta\alpha\alpha^{-1}=\alpha\beta\notin\{id,\beta\alpha\}$ $\Rightarrow$ 不是正规子群.

$\mathbb{Q}[\sqrt[4]{2}i]$: $\{id,\beta\alpha^2\}$

$\beta\alpha^3(\sqrt[4]{2})=\sqrt[4]{2}i$

$\alpha\beta\alpha^2(\sqrt[4]{2})=\alpha(-\sqrt[4]{2})=-\sqrt[4]{2}i$ $\Rightarrow \alpha\beta\alpha^2\neq\beta\alpha^3$

且 $\alpha(\sqrt[4]{2})=\sqrt[4]{2}i$ $\Rightarrow \alpha\beta\alpha^2\neq\alpha$ $\Rightarrow \alpha\beta\alpha^2\notin\{id,\beta\alpha^2\}\alpha$

$\Rightarrow$ 不是正规子群.

$\mathbb{Q}[\sqrt[4]{2}(1-i)]$ 与 $\mathbb{Q}[\sqrt[4]{2}(1+i)]$ 彼此共轭

$\mathbb{Q}[\sqrt[4]{2}]$ 与 $\mathbb{Q}[\sqrt[4]{2}i]$ 彼此共轭.

4.4.2. 设F关于 $f(x)$ 分裂域为L. $F\subset L\subset K$.

则 由 $F\subset L$ 是伽罗瓦扩张, 从而 $\exists\,\gamma\in L$, $\beta\in K$, 使

$L=F[\gamma]$, $K=L[\beta]$.

$\forall\varphi\in Gal(K/F)$. 知 $\varphi(\mu_\gamma(x))=\mu_\gamma(\varphi(x))$

$\Rightarrow \varphi(\gamma)$ 为 $\mu_\gamma(x)$ 根 $\Rightarrow \varphi|_L\in Gal(L/F)$.

并且任取 $\psi\in Gal(L/F)$. 只要给出 ψ: $\beta\to\mu_\beta(x)$ 根, 即可变为 $K\to K$ 的同构.

2

设 $Gal(L/F)=\{\varphi_1,\cdots,\varphi_n\}$.

并令等价类: $U_i=\{\varphi\mid\varphi|_L=\varphi_i,\ \varphi\in Gal(K/F)\}$.

$$\begin{array}{ccc}K&\xrightarrow{\varphi}&K\\ \cup&&\cup\\ L&\xrightarrow{\varphi_i}&L\end{array}$$

由定理3.3.2证明可知 $|U_i|=[K:L]\triangleq m$

故有: $g(x)=\prod_{\sigma\in Gal(K/F)}(x-\sigma(\alpha))=\prod_{i=1}^{n}\left(\prod_{\sigma\in U_i}(x-\sigma(\alpha))\right)$

$=\prod_{i=1}^{n}(x-\varphi_i(\alpha))^m$

$=\left(\prod_{i=1}^{n}(x-\varphi_i(\alpha))\right)^m$

$=f^m$

即证. (用到了 $F\subset L$ 是伽罗瓦扩张 $\Rightarrow\{\varphi_1,\cdots,\varphi_n\}=\{\varphi\mid\varphi(\alpha)=\alpha_i,1\le i\le n\}$.

α_i 为n个互不相同根. $n=[L:F]$).

3. 证明: (1) $\mathbb{Q}[\zeta]$ 即为 $\mathbb{Q}$ 关于 $\frac{x^{13}-1}{x-1}$ 的分裂域

且 $x^{13}-1$ 无重根 $((x^{13}-1,13x^{12})=1)$

故 $Gal(\mathbb{Q}[\zeta]/\mathbb{Q})=\{\varphi_i\mid\varphi_i(\zeta)=\zeta^i,1\le i\le12\}$

由13是素数,可知 $\mathbb{F}_{13}^*$ 是循环群

设 $\mathbb{F}_{13}^*=\langle g\rangle$

定义映射 η: $Gal(\mathbb{Q}[\zeta]/\mathbb{Q})\longrightarrow\mathbb{F}_{13}^*$

$\eta(\varphi_i)=g^i$

则明显 η 是单射, 且 $\forall g^k\in\mathbb{F}_{13}^*$, $\exists\,\eta(\varphi_k)=g^k$ $\Rightarrow$ 满射.

$\Rightarrow \eta$ 是双射

且 $\eta(\varphi_i\varphi_j)=\eta(\varphi_{i+j})=g^{i+j}=g^i\cdot g^j=\eta(\varphi_i)\eta(\varphi_j)$ $\Rightarrow \eta$ 是同构.

从而 $Gal(\mathbb{Q}[\zeta]/\mathbb{Q})\cong\mathbb{F}_{13}^*$.

(2) $\mathbb{Q}\subset\mathbb{Q}[\alpha]\subset\mathbb{Q}[\zeta]$

$[\mathbb{Q}[\zeta]:\mathbb{Q}]=12$, 从而只用证明: $[\mathbb{Q}[\alpha]:\mathbb{Q}]=2$.

即 α 的极小多项式次数为2.

3

令 $\beta=\zeta^2+\zeta^5+\zeta^6+\zeta^7+\zeta^8+\zeta^{11}$

则 $\alpha+\beta=-1$

$\alpha\beta=\left(\sum_{i=1}^{6}\zeta^{i^2}\right)\left(\sum_{j=1}^{6}\zeta^{2j^2}\right)$ (注意指数是二次剩余).

$=\sum_{i=1}^{6}\sum_{j=1}^{6}\zeta^{i^2+2j^2}$

同时注意到: $i^2+2j^2\equiv1\pmod{13}$ 与 $i^2+2j^2\equiv k^2\pmod{13}$ 解个数相同 ($\Leftrightarrow (ik^{-1})^2+2(jk^{-1})^2\equiv1\pmod{13}$).

$i^2+2j^2\equiv2\pmod{13}$ 与 $i^2+2j^2\equiv2k^2\pmod{13}$ 解个数相同.

$i^2+2j^2\equiv1\pmod{13}$ 在 $1\le i,j\le6$ 中共3个解:

$i=4,j=5$; $i=5,j=1$; $i=3,j=3$

所以 $i^2+2j^2\equiv2\pmod{13}$ 共3个解.

从而 $\alpha\beta=3\cdot\left(\sum_{i=1}^{12}\zeta^i\right)=-3$

从而 $(x-\alpha)(x-\beta)=x^2+x-3$

$\Rightarrow\alpha$ 极小多项式 $x^2+x-3=0$ 同时 $[\mathbb{Q}[\alpha]:\mathbb{Q}]=2$. 即证.

4. (1) 注意到: $\frac{x^p-1}{x-1}$ 不可约 ($\frac{(x+1)^p-1}{x}=x^{p-1}+C_p^1x^{p-2}+\cdots+C_p^{p-1}$, 由艾森斯坦知不可约)

从而 $\frac{x^p-1}{x-1}$ 为 ζ_p 的极小多项式

$\Rightarrow[\mathbb{Q}[\zeta_p]:\mathbb{Q}]=\deg\mu(x)=p-1$

且 $Gal(\mathbb{Q}[\zeta_p]/\mathbb{Q})=\{\varphi_1,\cdots,\varphi_{p-1}\}=\{\varphi_i\mid\varphi_i(\zeta_p)=\zeta_p^i,1\le i\le p-1\}$.

设 $\mathbb{F}_p^*=\langle g\rangle$. 映射 η: $Gal(\mathbb{Q}[\zeta_p]/\mathbb{Q})\longrightarrow\mathbb{F}_p^*$; $\eta(\varphi_i)=g^i$

η 显然为双射. 且 $\eta(\varphi_i\varphi_j)=\eta(\varphi_{i+j})=g^{i+j}=g^i\cdot g^j=\eta(\varphi_i)\eta(\varphi_j)$

$\Rightarrow Gal(\mathbb{Q}[\zeta_p]/\mathbb{Q})\cong\mathbb{F}_p^*$.

4

(2) $\zeta_{p^2}=e^{\frac{2\pi i}{p^2}}$ 为确定 $Gal(\mathbb{Q}[\zeta_{p^2}]/\mathbb{Q})$. 只用确定 $\varphi(\zeta_{p^2})$

而由 $0=\varphi(\zeta_{p^2}^{p^2}-1)=(\varphi(\zeta_{p^2}))^{p^2}-1$ $\Rightarrow\varphi(\zeta_{p^2})^{p^2}=1$

即 $\forall\varphi\in Gal(\mathbb{Q}[\zeta_{p^2}]/\mathbb{Q})$. φ 会将 ζ_{p^2} 映到它的根.

若 $\varphi(\zeta_{p^2})=\zeta_{p^2}^{pk}$, 则 $\forall\zeta\in\mathbb{Q}[\zeta_{p^2}]$, $\varphi(\zeta)\neq\zeta_{p^2}$ 与同构矛盾.

若 $\varphi(\zeta_{p^2})=\zeta_{p^2}^k$; $p\nmid k$. 则易于验证 φ 是同构.

从而 $\forall\varphi\in Gal(\mathbb{Q}[\zeta_{p^2}]/\mathbb{Q})$. $\varphi(\zeta_{p^2})=\zeta_{p^2}^k$, $p\nmid k$.

故 $[\mathbb{Q}[\zeta_{p^2}]:\mathbb{Q}]=|Gal(\mathbb{Q}[\zeta_{p^2}]/\mathbb{Q})|=p(p-1)$.

(3) $[\mathbb{Q}[\zeta_{p^2}]:\mathbb{Q}[\zeta_p]]=\frac{[\mathbb{Q}[\zeta_{p^2}]:\mathbb{Q}]}{[\mathbb{Q}[\zeta_p]:\mathbb{Q}]}=\frac{p(p-1)}{p-1}=p$

一方面: $\mathbb{Q}[\zeta_{p^2}]\subset\mathbb{Q}[\zeta_p][\zeta_{p^2}]$

另一方面, $\mathbb{Q}[\zeta_p][\zeta_{p^2}]\subset\mathbb{Q}[\zeta_{p^2}]$ $\Rightarrow\mathbb{Q}[\zeta_{p^2}]=\mathbb{Q}[\zeta_p][\zeta_{p^2}]$.

而 ζ_{p^2} 有零化多项式: $x^p-\zeta_p=0$. (*)

其根为 ζ_{p^2}, $\zeta_p\zeta_{p^2}$, $\cdots$, $\zeta_p^{p-1}\zeta_{p^2}$

由扩张次数为p. 故 (*) 为 ζ_{p^2} 极小多项式 $\Rightarrow\mathbb{Q}[\zeta_{p^2}]$ 即是 $\mathbb{Q}[\zeta_p]$ 关于(*)的分裂域.

$\Rightarrow\mathbb{Q}[\zeta_{p^2}]\supset\mathbb{Q}[\zeta_p]$ 是伽罗瓦扩张.

5

5. (1) 注意到 $\mathbb{Q}[\zeta_n]$ 即为 $\mathbb{Q}$ 关于 x^n-1 分裂域

$\Rightarrow\mathbb{Q}[\zeta_n]\supset\mathbb{Q}$ 是伽罗瓦扩张

(2) $(x^{12}-1)=(x^6+1)(x^6-1)$

$=(x^2+1)(x^4-x^2+1)(x^3+1)(x^3-1)$

$=(x^2+1)(x+1)(x-1)(x^4-x^2+1)(x^2-x+1)(x^2+x-1)$

$\zeta_{12}=e^{\frac{\pi i}{6}}=\frac{\sqrt3}{2}+\frac12 i$, 代入验证可知其极小多项式为

$x^4-x^2+1=0$

$e^{\frac{2\pi i}{3}}-e^{\frac{\pi i}{3}}+1=-\frac12+\frac{\sqrt3}{2}i-\frac12-\frac{\sqrt3}{2}i+1=0$.

$x^4-x^2+1=0\Leftrightarrow(x^2-\frac12)^2+\frac34=0$

$\Leftrightarrow x^2-\frac12=\pm\frac{\sqrt3}{2}i$

$\Leftrightarrow x^2=\frac12\pm\frac{\sqrt3}{2}i$

$\Leftrightarrow x=\zeta_{12},\zeta_{12}^7,\zeta_{12}^5,\zeta_{12}^{11}$

所以 $Gal(\mathbb{Q}[\zeta_n]/\mathbb{Q})=\{\varphi_1,\varphi_2,\varphi_3,\varphi_4\}$

$\varphi_1(\zeta_{12})=\zeta_{12}$, $\varphi_2(\zeta_{12})=\zeta_{12}^7$, $\varphi_3(\zeta_{12})=\zeta_{12}^5$, $\varphi_4(\zeta_{12})=\zeta_{12}^{11}$.

(3) 一方面, $\mathbb{Q}[\zeta_n+\zeta_n^{-1}]\subset\mathbb{Q}[\zeta_n]$, $\mathbb{Q}[\zeta_n+\zeta_n^{-1}]\subset\mathbb{R}$

$\Rightarrow\mathbb{Q}[\zeta_n+\zeta_n^{-1}]\subset\mathbb{Q}[\zeta_n]\cap\mathbb{R}$.

另一方面, $\forall r\in\mathbb{Q}[\zeta_n]\cap\mathbb{R}$.

有 $r=f(\zeta_n)$, $f(x)\in\mathbb{Q}[x]$ 为k次多项式. ($k\le n-1$).

$Im(f(\zeta_n))=0$ $\Rightarrow r=Re(f(\zeta_n))$.

设 $f(x)=a_kx^k+\cdots+a_0$.

$f(\zeta_n)=a_k\zeta_n^k+\cdots+a_0$

$r=a_k Re(\zeta_n^k)+\cdots+a_0$.

$=a_k\frac{\zeta_n^k+\zeta_n^{-k}}{2}+\cdots+a_0$

综上, $\mathbb{Q}[\zeta_n]\cap\mathbb{R}=\mathbb{Q}[\zeta_n+\zeta_n^{-1}]$

只用说明: $\frac{\zeta_n^k+\zeta_n^{-k}}{2}\in\mathbb{Q}[\zeta_n+\zeta_n^{-1}]$. 归纳. n=1平凡. 设小于k时成立. k时.

$\frac{\zeta_n^k+\zeta_n^{-k}}{2}=\left(\frac{\zeta_n^{k-1}+\zeta_n^{-k+1}}{2}\right)(\zeta_n+\zeta_n^{-1})-\frac{\zeta_n^{-k+2}+\zeta_n^{k-2}}{2}$. 由归纳假设即知.

6

4.5.1 设Aut(X)表示集合X的自同构群，试证明

(1)若$G\times X\to X,(g,x)\to g\cdot x$是群G在X上的一个作用，$\forall g\in G$.定义映射

$X\xrightarrow{\rho(g)}X, x\to g\cdot x$.则$\rho(g)\in Aut(X)$且映射

$$\rho: G\to Aut(X), g\to \rho(g)$$

是群同态.

(2)若$\rho: G\to Aut(X)$是群同态，则映射

$$G\times X\longrightarrow X, (g,x)\to \rho(g)(x)$$

是一个群作用

(1) 验证：$\rho(g)\in Aut(X)$： $\rho(g)(x)=\rho(g)(y)\Rightarrow g\cdot x=g\cdot y\Rightarrow x=y\Rightarrow$单射

又$|X|=|X|\Rightarrow$双射.

同态：$\rho(g_1)\rho(g_2)x=\rho(g_1)(g_2\cdot x)=g_1(g_2\cdot x)=(g_1g_2)\cdot x=\rho(g_1g_2)(x)$

(2) 群作用：(1) $\rho(e)(x)=x$ (由ρ群同态$\Rightarrow\rho(e)=id$)

(2) $\rho(g_1)(\rho(g_2)\cdot x)=(\rho(g_1)\cdot\rho(g_2))\cdot x=\rho(g_1g_2)\cdot x$

4.5.2 20阶群中共有多少5阶元

注意到20阶群G的5阶子群都是循环群，并且每个5阶元都会对应G的5阶子群

由Sylow定理，Sylow-5子群个数$|P(G)|\equiv 1(mod\ 5)$

且 $|P(G)|\,|\,4\Rightarrow|P(G)|=1\Rightarrow$有4个5阶元.

4.5.3 证明15阶群一定是循环群.

由Sylow定理，15阶群G 5阶子群个数为1，3阶子群个数为1

考虑G在P(G)上的共轭作用 $G\times P(G)\to P(G),(g,H)\to gHg^{-1}$

由$|P(G)|=1\Rightarrow H\in P(G)$是G的正规子群.

考虑商同态 $G\longrightarrow G/H$. $|G/H|=5\Rightarrow$是循环群$\{e,\bar{a},\bar{a}^2,\bar{a}^3,\bar{a}^4\}$

$\Rightarrow G=\{H,aH,\cdots,a^4H\}$，由$aHa^{-1}=H$，可设$aga^{-1}=g^k$，$k=1$

若 $aga^{-1}=g \Rightarrow G$ 是15阶循环群.

若 $aga^{-1}=g^{-1}$，则 (ag) 的阶是10，$10\nmid 15$，矛盾！

$ag \quad a^2 \quad a^3g \quad a^4 \quad g \quad a \quad a^2g \quad a^3 \quad a^4g \quad e$

$\Rightarrow$ 只能是15阶循环群

4.5.4 证明6阶非Abel群一定同构于 S_3

6阶Abel群 G 只有1个 Sylow-3子群 $H=\{e,g,g^2\}$，则 $H\triangleleft G$

则 $\forall a\in G$，$aHa^{-1}=H \Rightarrow aga^{-1}=g^k$. 由不交换，$\exists a\in G$，$ag=g^{-1}a$

考虑 $\{e,g,g^2,a,ag,ag^2\}=G$.

$S_3=\{id,(12),(13),(23),(123)(132)\}$

同态 $G\xrightarrow{\varphi}S_3$，$\varphi(g)=(123)$，$\varphi(a)=(12)$，可知 φ 是同构.

$\Rightarrow G\cong S_3$

4.5.5 证明12阶群共有5个同构类

群 G 的 Sylow-3子群为1个或4个，Sylow-2子群为1个或3个.

(1) Sylow-3子群只有1个 H，则 $H\triangleleft G$. $H=\{e,g,g^2\}$ $\forall a\in G$ 有 $aga^{-1}=g^k$

1° G 交换，即 $ag=ga$，考虑一个4阶子群 I，则 $I\cong\mathbb{Z}_4$ 或 $I\cong\mathbb{Z}_2^2$

若 $I\cong\mathbb{Z}_4$，则取4阶元 a，$G=\{a^ig^j\mid i,j\in\mathbb{Z}\}$ 是循环群. $G\cong\mathbb{Z}_{12}$ ①

$\mathbb{Z}_{12}$

若 $I\cong\mathbb{Z}_2^2$，则设 $I=\{e,a,b,ab\}$ 有：

$G=\{I,gI,g^2I\}\cong\mathbb{Z}_2^2\oplus\mathbb{Z}_3$ ②

$\mathbb{Z}_2^2\oplus\mathbb{Z}_3$

2° G 非交换 即存在 a，$ag=g^{-1}a$. 考虑4阶子群 I，$I\cong\mathbb{Z}_4$ 或 $I\cong\mathbb{Z}_2^2$

必存在 $b\in I$，使 bg 不交换(否则变成1°).

$I\cong\mathbb{Z}_4$ 时，$I=\{e,a,a^2,a^3\}$，必有 a,g 不交换，即 $ag=g^{-1}a$

此时 $G=\{I,gI,g^2I\}=\{a^ig^j\mid ag=g^{-1}a,\ a^4=g^3=e\}$ ③

T

$I\cong\mathbb{Z}_2^2$ 时，$I=\{e,a,b,ab\}$，不妨 $ag=g^{-1}a$，则有 $bg=gb$，$abg=g^{-1}ab$

或 $bg=g^{-1}b$，$abg=gab$，所以两种情形本质相同.

此时 $G_1=\{a^ib^jg^k \mid ab=ba,\ ag=g^{-1}a,\ bg=gb,\ a^2=b^2=g^3=e\}$ D_6 ④

(2) G的Sylow-3子群有4个 即有8个3阶元 a.b.c.d, a^2、b^2、c^2、d^2

还剩4个元组成一个Sylow-2子群 H，则 $H\lhd G$.

$H\cong\mathbb{Z}_4$时，$H=\langle g\rangle$，有 $aga^{-1}=g^k$，若 $aga^{-1}=g^2$，$\Rightarrow ag^2a^{-1}=g^4=e\Rightarrow g^2=e$

矛盾！$\Rightarrow aga^{-1}=g$或$aga^{-1}=g^{-1}$

由 $G=\{H, aH, a^2H\}$，而 ag 的阶是3，

1° $ag=ga$，ag阶是12，矛盾.

2° $ag=g^{-1}a$，$(ag)^3=agagag=a^3g=g\neq e$ 矛盾.

$H\cong\mathbb{Z}_2^2$时，$H=\{e,a,b,ab\}$，一个Sylow-3子群$\langle g\rangle$，则

$gag^{-1}=a$ / $gag^{-1}=b$ / $gag^{-1}=ab$

由 ag 阶是3，故必有后两者.由对称性，可不妨

$gag^{-1}=b$，$gbg^{-1}=ab$，$gabg^{-1}=a$

此时 $G\cong A_4$ ⑤

$\mathbb{Z}_{12}$, $\mathbb{Z}_2^2\oplus\mathbb{Z}_3$, D_6, A_4, T

4.5.6 P.q不同素数，则pq或p^2q一定不是单群

(1) 不妨 $p<q$，则考虑.G的Sylow-q子群 $P(G)$，$|P(G)|\equiv 1\pmod q$.

$|P(G)|\mid p\Rightarrow |P(G)|=1$，则 $H\subseteq P(G)$是G正规子群

(2) 若 $p>q$，则 Sylow-p子群只有1个，从而正规

若 $p<q$，则 Sylow-q子群 $P(G)$，$|P(G)|\equiv 1\pmod q$，$|P(G)|\mid p^2$

$|P(G)|=1$或p^2，$|P(G)|=1$ 同上，$|P(G)|=p^2$时，由于q阶子群互不相交

考虑.Sylow-p子群Σ，Σ中子群一定与P(G)中子群交为单位元.

这说明剩下的p^2-1个元与单位元恰构成G唯一的Sylow-p子群

故为正规子群

4.5.7 证明200阶群一定不是单群

综上，G有12阶子群N，G在N的左陪集上的作用诱导了同态.

$G \xrightarrow{\varphi} S_5$，由G单群 $\Rightarrow \ker\varphi = \{e\} \Rightarrow \varphi$单射，而$S_5$只有一个60阶子群$A_5$，故$G \cong A_5$

S_n的$\frac{n!}{2}$阶群只有A_n

Lemma: G指数为2的子群是正规子群

Lemma: $n>4$时，S_n非平凡正规子群只有A_n

证1: $[G:H]=2$. $G=\{H, aH\}=\{H, Ha\}$

$\forall\ a\in H$. 自然有 $aHa^{-1}=H$

$a\notin H$，则$G=\{H, aH\}=\{H, Ha\} \Rightarrow aH=Ha \Rightarrow$正规.

证2: 首先$A_n \lhd S_n$，设$\{e\}\neq N\lhd S_n$，若$N\leq A_n$，则$N\lhd A_n$，矛盾.

若N包含奇置换，则$N\cap A_n \lhd A_n$且$A_n/(N\cap A_n)\cong NA_n/N=S_n/N$

$\Rightarrow |N\cap A_n| = \frac{|A_n|\cdot|N|}{|S_n|}=\frac{1}{2}|N|$

但$N\cap A_n \lhd A_n \Rightarrow |N\cap A_n|=1$或$\frac{n!}{2} \Rightarrow N\cap A_n=\{e\}$

则$|N|=2$，而$n\geq 5$时S_n无2阶正规子群，所以A_n是S_n唯一正规子群