抽象代数学

我们总结一下已知的域的知识

最小的域 $\mathbb{Q}$ 和 $\mathbb{Z}_p$ (p是素数)

常见的域 $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$, $\mathbb{Q}(\sqrt{2})$, ...

构造新域的方法：(1) 给定一个整区 R，一个极大理想 I，则 R/I 是一个域；(2) 给定一个整区 R，它的分式域 $\mathbb{F}_R$

性质：(1) 只有平凡的理想 $\{0\}$ 和域自身.

(2) 设 F_1, F_2 两个域，$F_1 \xrightarrow{\phi} F_2$ 一个环同态，则只有两种情形：① $\ker\phi=\{0\}$，ϕ 是单射，F_1 看成 F_2 的子域 (通过域同构 $F_1 \simeq \phi(F_1)$) ② $\ker\phi = F_1$，$\phi=0$.

1. 域的生成元(有限生成扩域)

设 $\mathbb{F}$ 是一个域，K 是它的扩域，S 是 K 的一个子集，$\mathbb{F}(S)$ 表示 K 的含 $\mathbb{F}\cup S$ 的最小子域，称为把 S 添加到基本域 $\mathbb{F}$ 上而得到的中间域

令 $\mathbb{F}[S]=\left\{\underset{\text{有限和}}{\sum_{\alpha} f_\alpha s_1^{n_1}\cdots s_m^{n_m}} \,\middle|\, \alpha=(n_1,\cdots,n_m)\ \forall s_i\in S,\ n_i\in\mathbb{Z}_{\geq 0},\ m\geq 0\right\}$

显然 $\mathbb{F}[S]\subseteq\mathbb{F}(S)$ 设 $T=\{uv^{-1} \mid u,v\in\mathbb{F}[S],\ v\neq 0\}$

$T\subseteq\mathbb{F}(S)$，且 T 是包含 $\mathbb{F}$ 和 S 的子域，因此 $T=\mathbb{F}(S)$

即$\mathbb{F}(S)$是由$\mathbb{F}$上S的有理表达式构成

性质：设$\mathbb{F}\subseteq K$，$S_1, S_2\subseteq K$，其中$\mathbb{F}, K$是域，则

$$\mathbb{F}(S_1)(S_2)=\mathbb{F}(S_1\cup S_2)$$

证明：首先$\mathbb{F}, S_1, S_2$均含于$\mathbb{F}(S_1)(S_2)\Rightarrow\mathbb{F}(S_1\cup S_2)\subseteq\mathbb{F}(S_1)(S_2)$（由$\mathbb{F}(S_1\cup S_2)$是包含$\mathbb{F}, S_1\cup S_2$的最小子域），另一方面$\mathbb{F}(S_1)\subseteq\mathbb{F}(S_1\cup S_2)$，且$S_2\subseteq\mathbb{F}(S_1\cup S_2)\Rightarrow\mathbb{F}(S_1)(S_2)\subseteq\mathbb{F}(S_1\cup S_2)$

定义 当S是有限集，$\mathbb{F}(S)$是$\mathbb{F}$的有限生成扩域.

当$S=\{a\}$，$\mathbb{F}(a)$是$\mathbb{F}$的单扩域.

显然 $\mathbb{F}(a_1, a_2, \cdots, a_n)=\mathbb{F}(a_1)(a_2)\cdots(a_n)$

2. 扩域作为向量空间.

观点：当$\mathbb{F}\subseteq K$，K能看作$\mathbb{F}$上的一个向量空间，

加法：K上加法.

数乘：$\forall a\in\mathbb{F}, \alpha\in K$，$a\cdot\alpha\in K$（$K$中乘法）

例如：$\mathbb{R}\subseteq\mathbb{C}$，

$[K:\mathbb{F}]=K$作为$\mathbb{F}$上空间的维数$=\dim_{\mathbb{F}}K$

若$[K:\mathbb{F}]<\infty$ 称K为$\mathbb{F}$的有限(次)扩域，否则，无限次扩域.

命题 设$\mathbb{F}\subseteq\mathbb{E}\subseteq K$是三个域，$[K:\mathbb{F}]$有限$\Leftrightarrow$ $[K:\mathbb{E}]$和$[\mathbb{E}:\mathbb{F}]$均有限，此时$[K:\mathbb{F}]=[K:\mathbb{E}]\cdot[\mathbb{E}:\mathbb{F}]$

证明：若$[K:\mathbb{F}]$有限，即K是$\mathbb{F}$上有限维空间，子空间$\mathbb{E}$也是有限维$\mathbb{F}$-空间，从而$[\mathbb{E}:\mathbb{F}]<\infty$，设$\{v_1,\cdots,v_n\}$是K作$\mathbb{F}$-空间的基，$\mathbb{F}\subseteq\mathbb{E}$，$\{v_1,\cdots,v_n\}$也是K作为$\mathbb{E}$-空间的生成元，$\Rightarrow[K:\mathbb{E}]\leqslant[K:\mathbb{F}]<\infty$

反之，设$[K:\mathbb{E}]=n$，$[\mathbb{E}:\mathbb{F}]=m$，$\{k_1,\cdots,k_n\}$是$\mathbb{E}$-空间K的基，$\{h_1,\cdots,h_m\}$是$\mathbb{F}$-空间$\mathbb{E}$的基，

$\forall x\in K$，$x=\sum_{i=1}^{n}a_ik_i$ $\quad a_i\in\mathbb{E}$，$a_i=\sum_{j=1}^{m}b_{ij}h_j$ $\quad i=1,\cdots,n.$ $\quad b_{ij}\in\mathbb{F}$

$\Rightarrow x=\sum_{i,j}b_{ij}h_jk_i$ 即$\{h_jk_i\}_{\substack{1\le i\le n\\1\le j\le m}}$是$\mathbb{F}$-空间K的生成元，若$x=0$，$\sum_{i,j}b_{ij}h_jk_i=0\Rightarrow\sum_{i=1}^{n}\left(\sum_{j=1}^{m}b_{ij}h_j\right)k_i=0$

$\Rightarrow\sum_{j=1}^{m}b_{ij}h_j=0$ $\quad i=1,\cdots,n$ $\Rightarrow b_{ij}=0$ $\quad i=1,\cdots,n,\ j=1,\cdots,m$

$\Rightarrow\{h_jk_i\}_{\substack{1\le i\le n\\1\le j\le m}}$ 线性无~~也~~关（在$\mathbb{F}$上）

推论 若$\mathbb{F}\subseteq K$是两个域，$[K:\mathbb{F}]=p$（素数），则$\mathbb{F}$与K之间没有中间域.

3. 代数元/超越元

定义 $\mathbb{F}\subseteq K$ 两个域，$\alpha\in K$.

(a) α 是 $\mathbb{F}$ 上代数元 $\Leftrightarrow$ 存在 $f(x)\neq 0\in\mathbb{F}[x]$，$f(\alpha)=0$

$\Leftrightarrow$ 存在 $n\in\mathbb{N}$，$1,\alpha,\alpha^2,\cdots,\alpha^n$ 线性相关（$\mathbb{F}$-相关），此时，最小多项式（次数最小），称为 α 的（在 $\mathbb{F}$ 上）极小多项式.

(b) α 是 $\mathbb{F}$ 上超越元 $\Leftrightarrow$ α 不是 $\mathbb{F}$ 上代数元 $\Leftrightarrow$ $1,\alpha,\alpha^2,\cdots,\alpha^n,\cdots$ 是$\mathbb{F}$上线性无关的

定理. 设 $\mathbb{F}\subseteq K$ 两个域，$\alpha\in K$. α 是 $\mathbb{F}$ 上代数元 $\Leftrightarrow$ $[\mathbb{F}(\alpha):\mathbb{F}]<\infty$，此时 $[\mathbb{F}(\alpha):\mathbb{F}]=$ 极小多项式次数.

证明：设 α 是 $\mathbb{F}$ 上代数元，极小多项式为 $p(x)$. 考虑

$$\begin{aligned}\mathbb{F}[x] &\xrightarrow{\phi} \mathbb{F}(\alpha)\\ x &\longmapsto \alpha\\ f(x) &\longmapsto f(\alpha)\end{aligned}$$

ϕ 是环~~满~~同态

$\ker\phi=(p(x))$

$\Rightarrow$ ϕ 诱导了环同构 $\dfrac{\mathbb{F}[x]}{(p(x))}\xrightarrow{\sim}\mathrm{Im}\,\phi$，$\mathrm{Im}\,\phi$ 是一个域，作为 $\mathbb{F}(\alpha)$ 的子域，包含 $\mathbb{F}$ 和 α，由 $\mathbb{F}(\alpha)$ 定义，$\mathrm{Im}\,\phi=\mathbb{F}(\alpha)$

作为 $\mathbb{F}$ 上向量空间，基为 $\{1,\alpha,\alpha^2,\cdots,\alpha^{n-1}\}$ $n=\deg p(x)$.

例：$f(x)=x^5+2x^2+2x+2\in\mathbb{Z}_3[x]$

$f(x)=(x^2+1)(x^3+2x+2)$ 不可约分解.

令 $K_1=\frac{\mathbb{Z}_3[x]}{(x^2+1)}$，$K_2=\frac{\mathbb{Z}_3[x]}{(x^3+2x+2)}$

$\mathbb{F}=\mathbb{Z}_3\subset K_1$，$\mathbb{Z}_3\subset K_2$　令 $\alpha=x+(x^3+2x+2)$

则 $[\mathbb{Z}_3(\alpha):\mathbb{Z}_3]=3$

推论（域论基本定理，Kronecker，1887）

设 $\mathbb{F}$ 是一个域，$f(x)$ 是 $\mathbb{F}[x]$ 上非常数多项式，则存在 $\mathbb{E}$ 作为 $\mathbb{F}$ 的扩域，$f(x)$ 在 $\mathbb{E}$ 中有一个根.

证明：设 $p(x)\in\mathbb{F}[x]$，$p(x)\mid f(x)$．$\mathbb{E}=\frac{\mathbb{F}[x]}{(p(x))}$ 令

$x+(p(x))=\alpha$，　$f(\alpha)=\bar{0}\in\mathbb{E}$.

定义 设 $\mathbb{E}$ 是 $\mathbb{F}$ 的扩域，若 $\mathbb{E}$ 中每个元均是 $\mathbb{F}$ 上代数元，则 $\mathbb{E}$ 是 $\mathbb{F}$ 的代数扩张（algebraic extension）．否则 $\mathbb{E}$ 是 $\mathbb{F}$ 的超越扩张.

例．$\mathbb{R}$ 不是 $\mathbb{Q}$ 的代数扩张.

定理（steinitz）设 $\mathbb{E}$ 是 $\mathbb{F}$ 上扩域，且 $[\mathbb{E}:\mathbb{F}]<\infty$，则 $\mathbb{E}=\mathbb{F}(u)$ $\Longleftrightarrow$ $\mathbb{E}$ 与 $\mathbb{F}$ 之间只有有限个中间域.

证明："$\Rightarrow$" 设 $\mathbb{E}=\mathbb{F}(u)$，u 在 $\mathbb{F}[x]$ 中极小多项式为 $f(x)$，则 $\mathbb{E}\cong\frac{\mathbb{F}[x]}{(f(x))}$（$f(x)$ 不可约），设 $\mathbb{F}\subseteq K\subseteq\mathbb{E}$，$K$ 是一个中间域，

设u在K上极小多项式为$g(x)\in K[x]$

$f(x)=g(x)q(x)+r(x)$ 代入$x=u$，得$r(u)=0$，

但$\deg r(x)<\deg g(x)$，$r(x)\in K[x]\Rightarrow r(x)=0$，即$g(x)|f(x)$（在$K[x]$中） 设$K'$是由$\mathbb{F}$以及$g(x)$的系数生成的$\mathbb{E}$的子域，$K'\subseteq K$，$u$在$K'$上极小多项式为$g(x)$，$\Rightarrow$

$[\mathbb{E}:K]=\deg g(x)=[\mathbb{E}:K']\Rightarrow[K:K']=1\Rightarrow K=K'$

$\Rightarrow$任一中间域由$\mathbb{F}$和$f(x)$的因式的系数（在$\mathbb{E}[x]$中）生成，只有有限个

反之，设$\mathbb{E}/\mathbb{F}$的中间域有限，若$\mathbb{F}$是有限域$|\mathbb{E}|<\infty$，从而只有$\mathbb{E}^*=\mathbb{E}\setminus\{0\}=\langle u\rangle$循环群，只有有限个子群，从而只有有限个中间域，若$|\mathbb{F}|=\infty$，$\forall u,v\in\mathbb{E}$，$u,v\notin\mathbb{F}$，考虑$\mathbb{F}\subseteq\mathbb{F}(u,v)$，$\mathbb{F}(u+cv)\subseteq\mathbb{F}(u,v)$，$\forall c\in\mathbb{F}$

只有有限个中间域$\Rightarrow\exists d\in\mathbb{F}$，$d\neq c$ $\mathbb{F}(u+cv)=\mathbb{F}(u+dv)=K$，$u+cv,u+dv\in K\Rightarrow(c-d)v\in K\Rightarrow v\in K\Rightarrow u\in K$

即$\mathbb{F}(u,v)=\mathbb{F}(u+cv)$，因为$[\mathbb{E}:\mathbb{F}]<\infty$，至多有限个$u_1,\cdots,u_\ell\notin\mathbb{F}$ $\mathbb{E}=\mathbb{F}(u_1,\cdots,u_\ell)$，由上讨论，

$$\mathbb{F}(u_1,\cdots,u_\ell)=\mathbb{F}(u_1+c_2u_2+\cdots+c_\ell u_\ell),\ \exists c_1,\cdots,c_\ell\in\mathbb{F}.$$

作业 Page 128-129，1，2，3，5，6，7，8.

例 设$\mathbb{F}$是一个域，$\operatorname{char}\mathbb{F}=0$，$a,b$是$\mathbb{F}$上代数元，则存在$c\in\mathbb{F}(a,b)$，使得$\mathbb{F}(a,b)=\mathbb{F}(c)$.

证明：设$p(x)$，$q(x)$分别是a,b的极小多项式，存在K，$\mathbb{F}\subset K$，在K中，$a_1,\cdots,a_m$和$b_1,\cdots,b_n$分别是$p(x)$，$q(x)$的全部不同根，$a_1=a$，$b_1=b$. 因为$\mathbb{F}$无限，$\exists d\in\mathbb{F}$，$a_i\neq a+d(b-b_j)$ $\forall j>1$，令$c=a+db$

考虑多项式$q(x)$和$r(x)=p(c-dx)\in\mathbb{F}(c)[x]$

$q(b)=r(b)=0$，设b在$\mathbb{F}(c)$上极小多项式为$s(x)$，则$s(x)\mid q(x)$，$s(x)\mid r(x)$. 设$\exists b'\neq b$，$s(b')=0$，则

$q(b')=r(b')=0$ 则$b'=b_j$ $\exists j$，$j>1$，$r(b_j)=0\Rightarrow$

$c-db_j$是$p(x)$的根，则$\exists i$，$a_i=c-db_j$，即$a_i=a+d(b-b_j)$

和d的取法矛盾！因此$s(x)=(x-b)^l$ 但$s(x)$不可约，

$s(x)=x-b\Rightarrow b\in\mathbb{F}(c)\Rightarrow a\in\mathbb{F}(c)\Rightarrow\mathbb{F}(a,b)=\mathbb{F}(c)$.