抽象代数 II 讲义-③　　授课时间：2019年9月19日

§1 十域

定义1. 代数系统 $(F,+,\cdot)$ 称为域，如果满足如下条件：

1) $(F,+)$ 为交换群

2) $(F\setminus\{0\},\cdot)$ 为交换群

3) $\forall x,y,z\in F$, $x\cdot(y+z)=x\cdot y+x\cdot z$

素域：设 F 为域，e 为 F 的乘法单位元. 若 e 在加法群 $(F,+)$ 中的阶数有限，即存在最小 $m\in\mathbb{Z}$ 使得 $me=0$，则 m 必为素数

否则，$m=m_1m_2\Rightarrow (m_1m_2)e=(m_1e)(m_2e)=0\Rightarrow m_1e=0$ 或 $m_2e=0$

由 m 选取的极小性，m_1,m_2 不能都为 m 的真因子. 称元 e 的阶数 p 称为域 F 的特征. 若 e 的阶数为无穷，则称 F 的特征为 0 (因为总有 $0\cdot e=0$) 域的特征记为 $\mathrm{Char}(F)$ 或 $\chi(F)$.

定理1. 设 F 为域. 若 $\mathrm{char}(F)=0$，则 F 包含一子域 F_0 同构于 $\mathbb{Q}$

若 $\mathrm{char}(F)=p\neq 0$，则 F 包含一子域 F_0 同构于 $F_p=\mathbb{Z}/p\mathbb{Z}$.

F_0 是 F 中所有包含单位元 e 的子域的交. 即为包含 e 的最小子域，称为 F 的素域. 若 $\mathrm{char}(F)=p\neq 0$，则 $\forall a,b\in F$，都有

$$(a+b)^p=a^p+b^p \quad (\text{"大一新生之梦"}).$$

(注) 整环 R 为域当且仅当 R 只有平凡理想 $\{0\}$ 或 R.

证明：$\Rightarrow$ 若 R 为域. I 为 R 的理想. 若 $I\neq\{0\}$. 则存在 $a\in I$ 且 $a\neq 0$，则 a 在 R 中存在逆元 b 存在且满足 $b\cdot a=e\in I$

所以 $I=R$. $\Leftarrow$ 若 R 只有平凡理想 $\{0\}$ 或 R，则 $\forall a\in R$，若 $a\neq 0$

由 a 生成的理想 $\langle a\rangle=R$，则 $\exists b\in R$，$b\cdot a=e$，所以 a 可逆.

设 $\varphi: F_1 \to F_2$ 为域同态. 由于 $\ker(\varphi) \trianglelefteq F_1$ 为 F_1 的理想, 所有 $\ker(\varphi)=\{0\}$ 或 $\ker(\varphi)=F_1$. 即非平凡域同态必为单射.
$\Rightarrow$ 满域同态必为域同构.

域论中最重要的概念是域扩张: 设 E, F 皆为域. 若 $E \subseteq F$, 则称 F 为 E 的域扩张或简称扩张, E 称为 F 的子域.
域的研究很重要的观点是: F 可以看成 E 的线性空间!
F 作为 E 上的线性空间的维数 $\dim_E(F)$ 称为 F 关于 E 的域扩张次数, 记为 $[F:E]$. 若 $[F:E]<+\infty$, 则称 F 为 E 的有限扩张, 否则为无限扩张.

扩张次数的塔定律公式: 若 $E \subseteq F \subseteq L$, 则有 $[L:E]=[L:F][F:E]$.

设 S 为 F 的一个子集. F 中包含 E 和 S 的一切子域的交, 记作 $E(S)$, 称为 E 上添加 S 得到的子域, 或称为 S 在 E 上生成的子域.
F 称为 E 的单扩张, 若 $\exists \alpha \in F$ 使得 $F=E(\alpha)$.

定义2. 设 F 为 E 的域扩张, 且 $\alpha \in F$. 若 $[E(\alpha):E]$ 有限, 则称 α 为 E 上的代数元, 若 $[E(\alpha):E]=+\infty$, 则 α 为 E 上超越元.

(注) 小性质: 任何 E 的有限扩张皆为代数扩张

定理2. 设 F 为 E 的域扩张且 $\alpha \in F$. 1) 若 α 在 E 上代数的, 则存在不可约多项式 $f \in E[x]$ 使得 $f(\alpha)=0$ 且 $E(\alpha) \cong E[x]/(f)$.
2) 若 α 为超越元, 则 $E(\alpha) \cong E(x)$.

定理3. 设 F 为有限域, 则 F 为 $\mathbb{Z}/p\mathbb{Z} \triangleq \mathbb{F}_p$ 上线性空间且 $|F|=p^k$ $(k \geq 1)$.

定义：设F为域且$f \in F[x]$，K为F的扩域且满足

1) f在K内完全分解成一次因式的乘积，即 $f = c(x-\alpha_1)\cdots(x-\alpha_n)$，$\alpha_i \in K$

2) $K = F(\alpha_1, \cdots, \alpha_n)$

则称K为多项式$f(x)$的分裂域.

定理4. 每个正次数多项式$f \in F[x]$都有一个分裂域且任意两个分裂域为F-同构.

定义：设F为域. 若在$F[x]$中不可约多项式在K内有一根，则在K内可以完全分解成一次因式的乘积，则称K/F为正规扩张

性质：K/F为正规扩张 $\Leftrightarrow$ K为$F[x]$的一个多项式的分裂域

定义：设K/F为有限扩张且E为K的代数扩张. 若E/F为正规扩张且存在中间域L满足$F \subset K \subset L \subset E$且$L/F$正规则$L=E$，我们称$E$为$F$关于$K$的正规闭包.

定义：$F[x]$中不可约多项式$p(x)$称为F上可分多项式，如果$p(x)$在其分裂域内没有单重根. 以F上代数元，若以α为根的多项式为F上的可分多项式，则称α为F上可分的. 代数扩张K/F称为可分扩张若K中每个元素在F上皆为可分的.

例3 $F = \mathbb{F}_p(t)$，$f(x) = x^p - t$在F上不可分.

定理5. 任何有限可分扩张$F = E(\alpha_1, \cdots, \alpha_r)$皆为单扩张（本原元定理）

定理6. 有限扩张E/F为可分正规的 $\Leftrightarrow$ E是F上一个可分多项式的分裂域

迹与范数：

设 F 为特征为零的域. 对于矩阵 $A=(a_{ij})\in F^{n\times n}$，我们有矩阵的迹 (trace) 为：$Tr(A)=a_{11}+a_{22}+\cdots+a_{nn}$，矩阵的范数 (Norm) 为：$N(A)=|A|$. 注意 $\forall A,B\in F^{n\times n}$，满足 $Tr(A+B)=Tr(A)+Tr(B)$ 和 $N(AB)=N(A)\cdot N(B)$.

设 α 为 F 上代数元且其极小多项式为 $P=x^n+\sum_{i=0}^{n-1}p_i x^i\in F[x]$，满足 $P(\alpha)=0$. 则有扩张次数 $[F(\alpha):F]=n$ 并且 $\{1,\alpha,\cdots,\alpha^{n-1}\}$ 为线性空间 $F(\alpha)$ 在 F 上的一组基底. 设 $\lambda_1,\cdots,\lambda_n\in F$ 为 P 的 n 个互不相同的根，则由韦达定理知：$p_{n-1}=-(\lambda_1+\cdots+\lambda_n)$，$p_0=(-1)^n\lambda_1\cdots\lambda_n$

对 $\forall\beta\in F(\alpha)$，定义线性映射 ϕ_β：$F(\alpha)\longrightarrow F(\alpha)$ 满足 $\phi_\beta(\gamma)=\beta\cdot\gamma$，$\forall\gamma\in F(\alpha)$. 称 ϕ_β 为乘 β 对应的乘法映射. 由定义可知 ϕ_β 是线性空间 $F(\alpha)$ 上的线性映射. 取定 $F(\alpha)$ 的一组基底 $\{\alpha_1,\cdots,\alpha_n\}$，则有 $\phi_\beta(\alpha_i)=\sum_{j=1}^{n}m_{ij}\alpha_j$. 令 $M_\beta=(m_{ij})\in F^{n\times n}$，则有

$$\phi_\beta\begin{pmatrix}\alpha_1\\ \alpha_2\\ \vdots\\ \alpha_n\end{pmatrix}=M_\beta\begin{pmatrix}\alpha_1\\ \alpha_2\\ \vdots\\ \alpha_n\end{pmatrix}.$$

我们称矩阵 M_β 为 ϕ_β 关于基底 $\{\alpha_1,\cdots,\alpha_n\}$ 的矩阵表示.

定义：称 $Tr(M_\beta)$ 为 β 关于 F 的迹 (Trace)，记为 $Tr_{F(\alpha)/F}(\beta)$

也称 $\det(M_\beta)$ 为 β 的范数 (Norm).

(注记) 上述迹与范数的定义实际上不依赖于基底选取. 因为对于 $F(\alpha)$ 的另一组基底 $\{\tilde{\alpha}_1,\cdots,\tilde{\alpha}_n\}$，我们有 $\tilde{M}_\beta=B^{-1}M_\beta B$，其中

$$\begin{pmatrix}\alpha_1\\ \alpha_2\\ \vdots\\ \alpha_n\end{pmatrix} = B\begin{pmatrix}\widehat{\alpha}_1\\ \widehat{\alpha}_2\\ \vdots\\ \widehat{\alpha}_n\end{pmatrix}$$

即 $\widehat{M}_\beta$ 与 M_β 相似，因为相似矩阵对应的特征多项式是一样的。

第二个矩阵 A，设其特征多项式为：

$$|\lambda I - A| = \lambda^n + a_{n-1}\lambda^{n-1} + \cdots + a_0 = (\lambda-\lambda_1)\cdots(\lambda-\lambda_n)$$

那么可以得到：

$$\begin{cases} Tr(A) = -a_{n-1} = \lambda_1 + \cdots + \lambda_n \\ \det(A) = (-1)^n a_0 = \lambda_1 \cdots \lambda_n \end{cases}$$

这样可以相应特征多项式一样的矩阵所对应的迹也是一样的。

例子 $F=\mathbb{Q}$，$\alpha = \sqrt{-5}$ $E = \mathbb{Q}(\sqrt{-5})$.

$\beta = 1+\sqrt{-5}$ 取 $\mathbb{Q}(\alpha)$ 的一组基 $\{1, \alpha\}$

$$\beta \cdot 1 = 1+\sqrt{-5} = 1+\alpha = (1,1)\begin{pmatrix}1\\ \alpha\end{pmatrix}$$

$$\beta\cdot\alpha = (1+\sqrt{-5})\sqrt{-5} = -5+\sqrt{-5} = (-5,1)\begin{pmatrix}1\\ \alpha\end{pmatrix}$$

$$M_\beta = \begin{pmatrix}1 & 1\\ -5 & 1\end{pmatrix}$$

则 $Tr_{\mathbb{Q}(\sqrt{-5})/\mathbb{Q}}(\beta) = 2$

且 Norm of β 为：$N_{\mathbb{Q}(\sqrt{-5})/\mathbb{Q}}(\beta) = |M_\beta| = 6$