第 8 章　域

在深入探索了环的丰富结构与性质之后，本章迈向更为精致且强大的一类特殊的环——域，并聚焦于域的几个核心主题.

首先，探讨分式域，它展示了如何通过扩展整环的元素集合来构造域的过程. 其次，从域元素所构成集合的包含关系，刻画出素域和扩域关系，从而更全面地把握域的结构与性质. 再次，着重介绍域论中一个极其重要的定理——Galois 基本定理. 它是解决多项式方程的根式可解性问题最核心的工具，同时也揭示了域扩张与群论之间的深刻联系. 最后，特别值得一提的是有限域，因其元素个数有限而具有独特的魅力. 在有限域中，所有元素都满足特定的代数关系，这些关系不仅提供了一种研究有限代数结构的理想模型，还使其在编码理论、密码学等领域有着广泛的应用.

通过本章的学习，我们将深入剖析域的结构与性质，揭示其背后的数学奥秘.

本章的知识要点：

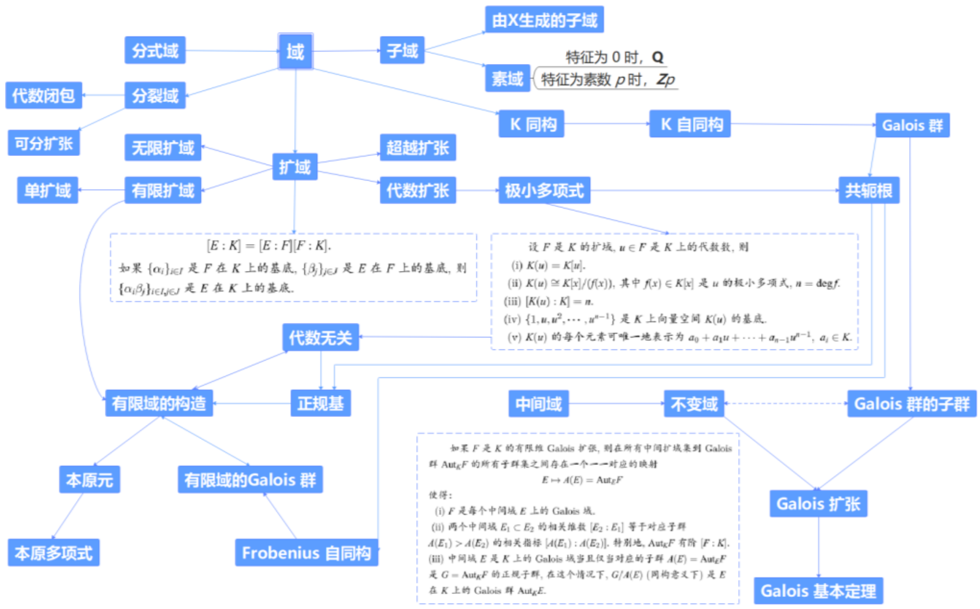

图 8-1 域知识点图谱

8.1 分式域

从整数集 Z 构造出有理数集 Q 是经典和重要的方法. 运用该方法可以从整环构造出对应的分式域.

为此，我们首先介绍等价关系 R.

定理 8.1.1 设 A 是一个整环. 令 $E=A\times A^*$，在 E 上定义关系 $R:(a,b)R(c,d)$，如果 $ad=bc$，则 R 是 E 上的**等价关系**，即有

(i) 自反性：对任意$(a,b)\in E$，有$(a,b)R(a,b)$.

(ii) 对称性：如果$(c,d)R(a,b)$，则$(c,d)R(a,b)$.

(iii) 传递性：如果$(c,d)R(a,b)$和$(c,d)R(e,f)$，则$(a,b)R(e,f)$.

记$\frac{a}{b}=C_{(a,b)}=\{(e,f)\mid E,(a,b)R(e,f)\}$为$(a,b)$的等价类.

我们在商集E/R上定义加法和乘法如下：

$$\frac{a}{b}+\frac{c}{d}=\frac{ad+bc}{bd}$$

$$\frac{a}{b}\bullet\frac{c}{d}=\frac{ac}{bd}$$

则E/R关于加法构成一个交换群，零元为$\frac{0}{b},\frac{a}{b}$的负元为$\frac{-a}{b}$.

$(E/R)^*=E/R\setminus\left\{\frac{0}{b}\right\}$关于乘法构成一个交换群，单位元为$\frac{b}{b},\frac{a}{b}$的逆元$\frac{a}{b}$.

因此，E/R构成一个域，叫做A的**分式域**.

定理 8.1.2 交换环A有分式域的充要条件是R为整环.

例 8.1.1 取A=Z，则Z是一个整环，从而有分式域，叫做Z的**有理数域**，记作Q.

例 8.1.2 取$A=Z/pZ$，其中p为素数，则A是一个整环，从而有分式域，叫做Z/pZ的p**-元域**，记为F_p或$GF(p)$.

例 8.1.3 设K是一个域，则$A=K[X]$是一个整环，从而有分式域，叫做$K[X]$的**多项式分式域**，记为$K[X]$，即

$$K[X]=\left\{\frac{f(X)}{g(X)}\mid f(X),g(X)\in K[X],g(X)\neq 0\right\}.$$

8.2 素域与扩域

上一章已经介绍了一般的域和子域的概念，本节首先考虑“最小”的子域.

定义 8.2.1 如果一个域不含真子域，则称其为素域.

例 8.2.1 有理数域 $\mathbb{Q}$ 是素域. $F_p=\mathbb{Z}/p\mathbb{Z}$ 是素域.

定理 8.2.1 设 F 是一个域. 如果 F 的特征为 0，则 F 有一个与 $\mathbb{Q}$ 同构的素域. 如果 F 的特征为 p，则 F 有一个与 F_p 同构的素域.

证 略.

接下来, 从集合的包含关系角度讨论域的性质.

设 F 是一个域, $X\subset F$, 则包含 X 的所有子域的交集仍是包含 X 的子域, 叫作**由 X 生成的子域**. 如果 F 是 K 的扩域及 $X\subset F$, 则由 $K\subset X$ 生成的子域叫作 **X 在 K 上生成的子域**, 记作 $K(X)$. 如果 $X=\{u_1, \cdots, u_n\}$, 则 F 的子域 $K(X)$记作 $K(u_1, \cdots, u_n)$.

定义 8.2.2 设 F 是一个域. 如果 K 是 F 的子域, 则称 F 是 K 的**扩域**. 如果 $X=\{u\}$, 则称 $K(u)$为 K 的**单扩域**.

例 8.2.2 有理数域 $\mathbb{Q}$ 是实数域 $\mathbb{R}$ 和复数域 $\mathbb{C}$ 的子域, 复数域 $\mathbb{C}$ 是 实数域 $\mathbb{R}$ 的扩域, 实数域 $\mathbb{R}$ 是有理数域 $\mathbb{Q}$ 的扩域.

例 8.2.3 $F_{2^8}=F_2[x]/(x^8+x^4+x^3+x+1)$是 F_2 的扩域.

8.2.1 有限扩域

本小节，从线性空间角度讨论域的性质.

如果 F 是 K 的扩域, 则 $1_F=1_K$. 而且, F 可作为 K 上的线性空间. 事实上, 对任意 α，$\beta\in F, k\in K$, 有 $\alpha+\beta\in F, k\cdot\alpha\in F$.

用 $[F:K]$ 表示 F 在 K 上线性空间的维数. 如果 $[F:K]$ 是有限或无限的, 则称 F 是 K 的**有限扩域**或**无限扩域**.

定理 8.2.2 设 E 是 F 的扩域, F 是 K 的扩域, 则 $[E:K]=[E:F][F:K]$. 而且, 如果$\{\alpha_i\}_{i\in I}$是 F 在 K 上的基底, $\{\beta_j\}_{j\in J}$是 E 在 F 上的基底, 则$\{\alpha_i\beta_j\}_{i\in I, j\in J}$是 E 在 K 上的基底.

证 首先, 证明$\{\alpha_i\beta_j\}_{i\in I, j\in J}$是 E 在 K 上的生成元.

事实上, 对任意 $c\in E$, 根据$\{\beta_j\}_{j\in J}$是 E 在 F 上的基底, 存在 $b_j\in F, j\in J$ 使得

$$c=\sum_{j\in J} b_j\beta_j.$$

再根据$\{\alpha_i\}_{i\in I}$是 F 在 K 上的基底, 存在 $a_{ij}\in K, i\in I$ 使得

$$b_j=\sum_{i\in I} a_{ij}\alpha_i.$$

从而,

$$c=\sum_{j\in J}\left(\sum_{i\in I} a_{ij}\alpha_i\right)\beta_j=\sum_{i\in I,j\in J} a_{ij}\alpha_i\beta_j.$$

其次, 证明$\{\alpha_i\beta_j\}_{i\in I,j\in J}$在 K 上线性无关.

事实上, 若存在 $a_{ij}\in K, i\in I, j\in J$ 使得

$$\sum_{i\in I,j\in J} a_{ij}\alpha_i\beta_j=0.$$

即

$$\sum_{j\in J}\left(\sum_{i\in I} a_{ij}\alpha_i\right)\beta_j=0.$$

因为$\sum_{i\in I} a_{ij}\alpha_i\in F$, 且$\{\beta_j\}_{j\in J}$是 E 在 F 上的基底, 所以$\sum_{i\in I} a_{ij}\alpha_i=0, j\in J$. 又因为 $a_{ij}\in K$ 以及 $\{\alpha_i\}_{i\in I}$是 F 在 K 上的基底, 得到 $a_{ij}=0, i\in I, j\in J$.

进一步, 有$[E:K]=[E:F][F:K]$.

推论 8.2.1 设 E 是 K 的有限扩域的充要条件是 E 是 F 的有限扩域, 且 F 是 K 的有限扩域.

例 8.2.4 数域 $\mathbb{Q}(\sqrt{2})$是 $\mathbb{Q}$ 的有限扩域, 且$[\mathbb{Q}(\sqrt{2}):\mathbb{Q}]=2$.

8.2.2 代数扩域

本小节从多项式的根的角度讨论扩域.

定义 8.2.3 设 R 是一个整环, K 是包含 R 的一个域, F 是 K 的一个扩域.

(1) 对于 F 的元素 u, 如果存在一个非零多项式 $f\in R[x]$使得 $f(u)=0$, 则称 u 为整环 R 上的**代数数**.

(2) 对于 F 的元素 u, 如果存在一个非零的首一多项式 $f\in R[x]$使得 $f(u)=0$, 则称 u 为整环 R 上的**代数整数**.

(3) 对于 F 的元素 u, 如果不存在任何非零多项式 $f\in R[x]$使得 $f(u)=0$, 则称 u 为整环 R 上的**超越数**.

进一步, 当 K 是整环 R 的分式域时, 人们有时就称为 K 上的代数数和超越数. 这时, 与代数相关的多项式就可以要求其是首一多项式. 如果 F 的每个元素都是 K 上的代数数, 则 F 称为 K 的**代数扩张**. 如果 F 中至少有一个元素是 K 上的超越数, 则 F 称为 K 的**超越扩张**.

注：对于 $u\in K$, 有 u 是一次多项式 $f(x)=x-u\in K[x]$的根, 故 u 是 K 上的代数数.

例 8.2.5 (1) $u=\sqrt{2}$是整数环 $\mathbb{Z}$ 上的代数整数, 因为有首一多项式 $f(x)=(x-\sqrt{2})(x+\sqrt{2})=x^2-2\in\mathbb{Z}[x]$使得 $f(u)=0$. 故 $\mathbb{Q}(\sqrt{2})$是代数扩张.

(2) $u=\frac{1+\sqrt{5}}{2}$是整数环 $\mathbb{Z}$ 上的代数整数，因为有首一多项式 $f(x)=(x-\frac{1+\sqrt{5}}{2})(x-\frac{1-\sqrt{5}}{2})=x^2-x-1\in\mathbb{Z}[x]$使得 $f(u)=0$. 故 $\mathbb{Q}(\frac{1+\sqrt{5}}{2})$是代数扩张.

例 8.2.6 (1) 圆周率$\pi=3.14159265\cdots$是有理数域 $\mathbb{Q}$ 上的超越数.

(2) 自然对数底 $e=2.71828182\cdots$是有理数域 $\mathbb{Q}$ 上的超越数.

(3) $2^{\sqrt{2}}$是有理数域 $\mathbb{Q}$ 上的超越数.

(4) $\sum_{n=1}^{\infty}\frac{1}{2^{n!}}$是有理数域 $\mathbb{Q}$ 上的超越数.

下面建立多项式环和多项式分式域与域扩张之间的关系.

设 F 是 K 的扩域, $u\in F$, 则可以构造 $K[x]$到 $K[u]$的一个同态.

$$\varphi: K[x]\to K[u]$$
$$h(x)\mapsto h(u)$$

且上述环同态可拓展为 $K(x)$到 $K(u)$的一个域同态.

$$\varphi: K(x)\to K(u)$$
$$\frac{h(x)}{g(x)}\mapsto\frac{h(u)}{g(u)}$$

根据环同态基本定理，有同构

$$\bar{\varphi}: K[x]/\ker(\varphi)\to K(u),$$

其中 $\ker(\varphi)=\{h(x)\in K[x]\mid h(u)=0\}$.

分两种情况讨论：

(1) u 是 K 上超越数. $\ker(\varphi)=\{0\}$. 因此, φ是环同构，也是域同构，即有：

定理 8.2.4 如果 F 是 K 的扩域, $u\in F$ 是 K 上的超越数，则存在一个在 K 上为恒等映射的域同构 $K(u)\cong K(x)$.

(2) u 是 K 上代数数. $\ker(\varphi)\neq\{0\}$是素理想. 而 $K[x]$是主理想环，故存在次数最小的首一不可约多项式 $f(x)$使得 $\ker(\varphi)=(f(x))$，即有：

引理 8.2.1 设 F 是域 K 的扩域, $u\in F$ 是 K 上的代数数，则存在一个在 K 上的首一不可约多项式 $f(x)$使得 $f(u)=0$.

由此，可以建立代数数与多项式的对应关系.

定义 8.2.4 设 F 是域 K 的扩域, $u\in F$ 是 K 上的代数数. 满足 $f(u)=0$ 的首一不可约多项式 $f(x)$称为 u 的**极小多项式**或**定义多项式**. 将此不可约多项式 $f(x)$的次数 $\deg f$ 定义为 u 在 K 上的**次数**，并将此不可约多项式 $f(x)$的其他根称作 u 的**共轭根**.

例 8.2.7 $\sqrt{2}$在 Q 上的极小多项式是 $f(x)=x^2-2$, 次数为 2, 共轭根为$-\sqrt{2}$.

下面考虑由代数数生成的域.

定理 8.2.5 设 F 是域 K 的扩域, $u\in F$ 是 K 上的代数数, 则

(*i*) $K(u)=K[u]$.

(*ii*) $K(u)\cong K[x]/(f(x))$, 其中 $f(x)\in K[x]$是 u 的极小多项式, $n=\deg f$.

(*iii*) $[K(u):K]=n$.

(*iv*) $\{1, u, u^2, \cdots, u^{n-1}\}$是 K 上向量空间 $K(u)$的基底.

(*v*) $K(u)$的每个元素可唯一地表示为 $a_0+ a_1u+\cdots+ a_{n-1}u^{n-1}$, $a_i\in K$.

证 设 u 的极小多项式为 $f(x)$, $n=\deg f$.

(*i*) 对任意$\frac{h(u)}{g(x)}\in K(u)$, $g(u)\neq 0$, 有多项式 $g(x)$与 $f(x)$互素. 根据多项式广义欧几里得除法, 存在 $s(x), t(x)\in K[x]$使得 $s(x)\cdot g(x)+t(x)\cdot f(x)=1$. 从而, $s(u)g(u)=1$. 因此,

$$\frac{h(u)}{g(x)}=\frac{s(u)\cdot h(u)}{s(u)\cdot g(x)}=s(u)\cdot h(u)\in K[u],$$

$K(u)\subset K[u]$. 这说明, $K(u)=K[u]$.

(*ii*) 考虑 $K[x]$到 $K[u]$的映射φ: $g(x)\mapsto g(u)$.

易知, φ是满的环同态. 根据环同态基本定理, 有 $K[x]/\ker(\varphi)\cong K(u)$, 而 $\ker(\varphi)=(f(x))$, 即得.

(*iv*) 对任意 $g(x)\in K[x]$, 根据多项式欧几里得除法, 存在 $q(x), r(x)\in K[x]$使得

$$g(x)=q(x)\cdot f(x)+r(x),\ 0\leq \deg r<\deg f.$$

因此, $g(u)=r(u)$. 这说明, $\{1, u, u^2, \cdots, u^{n-1}\}$是 $K(u)$的生成元.

又因为 $f(x)$是使得 $f(x)=0$ 的次数最小的多项式, 所以$\{1, u, u^2, \cdots, u^{n-1}\}$在 K 上线性无关. 因此, $\{1, u, u^2, \cdots, u^{n-1}\}$是 K 上向量空间 $K(u)$的基底.

(*iii*) 和 (*v*) 由 (*iv*) 可得.

例 8.2.8 多项式 x^2-x-1 是 Q 上的不可约多项式.

例 8.2.9 多项式 x^3-3x-1 是 Q 上的不可约多项式.

例 8.2.10 F_2 上的 4 次以下的不可约多项式与可约多项式是：

(1) 一次不可约多项式： $x,\ \ x+1$；

(2) 二次不可约多项式： x^2+x+1；

(3) 二次可约多项式： x^2， $x^2+1=\left(x+1\right)^2$， $x^2+x=x\left(x+1\right)$；

(4) 三次不可约多项式：$x^3+x+1,\quad x^3+x^2+1$；

(5) 三次可约多项式为：$x^3,\quad x^3+x,\quad x^3+x^2,\quad x^3+x^2+x,$
$x^3+x^2+x+1=(x+1)(x^2+1),$.
$x^3+1=(x+1)(x^2+x+1)$

下面从线性空间的角度讨论域中元素间的关系.

定义 8.2.5 设F是域K的扩域, $a_1,a_2,\cdots,a_n$是F的n个元素. 如果存在一个非零多项式$f\in K[x_1,\cdots,x_n]$使得$f(a_1,a_2,\cdots,a_n)=0$，则称$a_1,a_2,\cdots,a_n$在K上**代数相关**. 否则，$a_1,a_2,\cdots,a_n$叫作**代数无关**.

注：所谓$a_1,a_2,\cdots,a_n$代数无关，即如果有多项式$f\in K[x_1,\cdots,x_n]$使得$f(a_1,a_2,\cdots,a_n)=0$，则$f=0$.

例 8.2.11 $\pi=3.14\cdots$和自然对数底$e=2.718\cdots$ 在 $\mathbb{Q}$上代数无关.

定理 8.2.6 设F是域K的有限生成扩域，则F是K的代数扩张，或者存在代数无关元$\theta_1,\cdots,\theta_t$使得F是$K(\theta_1,\cdots,\theta_t)$的代数扩张.

证 设F在域K的有限生成元为$S=a_1,a_2,\cdots,a_n$. 若S中的每个元素在K上代数相关，则F是K的代数扩张. 否则，S中有元素在K上代数无关，设为θ_1. 用$K(\theta_1)$代替K作讨论. 如此下去，即得.

下面从域的同构扩充到扩域的同构.

设σ: $K\to L$ 是域同构. 对于 $f(x)=a_nx^n+a_{n-1}x^{n-1}+\cdots+a_1x+a_0\in K[x]$, 记

$$\sigma(f)(x)=\sigma(a_n)x^n+\sigma(a_{n-1})x^{n-1}+\cdots+\sigma(a_1)\,x+\sigma(a_0),$$

易知f和$\sigma(f)$同为可约或不可约多项式.

定理 8.2.7 设σ: $K\to L$ 是域同构. u 是 K 的某个扩域中的元素, v 是 L 的某个扩域中的元素, 假设

(*i*) u 是 K 上的超越数, v 是 L 上的超越数;

或者,

(*ii*) u 是 K 上的代数数, u 的极小多项式为$f(x)\in K[x]$, v 是多项式$\sigma(f)\in L[x]$的根,

则σ可扩充为扩域 $K(u)$到 $L(v)$的同构φ, 并将 u 映射到 $v=\varphi(u)$.

证 考虑 $K(u)$到 $L(v)$的映射

$$\varphi\colon \frac{h(u)}{g(u)} \mapsto \frac{\sigma(h)(v)}{\sigma(g)(v)}.$$

这个φ是 $K(u)$到 $L(v)$的同构，且满足$\varphi|_K=\sigma$，$\varphi(u)=v$. 事实上，只需说明φ是一对一的.

若$\sigma(h)(v)=0$，根据假设条件，

在情形 (i) 下，有 $\sigma(h)=0$，从而 $h=0$.

在情形 (ii) 下，有$\sigma(f)|\sigma(h)$，从而$f|h$，即有 $h(u)=0$.

结论成立.

定理 8.2.8 设 E 和 F 都是域 K 的扩域，$u\in E$，$v\in F$. 则 u 和 v 是同一不可约多项式 $f(x)\in K[x]$的根当且仅当存在一个 K 的同构 $K(u)\cong K(v)$，其将 u 映射到 v.

证 取$\sigma=\mathrm{id}_K$为 K 上的恒等变换，σ是 K 到自身的同构，且$\sigma(f)=f$. 应用定理 8.2.7 即得.

定理 8.2.9 设 K 是一个域，$f\in K[x]$是次数为 n 的多项式，则存在 K 的单扩域 $F=K(u)$使得

(i) $u\in F$ 是 f 的根.

(ii) $[K(u):K]\leq n$，等式成立当且仅当 f 是 $K[x]$中的不可约多项式.

证 不妨设 $f\in K[x]$是不可约多项式，则商环 $K[x]/(f)$是一个域.

考虑 $K[x]$到 $K[x]/(f)$的自然同态

$$s\colon g(x)\mapsto g(x) \pmod{f(x)}.$$

易知，$s|_K$ 是 K 到 $s(K)$的同构，且 F 是 $s(K)$的扩域.

对于 $x\in K[x]$，令 $u=s(x)$，有

$$F=K(u)\text{及 } f(u)=0.$$

则 (i) 成立.

从定理 8.2.5 即可推出 (ii).

推论 8.2.2 设 K 是一个域，$f\in K[x]$是次数为 n 的不可约多项式. 设α是 $f(x)$的根，则α在 K 上生成的域为 $F=K(\alpha)$，且 $[K(\alpha): K]=n$.

定义 8.2.6 设K是一个域，$f\in K[x]$是次数为$n\geq 1$的多项式. 对于K的一个扩域F，如果f在$F[x]$中可完全分解成一次因式的乘积，即

$$f(x)=\alpha(x-u_1)(x-u_2)\cdots(x-u_n),$$

且$F=K(u_1,\cdots,u_n)$,其中$\alpha\in K$，$u_1,\cdots,u_n$是f在F中的根，则称F为**多项式f在K上的分裂域**或**根域**.

注：设S是$K[x]$中一些次数≥ 1的多项式组成的集合. 对于K的一个扩域F, 如果S中的每一个多项式f在$F[x]$中可完全分解成一次因式的乘积，且F由S中的所有多项式的根在K上生成，则称 F 为**多项式集合S在K上的分裂域**.

例 8.2.12 $x^p - x$在F_p的分裂域是F_p.

证：在F_p上有$x^p - x = x(x-1)\cdots\big(x-(p-1)\big)$.

例 8.2.13 设E是q元有限域，则$x^q - x$在E的素域F_p的分裂域是E.

定理 8.2.10 设K是一个域,$f \in K[x]$的次数为$n \geq 1$, 则存在f的一个分裂域F且$[F:K] \leq n!$.

证 对 $n = degf$ 作数学归纳法.

如果$n = 1$, 则f在 K 上可完全分解，故$F = K$是分裂域.

如果$n > 1$, f在K上不能完全分解，设$g \in K[x]$是f的次数大于 1 的不可约因式，则存在K的一个单扩张$K(u)$使得u是g的根，且$[K(u):K] = \deg g > 1$. 因此，在$K(u)$[x]中有分解式$f(x) = (x-u)h(x)$, 其中 $\deg h = n-1$. 由归纳假设，存在h在$K(u)$上的次数$\leq (n-1)!$的分裂域F. 易知,F在K上的次数

$$[F:K] = [F:K(u)][K(u):K] \leq (n-1)!\,n = n!.$$

下面讨论不能进行代数扩张的域 (“最大”的域)，也就是在该域上多项式总有解的域.

定理 8.2.11 在域F上的以下条件等价：

(*i*) 每个非常数多项式$f \in F[x]$ 在F中有根

(*ii*) 每个非常数多项式$f \in F[x]$在F中可完全分解.

(*iii*) 每个不可约多项式$f \in F[x]$的次数为 1.

(*iv*) 除了F以外，不存在F的代数扩张.

证 (*i*)⇒(*ii*). 对f的次数 $\deg f = n$作数学归纳法.

$n = 1$时, $f(x)$为一次多项式，结论成立.

假设结论对次数$\leq n-1$ 的多项式成立. 对于非零$n \geq 2$次多项式$f(x)$, 由(i)知, $f(x)$在F中有根$x=a$. 根据多项式欧几里德除法可得到$x-a \mid f(x)$, 或$f\ (x)=f_1(x)(x-a)$, 其中$degf_1=n-1$. 根据归纳假设, $f_1(x)$在F中可完全分解，故$f \in F[x]$在F中可完全分解.

(ii) ⇒ (iii). 结论显然成立.

(iii) ⇒(iv). 设E是F的一个代数扩张，则对于任意$u \in E$,因为u是F上的代数元，由定理 8.2.5, 存在不可约多项式$f(x) \in F[x]$使得$f(u)=0$. 由(iii)知, $f(x)=a_1x+a_2, a_1, a_2 \in F$. 从而，$u=-(a_1^{-1})a_2 \in F$. 这说明, $E \subset F$, 故$E=F$, 结论成立.

(iv)⇒(i). 设$f(x)$是F上的非常数多项式，由定理 8.2.5, 存在$f(x)$的根u 使 $F(u)$ 为 F 的代数扩张. 由(iv)知, $F(u)=F$. 故, $u \in F$, 结论成立.

定义 8.2.7 设F是一个域. 如果域F满足定理 8.2.11 的等价条件，则称F为**代数闭包**.

定义 8.2.8 设K是一个域, f是K上的不可约多项式. 如果F是f在K上的一个分裂域，且f在F中的根都是单根，则称f是**可分的**.

定义 8.2.9 设F是域K是一个扩域, u是K上的代数数. 如果u在K上的极小多项式是可分的，则称u在K上是可分的. 如果F中的每个元素u在K上都是可分的，则称F为K的**可分扩张**.

8.3 Galois 基本定理

定义 8.3.1 设E和F是域K的扩域. 对于一个非零映射$\sigma: E \to F$，如果σ是一个域同态，且σ在K上为恒等映射，则称σ为K-**同态**. 特别地，当σ是一个域同构时，则称σ为K-**同构.**

注：K-同态和K-同构都要求K中的元素是不变元，即在同态或同构映射下保持不变.

对于一个自同构$\sigma: F \to F$,如果σ是K-同构，则称σ为K-**自同构**. F的所有K-自同构组成的群叫作F在K上的**伽罗瓦**(Galois)群，记作 $\mathrm{A}ut_KF$.

对于中间域$E: K \subset E \subset F$, 也有F在E上的 Galois 群 $\mathrm{A}ut_EF$.

定理 8.3.1 设F是K的扩域, $f \in K[x]$. 若$u \in F$是f的根, $\sigma \in \mathrm{A}ut_KF$, 则$\sigma(u)$也是$f$的根.

设F是K的扩域，E是中间域. 设H是$G=\mathrm{Aut_K F}$的子群. 定义

$$I(H)=\{v\in F \mid \sigma(v)=v,\sigma\in H\}$$

和

$$A(E)=\{\sigma\in \mathrm{Aut}_K F \mid \sigma(u)=u,u\in E\}.$$

$I(H)$是由F中在子群H的自同构下保持不变的元素组成的集合．$A(E)$是由$\mathrm{G}=\mathrm{Aut_K F}$中使中间域$E$中的元素保持不变的自同构组成的集合.

定理 8.3.2 设F是K的扩域，E是中间域以及H是$\mathrm{Aut_K F}$的子群，则

(i) $I(H)$是扩域F的中间域.

(ii) $A(E)$ 是$\mathrm{Aut_K F}$的子群.

注：中间域$I(H)$叫作H在F中的**不变域**. 易知，

$$I(G)=K,I(\{e\})=F.$$

$$A(F)=\{e\},A(K)=G.$$

定义 8.3.2 设F是K的扩域.如果 Galois 群$\mathrm{Aut_K F}$的不变域是K，则F叫作K的 Galois **扩张**.

注：对于中间域$E:K\subset E\subset F$，如果 Galois 群 $\mathrm{Aut_E F}$的不变域是E，则 F叫作E的 Galois 扩张.

注：设域F是K的 Galois 扩张，则对任意的$u\in F\backslash K$,存在$\sigma\in \mathrm{Aut}_K P$ 使得$\sigma(u)\neq u$. 设域F是E的 Galois 扩张，则对任意的$u\in F\setminus E$,存在$\sigma\in \mathrm{Aut}_E F$使得$\sigma(u)\neq u$.

注：给定E,可得$A(E)$,进而得$I\big(A(E)\big)$,它使得$A(E)=\mathrm{Aut}_{I(A(E))}F$. 故

$$A(E)=\mathrm{Aut}_E F \Leftrightarrow I\big(A(E)\big)=E.$$

即E有 Galois 子群 $\mathrm{Aut_E F}$的充要条件是$I\big(A(E)\big)=E$.

注：给定$H<G$,可得$I(H)$,进而得$A\big(I(H)\big)$使得$A\big(I(H)\big)=\mathrm{Aut}_{I(H)}F$. 故

$$H=\mathrm{Aut}_{I(H)}F \Leftrightarrow A\big(I(H)\big)=H.$$

如果$\mathrm{E}=\mathrm{I}\big(A(E)\big)$,则称**中间域$E$是闭的**. 例如$K$和$F$都是闭域

如果$\mathrm{H}=\mathrm{A}\big(I(H)\big)$,则称**子群$H$是闭的**. 例如$\{\mathrm{e}\}$和G都是闭子群

定理 8.3.3 设F是K的扩域，则在其闭中间域与 Galois 群$\mathrm{G}=\mathrm{Aut_K F}$的闭子群之间存在一一对应的映射：

$$E\mapsto A(E)=\mathrm{Aut}_E F.$$

由此，定理 8.3.1 可以推广为：

定理 8.3.4 设F是K的扩域，E是F的中间域, $f \in E[x]$. 如果$u \in F$是f的根， $\sigma \in A(E)$, 则 $\sigma(u)$ 也是f的根.

定理 8.3.5 (Galois 理论的基本定理) 如果F是K的有限维 Galois 扩张，则在所有中间扩域集到 Galois 群 $\mathrm{Aut}_{\mathrm{K}}\mathrm{F}$的所有子群集之间存在一个一一对应的映射

$$E \mapsto A(E) = \mathrm{Aut}_{\mathrm{E}} F$$

使得：

(*i*) F是每个中间域E上的 Galois 域.

(*ii*) 两个中间域$E_1 \subset E_2$的相关维数$[E_2 : E_1]$等于对应子群 $A(E_1) > A(E_2)$的相关指标$[A(E_1) : A(E_2)]$.特别地，$\mathrm{Aut}_{\mathrm{K}}\mathrm{F}$有阶$[F:K]$.

(*iii*) 中间域E是K上的 Galois 域当且仅当对应的子群$\mathrm{A}(E) = \mathrm{Aut}_{\mathrm{E}}\mathrm{F}$ 是 $G = \mathrm{Aut}_{\mathrm{K}}\mathrm{F}$ 的正规子群，在这个情况下, $G/A(E)$ (同构意义下) 是E 在K上的 Galois 群 $Aut_K E$.

8.4 有限域

8.4.1 有限域的构造

设F_q是q元有限域，其特征p为素数，则F_q包含素域$F_p = \mathbb{Z}/p\mathbb{Z}$，是$F_p$上的有限维线性空间. 设$n = \left[F_q : F_p\right]$，则$q = p^n$，即$q$是其特征$p$的方幂. 根据定理 8.2.5 有

定理 8.4.1 设$K = Z/pZ$是一个有限域，其中p是素数. 设$p(x)$是$K[X]$中的n次不可约多项式，则

$$K[X]/\left(p(x)\right) = \left\{a_{n-1}x^{n-1} + \cdots a_1 x + a_0 \mid a_i \in K\right\}$$

（因为$a_i \in K, |K| = p$，所以n个系数共有$\underbrace{p \cdot p \cdots p}_{n} = p^n$种情况）

构成一个域, 记为F_{p^n}. 这个域的元素个数为p^n.

注：F_{p^n}中的加法和乘法是：

$$f(x) + g(x) = \left((f+g)(x)\left(\operatorname{mod} p(x)\right)\right).$$

$$f(x)g(x) = \left((fg)(x)\left(\operatorname{mod} p(x)\right)\right).$$

例 8.4.1 设$F_2 = Z/2Z$，则$p(x) = x^8 + x^4 + x^3 + x + 1$是$F_2[X]$中的 8 次不可约多项式. 事实上，我们有

$$F_{2^8} = F_2[X]/\left(x^8+x^4+x^3+x+1\right) = \left\{a_7x^7+\cdots a_1x+a_0 \mid a_i \in \{0,1\}\right\}$$

F_{2^8} 中的加法和乘法是：

$$f(x)+g(x) = \left((f+g)(x)\left(\bmod x^8+x^4+x^3+x+1\right)\right).$$

$$f(x)g(x) = \left((fg)(x)\left(\bmod x^8+x^4+x^3+x+1\right)\right).$$

另一方面，单独考虑非零元，可以证明：$F_q^* = F_q\{0\}$是$q-1$阶循环乘群. 为此，先讨论F_q^*的一些性质.

定理 8.4.2 F_q^*的任意元a的阶整除$q-1$.

证 (方法一) 设$H =< a >$是a生成的循环群，根据推论 8.2.1，有 $\mathrm{ord}(a) = |H|$且$|H| \mid |F_q^*|$，即 $\mathrm{ord}(a) \mid q-1$.

(方法二) 设$F_q^* = a_1, a_2, \cdots, a_{q-1}$，则$a \cdot a_1, a \cdot a_2, \cdots, a \cdot a_{q-1}$是 $a_1, a_2, \cdots, a_{q-1}$的一个排列，其中$a \in F_q^*$.因此，$(a \cdot a_1)(a \cdot a_2)\cdots(a \cdot a_{q-1}) = a_1a_2\cdots a_{q-1}$，即$a^{q-1}(a_1\cdots a_{q-1}) = a_1\cdots a_{q-1}$.两端右乘$(a_1a_2\cdots a_{q-1})^{-1}$，得$a^{q-1}=1$. 类似于定理 4.1.1 的证明，有 $\mathrm{ord}(a) \mid q-1$.

定义 8.4.1 如果有限域F_q的元素g是F_q^*的生成元，即阶为$q-1$，则称g为F_q的**本原元**. 此时，有$F_q = 0 \cup < g \geq \{0, g^0 = 1, g, \cdots, g^{q-2}\}$. 同时，称本原元 g 的极小多项式为**本原多项式**.

定理 8.4.2 每个有限域都有本原元. 如果g是F_q的本原元，则g^d是F_q的本原元当且仅当$\gcd(d, q-1) = 1$. 特别地，F_q有$\varphi(q-1)$个本原元.

推论 8.4.1 设 $q = p^n$，p为素数，$d \mid q-1$，则有限域 F_q 中有阶为 d 的元素.

推论 8.4.2 设p为素数，则存在整数g遍历模p简化剩余系，即存在模p原根.

类似于模p原根的构造方法 (定理 4.2.7), 也有有限域F_{p^n}的本原元构造方法.

定理 8.4.3 给定有限域F_{p^n}，其中p为素数. 设p^n-1的所有不同素因数是 $q_1, \cdots, q_s$，则g是 F_{p^n} 中本原元的充要条件是

$$g^{\frac{p^n-1}{q_i}} \neq 1,\ i = 1, \cdots, s.$$

8.4.2 有限域的 Galois 群

定理 8.4.5　设F_q是$q=p^n$元有限域，σ是F_q到自身的映射，$\sigma\colon \alpha\mapsto a^p$，则$\sigma$是$F_q$的自同构，且$F_q$中在$\sigma$下的不动元是素域$F_p$的元素，而$\sigma$的$n$次幂是恒等映射.

证　根据定理 7.2.1 以及定理 8.3.4, 有

$$\sigma(a+b)=(a+b)^p=d^p+b^p=\sigma(a)+\sigma(b),$$

$$\sigma(ab)=(ab)^p=d^pb^p=\sigma(a)\sigma(b).$$

因此，σ是F_q的自同构. 因为

$$\sigma^2(a)=\sigma(a^p)=a^{p^2},\cdots,\sigma^j(a)=\sigma\left(a^{p^{j-1}}\right)=a^{p^j},\cdots,\sigma^n(a)=a^{p^n}=a,$$

所以σ^j的不动元是$x^{p^j}-x$的根. 特别地，当$j=1$时，σ的不动元是x^p-x的根，这些根就是素域F_p的p个元素. 而当$j=n$时，σ的不动元是x^q-x的根，这些根就是域F_q的所有q个元素. 因此，σ^n是恒等映射，σ的逆映射是σ^{n-1}.

注：定理 8.4.5 中的映射σ叫作 Frobenius **自同构**.

推论 8.4.3　设F_q是$q=p^n$元有限域，设$\sigma\colon a\mapsto a^p$是$F_q$到自身的映射，$\{\alpha_1,\alpha_2,\cdots,\alpha_d\}$是$F_q$的子集，且在$\sigma$下保持不变，即$\{\sigma(\alpha_1),\sigma(\alpha_2),\cdots,\sigma(\alpha_d)\}$是$\{\alpha_1,\alpha_2,\cdots,\alpha_d\}$的一个置换，则$f(x)=(x-\alpha_1)(x-\alpha_2)\cdots(x-\alpha_d)$是$F_q$上的多项式.

证　因为多项式f的系数是$\alpha_1,\alpha_2,\cdots,\alpha_d$的对称多项式，所以它们在$\sigma$下保持不变，即它们属于$I(<\sigma>)=F_p$.

定理 8.4.6　设F_q是$q=p^n$元有限域，σ是F_q到自身的映射，$\sigma\colon a\mapsto a^p$. 如果$\alpha$是$F_q$的任意元，则$\alpha$在$F_p$上的共轭元是元素是$\sigma^j(\alpha)=\alpha^{p^j}$.

证　设$d=[F_p(\alpha)\colon F_p]$，则$F_p(\alpha)$可作为有限域$F_{p^d}$(在同构意义下).

因此，α满足$x^{p^d}=x$，但不满足$x^{p^j}=x$，$1\leqslant j<d$.

由此，重复应用σ，就得到d个不同元$\alpha,\sigma(\alpha)=\alpha^p,\cdots,\sigma^{d-1}(\alpha)=\alpha^{p^{d-1}}$.

断言：这些元素是α的极小多项式的全部根. 事实上，设α的极小多项式为

$$f(x)=x^d+a_{d-1}x^{d-1}+\cdots+a_1x+a_0,\quad a_i\in F_p$$

则$f(\alpha)=\alpha^d+a_{d-1}\alpha^{d-1}+\cdots+a_1\alpha+a_0=0$. 两端作$p$次方，根据定理 7.2.1，并注意到$a_i^p=a_i, 0\le i<d$，有

$$f(\alpha^p)=(\alpha^p)^d+a_{d-1}(\alpha^p)^{d-1}+\cdots+a_1\alpha^p+a_0=f(\alpha)^p=0.$$

依次继续作p次方，对于$1\le j<d$，有

$$f\left(\alpha^{p^j}\right)=\left(\alpha^{p^j}\right)^d+a_{d-1}\left(\alpha^{p^j}\right)^{d-1}+\cdots+a_1\alpha^{p^j}+a_0=f(\alpha)^{p^j}=0.$$

推论 8.4.4 设F_q是$q=p^n$元有限域，σ是F_q到自身的映射,$\sigma:\alpha\mapsto\alpha^p$.设$f(\mathrm{x})$是$F_p$上的$d$次首一不可约多项式. 如果$\alpha$是$f(x)$在$F_q$中的根，则$\alpha,\sigma(\alpha)=\alpha^p,\cdots,\sigma^{d-1}(\alpha)=\alpha^{p^{d-1}}$是$F_q$中的全部根，其中$d$是使得 $\sigma^d(\alpha)=\alpha$ 的最小正整数.

证 设e是使得$\sigma^e(\alpha)=\alpha$成立的最小正整数，则由推论 8.4.3 知，$g(x)=(x-\alpha)\big(x-\sigma(\alpha)\big)\cdots\big(x-\sigma^{e-1}(\alpha)\big)$是$F_p$上的多项式. 因为$f(x)$是$\alpha$的极小多项式，所以$f(x)\mid g(x)$. 从而$d\le e$,且 $\alpha,\sigma(\alpha)=\alpha^p,\cdots,\sigma^{d-1}(\alpha)=\alpha^{p^{d-1}}$ 是$f(x)$ 的 d 个不同根，故结论成立.

定理 8.4.7 F_{q^n}在F_q上的自同构集合在映射的复合运算下构成一个阶为n的循环群,其生成元为自同构 $\sigma_q(\alpha)=\alpha^q$.

证 设β是F_{q^n}中的本原元，则β在F_q上的阶为q^n-1,且其极小多项式$p(x)=x^n+a_{n-1}x^{n-1}+\cdots+a_1x+a_0\in F_q[x]$有根

$$\beta,\sigma_q(\beta)=\beta^q,\sigma_q^2(\beta)=\beta^{q^2},\cdots,\sigma^{n-1}(\beta)=\beta^{q^{n-1}}.$$

设$f(x)$是F_q上的多项式. 因为F_{q^n}在F_q上的自同构τ保持$f(x)$的系数不变，所以$f(\alpha)=0$的充要条件是$f\big(\tau(\alpha)\big)=0$. 换句话说，$\tau$对$f(x)$在$F_{q^n}$中的根进行了置换. 特别地，对于$p(x)$的根$\beta$，存在$i$使得$\tau(\beta)=\beta^{q^i}$. 故

$$\sigma_q^i(\beta)=\sigma_q\left(\sigma_q^{i-1}(\beta)\right)=\beta^{q^i}=\tau(\beta).$$

因为β是F_{q^n}的本原元，得$\tau=\sigma_q^i$. 因此，F_{q^n}在F_q上的自同构集是一个阶为n的循环群，其生成元为自同构$\sigma_q(\alpha)=\alpha^q$.

8.4.3 有限域的正规基

最后，再次从向量空间的基底角度考虑有限域. 易知,

设α是F_q上次数为n的F_{q^n}中的元素，则$1,\alpha,\alpha^2,\cdots,\alpha^{n-1}$构成$F_{q^n}$在$F_q$上的一组基底，称作**多项式基底**. 结合上述知识，我们可以找到另外一种形式的基底.

定义 8.4.2 F_{q^n}在F_q上形如$\alpha,\alpha^q,\alpha^{q^2},\cdots,\alpha^{q^{n-1}}$的基底叫作$F_q^n$在$F_q$上的正规基.

定理 8.4.8 有限域F_{q^n}在其子域F_q上有正规基存在.

证 略.

例 8.4.2 求$F_{2^4}=F_2[x]/(x^4+x+1)$中的正规基.

解 (*i*) 对于$\beta=x$,有

$$\begin{aligned} \beta &= x, \\ \beta^2 &= x^2, \\ \beta^4 &= x+1, \\ \beta^8 &= x^2+1, \end{aligned}$$

所以，$\beta, \beta^2, \beta^{2^2}, \beta^{2^3}$不构成一组基底.

(*ii*) 对于$\beta = x^3$,有

$$\begin{aligned} \beta = x^3 &= x^3, \\ \beta^2 = x^6 &= x^3 + x^2, \\ \beta^4 = x^{12} &= x^3 + x^2 + x + 1, \\ \beta^8 = x^9 &= x^3 + x, \end{aligned}$$

所以,$\beta, \beta^2, \beta^{2^2}, \beta^{2^3}$ 构成一组基底，是正规基.