第 10 章 扩　域

利用已知的域构造更广范围的域（即扩域）是域论中常见的研究域的方法，就如同，有理数域可以扩成实数域，实数域可以扩成复数域一样．这一章我们主要研究域的各种扩展域单扩域、代数扩域、一种特殊的代数扩域--多项式的分裂域．另外，我们还将讨论域的特征及有限域的结构．

§1 域的特征

给定一个域F，则F关于加法构成一个加群$(F,+)$．在加群$(F,+)$中，所有的非零元素都具有一个非常特殊的规律，即它们的阶都相同．实际上，这种特性在一般的无零因子环中也成立．这种特性可以从下面的定理得到证明．

定理 1 在一个没有零因子的环R里所有不等于零的元对于加法来说阶都是一样的．特别地，在域中所有非零元的阶相同．

证明　若R的每一个不等于零的元的阶都是无限大，结论显然成立．

假定R的某一个元$a \neq 0$的阶是有限整数n，即$ord(a)=n$．对于任意$b \in R, b \neq 0$，记$ord(b)=n'$．下证$n'=n$．由环的特性知

$$(na)b = a(nb) = 0 .$$

由于$a \neq 0$，且R无零因子，可得$nb=0$，从而$n' \mid n$．同理可得$n \mid n'$．所以$n=n'$．

由于域为无零因子环，所以域中任两个非零元的阶相同．

下面我们仅考虑域的情形．

定义 1 域中非零元的阶称为域的特征．

关于域的特征，是一个很重要的概念，因为它对域的构造都有决定性的作用．现在 我们进一步证明．

定理 2 如果域F的特征为有限数n，则n一定为素数．

证明　假如n不是素数可设$n=n_1n_2$，n_1,n_2为n的真因子．那么对于F的任一个不等于零的元a，有

$$(n_1a)(n_2a) = (n_1n_2)a^2 = 0 .$$

所以　$n_1a=0$或$n_2a=0$．矛盾．得证．

推论 整环，除环的特征为有限数时，特征一定为素数。

有了域的特征，给定域F，我们可以进一步证明F的最小域的结构．

定理 3 令E是一个域．若E的待征是∞，那么E含有一个与有理数域Q同构的子域；若E的特征是素数p，那么E含有一个与Z_p同构的子域，其中Z_p为模p的剩余类环．

证明　域E包含一个单位元e，因此E也包含所有ne（n是整数）．令R'是所有ne作成的集合．令

$$\phi: n \to ne$$

显然是整数环Z到R'的一个同态满射．

情形 1．E的特征是∞．这时ϕ是一个同构映射$Z \cong R'$．从而R'的商域F'同构于Z的商域即有理数域．

情形 2．E的待征是素数p，由同态基本定理知

$$Z/\ker\phi \cong R'.$$

下证 $\ker\phi = (p)$.

由 $p \to pe = 0$，知 $p \in \ker\phi$，从而 $(p) \subseteq \ker\phi$；

反过来，若 $(p) \neq \ker\phi$，则存在 $a \in \ker\phi, a \notin (p)$，即 $\phi(a) = e$，且 $(a, p) = 1$. 从而存在 $u, v \in Z$，使

$$ua + pv = 1 \in \ker\phi,$$

从而 $Z = \ker\phi$. 矛盾. 所以 $\ker\phi = (p)$. 得证.

定义 2 一个域叫做一个素域，假如它不含真子域.

由定理 1 知道一个素域或是与有理数域同构，或是与 $Z/(p)$ 同构.

§2 扩域

由上一节，我们知道，任意域都是一个素域的扩域. 现在我们介绍一种研究域的普通方法，即给定一个任意域 F，如何找到的 F 所有扩域 E.

现在描述一下一般扩域的结构.

令 E 是域 F 的一个扩域. 我们从 E 里取出一个子集 S 来. 我们用 $F(S)$ 表示含 F 和 S 的 E 的最小子域，把它叫做添加集合 S 于 F 所得的扩域. $F(S)$ 的存在容易看出. 因为，E 的确有含 F 和 S 的子域，例如 E 本身. 一切这样的子域的交集显然是含 F 和 S 的 E 的最小子域.

容易证明 $F(S)$ 刚好包含 E 的一切可以写成

$$f(S) = \left\{ \frac{f_1(\alpha_1, \alpha_2, \cdots, \alpha_n)}{f_2(\beta_1, \beta_2, \cdots, \beta_m)} \mid \forall \alpha_1, \cdots, \alpha_n, \beta_1, \cdots, \beta_m \in S, f_1, f_2 \text{为} F \text{上任两个多元多项式} \right\}$$

若 S 是一个有限集 $S = \{\alpha_1, \alpha_2, \cdots, \alpha_n\}$，那么我们也把 $F(S)$ 记作

$$F(S) = F(\alpha_1, \alpha_2, \cdots, \alpha_n)$$

叫做添加元素 $\alpha_1, \alpha_2, \cdots, \alpha_n$ 于 F 所得的子域.

为了便于讨论添加有限个元素所得的子域，我们说明下述的一般定理.

定理 1 令 E 是域 F 的一个扩域，而 S_1 和 S_2 是 E 的两个子集，那么

$$F(S_1)(S_2) = F(S_1 \cup S_2) = F(S_2)(S_1).$$

证明 $F(S_1)(S_2)$ 是一个包含 F, S_1 和 S_2 的 E 的子域，而 $F(S_1 \cup S_2)$ 是包含 F 和 $S_1 \cup S_2$ 的 E 的最小子域. 因此

$$F(S_1)(S_2) \supset F(S_1 \cup S_2). \tag{1}$$

另一方面，$F(S_1 \cup S_2)$ 是一个包含 F, S_1 和 S_2 的 E 的子域，因而是包含 $F(S_1)$ 和 S_2 的 E 的子域. 但 $F(S_1)(S_2)$ 是包含 $F(S_1)$ 和 S_2 的最小子域，因此

$$F(S_1)(S_2) \subset F(S_1 \cup S_2). \tag{2}$$

由(1)和(2)得

$$F(S_1)(S_2) = F(S_1 \cup S_2).$$

同样可以得到

$$F(S_2)(S_1) = F(S_1 \cup S_2).$$

得证.

根据定理 1，我们可以把添加—个有限集归结为陆续添加单个的元素，例如

$$F(\alpha_1,\alpha_2,\cdots,\alpha_n)=F(\alpha_1)(\alpha_2)\cdots(\alpha_n),$$

所以首先我们考虑添加一个元素的扩域的情况.

定义 1 添加一个元素α于域F所得的扩域$F(\alpha)$叫做域F的—个单扩域(扩张).

单扩域是最简单的扩域，假定$E=F(\alpha)$是域F的单扩域，而α是E的一个元．根据α的特性，将单扩域$F(\alpha)$进行分类.

定义 2 α是$F[x]$的一个多项式的根，即存在不全为零的元$a_0,a_1,\cdots,a_n$，使得

$$a_0+a_1\alpha+\cdots+a_n\alpha^n=0,$$

则称α是F上的一个代数元.

否则，α就叫做F上的一个超越元．显然，若α为F上的一个超越元，则对于F上任何非零多项式$F(x)$，满足$F(\alpha)\neq 0$.

定义 3 若α是F上的一个代数元，$F(\alpha)$就叫做F的一个单代数扩域．若α是F上的一个超越元，$F(\alpha)$ 就叫做F的一个单超越扩域.

定义 4 $F[x]$中满足条件$p(\alpha)=0$的次数最低的多项式

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

叫做元α的在F上的最小多项式．n叫做α的在F上的次数.

容易证明，α的在F上的最小多项式$p(x)$在$F[x]$中既约.

例 1 若$F[\alpha]$表示F上一切α的多项式的集合，按多项式的运算构成环．证明：$F(\alpha)$为$F[\alpha]$的商域.

证明 显然$F[\alpha]$的商域$\subset F(\alpha)$；

另一方面，$F[\alpha]$的商域包含F也包含α，因此，由$F(\alpha)$的定义，$F(\alpha)\subset F[\alpha]$的商域．所以 $F(\alpha)=F[\alpha]$的商域.

下列定理反映了单扩域的结构.

定理 2 若α是F上的一个超越元，那么$F(\alpha)\cong F[x]$的商域；若α是F上的—个代数元，那么

$$F(\alpha)\cong F[x]/(p(x)),$$

其中这里$p(x)$是$F[x]$一个唯一确定的、最高系数为1的不可约多项式式，并且$p(\alpha)=0$.

证明 令$F[\alpha]$为包含F上α的多项式环

$$F[\alpha]=\{f(\alpha)\mid f(x)\in F[x]\}$$

作一个$F(x)\to F[\alpha]$的映射

$$\phi:\ f(x)\to f(\alpha),\quad \forall f(x)\in F[x],$$

则ϕ是多项式环$F[x]$到$F[\alpha]$的同态满射．现在我们分两个情形来考察$F(\alpha)$的结构.

（1）若α是F上的超越元，ϕ为同构映射，所以

$$F[\alpha]\cong F[x]$$

由第 9 章第 4 节知$F[\alpha]$的商域$\cong F[x]$的商域．由例 1 知$F(\alpha)\cong F[x]$的商域.

（2）α是F上的代数元，由同态基本定理

$$F[\alpha]\cong F[x]/\ker\phi.$$

易知$\ker\phi$为主理想，且$\ker\phi=(p(x))$，其中$p(x)$为α的最小多项式，所以$p(x)$既约．从而$F[x]/\ker\phi$为域．所以$F[\alpha]=F(\alpha)$.

从定理 2 我们知道，若α是域F上的一个代数元$F(\alpha)$的每一个元都可以唯一的表成

$$\sum_{i=0}^{n-1} a_i \alpha^i \qquad (a_i \in F)$$

的形式，这里n是$p(x)$的次数，$p(x)$为α的最小多项式．

以上的讨论是在域F有扩域E的前提下进行的．现在我们问，若是只给了一个域F，是不是有F的单扩域存在?F的单超越扩域的存在容易看出．我们知道，F上的一个未定元x的多项式环$F[x]$和$F[x]$的商域都是存在的．$F[x]$的商域显然是包含F和x的最小域，由定理 2 知$F[x]$的商域就是F的一个单超越扩域，并且F的任何单超越扩域都是同构的．

下面我们讨论给定域F及F上的不可约多项$p(x)$，是否存在F的扩域K包含多项式$p(x)$的一个根α．

定理 3　对于任一给定域F以及F上一元多项式环$F[x]$的不可约多项式

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

总存在F的单代数扩域$F(\alpha)$, 其中α在F上的极小多项式是$p(x)$.

证明　有了F和$p(x)$，我们可以作剩余类环

$$K = F[x]/(p(x)).$$

因为$p(x)$是不可约多项式，所以K是一个域.

我们知道$K = \{\overline{r(x)} \mid r(x)\text{的次数小于}n\}$，$K$的子集

$$\overline{F} = \{\overline{a} \mid \forall a \in F\},$$

构成K的子域并且与F同构，所以K可以看作F的扩域．现在证明K含有$p(x)$的一个根．可以验证对于$\overline{x} \in K$，

$$p(\overline{x}) = \overline{p(x)} = \overline{0},$$

所以$\overline{x}$是$p(x)$的一个根．定理得证．

给了域F和$F[x]$的一个最高系数为1的不可约多项式$p(x)$，可能存在若干个单代数扩域，均都满足定理 3 的要求．但我们有

定理 4　令$F(\alpha)$和$F(\beta)$是域F的两个单代数扩域，并且α和β在F上有相同的最小多项式$p(x)$．那么$F(\alpha)$和$F(\beta)$同构.

证明非常简单，留作习题。

定义 5　域F的一个扩域E叫做$F[x]$的n次多项式$f(x)$在F上的一个分裂域(或根域)，假如E包含F及$f(x)$的所有根，而E的的任意真子域不包含$f(x)$的所有的根.

例3　设$F = Z/(2)$，则

$$f(x) = x^3 + x + 1$$

是$F[x]$中的既约多项式，并且$F[x]/(f(x))$是$f(x)$在F上的分裂域.

根据定理 3 我们可以进一步证明给定F及$F[x]$上的多项式$f(x)$，分裂域是存在的。

定理 5　给了域F上一元多项式环$F[x]$的一个n次多项式$f(x)$，一定存在$f(x)$在F上的分裂域E.

证明　用归纳法：

当$n = 1$，$E = F$即可.

假设$n \le m$时，结论成立.

当$n = m+1$时，若$f(x)$在$F[x]$上可约，则存在次数小于m的多项式$f_1(x), g_1(x)$

使：

$$f(x)=f_1(x)g_1(x)$$

由归纳假设知存在 $f_1(x)$ 在 F 上的分裂域 E_1，包含 $f_1(x)$ 的所有根 $\alpha_1,\alpha_2,\cdots\alpha_{n_1}$． $g_1(x)$ 视为 $F(\alpha_1,\alpha_2,\cdots\alpha_{n_1})$ 上的次数小于 n 的多项式，故存在 $g_1(x)$ 在 $F(\alpha_1,\alpha_2,\cdots\alpha_{n_1})$ 上的分裂域 E，含有 $g_1(x)$ 的所有根．从而 E 含有 $f(x)$ 的所有根，是 $f(x)$ 在 F 上的分裂域．若 $f(x)$ 在 $F[x]$ 中既约，由定理 3，存在 F 的扩域 K 含有 $f(x)$ 的一个根 θ．于是，在 $K[x]$ 中，

$$f(x)=(x-\theta)g(x)\text{；}$$

再利用归纳假设，由于 $g(x)$ 的次数为 $n-1$，故存在 $g(x)$ 在 K 上的分裂域 E，含有 $g(x)$ 的所有根，从而 E 也含有 $f(x)$ 的所有根．是 $f(x)$ 在 F 上的分裂域．　证毕

例2　设 K 是多项式

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

在 Q 上的分裂域．令 $\omega=\dfrac{1+\sqrt{3}i}{2}$，则 x^2+x+1 的根为 ω，ω^2；而 x^3-3 的根为 $\sqrt[3]{3}$，$\sqrt[3]{3}\omega$，$\sqrt[3]{3}\omega^2$．这样由分裂域的定义

$$K=Q(\omega,\omega^2,\sqrt[3]{3},\sqrt[3]{3}\omega,\sqrt[3]{3}\omega^2)=Q(\omega,\sqrt[3]{3})\,.$$

以上内容说明了给定域 F 及 $F[x]$ 上的多项式 $f(x)$，一定存在 F 的扩域包含 $f(x)$ 的所有的根．下面我们考虑更一般的问题，给定域 F，是否存在一个扩域 E，包含 $F[x]$ 上的所有多项式的根．回答是肯定的，首先我们给出一些相关的概念．

定义 6　若域 F 的一个扩域 E 的每一个元都是 F 上的一个代数元, 那么 E 叫做 F 的一个代数扩域(扩张)．

定义 7 假定 E 是域 F 的一个扩域．那么对于 E 的加法和 $F\times E$ 到 E 的乘法来说，E 作成 F 上的一个向量空间．若 E 为 F 上的有限维空间，则 E 叫做域 F 的一个有限扩域．$(E:F)$ 表示 E 为 F 上向量空间的维数．

定理 6　设 θ 是 $F[x]$ 中 n 次既约多项式 $f(x)$ 的一个根，则 $F(\theta)$ 是 F 上的有限扩域．

证明　因为 $F(\theta)$ 中每一元都可以表成 F 上次数小于 n 的 θ 的多项式，故

$$1,\theta,\theta^2,\cdots,\theta^n$$

是 $F(\theta)$ 的一组生成元，又

$$\sum_{i=0}^{n-1}a_i\theta^i=0\Rightarrow a_i=0\text{，}\ i=0,1,\cdots,n-1\text{，}$$

故 $F(\theta)$ 是 F 上 n 维向量空间，有一组基为

$$1,\theta,\theta^2,\cdots\theta^{n-1}\,.$$

即 $F(\theta)$ 是 F 的一个有限扩域，并且 $(F(\theta):F)=n$．

关于有限扩域，有下列重要结论

定理 7 域 F 的有限扩域一定是 F 的代数扩域．

证明　设 $(E:F)=n$，则存在一组基

$$1,\theta,\theta^2,\cdots,\theta^{n-1}$$

而 $n+1$ 个向量

$$1,\theta,\theta^2,\cdots,\theta^n\text{，}$$

线性相关．即存在$n+1$个不全为零的$a_i \in F$，使

$$\sum_{i=0}^{n} a_i \theta^i = 0 .$$

亦即θ满足$F[x]$中多项式$\sum_{i=0}^{n} a_i x^i$．故E是F上的代数扩域.

注： 定理 7 的逆命题不成立．例如，一切代数数作成有理数域Q的一个扩域E，E是Q上的代数扩域．如果$(E:Q)$有限，设为n．取$Q[x]$中$n+1$次既约多项式

$$f(x) = x^{n+1} + x + 3$$

的一个根$\theta \in E$，E中的$n+1$个元$1, \theta, \cdots, \theta^n$在$Q$上线性无关，这与$(E:Q)=n$矛盾．说明$E$是$Q$的无限扩域.

定理 8 令 K是域F的有限扩域，而E是K的有限扩域，那么E也是F的有限扩域，并且

$$(E:F) = (E:K)(K:F) .$$

证明 设$(K:F)=r$，$(E:K)=s$，而$\alpha_1, \alpha_2, \cdots, \alpha_r$是向量空间$K$在域$F$上的一个基，$\beta_1, \beta_2, \cdots, \beta_s$是向量空间$E$在域$K$上的一个基.

下证rs个元构成向量空间E在域F上的一个基.

$$\alpha_i \beta_j \quad (i = 1,2,\cdots,r;\ j = 1,2,\cdots,s) \tag{1}$$

显然向量空间E中任意元素可以表示rs个元系数为域F上元的线性组合.

下证（1）中元素在F上线性无关．若

$$\sum_{i,j} a_{ij} \alpha_i \beta_j = 0 \quad (a_{ij} \in F),$$

那么

$$\sum_j (\sum_i a_{ij} \alpha_i) \beta_j = 0, \qquad \sum_i a_{ij} \alpha_i \in K .$$

由$\beta_j, 0 \le j \le s$在K上的线性无关性有，

$$\sum_i a_{ij} \alpha_i = 0 \text{，（} j = 1,2,\cdots,s \text{）}.$$

由$\alpha_i, 0 \le i \le r$在F上的线性无关性知，

$$\alpha_{ij} = 0 \text{（} i = 1,2,\cdots,r;\ j = 1,2,\cdots,s \text{）}.$$

这就是说，（1）的rs个元为E在F上的一组基．定理得证.

由定理 6 与定理 8 有下列结论.

推论 E为F的代数扩域，任给$\alpha_1, \alpha_2, \cdots, \alpha_r$为$F$上的代数元，则$F(\alpha_1, \alpha_2, \cdots, \alpha_r)$为$F$上有限扩域.

定理 若K是F上的代数扩域，E是K上的代数扩域，则E也是F上的代数扩域.

证明 任取$\theta \in E$，设θ在K上的最小多项式为

$$f(\theta) = a_0 \theta^n + a_1 \theta^{n-1} + \cdots + a_n .$$

显然，$F(a_0)$是F上的有限扩域，由归纳法可证，$F(a_0, a_1, \cdots, a_n)$也是F上的有限扩域．又$F(a_0, a_1, \cdots, a_n)(\theta)$是$F(a_0, a_1, \cdots, a_n)$上的有限扩域，故$F(a_0, a_1, \cdots, a_n)(\theta)$也是$F$

上的有限扩域，从而是 F 上的代数扩域．因此 θ 也是 F 上的代数元．故 E 是 F 上的代数扩
证毕

定义 8 域 E 为一个代数闭域，如果没有 E 的代数扩域 E'，使 E 为 E' 的真子域．

定理 10 对于每一个域 F 都存在 F 的代数扩域 E，使得 E 是代数闭域．

定理的证明比较复杂，这里略过．

从定理 10 知，给定域 F，一定存在 F 的扩域 E，使 E 包含 F 上所有多项式的根．

例 3 复数域 C 就是一个代数闭域．

证明 设 K 是 C 的一个代数扩域，$\theta \in K$，θ 是 C 上一个既约多项式的根．但 C 中仅有一次既约多项式，故 $\theta \in C$，从而 $K = C$．

例 4 设 K 是 F 的代数扩域，且 $F[x]$ 中每一多项式的分裂域均为 K 的子域，则 K 是代数闭域．

证明 否则，设 K 有真代数扩域 E，则存在 $a \in E$，$a \notin K$，由于 E 也是 F 的代数扩域，从而 a 是 F 上的代数元，进而是 F 上某 $f(x)$ 的根．但 $F[x]$ 中每一多项式的根均在 K 中，与 $a \notin K$ 矛盾．

§3 有限域

有限域在应用密码学、编码理论以及许多其它应用技术领域中有着极其广泛的应用．本节主要讨论有限域的结构及其特例．

它的定义很简单

定义 1 一个只含有限个元素的域叫做有限域．

显然，一个特征是 p 的素域就是一个有限域．

定理 1 一个有限域 E 有 p^n 个元素，这里 p 是 E 的特征而 n 是 E 在它的素域 Δ 上的次数．

证明 E 为有限域，由第 1 节知特征一定是一个素数 p．

把 E 所含的素域记作 Δ．因为 E 只含有限个元，所以它一定是 Δ 的一个有限扩域，设 $(E:\Delta)=n$．这样，E 的每个元可以唯一的写成

$$a_1\alpha_1 + a_2\alpha_2 + \cdots + a_n\alpha_n$$

的形式，这里 $a_i \in \Delta$，而是

$$\alpha_1, \alpha_2, \cdots, \alpha_n$$

向量空间 E 在 Δ 上的一个基．由于 Δ 只有 p 个元，所以对于每一个 a_i 有 p 种选择法，因而 E 一共有 p^n 个元．证毕

定理 2 令有限域 E 的特征是素数 p，E 所含的素域是 Δ，而 E 有 $q = p^n$ 个元．那么 E 是多项式 $x^q - x$ 在 Δ 上的分裂域．任何两个这样的域都是同构．

证明 E 的不等于零的元对于乘法来说，做成一个群．这个群的阶是 $q-1$，单位元是 1．所以

$$\alpha^{q-1} = 1, \quad \alpha \in E, \quad \alpha \neq 0.$$

由于 $0^q = 0$，所以有

$$\alpha^q = \alpha, \quad \alpha \in E.$$

因此用$\alpha_1,\alpha_2,\cdots,\alpha_q$来表示$E$的元，在$E$里多项式

$$x^q - x = \sum_{i=1}^{q}(x-\alpha_i)\,.$$

而且显然

$$E = \Delta(\alpha_1,\alpha_2,\cdots,\alpha_q)\,.$$

这样，E是多项式$x^q - x$在Δ上的分裂域.

但特征为p的素域都同构，而多项式$x^q - x$在同构的域上的分裂域都同构．得证.

现在我们来看一个获得有限域的方法.

定理 3 令Δ是特征为p的素域，而$q = p^n (n \geq 1)$．那么多项式$x^q - x$在Δ上的分裂域E是一个有q个元的有限域.

证明 $E = \Delta(\alpha_1,\alpha_2,\cdots\alpha_q)$,　这里$\alpha_i$是

$$f(x) = x^q - x$$

在域E里的根．由于E的特征是p，$f(x)$的导数

$$f'(x) = p^n x^{q-1} - 1 = -1$$

所以$f(x)$与$f'(x)$互素．这样$f(x)$的q个根都不相同．我们断言，$f(x)$的这q个根都作成E的一个子域E_1，这是因为，

$$(\alpha_i - \alpha_j)^{p^n} = \alpha_i^{\,p^n} - \alpha_j^{\,p^n} = \alpha_i - \alpha_j\,,$$

$$\left(\frac{\alpha_i}{\alpha_j}\right)^{p^n} = \frac{\alpha_i^{\,p^n}}{\alpha_j^{\,p^n}} = \frac{\alpha_i}{\alpha_j}(\alpha_j \neq 0)\,.$$

这就是说，$\alpha_i - \alpha_j$和$\dfrac{\alpha_i}{\alpha_j}(\alpha_j \neq 0)$仍是$f(x)$的根而属于$E_1$，因而$E_1$是$E$的一个子域． 但$E_1$含$\Delta$，也含一切$\alpha_i$，所以$E_1$就是多项式$x^q - x$在$\Delta$上的分裂域．这样$E = E_1$，而$E$恰有$q$个元． 得证.

以上证明了给定素数p和正整数n，有且只有（在同构意义下）一个恰好含p^n个元的有限域存在.

有限域常称作 Galois 域，有p^n个元素的有限域通常记做$GF(p^n)$.

例 1 令Δ是特征为p的素域，$f(x)$是Δ上的n次既约多项式，$\theta_i\ (1 \leq i \leq n)$是$f(x)$的所有根，于是$\Delta(\theta_1,\cdots,\theta_n)$是$f(x)$在$\Delta$上的分裂域．而$\Delta$的特征为$p$，所以$\Delta(\theta_1,\cdots,\theta_n)$有$p^n$个元素，由上面的定理，$\Delta(\theta_1,\cdots,\theta_n)$同构于$GF(p^n)$.

定理 4 （I）有限域$GF(p^n)$的子域是$GF(p^m)$的形式，其中$m \mid n$.

(II) 对n的任一因子m，有限域$GF(p^n)$有且仅有一个子域$GF(p^m)$.

证明 设T是有限域$E = GF(p^n)$的子域，Δ是E的素域，由

$$[E:T]\cdot[T:\Delta] = [E:\Delta] = n$$

知$[T:\Delta] = m$必整除n；T是元素个数为p^m的有限域．这样T是$x^{p^m} - x$在Δ上的分裂域。注意到T是E的子域，故

$$T=\{a\in E\mid a^{p^m}-a=0\}.$$

这样E中元素个数为p^m的子域T有且仅有一个，由$x^{p^m}-x$在E中的一切根组成．得证．

我们知道，单扩域是比较容易找到的一种扩域．现在，我们有进一步证明，一个有限域一定是它所含素域的一个单扩域．我们先证明

引理 令G是一个有限交换群，而m是G的元的阶中最大的一个．那么m能被G的每一元的阶整除．

证明 容易看出若a和b是G的两个元，a的阶是l_1，b的阶是l_2，而$(l_1,l_2)=1$，那么ab的阶是l_1l_2．假定G的元c的阶n不能整除m，那么有素数p存在，使

$$m=p^im_1,(p,m_1)=1，\ n=p^jn_1,j>i.$$

令m是元d的阶，于是$a=d^{p^i}$的阶是m_1，$b=c^{n_1}$的阶是 p^j．根据前面的结论，ab的阶是$p^jm_1>m$．这与m是G的元的阶中最大的一个的假设矛盾．证完．

定理 5 一个有限域E是它的素域Δ的一个单扩域．

证明 设E含有q个元．E的非零元对E的乘法来说作成一个交换群G，它的阶是$q-1$．令m是G的元的阶中最大的一个，那么由引理

$$\alpha_i^{\ m}=1,$$

对于任意$\alpha_i\in G$．这就是说，多项式

$$x^m-1$$

至少有$q-1$个不同的的根．因此$m\geq q-1$，但由于m整除G的阶，故$m\leq q-1$．所以有$m=q-1$．这就是说G有一个元α，它的阶是$q-1$，因而G是一个循环群$G=(\alpha)$．这样，E是添加α于Δ所得的单扩域 $E=\Delta(\alpha)$．定理得证．

§4 编码（有限域的一个应用）

在数字通讯中总是要把信息编码为 0，1 字符串发送，这个字符串实际上就是有限域$GF(2)$上的一个n维向量，由于信道是常常受到干扰的，如何加工改造信息编码，使得接收方能够从可能错误的字符串中尽可能正确的读出发送方的意图，是编码理论要解决的问题．

取定正整数n，设$F=GF(2)$，F^n为所有向量$\alpha=(a_1,\cdots,a_n)$，$a_i\in F$组成的n维向量空间．称F^n的一个非空子集M为一个码，M中的元素为码字。我们的问题是：

A. 如何简单地构造一个码M．

B. 如何使这个码能有效地判断，对任意字x是否有$x\in M$．

C. 如何使这个码能有效地判断，一个给定的字α来源于M中的哪个码字α'．

一般说来，数字正确地通过信道的概率比发生错误的概率要大些．我们给出背景知识。

定义 1 在F^n中任取两个字

$$x=(x_1,\cdots,x_n)，\ y=(y_1,\cdots,y_n).$$

规定 Hamming 距离$\rho(x,y)$为x，y中不相等的分量对$x_i\neq y_i$的个数，简称距离；Hamming 重量$W(x)$为x中非零分量的个数，简称x的重量．

显然，$\rho(x,y)$满足通常意义下距离的性质：

1．$\rho(x,y)=0$，当且仅当$x=y$．

2．$\rho(x,y)=\rho(y,x)$．

3．对任意$x,y,z\in F^n$，

$$\rho(x,y)+\rho(y,z)\geq\rho(x,z).$$

于是可以定义M是一个码，$\alpha\in F^n$，α到M的距离

$$\rho(\alpha,M)=\min\{\rho(\alpha,x),x\in M\},$$

M的最小距离：

$$\rho(M,M)=\min\{\rho(x,y),x,y\in M;x\neq y\}.$$

而且

$$\rho(x,y)=W(x-y).$$

前面的问题 C 实际上就是下面的

最大似然译码原理：$M\subseteq F^n$是一个码而$\alpha\in F^n$（假定为接收码）．若存在唯一的$\alpha'\in M$满足条件$\rho(\alpha,\alpha')=\rho(\alpha,M)$，则我们将认定$\alpha$就是码字$\alpha'$（假定为发送码），并将字$\alpha$译为$\alpha'$.

定义 2　一个码M称作可纠正t个差错的纠错码，如果对满足$\rho(\alpha,M)\leq t$的字α，总有唯一的$\alpha'\in M$使$\rho(\alpha,\alpha')=\rho(\alpha,M)$.

容易证明

定理 1 若码M的最小距离$\rho(M,M)=2t+1$，t是正整数，则M是可纠正t个差错的纠错码.

这样，构造最小距离尽可能大的码就是解决问题 C 的一个办法．下面我们一次解决上面三个问题．先是问题 A.

定义 3 F^n的一个k维子空间L称作(n,k)线性码．如果L中的任一码字都是F^n中k个线性无关向量的线性组合.

于是可以这样构造L：在F^n中选k个无关向量$g_1,g_2,\cdots,g_k$，设

$$G=\begin{pmatrix}g_1\\ \vdots\\ g_k\end{pmatrix}=\begin{pmatrix}g_{11}&g_{12}&\cdots&g_{1n}\\ g_{21}&g_{22}&\cdots&g_{2n}\\ \cdots&\cdots&\cdots&\cdots\\ g_{k1}&g_{k2}&\cdots&g_{kn}\end{pmatrix},$$

则L中任一码字可唯一地表成$(\alpha_1,\cdots\alpha_k)\cdot G$，$\alpha_i\in F$，且这种形式的向量都是$L$中的码字．称矩阵$G$为码$L$的生成矩阵.

通过这个L来看问题 B．令齐次线性方程组

$$G\cdot x^T=\begin{pmatrix}g_{11}&\cdots&g_{1n}\\ \cdots&\cdots&\cdots\\ g_{k1}&\cdots&g_{kn}\end{pmatrix}\cdot\begin{pmatrix}x_1\\ \vdots\\ x_n\end{pmatrix}=\begin{pmatrix}0\\ \vdots\\ 0\end{pmatrix},$$

（其中x^T是$x=(x_1,\cdots x_k)$的转置矩阵）的解空间为L^*，这是F^n的一个$n-k$维子空间．取L^*的一组基构成

$$H=\begin{pmatrix}h_1\\ \vdots\\ h_{n-k}\end{pmatrix}=\begin{pmatrix}h_{11}&\cdots&h_{1n}\\ \cdots&\cdots&\cdots\\ h_{n-k,1}&\cdots&h_{n-k,n}\end{pmatrix}。$$

易知，F^n的向量$\alpha\in L$当且仅当$H\cdot\alpha^T=\theta$，这里θ是零向量．这样对任意

$\alpha \in F^n$，只要计算$H \cdot \alpha^T$的值是否为零，就可以解决问题 B 了．称H为码L的校验矩阵.

最后来看问题 C，根据前面的定理 1，重要的是计算L的最小距离．由于L对减法封闭，有

$$\rho(L,L) = \min\{\rho(x,y) = W(x-y), x,y \in L, x \neq y\}$$
$$= \min\{W(\alpha), \alpha \in L, \alpha \neq 0\}.$$

设(n,k)线性码L有生成矩阵G和校验矩阵H．已知$\alpha \in L$当且仅当$H \cdot \alpha^T = \theta$，若$H$的$n$个列向量为$\alpha_1,\cdots\alpha_n$而$\alpha = (a_1,\cdots,a_n)$，则$H \cdot \alpha^T = \theta$．即是

$$a_1\alpha_1 + a_2\alpha_2 + \cdots + a_n\alpha_n = \theta.$$

如果列向量$\alpha_1,\cdots\alpha_n$的秩是s，则a_i中非零个数就一定大于s，即$W(\alpha) > s$；并且存在

$$\beta = (\underbrace{1,1,\cdots,1}_{s+1个},0,\cdots,0) \in L,$$

即$W(\beta) = s+1$，于是$\rho(L,L) = s+1$．这样，我们就知道了选取的码有多大的纠错能力来解决问题 C.

以上只是很浅地介绍了编码理论的部分内容；编码理论是现代通讯理论于基础数学高度结合的一个领域，是代数学一个直接而深刻的应用．进一步的讨论还将涉及有限域上的代数几何等．应该说，编码理论已成为“数学技术”的一个组成部分．有兴趣的读者可以参看相应的参考书.

习题

1．设$a \in F$，证明a是F上的一个代数元，并且$F(a) = F$．

2．对于任意给定域F以及F上一元多项式环$F[x]$中的不可约多项式

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

总存在F的单代数扩域$F(\alpha)$，其中α在F上的最小多项式是$p(\alpha)$．

3．令Q为有理数域，求复数i和$\dfrac{2i+1}{i-1}$在Q上的最小多项式？

$Q(i)$与$Q(\dfrac{2i+1}{i-1})$是否同构？

4． 若K是F的扩域，$[K:F] = p$， p是素数．证明：不存在K的子域T，满足$F \subset T \subset K$．

5．若E是F的代数扩域，a是E上的一个代数元，证明：a是F上的一个代数元.

6．若E是F的代数扩域，， $a \in E$，则存在$f(x) \in F[x]$，使得

$a^{-1}=f(a)$.

7．设三个域满足：$F\subset I\subset E$．假定$(I:F)=m$．E的元α在F上的次数是n，并且$(m,n)=1$,证明：α在I上的次数也是n.

8．设θ是$F[x]$中n次既约多项式$f(x)$的一个根，证明：$F[\theta]$是F上有限扩域.

9．证明：Q为有理数域，$Q(\sqrt{-1})$和$Q(\sqrt{2})$不同构.

10．设F是特征为p的域，$f(x)$是$F[x]$中既约多项式，证明：$f(x)$在F的扩域E中有重根的充要条件是$f(x)$可表成x^p的多项式.

11．令E是有理数域，x^3-a是F上的既约多项式，而t是x^3-a的一个根．证明：$E(t)$不是x^3-a在F上的分裂域.

12．设$f(x)$是$F[x]$中任意n次多项式$(n>0)$，证明：$f(x)$的分裂域E对于F的次数$[E:F]\le n!$.

13．求$\sqrt{3}+\sqrt{5}$在有理数域Q上一个极小多项式及其分裂域.

14．令$F=GF(p^n)$，证明：对于n的每一个正因子m，有且仅有一个F的子域$GF(p^m)$.

15．证明：一个有限域一定有真代数扩域.

16．证明：有限域$F=GF(p^n)$的乘群$(F^*,\circ)$是p^n-1阶的循环群.

17．证明：4元域不能同构于一个8元域的子域.

18．Δ是特征为2的素域，求$\Delta[x]$上所有3次既约多项式.

19．求特征是2的素域Δ上既约多项式$f(x)$，使得$GF(8)$是$f(x)$在Δ上的分裂域.

20．在F^4上设计校验矩阵，给出一个尽量好的线性码.