5 有限域的结构

5.1 有限域的定义与构造,域扩张

域：F被称为一个域*(field)*，如果F是一个有单位元$1(\neq 0)$的交换环，并且它的每一个非零元都可逆.域F有两个代数运算：加法和乘法，F关于加法构成**Abel**群，F的所有非零元组成的集合F^*关于乘法也构成**Abel**群，并且适合乘法对于加法的分配律.

有理数域Q，实数域R，复数域C都是域，当**p**为素数时，模**p**的剩余类环Z_p也是一个域，称为模**p**的剩余类域.一个域中若只有有限个元素，则称它为*有限域(finite field)*或*Galois域(galois field)*.

子域与扩域：设F是域，K是F的子集，如果K在F的运算下也构成一个域，则称K为F的*子域(subfield)*，F为K的*扩域(extension field)*或*域扩张(field extension)*，记作K/F，特别的如果$K\neq F$则称K为F的*真子域*，K的包含F的任一子域称为K/F的*中间域(intermediate field)*.

域的特征：设F是域，如果存在正整数**n**使得对任何$r\in R, n\cdot r=0$，但对于任何小于**n**的正整数$n', n'\cdot r\neq 0$，则称**n**为域F的特征，否则称域F的特征为**0**.域F的特征记作$char(F)$.

素域：一个域如果不包含任何真子域，则称为*素域*.如果一个域F的子域作为域是素域，则称该子域为F的*素子域*.任意多个子域的交仍然是子域，可以证明一个域的素子域实际上就是该域的所有子域的交.

有理数域**Q**和阶为素数**p**的**Galois**域F_p都是素域.一个域F的素子域在特征为**p**时同构于阶为**p**的**Galois**域F_p，在特征为**0**时同构于有理数域**Q**.

有限域的构造：由3.4我们已经知道，R是一个有单位元的交换环，$M\subseteq R$是R的一个理想，则M是R的极大理想当且仅当R/M是域.利用这条性质，我们可以从小的有限域出发构造大的有限域.

定理：设F_q是含有q个元素的有限域，其中$q=p^r, p$为素数.如果$m(x)=a_0+a_1x+\cdots+a_nx^n$是$F_q[x]$的**n**次不可约多项式，则$F_q[x]/(m(x))$是含有$q^n$个元素的有限域，并且它的每一个元素可以唯一地表示成$c_0+c_1x+\cdots+c_{n-1}x^{n-1}$，其中$c_i\in F_q, 0\leq i<n, u=x+(m(x)), u$满足$a_0+a_1u+\cdots+a_nu^n=0$.

证明：由于$m(x)$是$F_q[x]$的**n**次不可约多项式，因此$(m(x))$是$F_q[x]$的一个极大理想.根据上面的结论有$F_q[x]/(m(x))$是一个域，由$m(x)=a_0+a_1x+\cdots+a_nx^n$是$F_q[x]$的**n**次不可约多项式，$F_q[x]/(m(x))$中的元素形如$c_0+c_1x+\cdots+c_{n-1}x^{n-1}+(m(x))$，(由带余除法得到)，则由带余除法的过程知这种表示是唯一的，且$c_i\in F_q, 0\leq i<n$，因此每个c_i都有q种选取方式，从而$|F_q[x]/(m(x))|=q^n$，$F_q[x]/(m(x))$是一个含q^n个元素的有限域.

令$u=x+(m(x))$，作单同态$\sigma: F_q\to F_q[x]/(m(x)), a\longmapsto a+(m(x))$可以将$a$与$a+(m(x))$等同，从而有$c_0+c_1x+\cdots+c_{n-1}x^{n-1}+(m(x))=[c_0+(m(x))]+[c_1+(m(x))][x+(m(x))]+\cdots+[c_{n-1}+(m(x))][x+(m(x))]^{n-1}=c_0+c_1u+\cdots+c_{n-1}u^{n-1}$.因此$F_q[x]/(m(x))$中的元素可以唯一地表示成$c_0+c_1x+\cdots+c_{n-1}x^{n-1}$，其中$c_i\in F_q, 0\leq i<n, u=x+(m(x))$，因为$a_0+a_1u+\cdots a_nu^n=a_0+a_1x+\cdots a_nx^n+(m(x))=(m(x))$故在商环$F_q[x]/(m(x))$中有$a_0+a_1u+\cdots+a_nu^n=0$.

可以证明：有限域F的元素个数**q**一定是一个素数**p**的方幂，其中**p**是域F的特征.这个定理给出了从**q**元有限域F_q出发构造出q^n元有限域的方法：首先在$F_q[x]$中找到一个**n**次不可约多项式$m(x)$，然后作商环$F_q[x]/(m(x))$，即为一个q^n元的有限域，且每个元素可以唯一的表示，我们尝试将这样的方法推广到任何一个域F.

例如，对于实数域**R**，在**R**[**x**]中取**2**次不可约多项式$m(x) = x^2 + 1$，作商环$R[x]/(x^2 + 1)$，则它是一个域且$R[x]/(x^2 + 1) = \{a + bu|a, b \in R\}$，其中$u = x + (x^2 + 1)$满足$u^2 + 1 = 0$，可以构建$R[x]/(x^2 + 1)$到**C** 的映射$\sigma, \sigma(a + bu) = a + bi$，容易验证$\sigma$是一个环同构.虽然R中不存在$\sqrt{-1}$，但是在域$R[x]/(x^2 + 1)$中有$u^2 = -1$从而$u = \sqrt{-1}$，这里将$-1$与$-1 + (x^2 + 1)$等同.

域扩张：K是F的子域，M是F的任何子集.$K(M)$定义为F中所有含有M和K的子域的交，称为添加M中的元素得到的K的*扩域/扩张*.显然$K(M)$是含有K和M的最小的子域.当$M = \{\alpha_1, \alpha_2, \cdots, \alpha_n\}$时，我们记$K(M) = K(\alpha_1, \alpha_2, \alpha_n)$.特别地称$K(\alpha)$为*单扩域/单扩张*，$\alpha$称为$K(\alpha)$在$K$上的定义元，有$F(\alpha) = F[\alpha]$.

代数扩张：设K是域F的一个子域，$\alpha \in F$，如果α满足K上的一个非零多项式，则称α是K上的*代数元*，不是代数元的元素称为*超越元*.如果一个扩张K/F，K的每一个元素都是F上的代数元，则称域扩张K/F是*代数扩张(algebraic extension)*

有限扩张：设K/F是一个域扩张，则K可以看成是域F上的一个线性空间，它的加法运算是域K中的加法，它的纯量乘法运算是域F的元素与K的元素作K中的乘法运算.K作为域F上的线性空间的维数称为K在F上的*次数(degree of K over F)*，记作$[K : F]$.如果$[K : F]$是有限的，则称K是F上的*有限扩张(finite extension)*，此时K作为F上的线性空间的一个基也叫做域扩张K/F的一个*基(basis)*.

K/F是有限扩张，则K的每个元素都是F上的代数元.进而有限扩张一定是代数扩张.

K/F是域扩张，$\alpha \in K$且α是F上的代数元.如果α在F上的极小多项式$m(x)$的次数为**n**，则$[F(\alpha) : F] = n$，且$1, \alpha, \alpha^2 \cdots \alpha^{n-1}$是$F(\alpha)/F$的一组基.

设有三个域$F \subseteq L \subseteq K$，则$[K : F]$有限当且仅当$[K : L]$和$[L : F]$都有限，此时有$[K : F] = [K : L][L : F]$.

分裂域：$f(x)$是域F上的一个$n(\geq 1)$次多项式，域扩张E/F称为$f(x)$在F上的一个*分裂域(splitting field)*，如果满足：

(1)$f(x)$在$E[x]$中完全分解成一次因式的乘积$f(x) = c(x - \alpha_1)(x - \alpha_2) \cdots (x - \alpha_n), \alpha_i \in E, 1 \leq i \leq n;$

(2)$E = F(\alpha_1, \alpha_2, \cdots \alpha_n)$.

设$f(x)$是域F上的多项式，$n = deg(f(x)) \geq 1$.那么$f(x)$的分裂域一定存在，且$[E : F] \leq n!$

5.2 有限域的特征性质