本节讨论有限域的结构和性质，主要结论有：

有限域的阶是其特征的方幂，

有限域的乘法群是循环群，

有限域是其素子域的单代数扩张，

有限域的有限扩张是单代数扩张，

设 F 是域，若 F 是有限域，即$|F|<\infty$，则 F 的特征一定是素数，

设 Char $F=p>0$，则 F 包含 $Z_p$，进而，F 是 $Z_p$ 上的有限维向量空间，

若设$|F:Z_p|=n$，则域 F 所含的元素个数为 $p^n$，即有限域的阶是其特征的方幂

**定理 5.1** 对任意素数 p 和正整数 n，在同构意义下存在唯一的 $p^n$ 阶有限域

**证:** 首先，$f(x)=x^{p^n}-x$ 在 Z 上的分裂域 E 就是一个 $p^n$ 阶有限域，

设 F 是 f(x)在 E 中所有根的集合，则对属于 F 的任意 a，b，

我们有$(a-b)^{p^n}=a^{p^n}-b^{p^n}=a-b$，$(ab^{-1})^{p^n}=a^{p^n}(b^{p^n})^{-1}=ab^{-1}$

即 $a-b$，$ab^{-1}$ 属于 F，因而 F 是 E 的子域，

又因为 f(x)无重根($f'(x)=-1$)，所以 F 的阶为 $p^n$

若 c 属于 $Z_p$ 则 $c=c^p$，从而 $c=c^{p^n}$，即 c 属于 F，从而 $E=Z_p(F)\subseteq F\subseteq E$，即 E=F

其次，$p^n$ 阶域是唯一的，

设 F 是任意一个 $p^n$ 阶域，则 $F-\{0\}$是 $p^n-1$ 阶乘法群，

所以对属于 $F-\{0\}$的任意 a，有$a^{p^n-1}=1$，从而对属于 F 的任意 a，有$a^{p^n}=a$，

即 F 中的元素都是属于 Z[x]的 $f(x)=x^{p^n}-x$ 的根，

所以 F 恰是 f(x)在 $Z_p$ 上的分裂域，

由分裂域的唯一性可知，$p^n$ 阶有限域是唯一的

因为对每个 $p^n$，在同构意义下仅存在一个 $p^n$ 阶域，

所以我们将其记为 $GF(p^n)$，并称其为 $p^n$ 阶伽罗瓦域

**定理 5.2** $GF(p^n)$的所有子域形式为 $GF(p^m)$，其中 $m|n$，

**证:** 设 $GF(p^m)$是 $GF(p^n)$的子域，若$|GF(p^n):GF(p^m)|=t$，则 $p^n=(p^m)^t$，即 $m|n$

若 $m|n$，设 $n=mt$，则 $g(x)=x^{p^m}-x$ 的根都是 $f(x)=x^{p^n}-x$ 的根，

若令 $f(x)$和 $g(x)$的根的集合分别为 E 和 F，则 E 和 F 分别是 $p^n$ 阶和 $p^m$ 阶有限域且 F 包含于 E，即 $p^n$ 阶域有 $p^m$ 阶子域

由上面的讨论可知，有限域的结构与多项式$x^{p^n}-x$ 的根有着非常密切的关系，

而 0 是$x^{p^n}-x$ 的根，所以，实际上有限域的结构与多项式$a^{p^n-1}-1$ 的根密切相关

为此，我们有必要对多项式 $x^n-1$ 的根组成的代数系统进行更详细的讨论，

**定义 5.1** 设 F 是素域，n 属于 $Z^+$，属于 F[x]的多项式 $x^n-1$ 在 F 上的分裂域为 E

称 $x^n-1$ 在 E 中的根为 F 上的 n 次单位根，并称 E 为 F 上的 n 次单位根域

当 Char F=p，且 $p|n$ 时，若令 $n=p^sk$，$(p,k)=1$，则 $x^n-1=x^{p^sk}-1=(x^k-1)^{p^s}$

这表明 $x^n-1$ 与 $x^k-1$ 在 F 上的分裂域相同，

因此，当 Char F=p 时，我们总假定对于多项式 $x^n-1$，有$(p,n)=1$，

**命题 5.1** 设 F 是素域 ，若 Char F=p＞0 且(n , p)=1 ,

则 F 上的 n 次单位根关于域的乘法运算构成 n 阶循环群 ，

**证:** 设 $f(x)=x^n-1$ 属于 F[x]

因为 $f'(x)=nx^{n-1}$ , $(f'(x) , f(x))=1$ ,

所以 f(x)无重根 ，即 F 上有 n 个不同的 n 次单位根 ，

设这 n 个根构成集合 E，知 E 是 f(x)在 F 上的分裂域的乘法交换子群

下面再证明 E 是循环群即可 ，

不妨设 n＞1 且 $n=p_1^{r_1}p_2^{r_2}\cdots p_s^{r_s}$

其中 $p_i$ 是互不相同的素数 , $r_i$ 是正整数 , $i=1 , 2 , \cdots , s$ ,

因为多项式 $f_i(x)=x^{\frac{n}{p_i}}-1$ 在其分裂域中最多有$\frac{p}{p_i}$个根 ，

因为$\frac{n}{p_i}<n$，所以存在属于 E 的$\alpha_i$，使$\alpha_i^{\frac{n}{p_i}}\neq 1$ 成立 ，

记$\alpha_i^{\frac{n}{p_i^{r_i}}}=\beta_i$，则$\beta_i^{p_i^{r_i}}=1$，从而$\beta_i$ 的阶为$p_i^{r_i}$ ，

否则若$\beta_i^{p_i^{t_i}}=1 , t_i<r_i$，则$\alpha_i^{\frac{n}{p_i}}=\left(\alpha_i^{\frac{n}{p_i^{r_i}}}\right)^{p_i^{r_i-1}}=\beta_i^{p_i^{r_i-1}}=\left(\beta_i^{p_i^{t_i}}\right)^{p_i^{r_i-1-t_i}}=1$

这与$\alpha_i^{\frac{n}{p_i}}\neq 1$ 相矛盾 ，所以$\beta_i$ 的阶为$p_i^{r_i}$

若令 $u=\prod_{i=1}^{s}\beta_i$ , 则根据第二章推论 5.2(3)可知, u 的阶为 n,

所以 E 是 n 阶循环群 ，

既然域 F 上的 n 次单位根关于域的乘法运算构成 n 阶循环群 ，

则该群中必含有阶为 n 的元素 ，

**定义 5.2** 设 F 是素域，称 F 上阶为 n 的 n 次单位根为 F 上的本原 n 次单位根

**推论 5.1** 设 F 是素域，

若 Char F=p＞0，(n，p)=1，则存在 F 上的本原 n 次单位根

**推论 5.2** 有限域的乘法群是循环群，有限域是其素子域的单代数扩张，

**证:** 设 F 是 $p^n$ 阶域，则 F 由属于 $Z_p[x]$的$x^{p^n}-x$ 的全部根组成，

进而属于 $Z_p[x]$的$x^{p^n-1}-1$ 的所有根的集合是 F 的乘法群，

由命题 5.1 可知，该群为循环群，

若 a 是该群的生成元，

则 $F=\{0,\alpha,\alpha^2,\cdots,\alpha^{p^n-1}\}=Z_p(\alpha)$，即有限域是其素子域的单代数扩张，

**推论 5.3** 有限域的有限扩张是单代数扩张

**证:** 设 F 是有限域，包含 F 的 E 是有限扩张，

因为包含 $Z_p$ 的 F 是有限扩张，所以包含 $Z_p$ 的 E 是有限扩张，即 E 是有限域，

从而，包含 $Z_p$ 的 E 是单代数扩张，

若设 $E=Z_p(\alpha)$，其中α是 $Z_p$ 上的代数元，则 $E=F(\alpha)$，α是 F 上的代数元

**例 5.1** 设 $F=GF(3^6)$，α是 F 的乘法群的一个生成元，

求 F 的所有子域及每个子域的乘法群的一个生成元，

**解:** 由定理 5.2 可知，F 的子域形式为 $GF(3^k)$，k=1，2，3，6，

因为子域 $GF(3^k)$的乘法群是 F 的乘法群的子群，而α是 F 的乘法群的生成元

所以可设$\alpha^i$是 $GF(3^k)$的乘法群的生成元，

根据第二章推论 5.2(1)可取 $i=\frac{3^6-1}{3^k-1}$

故子域 $GF(3)$，$GF(3^2)$，$GF(3^3)$，$GF(3^6)$的乘法群的生成元依次为$\alpha^{364}$，$\alpha^{91}$，$\alpha^{28}$，α

**例 5.2** 求属于 $Z_3[x]$的多项式 $f(x)=x^9-x$ 在 $Z_3$ 上的分裂域 E，

**解:** 由定理 5.1 的证明可知，E 是 $f(x)$所有根的集合，且$|E|=9$，

显然，$x^2+1$ 是 $Z_3[x]$中的不可约元，

因为 i 是 $x^2+1$ 的根，所以$|Z_3(i):Z_3|=2$，$|Z_3(i)|=3^2=9$，

因为 $f(i)=0$，所以 i 属于 E，因此，$Z_3(i)$包含于 E，

又由$|Z_3(i)|=|E|$可知 $Z_3(i)=E$，

注意，在上例中，尽管 $Z_3(i)=E$，但是 i 不是 E 的乘法群的生成元，

由定理 5.1 可知

$p^n$ 阶域可以通过求属于 $Z[x]$的多项式 $f(x)=x^{p^n}-x$ 在 $Z_p$ 上的分裂域得到，

例 5.2 启发我们可以用另外一种方式构造有限域

即在 $Z_p[x]$中找出一个 n 次不可约元及其一个根，

将这个根添加到 $Z_p$ 中即可得到 $p^n$ 阶域，

**例 5.3** 构造一个 8 阶有限域，

**解:** 因为 $8=2^3$，所以需要找一个 $Z_2[x]$中的 3 次不可约元，

易知，$g(x)=x^3+x^2+1$ 是 $Z_2[x]$中的一个不可约元，

令$\alpha$是 $g(x)$的一个根，则 $Z_2(\alpha)$为 8 阶有限域，

$Z_2(\alpha)=\{0,1,\alpha,\alpha+1,\alpha^2,\alpha^2+1,\alpha^2+\alpha,\alpha^2+\alpha+1\}$，