设包含 F 的 E 是域的扩张，

我们可以通过在 F 中逐渐添加“独立”元素的方式来了解 E 的结构，

因此，我们有必要先了解添加一个元素α的单扩张 $F(\alpha)$的结构，

定义 2.1 设 F 是一个域，

称在 F 上添加一个元素α得到的扩域 $F(\alpha)$是域 F 的单扩张

若α是 F 上的代数元，则称包含 F 的 $F(\alpha)$是单代数扩张，

若α是 F 上的超越元，则称包含 F 的 $F(\alpha)$是单超越扩张，

可以证明，包含 Q 的 $Q(\sqrt{2})$是单代数扩张，包含 Q 的 $Q(\pi)$是单超越扩张，

下面我们来描述单代数扩张的结构，

定理 2.1 设α是域 F 上的 n 次代数元，f(x)是α在 F 上的极小多项式，

记 $F[\alpha]=\{g(\alpha)|g(x)\in F[x]\}$，那么

(1)$F(\alpha)=F[\alpha]$

(2)$F(\alpha)\cong F[x]/\langle f(x)\rangle$

(3)$|F(\alpha):F|=n$，且 $1,\alpha,\cdots,\alpha^{n-1}$ 是包含 F 的扩张 $F(\alpha)$的一组基底，

证: (1)显然，有 $F[\alpha]$包含于 $F(\alpha)$，

反之，考虑 $F(\alpha)$中的任意元素 $\frac{g(\alpha)}{h(\alpha)}$，其中 $h(\alpha)$不为 0，

因为 f(x)是不可约元，所以$(f(x),h(x))=1$ 或 $f(x)|h(x)$，

而α不是 h(x)的根，因此只能有$(f(x),h(x))=1$，

进而存在属于 F[x]的 u(x)，v(x)，使得 $f(x)u(x)+h(x)v(x)=1$，

令 $x=\alpha$，代入得 $1=f(\alpha)u(\alpha)+h(\alpha)v(\alpha)=h(\alpha)v(\alpha)$，

因此，$\frac{g(\alpha)}{h(\alpha)}=\frac{g(\alpha)v(\alpha)}{h(\alpha)v(\alpha)}=g(\alpha)v(\alpha)$属于 $F[\alpha]$，即 $F[\alpha]$包含 $F(\alpha)$，所以 $F(\alpha)=F[\alpha]$

(2)由 $F(\alpha)=F[\alpha]$，易知$\varphi: F[x]\to F(\alpha)$，$g(x)\to g(\alpha)$是环的满同态，

再由环同态基本定理得 $F[x]/\mathrm{Ker}\varphi\cong F(\alpha)$，

又由本章定理 1.3(2)有 $\mathrm{Ker}\varphi=\langle f(x)\rangle$，所以，$F[x]/\langle f(x)\rangle\cong F(\alpha)$，

(3)首先，指出 $1,\alpha,\cdots,\alpha^{n-1}$ 在 F 上线性无关，

如若不然，则存在 F 中不全为 0 的元素 $a_0,a_1,\cdots,a_{n-1}$，

使得 $a_0+a_1\alpha+\cdots+a_{n-1}\alpha^{n-1}=0$，

即存在一个以α为根的 F[x]中的非零多项式 $a_0+a_1\alpha+\cdots+a_{n-1}\alpha^{n-1}$

但是这与α是域 F 上的 n 次代数元相矛盾，因此，$1,\alpha,\cdots,\alpha^{n-1}$ 在 F 上线性无关

其次，指出 $F(x)$中任意一个元素可以由 $1,\alpha,\cdots,\alpha^{n-1}$ 表示，

令 $g(\alpha)$属于 $F[\alpha]=F(\alpha)$，由带余除法可知存在属于 F[x]的 q(x)，r(x)

使得 $g(x)=f(x)q(x)+r(x)$，$r(x)=0$ 或 $\deg r(x)<\deg f(x)$

令 $x=\alpha$，代入上式得 $g(\alpha)=r(\alpha)$，即 $g(\alpha)$可由 $1,\alpha,\cdots,\alpha^{n-1}$ 表示，

综上，$1,\alpha,\cdots,\alpha^{n-1}$ 是包含 F 的扩张 $F(x)$的一组基底，从而$|F(\alpha):F|=n$，

若 f(x)是α在域 F 上的极小多项式，则有单代数扩张 F(α)包含 F

若β是 f(x)的另一个根，则又有单代数扩张 F(β)包含 F

那么这两个扩张之间有什么关系呢?

为了回答这个问题，我们给出如下符号，

设φ是域 F 到域$\overline{F}$的域同构，

对属于 F[x]的任意多项式 $f(x)=a_nx^n+\cdots+a_1x+a_0$

记 $f^{\varphi}(x)=\varphi(a_n)x^n+\cdots+\varphi(a_1)x+\varphi(a_0)$，

易知，当且仅当 $f^{\varphi}(x)=f_1^{\varphi}(x)f_2^{\varphi}(x)\cdots f_t^{\varphi}(x)$时，$f(x)=f_1(x)f_2(x)\cdots f_t(x)$

当且仅当 f(x)是 F[x]中的不可约元时，f(x)是 F[x]中的不可约元

定理 2.2 设φ是 F 到$\overline{F}$的域同构，

若α是 F[x]中不可约元 f(x)的一个根，β是 $f^{\varphi}(x)$的一个根，

则存在 F(α)到$\overline{F}(\beta)$的域同构τ，使得$\tau(\alpha)=\beta$，$\tau|_F=\varphi$，

证: 设 deg f(x) = n，则

F(α)中任意元素可以唯一地表示成 $\sum_{i=0}^{n-1}a_i\alpha^i$ 的形式, 其中a_i属于 F

$\overline{F}(\beta)$中任意元素可以唯一地表示成 $\sum_{i=0}^{n-1}b_i\beta^i$ 的形式, 其中b_i属于$\overline{F}$

那么易证$\tau: F(\alpha)\to\overline{F}(\beta), \sum_{i=0}^{n-1}a_i\alpha^i\to\sum_{i=0}^{n-1}b_i\beta^i$ 是域同构

且τ在 F 上的限制恰为φ，$\tau(\alpha)=\beta$，

在上述定理中，若令$\overline{F}=F$，$\varphi=id_F$，则我们有下列推论

推论 2.1 设 F 是域，$f(x)$是 $F[x]$中的不可约元，

若α和β是 $f(x)$在 F 的某个扩域中的根，

则存在 $F(\alpha)$到 $F(\beta)$的域同构τ，使得$\tau(\alpha)=\beta$，$\tau|_F=id_F$

至此，我们知道单代数扩张与极小多项式的根的选取无关，

并且它的结构也可以确定，

下面我们来探讨单超越扩张的结构，

设 x 是域 F 的未定元，则由未定元的定义可知，x 一定是 F 上的超越元，

则单超越扩张 $F(x)$恰是一元多项式环 $F[x]$的分式域

$$\left\{\frac{f(x)}{g(x)}\middle|\, f(x), g(x)\in F[x], g(x)\neq 0\right\}$$

也就是说，任意一个域都有单超越扩张，

定理 2.3 设α是域 F 上的超越元，x 是 F 的未定元，则 $F(x)\cong F(\alpha)$，

证: 映射$\varphi: F(x)\to F(\alpha)$，$\frac{f(x)}{g(x)}\to\frac{f(\alpha)}{g(\alpha)}$是环的满同态,下面指出$\varphi$是单射

如果$\varphi\left(\frac{f(x)}{g(x)}\right)=\frac{f(\alpha)}{g(\alpha)}=0$，则 $f(\alpha)=0$，又若 $f(x)$不为 0，则α是域 F 上的代数元，矛盾

因此，$f(x)=0$，$\frac{f(x)}{g(x)}=0$，即φ是单射，所以 $F(x)\cong F(\alpha)$，

由定理 2.3 可知，在同构意义下，域 F 的单超越扩张是唯一的，

即为 $F[x]$的分式域 $F(x)$，

例 2.1 设α是 Q[x]中不可约元 $f(x)=x^2-x+2$ 的根 ，

试将 Q(α)中的非零元 $2\alpha^3+4\alpha+1$ 用包含 Q 的扩张 Q(α)的一组基底表示 ，

并求 $2\alpha^3+4\alpha+1$ 的逆元 ，

解: 由本章定理 1.4 可知 ，f(x)是α在 Q 上的极小多项式 ，

则 1 , α是包含 Q 的扩张 Q(α)的基底 ，

令 $g(x)=2x^3+4x+1$, 则由带余除法可知 , $g(x)=f(x)(2x+2)+2x-3$,

那么 $g(\alpha)=2\alpha^3+4\alpha+1=2\alpha-3$,

因为 g(α)不为 0 , 即α不是 g(x)的根 ，所以 f(x)∤g(x) ,

再由 f(x)是不可约元知(f(x) , g(x))=1 ,

从而 ，根据辗转相除法可得 $\frac{4x^2+6x+6}{11}f(x)+\frac{-2x-1}{11}g(x)=1$

令 x=α , 代入上式得$\frac{-2\alpha-1}{11}g(\alpha)=1$, 即 $2\alpha^3+4\alpha+1$ 的逆元为$\frac{-2\alpha-1}{11}$

例 2.2 设α是属于 $Z_2[x]$的多项式 $f(x)=x^2+x+\overline{1}$的一个根 ，

试将 $Z_2(\alpha)$中每个元素用包含 Z_2 的扩张 $Z_2(\alpha)$的一组基底表示出来 ，

并求 $Z_2(\alpha)$中每个元素在 Z_2 上的极小多项式 ，

解: 首先 ，由于 $f(\overline{0})=\overline{1}\neq\overline{0}$, $f(\overline{1})=\overline{1}\neq\overline{0}$ ，

所以 $f(x)=x^2+x+1$ 是 Z[x]中的不可约元

从而 , f(x)是α在 Z_2 上的极小多项式 ，

那么 1 , α是包含 Z_2 的扩张 $Z_2(\alpha)$的一组基底 ，

即 $Z_2(\alpha)$中的元素均可以唯一地写成 a+bα , a , b 属于 Z_2 的形式 ，

但是 Z_2 中只有两个元素 ，且$\alpha\neq\alpha+\overline{1}$ ，所以 $Z_2(\alpha)=\{\overline{0}$ ，$\overline{1}$, α , $\alpha+\overline{1}\}$,

另外 ，我们容易验证 $f(\alpha+\overline{1})=(\alpha+\overline{1})+(\alpha+\overline{1})+\overline{1}=\overline{0}$

所以 , $f(x)=x^2+x+\overline{1}$是α和$\alpha+\overline{1}$的极小多项式 ，

另外 ，以$\overline{0}$为根、次数最低的多项式为 x，以$\overline{1}$为根、次数最低的多项式为 $x-\overline{1}$ ，

所以 ，$\overline{0}$ ，$\overline{1}$的极小多项式分别为 x 和 $x-\overline{1}$