所谓域的扩张是指，若域 E 是域 F 的扩域，则称 E 是 F 的扩张，记为 $E \supseteq F$

本节我们将首先讨论如何通过添加元素的方式得到域的扩张;

其次将添加的元素分为代数元和超越元两类，并初步研究它们的一些性质;

最后从向量空间出发，讨论域的扩张次数，

一、域的扩张的构造

我们知道，域按照特征可以分为两类:

一类是特征为零的域，一类是特征为素数的域，

我们比较熟悉的有理数域 Q 是特征为零的域，

剩余类环 Z_p(p 为素数)是特征为素数 p 的域，

我们将指出，任意一个域都可以看做是 Q 或 Z_p 的扩域，

因此可以通过域的扩张来研究域，

我们采用的域的扩张的构造方式就是在已知的域上添加元素

定义 1.1 除自身外不再含有其他子域的域称为素域，

显然，Q 和 Z_p 都是素域，

定理 1.1 设 F 是域，若 Char F=p(p 是素数)，则 F 包含一个同构于 Z_p 的子域

若 Char F=0，则 F 包含一个同构于 Q 的子域，

证: 我们先来构造一个整数环 Z 到域 F 的环同态

$\varphi: Z \to F, n \to n \cdot 1$，其中 1 是 F 的单位元，

根据环同态基本定理可知 $Z/\mathrm{Ker}\,\varphi = \mathrm{Im}\,\varphi$，

另外，$\mathrm{Ker}\,\varphi = \{n \in Z | n \cdot 1 = 0\} = \langle \mathrm{char}\ F \rangle$，

当 Char F=p 时，有 $Z_p = Z/\langle p \rangle \cong \mathrm{Im}\,\varphi$，即 F 包含一个同构于 Z_p 的子域，

当 Char F=0 时，有 $Z \cong \mathrm{Im}\,\varphi$，即 F 包含一个同构于 Z 的子环，

再根据第三章定理 6.2 可知，F 包含一个同构于 Q 的子域，

推论 1.1 设 F 是素域，若 Char F=p(素数)，则 $F\cong Z_p$，若 Char F=0，则 $F\cong Q$，

上面的论述说明，特征为零的域是 Q 的扩域，特征为素数 p 的域是 Z_p 的扩域

因此，任何一个域都可以看做是某个已知域的扩域，

下面我们来构造一个已知域的扩域，

设 E 是已知域 F 的扩域，S 是 E 的非空子集，

则 E 中总有包含 F 和 S 的子域，例如 E 本身，

包含 F 和 S 的 E 的所有子域的交，仍然是 E 的子域，

若用 F(S)表示这个域，则 F(S)是包含 F 和 S 的 E 的最小子域，

关于域 F(S)的具体结构，我们有

$F(S)=\{\frac{f(s_1,s_2,\cdots s_m)}{g(s_1,s_2,\cdots s_m)} \mid g(x_1,x_2,\cdots,x_m), f(x_1,x_2,\cdots,x_m)\in F[x_1,x_2,\cdots,x_m],$

$g(s_1,s_2,\cdots s_m)\neq 0,\ s_1,s_2,\cdots s_m\in S, m\in Z^*\}$,

事实上，若令上式的右端为$\overline{F}$，则显然有，$\overline{F}$是 F(S)的子集，即$\overline{F}$包含于 F(S)，

再由子域的判别定理可知，$\overline{F}$是 E 的子域，且$\overline{F}$包含 F 和 S，

那么根据 F(S)的定义有 F(S)包含于$\overline{F}$，因此，$F(S)=\overline{F}$，

若 $S=\{\alpha_1,\alpha_2,\cdots,\alpha_n\}$，则记 F(S)为 $F(\alpha_1,\alpha_2,\cdots,\alpha_n)$，

特别地，我们有 $F(\alpha)=\{\frac{f(\alpha)}{g(\alpha)} \mid f(x), g(x)\in F(x), g(\alpha)\neq 0\}$，

定理 1.2 设 E 是 F 的一个扩域，A 和 B 是 E 的两个非空子集合，

则 F(AUB)=F(A)(B)=F(B)(A)，

证: 因为 AUB=BUA，所以，只需证明 F(AUB)=F(A)(B)，

因为 F(A)(B)是域，且当然包含 F，A 和 B，所以包含 F 和 AUB，

又由于 F(AUB)是包含 F 和 AUB 的最小域，所以 F(AUB)包含于 F(A)(B)，

反之，由于 F(A)(B)是包含 F(A)和 B 的最小域，

而 F(AUB)是域，并且包含 F，A 和 B，

所以 F(AUB)包含 F(A)和 B，于是 F(AUB)包含 F(A)(B)，F(AUB)=F(A)(B)

定理 1.2 说明域的扩张与添加元素的次序无关，

特别地，根据定理 1.2，我们有 $F(\alpha_1,\alpha_2,\cdots,\alpha_n)=F(\alpha_1)(\alpha_2)\cdots(\alpha_n)$，

因此，在域的扩张当中，最重要的是添加一个元素的包含 F 的单扩张 $F(\alpha)$

在下一节中我们将重点研究单扩张的结构，

二、代数元、超越元与极小多项式

尽管域的扩张与添加元素的次序无关，但是与添加元素的性质有关，

我们将添加的元素分为如下两类，

定义 1.2 设 E 是域 F 的扩张，对于属于 E 的α，

若存在一个属于 F[x]的非零多项式 $f(x)$，使得 $f(\alpha)=0$，

则称α是 F 上的代数元，否则称α是 F 上的超越元，

有理数域上的代数元称为代数数，超越元称为超越数，

法国数学家埃尔米特证明了 e 是超越数，

德国数学家林德曼证明了π是超越数，

定义 1.3 如果α是域 F 上的代数元，

则称 F[x]中以α为根、次数最低、首项系数为 1 的非零多项式

为α在 F 上的极小多项式，

若α是域 F 上的代数元，则在 F 上必有以α为根的多项式，

特别地，

在以α为根的多项式中一定可以找到次数最低、首项系数为 1 的多项式，

因此，代数元一定有极小多项式，

关于极小多项式我们有如下性质:

定理 1.3 设 f(x)是α在域 F 上的一个极小多项式，则

(1)f(x)是 F[x]中的不可约元，

(2)当且仅当 f(x)|g(x)时，g(x)是 F[x]中以α为根的多项式，

(3)α在 F 上的极小多项式是唯一的，

证: (1) 设 g(x)是 f(x)的因子，则存在属于 F[x]的 h(x)，使得 f(x)=g(x)h(x)，

因为 f(α)=0，所以 g(α)h(α)=0，

由于 g(α)，h(α)属于 F(α)，所以 g(α)=0 或 h(α)=0，

若 g(α)=0，则根据 f(x)的取法可知，deg g(x)=deg f(x)，

从而，h(x)属于 F−{0}，即 g(x)~f(x)，

若 h(α)=0，同理可得，g(x)属于 F−{0}，即 g(x)是可逆元，

也就是说，f(x)只有平凡因子，从而 f(x)是不可约元，

(2) 由(1)知 f(x)是 F[x]中的不可约元，

因此，对 F[x]中任意多项式 g(x)有 f(x)|g(x)或(f(x)，g(x))=1，

若 g(x)是 F[x]中以α为根的多项式，则必有 f(x)|g(x)，

反之，若 f(x)|g(x)，则 g(α)=0，

(3) 若 f(x)，g(x)都是α的极小多项式，则由(2)的结论可知，

f(x)，g(x)互相整除，即它们相差 F 的一个非零元，

又因它们的首项系数相等，因而，f(x)=g(x)，

事实上，定理 1.3(1)的逆命题也是成立的，

定理 1.4 设 F 是域，f(x)是 F[x]中以α为根，首项系数为 1 的多项式，

若 f(x)是 F[x]中的不可约元，则 f(x)是α在 F 上的极小多项式，

证: 设 g(x)是 F[x]中以α为根的多项式，

因为 f(x)是 F[x]中的不可约元，所以 f(x)|g(x)，即 deg f(x)⩽deg g(x)，

从而根据极小多项式的定义得证

因为代数元的极小多项式是唯一的，所以我们可以给出如下定义，

定义 1.4 设 f(x)是α在域 F 上的极小多项式，

若 deg f(x)=n，则称α是域 F 上的 n 次代数元，

例 1.1 试证明属于 R 的$\alpha=\sqrt{2}+\sqrt{3}$是有理数域上的 4 次代数元，

证: 首先，确定一个以α为根的有理系数多项式 f(x)，

因为$\alpha-\sqrt{2}=\sqrt{3}$，所以$(\alpha-\sqrt{2})^2=(\sqrt{3})^2$，即$\alpha^2-2\sqrt{2}\alpha+2=3$，

再由$\alpha^2-1=2\sqrt{2}\alpha$可得$\alpha^4-2\alpha^2+1=8\alpha^2$，即$\alpha^4-10\alpha^2+1=0$，

因此，α是 $f(x)=x^4-10x^2+1$ 的一个根，于是α是有理数域的代数元，

其次，$f(x)=x^4-10x^2+1$ 就是α在有理数域上的极小多项式，

对此，我们只要说明 f(x)是 Q[x]中的不可约元即可，

事实上，f(x)的 4 个根分别为$\sqrt{2}+\sqrt{3}$，$\sqrt{2}-\sqrt{3}$，$-\sqrt{2}+\sqrt{3}$，$-\sqrt{2}-\sqrt{3}$，

所以，f(x)不可能有 1 次有理系数因子，

另外，f(x)的 4 个根之中的任意两个根的和与积不可能同时为有理数，

所以 f(x)不可能有 2 次有理系数因子，从而多项式 f(x)是 Q[x]中的不可约元，

三、域的扩张次数

事实上，若域 E 是域 F 的扩域，则 E 是 F 上的向量空间

定义 1.5 设 V 是一个交换群，F 是一个域，

若映射$\varphi: F\times V\to V, (r, v)\to rv$ 满足下列条件:

(1)$r(u+v)=ru+rv$

(2)$(r+s)v=rv+sv$

(3)$(rs)v=r(sv)$

(4)$1v=v$，其中 r，s 属于 F，u，v 属于 V，1 是 F 的单位元，

则称 V 是域 F 上的向量空间，

例 1.2 证明若 E 是域 F 的扩张，则 E 是 F 上的向量空间，

证: 我们只要对属于 F 的 r，属于 E 的 a 定义 ra 为域 E 中的乘法运算即可，

每个域都可以看做其素子域上的向量空间，

可验证，线性代数中有关向量空间的诸多概念、性质等在域的扩张中仍然成立

定义 1.6 设 E 是域 F 的扩张，若将 E 视为 F 上的向量空间，

则向量空间的基底称为包含 F 的扩张 E 的基底，

向量空间的维数称为包含 F 的扩张 E 的扩张次数，并用|E: F|表示，

若|E : F|＜∞，则称包含 F 的 E 为有限扩张，否则称包含 F 的 E 为无限扩张，

例 1.3 证明包含 Q 的扩张 $Q(\sqrt{2})$是有限扩张，包含 Q 的 Q(x)是无限扩张，

其中 x 是 Q 的未定元，

证: 令 $A=\{a+b\sqrt{2}|a,b\in Q\}$,

对属于 Q[x]的任意 f(x)，有 $f(x)=(x^2-2)q(x)+r(x)$, $r(x)=0$ 或 $\deg r(x)<2$,

则 $f(\sqrt{2})=r(\sqrt{2})$，即 $f(\sqrt{2})$属于 A,

再由属于 A 的$\frac{a+b\sqrt{2}}{c+d\sqrt{2}}=\frac{(ac-bd)+(bc-ad)\sqrt{2}}{c^2-2d^2}$可知，

$Q(\sqrt{2})=\left\{\frac{g(\sqrt{2})}{h(\sqrt{2})}\middle|\, g(x),h(x)\in Q[x],h(\sqrt{2})\neq 0\right\}$中的元素

可以表示为 $a+b\sqrt{2}(a,b\in Q)$的形式，

即 $Q(\sqrt{2})$中任意元素都能由 1，$\sqrt{2}$表示，

另一方面，如果 $a+b\sqrt{2}=0$, a, b 属于 Q，则 $a=b=0$，即 1，$\sqrt{2}$是线性无关的，

综上，1，$\sqrt{2}$是包含 Q 的扩张 $Q(\sqrt{2})$的基底，

因此，$|Q(\sqrt{2}):Q|=2$，即包含 Q 的 $Q(\sqrt{2})$是有限扩张，

要证明包含 Q 的 Q(x)是无限扩张，

只要我们能在 Q(x)中找到无限个线性无关的元素就可以了，

为此，考察集合$\{1,x,x^2,\cdots,x^n,\cdots\}$,

易知其中的任意有限个元素 $1,x,x^2,\cdots,x^n$ 是线性无关的，

这由下面的事实确定，

$a_0 1+a_1x+a_2x^2+\cdots+a_nx^n=0\Leftrightarrow a_0=a_1=a_2=\cdots=a_n=0$

其中 a_i 属于 Q, $0\leqslant i\leqslant n$,