下面出现的环都是交换含幺环。

1 Field extensions

设有两个环 A, B 和一个环同态 $f: A \to B$，再设 $a \in A, b \in B$，我们可以通过 f 定义他们的乘法为 $a \cdot b = f(a)b \in B$，这样环 B 就被赋予了一个 A-模结构。

Definition 1.1. 环 B 若被赋予一个 A-模结构，则称 B 是一个 A-代数。

设 B 是 A-代数，有 $f: A \to B$，设 C 也是 A-代数，有 $g: A \to C$，那么 A-代数之间的同态 $h: B \to C$，首先是 B 和 C 之间的环同态，还要和 A-模结构相容，即 $g = h \circ f$.

Definition 1.2. 设 B 是 A-代数,我们称呼 B 是有限生成 A-代数,如果他同构于 $A[x_1, \cdots, x_n]/\mathfrak{a}$,其中 $\mathfrak{a}$ 是 $A[x_1, \cdots, x_n]$ 的一个理想。一个环称为有限生成的就是指他作为 $\mathbb{Z}$-代数是有限生成的。如果 B 作为 A-模是有限生成的，则称 B 作为 A-代数是有限的。

如果 k 是一个域，则任意的 k-代数都是 k-矢量空间。与此同时，赋予 k-代数的 k-模结构的那个同态的核 $\ker(f)$ 作为域 k 中的理想，他只能是 k 本身或者 $\{0\}$，前者太平凡，我们舍去，后者得出了 $f: k \to f(k)$ 是一个域同构。

Definition 1.3. 如果域 K 是一个 k-代数，称 K 是 k 的一个域扩张，记作 K/k。如果域 K 还是一个有限生成 k-代数，称 K 是 k 的一个有限生成扩张。

因为 K 是 k-矢量空间，我们可以定义域扩张的大小为 $[K : k] = \dim_k(K)$. 若 $[K : k]$ 有限，称这个扩张是有限扩张。

前面说了，对于任意的 k-代数 K，k 都同构于 K 中的一个子域，所以通常也将域扩张定义为包含 k 的更大的域。为了行文的简练，必要的时候，我们就假设域扩张为包含我们的域更大的域。

Definition 1.4. 设 B 是环，A 是他的子环，如果对 $a \in B$，存在 $f \in A[x]$ 使得 $f(a) = 0$，称 a 在 A 上代数。如果 B 中任意的元素都在 A 上代数，则称 B 在 A 上代数。特别地，设 K/k 是一个扩张，若 K 在 k 上代数，则 K 被称为 k 的一个代数扩张。

每一个 k 中元素当然在 k 上代数，因为他是线性多项式的根。如果 α 有逆且在 k 上代数，那么他的逆 $1/\alpha$ 也在 k 上代数。实际上，因为 α 在 k 上代数，所以存在多项式 $f = \sum_{i=0}^{n} a_i x^i$ 使得 $f(\alpha) = 0$。很容易检验，多项式 $g = \sum_{i=0}^{n} a_{n-i} x^i$ 使得 $g(1/\alpha) = 0$ 成立，所以 $1/\alpha$ 在 k 上代数。

作为域扩张的例子，考虑多项式环 $k[x_1, \cdots, x_n]$ 是一个 k-代数，他的商域 $F(k[x_1, \cdots, x_n])$ 就是 k 的一个扩张，并且 $\dim_k(F(k[x_1, \cdots, x_n])) = \infty$，实际上，比如 $\{x_1, \cdots, x_1^n, \cdots\}$ 是线性无关的。或者，如果 $\mathfrak{m}$ 是 $k[x_1, \cdots, x_n]$ 的一个极大理想，则 $k[x_1, \cdots, x_n]/\mathfrak{m}$ 也是 k 的一个扩张，后面我们会看到这个扩张是一个有限扩张。

假如有一个域 K，而 k 是他的子域，那么必然存在一个 $\alpha \in K$ 但 $\alpha \notin k$，我们考虑 K 中包含 α 的最小的子域 $k(\alpha)$。首先 $k[\alpha] \subset k(\alpha)$，如果不存在多项式 $f \in k[x]$ 使得 $f(\alpha) = 0$，则 $k[\alpha] \cong k[x]$，所以包含 $k[\alpha]$ 的最小的域就是他的商域 $F(k[\alpha])$，即 $k(\alpha) = F(k[\alpha])$.

反之，如果存在多项式 $f \in k[x]$ 使得 $f(\alpha) = 0$，取 g 是 $k[x]$ 中以 α 为零点的次数最低的首一多项式，称为 α 的极小多项式。我们需要下面这个引理。

Lemma 1.1. *极小多项式不可约。如果 f 也以 α 为零点，则存在 $h \in k[x]$ 使得 $f = gh$.*

Proof. 假设可约，设 $g = g_1 g_2$，其中 g_1 和 g_2 都是次数比 g 低的多项式。那么在 α 处，我们有 $g_1(\alpha)g_2(\alpha) = 0$，所以 $g_1(\alpha)$ 和 $g_2(\alpha)$ 中至少有一个为零，而他们都是次数比 g 低的在 α 处为零的多项式，和极小多项式的选取矛盾。

辗转相除，我们有分解 $f = gh + r$，其中 r 是比 g 次数更低的多项式或者 $r = 0$。如果是前者，在 α 处 $r(\alpha) = f(\alpha) - g(\alpha)h(\alpha) = 0$，所以 r 和极小多项式的选取矛盾。 $\square$

通过 $x \mapsto \alpha$ 可以定义同态 $k[x] \to k[\alpha]$，他当然是满的，他的核是那些在 α 为零的多项式所构成的理想，从引理可以知道，他就是极小多项式生成的极大理想[1] (g)，所以 $k[\alpha] \cong k[x]/(g)$ 是一个域。因而 $k[\alpha]$ 就是我们想要的域 $k(\alpha)$，他同构于 $k[x]/(g)$，其中 g 是 α 的极小多项式。

所以，我们在 K 中分两种情况找到了包含 α 的最小的 k 的域扩张 $k(\alpha)$，这样的扩张称为单扩张，前者被称为（单）超越扩张，扩张的元素被称为超越元，后者被称为（单）代数扩张[2]。

Theorem 1.1. *域的单扩张总是存在的。*

Proof. 上面我们预设了一个比 k 大的域 K 的存在，免去了担心单扩张存在性的烦恼。现在有了上面单扩张的知识，我们也就可以直接构造单扩张来证明存在性。

如果 α 关于 k 超越，那么我们取 $k(\alpha)$ 为 $k[\alpha]$ 的商域 $F(k[\alpha])$，这显然是一个 k-代数，因此是一个 k 的扩张。如果 α 关于 k 代数，就取 $k[\alpha]$，他显然是一个 k-代数，并且同构于域 $k[x]/\mathfrak{m}$，其中 $\mathfrak{m}$ 是 α 的极小多项式生成的极大理想。 $\square$

Proposition 1.1. *两个单扩张同构，即 $k(\alpha) \cong k(\beta)$，当且仅当他们或者同为代数扩张且极小多项式相同，或者同为超越扩张。*

Proof. 如果 $k(\alpha)$ 是超越扩张，而 $k(\beta)$ 是代数扩张。前面已经知道 $\dim_k(k(\alpha)) = \infty$。如果 β 的极小多项式是 n 次的，那么 $k[x]/\mathfrak{m}$ 中 $\{1, x, \cdots, x^{n-1}, x^n\}$ 是线性相关的，即 $\dim_k(k(\beta)) \leq n < \infty$，所以 $k(\alpha) \ncong k(\beta)$.

现在，如果两者都是超越扩张，则 $k(\alpha) \cong F(k[x]) \cong k(\beta)$. 如果两者都是代数扩张，则 $k[x]/\mathfrak{m}_\alpha \cong k[x]/\mathfrak{m}_\beta$，即可推出 $\mathfrak{m}_\alpha = \mathfrak{m}_\beta$，继而拥有相同的极小多项式。反过来，如果有相同的极小多项式，则 $k(\alpha) \cong k[x]/\mathfrak{m} \cong k(\beta)$. $\square$

[1]若 k 是一个域，则多项式环 $k[x]$ 是一个主理想整环，他的极大理想被不可约多项式生成。

[2]下节我们会看到这个命名是合理的。

现在对 k 单扩张 α_1 得到了 $k(\alpha_1)$，再对其单扩张 α_2 就得到了 $k(\alpha_1)(\alpha_2)$，他也是 k 的一个扩张，不妨将其记作 $k(\alpha_1, \alpha_2)$. 如是继续，就可以得到 $k(\alpha_1, \cdots, \alpha_n)$。

Proposition 1.2. $k(\alpha_1)(\alpha_2) \cong k(\alpha_2)(\alpha_1)$.

Proof. 这里可以不妨假设，我们的域扩张都做成了包含的形式。因为 $k(\alpha_2)(\alpha_1)$ 是一个域，而 α_1 是他的元素，所以 $k(\alpha_1)$ 可以看成 $k(\alpha_2)(\alpha_1)$ 的子域，然后再对 $k(\alpha_1)$ 做 α_2 的单扩张，因为单扩张 $k(\alpha_1)(\alpha_2)$ 是 $k(\alpha_2)(\alpha_1)$ 中包含 α_2 的最小的域，所以 $k(\alpha_1)(\alpha_2) \subset k(\alpha_2)(\alpha_1)$。反过来同理。 □

上面这个简单的命题告诉我们,有限次单扩张的顺序无关紧要,于是,对于扩张 $k(\alpha_1, \cdots, \alpha_n)/k$，如果我们乐意，可以先超越扩张，然后再代数扩张。

2 Algebraic extensions

Definition 2.1. 设 A 和 B 是环，且 A 是 B 的子环。称 $x \in B$ 在 A 上整，如果他是某个 $A[x]$ 中的首一多项式的根。如果 B 中任意的元素都在 A 上整，则称 K 在 k 上整。

设 k 是一个域，如果 α 在 k 上整，则他在 k 上代数。反之，如果 α 在 k 上代数，则存在一个多项式 $f = \sum_{i=0}^{n} a_i x^i$ 使得 $f(\alpha) = 0$，此时首一多项式 $g = f/a_n$ 也满足 $g(\alpha)$，所以 α 在 k 上整。通过上面的讨论，我们发现在域上代数和在域上整等价。下面我们先证明几个关于整的结论，因为在域上面的等价性，他们也可以自然应用到域扩张上。

Proposition 2.1. 设 A 和 B 是环，且 A 是 B 的子环。以下命题等价：

(1) α 在 A 上整。

(2) $A[\alpha]$ 是一个有限生成 A-模。

(3) $A[\alpha]$ 包含在 B 的一个子环 C 中，C 是一个有限生成 A-模。

(4) 存在忠实 $A[\alpha]$-模 M，他作为 A-模时是有限生成的。

Proof. (1) ⇒ (2)：由于 α 在 A 上代数，他的满足方程 $\alpha^n + a_1\alpha^{n-1} + \cdots + a_n = 0$，那么通过 $\alpha^{n+r} = -(a_1\alpha^{n+r-1} + \cdots + a_n\alpha^r)$ 即可知 $A[\alpha]$ 是一个有限生成 A-模。

(2) ⇒ (3)：取 $C = A[\alpha]$.

(3) ⇒ (4)：取 $M = C$，这是一个忠实 $A[\alpha]$-模，因为如果 $aC = 0$，由 C 有单位元，所以 $a \cdot 1 = a = 0$.

(4) ⇒ (1)：因为 M 是 $A[\alpha]$-模，所以 $\alpha M \subset M$。因为 M 是有限生成 A-模，设 M 被 $\{x_1, \cdots, x_m\}$ 生成，则 $\alpha M \subset M$ 告诉我们对任意的 i 都成立 $\alpha x_i = \sum_{j=1}^{m} a_{ij} x_j$，其中 $a_{ij} \in A$。所以

$$\sum_{j=1}^{m} (\alpha\delta_{ij} - a_{ij}) x_j = 0,$$

左乘 $(\alpha\delta_{ij} - a_{ij})$ 的伴随矩阵，则 $\det(\alpha\delta_{ij} - a_{ij}) x_j = 0$ 对任意的 $1 \leq j \leq m$ 都成立，也即 $\det(\alpha\delta_{ij} - a_{ij}) M = 0$。由 M 的忠实性，$\det(\alpha\delta_{ij} - a_{ij}) = 0$，将行列式展开就是我们需要的首一多项式。 □

如果 $\{\alpha_1,\cdots,\alpha_n\}\subset B$ 都在 A 上整，那么 $k[\alpha_1,\cdots,\alpha_n]$ 也是一个有限生成 k-模，这只要利用 $k[\alpha_1,\cdots,\alpha_n]=k[\alpha_1,\cdots,\alpha_{n-1}][\alpha_n]$ 经过有限次归纳即可。

Proposition 2.2. 设 A 和 B 是环，且 A 是 B 的子环。则所有在 A 上整的元素构成 B 的一个子环。

Proof. 如果 α 和 β 在 A 上面整，$A[\alpha,\beta]$ 有限生成。因为 $A[\alpha\pm\beta]\subset A[\alpha,\beta]$ 和 $A[\alpha\beta]\subset A[\alpha,\beta]$，由上一个命题的(3)，$\alpha\pm\beta$ 和 $\alpha\beta$ 在 A 上面整。 □

设 K/k 是一个扩张，这个命题告诉我们 K 中在 k 上代数的元素构成 K 中的子环。并且，因为如果 α 代数，那么 $1/\alpha$ 也代数，所以 K 中在 k 上代数的元素构成 K 中的子域。特别地，现在我们终于可以说明，单代数扩张是代数扩张。

Proposition 2.3. 设 $A\subset B\subset C$ 是环，且 B 在 A 上整，C 在 B 上整，则 C 在 A 上整。这就是整的传递性。

Proof. 设 $x\in C$，因为 x 在 B 上整，所以存在方程 $x^n+\cdots+b_{n-1}x+b_n=0$，因为 $b_i\in B$ 都在 A 上整，所以 $B'=A[b_1,\cdots,b_n]$ 是有一个有限生成 A-模。由同一个首一多项式，x 也在 B' 上整，于是 $B'[x]$ 是一个有限生成 B'-模，由模的有限生成的传递性，则 $B'[x]$ 是一个有限生成 A-模，所以 x 在 A 上整。 □

Proposition 2.4. 设环 $A\subset B\subset C$，且 A 是 *Northerian* 的，C 是有限生成 A-代数，以及 C 或者是一个有限生成 B-模，或者 C 在 B 上整，那么，B 是一个有限生成 A-代数。

Proof. 在题目的条件下，由 Proposition 2.1，C 是一个有限生成 B-模与 C 在 B 上整等价。所以只对 C 是一个有限生成 B-模的情况证明。

令 $C=A[\bar{x}_1,\cdots,\bar{x}_m]\cong A[x_1,\cdots,x_m]/\mathfrak{a}$，以及令 y_1, y_2, $\cdots$, y_n 是 C 作为有限生成 B-模的生成元，那么存在

$$\bar{x}_i=\sum_i \alpha_{ij}y_j,\quad y_iy_j=\sum_k \beta_{ijk}y_k, \tag{1}$$

令 B_0 是由 $\alpha_{ij}\in B$ 和 $\beta_{ijk}\in B$ 生成的 A-代数，由于 A 是 Northerian 的，所以 B_0 是 Northerian 的[3]，以及 $A\subset B_0\subset B$.

由于 C 中的元素都是关于 $\{\bar{x}_i\}$ 的、系数处于 A 中的多项式，那么(1)告诉我们，这个元素可以写成 $\sum_i b_iy_i$，其中 $b_i\in B_0$，所以 C 是一个有限生成 B_0-模。而 B_0 是 Northerian 的就保证了 C 是一个 Northerian 的 B_0-模。因为 B 又是 C 的子模，所以 B 是一个有限生成 B_0-模。又 B_0 是一个有限生成 A-代数，所以 B 是一个有限生成 A-代数。 □

Proposition 2.5. 如果 K/k 是 L/K 都是扩张，则 L/k 是一个扩张。特别地，如果 K/k 和 L/K 都是代数扩张，则 L/k 是代数扩张。

[3]这是因为有限生成 A-代数同构于 $A[x_1,\cdots,x_{N_B}]/\mathfrak{a}_B$，而他是 Northerian 的。

Proof. 不妨设 $k \subset K \subset L$，第一点显然。K/k 和 L/K 都是代数扩张等价于 K 在 k 上整且 L 在 K 上整。由整的传递性，L 在 k 上整，所以 L/k 是一个代数扩张。 □

Proposition 2.6. 设 K/k 是 L/K 都是扩张，则 $[L:k] \leq [K:k]$. 特别地，如果 K/k 和 L/K 都是有限扩张且 $[K:k]=m$ 以及 $[L:K]=n$，则 L/k 是有限扩张且 $[L:k]=mn$。这就是说，有限扩张的有限扩张还是有限扩张。

Proof. 设 $\{a_1, \cdots, a_r\}$ 是 K 中的任意 k-代数无关组，而 $\{b_1, \cdots, b_s\}$ 是 L 中的任意 K-代数无关组，我们来证明 $\{a_i b_j\}$ 是 k-线性无关组。设 $\alpha = \sum_{i,j} c_{ij} a_i b_j$，其中 $c_{ij} \in k$，因为 $\sum_i c_{ij} a_i \in K$，所以如果 $\alpha = 0$，那么由 $\{b_1, \cdots, b_s\}$ 的 K-线性无关性，所以 $\sum_i c_{ij} a_i = 0$，然后再应用一次 $\{a_1, \cdots, a_r\}$ 的 k-线性无关性，就得到了对于任意的 i, j 都成立 $c_{ij} = 0$，于是 $\{a_i b_j\}$ 是 k-线性无关组。由此，维度的结论显然。 □

Proposition 2.7. 有限扩张等价于有限次单代数扩张。

Proof. 注意到单代数扩张是有限扩张,这是因为,如果他的极小多项式为 n 次的,那么 $\{1, x, \cdots, x^n\}$ 线性相关，而有限次有限扩张是有限扩张。

反之，设 K/k 不是代数扩张，那么存在一个元素 $\alpha \in K$ 是超越的。因为 $k \subset k(\alpha) \subset K$，所以 $[K:k] \geq [k(\alpha):k] = \infty$. 如果 K/k 是代数扩张，但不是有限次单代数扩张，则对于任何的 $n \in \mathbb{Z}^+$，一定存在一组 n 个元素的线性无关组，这和 $\dim_k K$ 有限矛盾。所以一个有限扩张由有限次单代数扩张而成。 □

Lemma 2.1. *Zariski's lemma*: 有限生成扩张是代数扩张。这还可以表述为，设 $\mathfrak{m}$ 是 $A = k[x_1, \cdots, x_n]$ 的一个极大理想，则 $A(\mathfrak{m}) = A/\mathfrak{m}$ 是 k 的一个代数扩张。

Proof. 归纳证明这个命题。

$n=1$ 的时候是简单的，$k[x]$ 中任意的极大理想 $\mathfrak{m}$ 都是由一个不可约多项式 f 生成的，所以 $\mathfrak{m} = (f)$，而单扩张的知识告诉我们，$k[\bar{x}] = k[x]/(f)$ 是一个代数扩张，他给 k 添加上了 f 的一个根。

对 n 个变元的情况，假设对任意的 $\mathfrak{m}$ 有 $A(\mathfrak{m}) = k[\bar{x}_1, \cdots, \bar{x}_n]$ 中的 $\{\bar{x}_i\}$ 都在 k 上代数。

对 $n+1$ 个变元的情况，$k[\bar{x}_0, \cdots, \bar{x}_n]$ 是 k 的一个有限生成扩张，那么他可以分解成有限个单扩张，$k[\bar{x}_0, \cdots, \bar{x}_n] = k(\bar{x}_0)[\bar{x}_1, \cdots, \bar{x}_n]$，其中 $k(\bar{x}_0)$ 是一个 k 的单扩张，根据归纳假设 $\bar{x}_1, \cdots, \bar{x}_n$ 都在 $k(\bar{x}_0)$ 上是代数的。如果 $k(\bar{x}_0)$ 在 k 上是代数的，那么所有的 $\bar{x}_i$ 就都是在 k 上代数的，也就是 $k[\bar{x}_0, \cdots, \bar{x}_n]$ 是 k 的代数扩张了。

假设 $k(\bar{x}_0)$ 是超越扩张，即 $k(\bar{x}_0) = F(k[\bar{x}_0])$，$k(\bar{x}_0)$ 是 $k[\bar{x}_0]$ 的商域。因为 $\bar{x}_i$ 在 $k(\bar{x}_0)$ 上是代数的，所以存在多项式

$$a_{i0}\bar{x}_i^{N_i} + a_{i1}\bar{x}_i^{N_i-1} + \cdots + a_{i,N_i+1} = 0,$$

其中 $a_{ij} \in k(\bar{x}_0) = F(k[\bar{x}_0])$。将其通分，可以得到一个新的等式，系数属于 $k[\bar{x}_0]$，为了符号上的简单，不妨直接设 $a_{ij} \in k[\bar{x}_0]$.

将等式两边乘以 $a_0^{N_i-1}$ 后可以看到 $a_{i0}\bar{x}_i$ 在 $k[\bar{x}_0]$ 上是整的，实际上，对所有的 $i>0$ 和 $\bar{x}_0$ 都可以找到这么一个 a_{i0}。由于在 $k[\bar{x}_0]$ 上整的元素构成一个环，而且 $k[\bar{x}_0]$ 是他的一个子环，特别地，所有的 $a_{i0}\in k[\bar{x}_0]$ 以及 $\bar{x}_0\in k[\bar{x}_0]$ 都是整的，所以我们可以说存在一个因子 $a=\prod_{i>0}a_{i0}$，对每一个 $\bar{x}_i$ 都成立 $a\bar{x}_i$ 在 $k[\bar{x}_0]$ 上是整的。

现在任取一个 $y\in k[\bar{x}_0,\cdots,\bar{x}_n]$，写作 $y=\sum y_{i_0\cdots i_n}\bar{x}_0^{N_{i_0}}\cdots\bar{x}_n^{N_{i_n}}$. 因为在 $k[\bar{x}_0]$ 上整的元素构成一个环，两边乘以 a^N 后可以得到 a^Ny 在 $k[\bar{x}_0]$ 上是整的，其中 N 足够大，因为所有的求和都是有限的，所以 N 总是可以选出来的。

我们已经证明了，随便取一个 $y\in k(\bar{x}_0)$，则存在 $N\in\mathbb{Z}^+$ 使得 $a^Ny\in k(\bar{x}_0)$ 在 $k[\bar{x}_0]$ 上整。由于 $k[\bar{x}_0]$ 作为域上的多项式环是唯一分解整环 [4]，所以 $a^Ny=f\in k[\bar{x}_0]$，或 $y=f/a^N\in k[\bar{x}_0]_a$，其中 $k[\bar{x}_0]_a$ 是 $k[\bar{x}_0]$ 关于 $\{1,a,a^2,\cdots\}$ 的分式环，而 a 和 $y\in k(\bar{x}_0)$ 的选取没有关系，只有 N 和 f 的选取和 y 有关系，但是不管取哪个 N，他们都在同一个分式环里面，而分式环又真包含于商环里面，所以

$$k(\bar{x}_0)\subset k[\bar{x}_0]_a\subsetneq k(\bar{x}_0),$$

这就完成了矛盾，故 $k(\bar{x}_0)$ 不可能是超越扩张，$k(\bar{x}_0)$ 是代数扩张。所以 $k[\bar{x}_0,\cdots,\bar{x}_n]$ 是 k 的代数扩张。 □

Proposition 2.8. 有限次单代数扩张等价于有限生成扩张。

Proof. 对有限次单代数扩张而成的域 $k(\alpha_1,\cdots,\alpha_m)$，由 $: x_i\mapsto\alpha_i$ 可以构造一个满的 k-代数同态 $\varphi: k[x_1,\cdots,x_m]\to k(\alpha_1,\cdots,\alpha_m)$，根据同构基本定理，$k(\alpha_1,\cdots,\alpha_m)\cong k[x_1,\cdots,x_m]/\ker\varphi$，所以 $k(\alpha_1,\cdots,\alpha_m)$ 是一个有限生成扩张。

反之，因为 $A(\mathfrak{m})=k[x_1,\cdots,x_n]/\mathfrak{m}=k(\alpha_1,\cdots,\alpha_m)$，其中 $m\le n$，由 Zariski's lemma，$A(\mathfrak{m})$ 是一个代数扩张，即 α_i 都在 k 上代数，所以 $A(\mathfrak{m})=k(\alpha_1)\cdots(\alpha_m)$，其中每一次单扩张都是代数的。 □

在某些书上，有限生成扩张被定义为有限次单代数扩张，通过上面的命题，我们知道了这两个定义是等价的。最后我们再提供一个 Zariski's lemma 的证明，他比上面的证明要短一些，用到了 Propostion 2.4。

Proof. 设 $A(\mathfrak{m})=k[\alpha_1,\cdots,\alpha_n]$，如果 $A(\mathfrak{m})$ 关于 k 不是代数扩张，因为有限生成扩张一定是有限次单扩张而成的（这些单扩张是否是代数的我们还不知道），那么假设 $\alpha_1,\cdots,\alpha_r$ 关于 k 超越。我们可以先单扩张这些超越元，至于剩下的则关于域 $B=k(\alpha_1,\cdots,\alpha_r)$ 代数。

现在因为 $A(\mathfrak{m})$ 是 B 的有限扩张，根据包含关系 $k\subset B\subset A(\mathfrak{m})$ 和 Propostion 2.4，我们可以得知 B 是一个有限生成 k-代数，设 $B=k[\beta_1,\cdots,\beta_s]$，其中每一个 β_i 都有着形式 f_i/g_i，

---

[4]假设 R 是唯一分解整环，$F(R)$ 是他的商域，假设 $x\in F(R)$ 在 R 上整，对于唯一分解整环有分解 $x=r/s$，其中 r 和 s 互素，那么就有方程

$$r^n+a_1r^{n-1}s+\cdots+a_ns^n=0,$$

其中 $a_i\in R$，因此 s 需要整除 r^n，而 r 和 s 互素，所以只能有 $s=\pm1$. 这就说明了 $x=\pm r\in R$.

而 $f_i, g_i \in k[\alpha_1, \cdots \alpha_r]$。但是，$k[\alpha_1, \cdots \alpha_r]$ 中有多项式 $h = g_1 g_2 \cdots g_s + 1$ 使得 h^{-1} 不能写成 $\beta_1, \cdots, \beta_s$ 的多项式，矛盾。 □

3 trans deg

上面一节解决了有限扩张的分类问题，即有限扩张就是有限生成扩张。如果一个扩张不是有限扩张，则，要么这个扩张包含超越元，或者，他是代数扩张却不能由有限次单代数扩张而成。这节要更细致地对非有限扩张进行分类。

Definition 3.1. 设 K/k 是一个扩张，一个 K 中的元素 t 被称为在 $\{u_1, \cdots, u_n\}$ 上关于域 $k(u_1, \cdots, u_n)$ 代数相关的，就是说存在一个非零多项式 $f \in k[u_1, \cdots, u_n][x]$，使得 $f(t) = 0$。

他有如下性质：

(1) 因为存在 $f(x) = u_i - x$，所以 u_i 是代数相关的。

(2) 如果 x 关于 $\{u_1, \cdots, u_n\}$ 相关,但是关于 $\{u_1, \cdots, u_{n-1}\}$ 无关,则 u_n 关于 $\{u_1, \cdots, u_{n-1}, x\}$ 相关。

(3) 如果 $\{v_i\}$ 相关于 $\{w_j\}$，且 u 相关于 $\{v_i\}$，则 u 相关于 $\{w_j\}$.

然后可以类比线性代数中基的性质以及证明。类比线性无关，我们定义 $\{u_i\}$ 代数无关如下：对任意的 i，u_i 不代数相关于其他 u_j.

Proposition 3.1. $\{u_i\}$ 是代数无关的当且仅当，如果多项式 f 使得 $f(u_1, \cdots, u_n) = 0$，那么 $f = 0$.

如果 $\{u_i\}$ 代数无关，那么他们之间不存在代数方程相互联系，所以他们也被称为超越独立。

Definition 3.2. 一个域 k 被称为代数闭域，就是说 $k[x]$ 中的每个多项式都可以分解为线性因子的乘积。等价地，任何多项式都在 k 中有至少一个根。

每一个域扩张都可以分解为先超越扩张，然后再代数扩张。分解不一定唯一，但是超越扩张的基数却是相同的，如果有限，那么就是次数相同。这个数就是所谓的超越次数。从这里很容易看出 $F(x_1, \cdots, x_n)$ 作为单纯的超越扩张 n 次，那么他的超越次数为 n。也可以这样定义，对于域扩张 E/F，E 中的极大代数无关集（超越基）的元素个数被称为超越次数。

Lemma 3.1. 设 E/F 和 E'/F' 是域扩张，且 $\varphi : E \to E'$ 是域同态满足 $\varphi(F) \subset F'$. 现在设 $f(x) \in F[x]$，若 $\alpha \in E$ 是 $f(x)$ 的根，则 $\alpha' = \varphi(\alpha)$ 是 $\varphi(f(x))$ 的根。

Proof. 设 $f(x) = \sum_i a_i x^i$，那么 $\varphi(f(x)) = \sum_i \varphi(a_i) x^i$，因此

$$\varphi(f(\alpha')) = \sum_i \varphi(a_i) \varphi(\alpha)^i = \varphi\left(\sum_i a_i \alpha^i\right) = \varphi\left(f(\alpha)\right) = 0.$$

□

特别地，如果 φ 是 E 的自同态，且在 F 上的限制为恒等映射，那么如果 α 是 $f(x)$ 的一个根，则 $\varphi(\alpha)$ 也是 $f(x)$ 的一个根。

Definition 3.3. 设 E/F 是域扩张，称所有 E 在 F 上的限制为恒等映射的自同态构成的群为这个域扩张的 *Galois* 群，群运算为复合，记作 $\mathrm{Gal}(E/F)$.

一般来说,如果 E/F 是有限扩张,那么他 Galois 群元的个数不多于 $[E:F]$,如果 $|\mathrm{Gal}(E/F)| = [E:F]$，则称扩张 E/F 是 Galois 扩张。

Theorem 3.1. *Galois* 理论基本定理：设 E/F 是 *Galois* 扩张，

(1) 设 H 是 $\mathrm{Gal}(E/F)$ 的子群,那么他和 E/F 的一个中间域 $L = \{x \in E : h(x) = x, \forall h \in H\}$ 存在一一对应，他的逆为 $L \mapsto \mathrm{Gal}(E/L)$. 且

$$[E:L] = |\mathrm{Gal}(E/L)|, \quad [L:F] = (G:\mathrm{Gal}(E/L)).$$

(2) 上述对应诱导 G 的所有正规子群和 E/F 的 *Galois* 子扩张 L/F 之间的一一对应，此时

$$\mathrm{Gal}(L/F) \cong \mathrm{Gal}(E/F)/\mathrm{Gal}(E/L).$$

如果一个域经过任意的代数扩张之后还是其本身，那么我们就称呼这个域是代数闭域。

Theorem 3.2. 对任意的域 k，在同构意义上唯一存在包含他代数闭域 $\bar{k}$。$\bar{k}$ 也被称为 k 的代数闭包。

Proposition 3.2. 任意多项式 $f \in k[x]$ 都在 $\bar{k}$ 中有根。

Definition 3.4. 一个域 k 被称为代数闭域，就是说 $k[x]$ 中的每个多项式都可以分解为线性因子的乘积。等价地，任何多项式都在 k 中有至少一个根。

Definition 3.5. 假设 P 是 F 的一个扩张，一个 P 中的元素 v 被称为在 $u_1, \cdots, u_n$ 上关于域 $F(u_1, \cdots, u_n)$ 代数相关的，就是说存在一个非零多项式 f，使得 $f(v) = 0$，这个多项式的系数是 $F[u_1, \cdots, u_n]$ 中的多项式。

4 Algebras and the proof of Hilbert's Nullstellensatz

Definition 4.1. 设 k 是代数闭域，如果 I 是 $k[x_1, \cdots, x_n]$ 的一个理想，记 $Z(I)$ 是这个理想的共同零点集，即 $Z(I)$ 是使得理想 I 内所有多项式都为 0 的点的集合。反过来，对于一个集合 $U \in k^n$，我们记 $I(U)$ 为所有在 U 上为零的多项式所构成的理想。

可以从 Zariski's lemma 推出 Hilbert's Nullstellensatz. 这就是 Atiyah&Maconald 第七章的习题 14：

Theorem 4.1. *Hilbert's Nullstellensatz:* 设 k 是代数闭域,假如我们有一个多项式 $f \in k[x_1, \cdots, x_n]$ 在 $Z(I)$ 为零，那么存在一个正整数 n 使得 $f^n \in I$，这就是说 $f \in r(I)$，其中 $r(I)$ 是 I 的半径，常常也记做 $\sqrt{I}$.

Proof. 让 $A = k[x_1, \cdots, x_n]$，I 是他的一个理想，假设 f 在 $Z(I)$ 上为 0，即 f 属于 $I(Z(I))$，但 f 不属于 $r(I)$。因为 $r(I)$ 是所有包含 a 的素理想之交，所以 f 必然不属于某个包含 T 的素理想 p，让 f' 是 f 在 $B = A/p$ 中的象，再设 $C = B[1/f']$，C 是一个有限生成的 k 代数，由 $1'/f', x_1'/1' \cdots, x_n'/1'$ 生成。取 m 是 C 中的一个极大理想，C/m 是一个域，也是一个有限生成 k 代数，由 Zariski's lemma，所以是一个 k 的有限扩张，但是 k 是代数闭域，所以也就是 k。

让 t_i 是 x_i 在映射

$$\psi : A \xrightarrow{\pi_1} B \xrightarrow{\phi} C \xrightarrow{\pi_2} C/m \xrightarrow[\cong]{\pi_3} k$$

的象 $t_i = \psi(x_i)$，我们记 $t = (t_1, \cdots, t_n)$，由于 $\psi(x_i) = t_i = x_i(t)$ 对任意的 x_i 都成立，所以对任意的 g 属于 A，我们有 $\psi(g) = g(t)$. 现在假设 g 是 I 的元素，那么 $\pi_1(g) = 0$，故 $g(t) = \psi(g) = 0$，这就是说 $t \in Z(I)$，此外，$\phi(\pi_1(f)) = f'/1'$ 是 C 里面的一个单位，因此 $\phi(\pi_1(f)) = f'/1'$ 不在 m 里面（否则 $m = C$），那么 $\psi(f)$ 不等于 0，所以 $f(t) = \psi(f)$ 不等于零，矛盾，证毕。 $\square$