Week15 摘要

本周的主要内容是“向子域F中添加元素u，得到最小扩域$F(u)$”。思路如下：

- 简单地探索$F(u)$的必要条件并证明它的充分性，给出了$F(u)$的一个表示；
- 问题：上面给出的$F(u)$的表示中，是否有元素同时被两种不同的方式表示了？即，上述给出的表示，是否有冗余？这个问题分两种情况解答：
  - 对于超越元而言，我们给出的每个表示都是不重复的；
  - 对于代数元而言，上述表示是可以简化的。本质上，这是由于代数元是域F上某多项式的根，借助这个多项式可以对很多表示进行化简；技术上，是通过u在F上的**极小多项式**做到的。
- `Week14`给出了通过模掉一个特定的多项式进行扩域的方式，我们证明这种扩域与本周给出的扩域是**同构**的。这个同构是通过**环同态定理**证明的。
- 引入了若干向量空间的基本概念。

回顾上节课的内容：
给定域$(K,+,\cdot)$，称$F\subset K$是K的子域，若$(F,+,\cdot)$是域，即以下条件成立：

- $0\in F, 1_K\in F.$
- $\forall a,b\in F, a+b\in F, -a\in F.$
- $\forall a,b\in F, a\cdot b\in F.$
- $\forall a\in F-\{0\}, a^{-1}\in F.$
  或者说，两种单位元在F中，且F对加法、乘法、加法逆、乘法逆封闭. 之所以不再重复运算要求，是因为运算的性质已经由“$(F,+,\cdot)$构成域”这一条件给定。

代数元与超越元

设$F\subset K$是子域，$u\in K$，若存在F上的非零多项式f，使得$f(u)=0$，则称u是F上的代数元. 若对F上任意的非零多项式f，都有$f(u)\neq 0$，则称u是F上的超越元.
这一对概念的最初提出，也是对数域而言的，这也是最经典的例子。例如，当$K=\mathbb{C}, F=\mathbb{Q}$时，我们有：

- $\sqrt{2},\sqrt{3},i$是$\mathbb{Q}$的代数元.
- e,π是$\mathbb{Q}$的超越元.

向子域中添加元素

> 问题：设$F \subset K$是子域，$u \in K$，问：K中包含$F \cup \{u\}$的最小子域是？或者说，求$F(u)$.

满足条件的子域一定是存在的，这由如下的结果保证：
任意一组子域的交仍然是子域。

我们首先看看$F(u)$的必要条件。
首先有，$\forall f \in F[x]$，有$f(u) \in F(u)$. 这是因为$f(u) = a_0 + a_1 u + \ldots + a_n u^n, a_i \in F$. 又$u \in F(u)$，有加法和乘法的封闭性即有$f(u) \in F(u)$.
又由域上乘法逆的封闭性，我们有：

$$\forall g \in F[x], g(u) \neq 0, \text{有} g(u)^{-1} \in F(u)$$

综合前两条性质，就有

$$\forall f, g \in F[x], g(u) \neq 0, \text{有} f(u)g(u)^{-1} \in F(u)$$

我们可以断言，上述的性质已经是$F(u)$的充分条件。

命题

设$F \subset K$为子域，$u \in K$，则K中包含$F \cup \{u\}$的最小子域$F(u)$是

$$\{f(u)g(u)^{-1} : f, g \in F[x],\ \ g(u) \neq 0\}$$

证明

记$L := \{f(u)g(u)^{-1} : f, g \in F[x],\ \ g(u) \neq 0\}$. 先证$F \cup \{u\} \subset L$. 这是因为，$\forall a \in F$，取$f = a, g = 1_K$，则有$a = f(u)g(u)^{-1}$. 对于$u$，取$f = x, g = 1_K$，则有$u = f(u)g(u)^{-1}$，仍然成立。

再证，对K的任意子域L'，只要有$F \cup \{u\} \subset L'$，则有$L \subset L'$. 这当然是成立的，上面我们对于必要条件的探索就已经证明了这一点。

最后证L确实是子域。

- 首先，加法和乘法幺元都在L中，因为$0, 1_K \in F \subset L$.
- 封闭性。$\forall f_1, g_1, f_2, g_2 \in F[x], g_1(u) \neq 0, g_2(u) \neq 0$，记$a = f_1(u)g_1(u)^{-1}, b = f_2(u)g_2(u)^{-1}$，我们有加法封闭：

$$\begin{aligned} a + b &= f_1(u)g_1(u)^{-1} + f_2(u)g_2(u)^{-1} \\ &= f_1(u)g_2(u)g_1(u)^{-1}g_2(u)^{-1} + f_2(u)g_1(u)g_2(u)^{-1}g_1(u)^{-1} \\ &= (f_1(u)g_2(u) + f_2(u)g_1(u))g_1(u)^{-1}g_2(u)^{-1} \\ &= (f_1g_2 + f_2g_1)(u)(g_1g_2)(u)^{-1} \in L \end{aligned}$$

加法逆封闭：

$$-a=-f_1(u)g_1(u)^{-1}=(-f_1)(u)g_1(u)^{-1}\in L$$

乘法封闭：

$$ab=f_1(u)g_1(u)^{-1}f_2(u)g_2(u)^{-1}=(f_1f_2)(u)(g_1g_2)(u)^{-1}\in L$$

乘法逆封闭：若$a\neq 0$，则有$f_1(u)\neq 0$，则有

$$a^{-1}=g_1(u)f_1(u)^{-1}$$

故L确实是子域，综上，原命题成立。

超越元的情形

记号同上，若u是F的超越元，则$\forall f_1,g_1,f_2,g_2\in F[x],g_1(u)\neq 0,g_2(u)\neq 0$，若$f_1(u)g_1(u)^{-1}=f_2(u)g_2(u)^{-1}$，则$f_1g_2=f_2g_1$.
换句话说，如果只考虑互素的情形，那么L中没有两个形如$f(u)g(u)^{-1}$的表示取到同一个值，亦即没有哪一个表示是多余的。少了任何一个这样的表示，都会破坏封闭性。

证明

由u是F上的超越元，则对任意$g\in F[x],g\neq 0$，有$g(u)\neq 0$. 我们已经有

$$F(u)=\{f(u)g(u)^{-1}:f,g\in F[x],\ \ g(u)\neq 0\}$$

若有

$$f_1(u)g_1(u)^{-1}=f_2(u)g_2(u)^{-1}$$

在等式两边同时乘以$g_1(u)g_2(u)$，则有

$$f_1(u)g_2(u)=f_2(u)g_1(u)$$

从而

$$0=f_1(u)g_2(u)-f_2(u)g_1(u)=(f_1g_2-f_2g_1)(u)$$

又由u为超越元，则有$f_1g_2-f_2g_1$是零多项式，那么$f_1g_2=f_2g_1$.

代数元的情形

显然，有些$F(u)$的形式并没有L那么复杂。例如，$\mathbb{R}\cup\{i\}$其实就是

$$\{a+bi:a,b\in\mathbb{R}\}$$

这其实是利用代数元的条件对L进行了化简。或者说，对于代数元，上述L的表示中有相当一部分是多余的。

极小多项式

设$F \subset K$是子域，$u \in K$是F的代数元，若$f \in F[x], f(u)=0$，f的首项系数是1_K. 若f是所有满足上述条件的多项式中次数最低的，则称f是u在F上的极小多项式。

上述幺元的条件并不是本质的，仅仅是为了确保唯一性。
根据这个定义，我们容易看出极小多项式的存在性。

例如，x^2+1是i在$\mathbb{Q}$上的极小多项式；幺元的条件排除了$2x^2+2$这样的多项式。

极小多项式的基本性质

沿用上述符号，关于极小多项式，我们有如下结论成立：

- $\forall h \in F[x], h(u)=0$，有$f \mid h$.
- f是F上的不可约多项式.

证明

设$h \in F[x], h(u)=0$. 作带余除法

$$h = qf + r, q, r \in F[x], \deg r < \deg f$$

则有

$$0 = h(u) = (qf+r)(u) = q(u)f(u) + r(u) = r(u)$$

由定义，f是满足$g(u)=0$的次数最低的非零多项式，则只能有$r=0$，即$h=qf$，即

$$f \mid h$$

再证f的不可约性。反证法，假设f在F上可约，则存在
$g_1, g_2 \in F[x], 1 \le \deg g_1, \deg g_2 < \deg f, f = g_1 g_2$，则有

$$0 = f(u) = (g_1 g_2)(u) = g_1(u) g_2(u)$$

这里又用到了**域**的一个关键性质，即两元素相乘为零，当且仅当其中有一个为零。这是一个并不平凡的性质，对于一般的环未必成立。
不妨设$g_1(u)=0$. 则g_1是比f的次数严格小，并且满足对u赋值为0的非零多项式，这与f的定义矛盾！从而f不可约。

推论

极小多项式是唯一的。
因为根据上述性质，如果有两个极小多项式，那么它们互相整除，又有首项系数都为幺元，故它们相等。

另一个证明思路

$I := \{h \in F[x] : h(u) = 0\}$构成$F[x]$的理想。并且若有$I = \{qf : q \in F[x]\}$，$f$首项系数为幺元，则$f$是极小多项式。

命题——$F(u)$的简化形式

设$F \subset K$是子域，$u \in K$是F的代数元，$f \in F[x]$是u在F上的极小多项式，则有

$$F(u) = \{r(u) : r \in F[x], \deg r < \deg f\}$$

并且，$\forall r_1, r_2 \in F[x], \deg r_1, \deg r_2 < \deg f$，则有

$$r_1(u) = r_2(u) \implies r_1 = r_2$$

亦即上述的表示一定是不重复的，少了谁都不行。

证明

先证后半部分。如果$r_1(u) = r_2(u)$，那么有

$$0 = r_1(u) - r_2(u) = (r_1 - r_2)(u)$$

由于$\deg(r_1 - r_2) < \deg f$，后者是极小多项式。因此只能有$r_1 - r_2 = 0$，即$r_1 = r_2$.
再证前半部分。记

$$L := \{r(u) : r \in F[x], \deg r < \deg f\}$$

显然有

$$L \subset F(u) = \{f(u)g(u)^{-1} : f, g \in F[x],\ \ g(u) \neq 0\}$$

下证

$$F(u) \subset L$$

任取$g \in F[x], g(u) \neq 0$. 我们证明存在$\phi \in F[x]$，使得

$$\phi(u) = g(u)^{-1}$$

由于f是F上的不可约多项式，则下面两个命题之一成立：

- $f \mid g$.
- 存在$v_1, v_2 \in F[x]$，使得$fv_1 + gv_2 = 1_K$.
  由于$f(u) = 0, g(u) \neq 0$, 则不可能有$f \mid g$. 故存在$v_1, v_2 \in F[x]$，使得$fv_1 + gv_2 = 1_K$. 两边赋值u，则有

  $$1_K = f(u)v_1(u) + g(u)v_2(u) = g(u)v_2(u)$$

  这里的v_2就是我们希望寻找的ϕ.

因此，表示$\{f(u)g(u)^{-1}: f, g \in F[x], \ g(u) \neq 0\}$不必有形如$g(u)^{-1}$的表示。现在就有

$$F(u) = \{h(u) : h \in F[x]\}$$

接下来只需要作带余除法，把次数降低到L中的次数即可。

$F(u)$的一个同构

沿用上述记号。考虑域F上多项式环$F[x]$，f是F上的不可约多项式（因为是极小多项式，所以不可约），考虑理想

$$I := \{qf : q \in F[x]\}$$

由f的不可约性，我们知道商环$F[x]/I$也是域。这个域与$F(u)$是同构的。

$$F[x]/I \cong F(u)$$

这个同构，可以由**环同态定理**证明。考虑映射

$$\phi : F[x] \to F(u), \phi(h) := h(u), \forall h \in F[x]$$

我们说明ϕ是一个环同态，$\ker \phi = I$，并且像集充满$F(u)$，进而由**环同态定理**可知

$$F[x]/I \cong F(u)$$

证明

首先证明ϕ是环同态。$\forall g, h \in F[x]$，有

$$\phi(g+h) = (g+h)(u) = g(u) + h(u) = \phi(g) + \phi(h)$$
$$\phi(gh) = (gh)(u) = g(u)h(u) = \phi(g)\phi(h)$$

即ϕ保持加法和乘法。因此ϕ是同态。还有ϕ的像集充满整个$F(u)$，因为前者就是

$$\{h(u) : h \in F[x]\}$$

最后证

$$\ker \phi = I$$

由

$$\forall h \in F[x], h \in \ker \phi \iff \phi(h) = 0 \iff h(u) = 0 \iff f \mid h$$

知上式成立。综上，由**环同态定理**，我们有

$$F[x]/I \cong F(u)$$

这个同构告诉我们，模一个不可约多项式，与将更大域中的元素添加进小域，最终得到的域是等价的。

以下结果不作要求：

定理

设$F \subset K$是子域，则下面两个命题等价。

- 存在$u \in K$是F上的代数元，使得$K = F(u)$.
- K中包含F的子域只有有限个.
  我们不证明完整的结论，只证明如下结论：
  若K中包含F的子域只有有限多个，F是无限集，则存在$u \in K$，使得$K = F(u)$.

证明

记

$$T := \{F(z) : z \in K\}$$

有条件，T是有限集，则T在包含关系下有极大元（亦即，不被T的其他元素包含的元素。）取$u \in K$，使得$F(u)$是T中包含关系下的极大元，即

$$\forall z \in K, F(u) \subset F(z) \implies F(u) = F(z)$$

下证$K = F(u)$. 对任意的$z \in K$，考虑集合

$$T' := \{F(az + u) : a \in F\} \subset T$$

注意T'是有限集，而F是无限集，故必须存在$a, b \in F, a \neq b$，使得

$$F(az + u) = F(bz + u) =: E$$

这是一种鸽笼原理的应用。注意$az + u \in E, bz + u \in E$，及封闭性，那么就有

$$(bz + u) - (az + u) = (b - a)z \in E$$

由$b - a \neq 0, b - a \in F \subset E$，有$(b - a)^{-1} \in F \subset E$，又有$(b - a)z \in E$，于是$z \in E$. 再有$az + u \in E$，最后就有$u \in E$，进而有$F(u) \subset E$. 又$F(u)$是$T$中的极大元，故有$E = F(u)$，则有$z \in F(u)$，最终有$K = F(u)$.

向量空间

给定域K，$(X,+)$是交换群，映射$\cdot: K\times X\to X$满足：

- $\forall a,b\in K,\forall x\in X$，有$a(bx)=(ab)x$.
- $\forall x\in X, 1_K x=x$.
- $\forall a,b\in K,\forall x\in X,(a+b)x=ax+bx$.
- $\forall a\in K,\forall x,y\in X,a(x+y)=ax+ay$.
  则称$(X,+)$在$\cdot$下构成K上的向量空间.

一个例子

对于域K与$n\in\mathbb{Z}^+$. 线性空间K^n. 加法定义为分量相加，数乘定义为分量相乘。

另一个例子

对于域$(K,+,\cdot)$，$F\subset K$是子域，则$(K,+)$构成F上的向量空间。

另另一个例子

回顾之前的内容，设$F\subset K$是子域，$u\in K$是F的代数元，$f\in F[x]$是u在F上的极小多项式，则有

$$F(u)=\{r(u):r\in F[x],\deg r<\deg f\}$$

F是$F(u)$的子域，于是$F(u)$按照域的乘法构成F上的向量空间。记$n:=\deg f$. 则有

$$1_K,u,u^2,\ldots,u^{n-1}$$

构成该空间的基。显然$F(u)$中所有的元素都可由它们的线性组合表示，现在还需证明它们是线性无关的。假设存在$a_0,a_1,\ldots,a_{n-1}$使得

$$a_0+a_1u+\ldots+a_{n-1}u^{n-1}=0$$

我们证明$a_i=0,i=0,1,\ldots,n-1$. 令$r=a_0+a_1x+\ldots a_{n-1}x^{n-1}\in F[x]$. 则有$r(u)=0$. 又有$f$是$u$在$F$上的极小多项式，$\deg r=n-1<\deg f$，故只能由$r=0$. 从而$a_i=0,i=0,1,\ldots,n-1$. 从而，我们说明了该空间的维数是$n$.