Week11摘要

Week11介绍的主要内容有：

- 模
- ”环上的Cayley定理“
- 环同态
- 理想
- 商环
- 环同态定理
- 多项式环的初步概念
  从**类比**的角度看，这些主题都在群论中有着相当明确的对应：模——群作用；Cayley定理；环同态——群同态；理想——正规子群；商环——商群；同态定理。这份笔记在叙述时，也着重强调了**类比**的思想。笔者认为，类比至少可以起到两方面的作用：帮助读者理解新的概念，以及强调旧的概念中的重要思想方法。尤其是，**理想——商环——环的同态定理**，对于我等并不专精数学的CS学生，其抽象性未免让人有些难以理解。为此，对于这三者，笔者在文中做了一些思路上的总结，希望帮助读者在抽象性中看到一些自然的清晰性，在此稍作推荐。详见后文”另一个对理想的定义的理解“和”我们如何理解同态定理“。

> 注：模的内容不会在考试中出现。

群，群作用，Cayley定理；环，模，“Cayley定理”

之前，我们研究过**群作用**。**群作用**是我们研究群的重要方法。通过研究一个群**作用**在某个集合上的结果，我们得以研究这个群自身的性质。在Sylow定理的证明中，我们就应用了这种方法。

那么，在**环**上，是否也存在类似的概念呢？有的兄弟，有的。这就是**模**。

在**群**中，我们还研究过Cayley定理，它将任意的群G映射到G的对称群$Sym(G)$上。那么，在环上，是否也有类似的结论？

模的概念

我们从一个例子开始引入**模**的概念。

回顾：线性空间

$\mathbb{R}^n$是$\mathbb{R}$上的向量空间，即满足：加法的结合律，存在加法零元，存在加法逆，加法的交换律；数乘的结合律，数乘的单位元，数乘与加法的两种分配律。
现在，我们现在可以用群论的语言描述为：

- $(\mathbb{R}^n,+)$是交换群。
- 数乘是作用（数域作用在交换群上）。
- 数乘满足两种分配律。

类比：模的严格定义

设$(R,+,\cdot)$是有幺元的环（对应向量空间中的$\mathbb{R}$），$(M,+)$是交换群（对应向量空间中的$\mathbb{R}^n$）。
$\rightarrow: R\times M\rightarrow M$。若有：

- $\rightarrow$是作用。即
  - 对任意$a,b\in R,x\in M$，有$a\rightarrow(b\rightarrow x)=(ab)\rightarrow x$
  - 对任意$x\in M$，有$1_R\rightarrow x=x$
- 满足作用关于加法的两种分配律。
  则称M在$\rightarrow$下构成左$R-$模。

例子

第一个例子：环$M_2(\mathbb{R})$, 交换群$(\mathbb{R}^2,+)$，作用（矩阵乘法），构成模。

第二个例子：从任何一个交换群$(M,+)$出发，都可以以如下的方式构造一个模。

考虑$R:=\{f|f:M\rightarrow M\text{是群同态}\}$。
定义R上的加法$+$：

$$\text{对任意}f,g\in R,\text{如下定义}f+g:\text{对任意}x\in M,(f+g)(x)=f(x)+g(x)$$

定义R上的乘法为映射的复合$\circ$。
容易验证$(R,+,\circ)$构成环。首先需要验证$+$和$\circ$都是封闭的。即对任意$f,g\in R$，$f+g$和$f\circ g$都是同态。事实上，对于任意$f,g\in R$:

$$(f+g)(x+y)=f(x+y)+g(x+y)=f(x)+f(y)+g(x)+g(y)=(f+g)(x)+(f+g)(y)$$

故$f+g$是也是同态。注意第三个等号用到了交换性。

$$(g\circ f)(x+y)=g(f(x)+f(y))=g(f(x))+g(f(y))=(g\circ f)(x)+(g\circ f)(y)$$

故$g\circ f$也是同态。
验证了封闭性之后，接着验证环的公理：

$(R,+)$是交换群

- 结合律：由M上的结合律保证。
- 幺元：将M的每个元素都映射到M的幺元的映射。
- 逆元：对于$f\in R$, 定义$-f:\text{对任意}x\in M,-f(x)=f(-x)$
- 交换律：由M上的交换律保证。

$(R,\circ)$是幺半群

- 结合律：由映射复合的结合律保证。
- 幺元：恒等映射。

分配律

对于任意$f,g,h\in R$, 任意$x\in M$,有：

$$((f+g)\circ h)(x)=(f+g)(h(x))=f(h(x))+g(h(x))=f\circ h(x)+g\circ h(x)$$

$$(f\circ(g+h))(x)=f((g+h)(x))=f(g(x)+h(x))=f(g(x))+f(h(x))=f\circ g(x)+f\circ h(x)$$

亦即对任意$f,g,h\in R$, 都有：

$$(f+g)\circ h=f\circ h+g\circ h$$

和

$$f\circ(g+h)=f\circ g+f\circ h$$

成立。这就是左右分配律

模结构

验证了$(R,+,\circ)$构成环之后，我们就得到如下的模结构：
R如下作用在M上：

$$\text{对任意}f\in R,x\in M,f\to x:=f(x)$$

我们可以验证：

$$(f\circ g)\to x=(f\circ g)(x)=f(g(x))=f\to(g(x))$$

$$id\to x=id(x)=x$$

当然分配律也成立。因此这构成一个模。

环上的"Cayley定理"

在群论的Cayley定理中，我们将任意的群映射到其上的对称群，得到了一个群到其上的对称群的单同态。（进一步地，若是将对称群限制为这个单同态的像集，就得到了任意的群到其对称群的的一个群同构）
对于环$(A,+,\circ)$，我们也想将它上的每个元素映射为一个映射，就像我们在Cayley定理中做的那样。如下定义：

$$\forall a\in A,L_a:A\to A\text{定义为}:\forall x\in A,L_a(x):=ax$$

我们有：对$a\in A$, L_a是$(A,+)$到自身的同态。这是因为

$$L_a(x+y)=a(x+y)=ax+ay=L_a(x)+L_a(y)$$

仿照前面例子的证明，我们可以知道$(\{L_a:a\in A\},+,\circ)$是一个环。并且有：

$$L_a+L_b=L_{a+b}$$

$$L_a\circ L_b=L_{ab}$$

进一步地，如果$(A,+,\circ)$有乘法幺元，则L是单射，并且$L_{1_A}=id_A$. 单射是因为：

$$L_a=L_b\implies L_a(1_A)=L_b(1_A)\implies a\circ 1_A=b\circ 1_A,\text{即}a=b$$

至此，$a\to L_a$就是环$(A,+,\circ)$到它的对称群上的一个单同态。进一步就可以得到一个同构。

> 以下的内容是考试要考的。

环同态

和群同态类似，简单来说，环同态就是**保持运算的映射。**
设$(R,+,\circ)$和$(S,+,\circ)$是环。$f:R\to S$，若有

$$\forall a,b\in R,f(a+b)=f(a)+f(b),f(ab)=f(a)f(b)$$

则称f为$(R,+,\circ)$到$(S,+,\circ)$的环同态。进一步，若f为双射，则称为环同构。

例子

第一个例子

$$\begin{bmatrix}a&b\\c&d\end{bmatrix}\to\begin{bmatrix}a&b&0\\c&d&0\\0&0&0\end{bmatrix}$$

是一个环同态。

第二个例子：矩阵与线性映射的同构

考虑

$$A:=\{f:f\text{是}\mathbb{R}^2\to\mathbb{R}^2\text{的线性映射}\}$$

则$(A,+,\circ)$构成环，其中$+$和$\circ$是映射的加法和复合；这个环与二阶实矩阵环$(M_2(\mathbb{R}),+,\cdot)$是同构的。这是因为，对于每个2阶实矩阵$B$，如下定义$f_B:\mathbb{R}^2\to\mathbb{R}^2$:

$$\forall x,y\in\mathbb{R},f_B(\begin{bmatrix}x\\y\end{bmatrix})=\begin{bmatrix}a&b\\c&d\end{bmatrix}\begin{bmatrix}x\\y\end{bmatrix}$$

我们有：

$$\forall B_1,B_2\in M_2(\mathbb{R}),f_{B1+B2}=f_{B1}+f_{B2},f_{B1B2}=f_{B1}f_{B2}$$

这一结论由矩阵加法和乘法的性质容易验证。因此$B \to f_B$确实是一个环同态。接下来我们证明单射性质和满射性质。以此说明$B \to f_B$是一个环同构。

单射性质：

注意，我们有

$$f_{B_1} = f_{B_2} \implies \forall x, y \in \mathbb{R}, B_1 \begin{bmatrix} x \\ y \end{bmatrix} = B_2 \begin{bmatrix} x \\ y \end{bmatrix}$$

分别取$\begin{bmatrix} x \\ y \end{bmatrix} = \begin{bmatrix} 1 \\ 0 \end{bmatrix}$和$\begin{bmatrix} x \\ y \end{bmatrix} = \begin{bmatrix} 0 \\ 1 \end{bmatrix}$即可证明$B_1 = B_2$.

满射性质：

任取$\mathbb{R}^2 \to \mathbb{R}^2$的线性映射$\sigma$. 记

$$\sigma(\begin{bmatrix} 1 \\ 0 \end{bmatrix}) = \begin{bmatrix} a \\ c \end{bmatrix}$$

$$\sigma(\begin{bmatrix} 0 \\ 1 \end{bmatrix}) = \begin{bmatrix} b \\ d \end{bmatrix}$$

则容易验证

$$\sigma = f_{\begin{bmatrix} a & b \\ c & d \end{bmatrix}}$$

这是因为

$$\begin{aligned} \forall x, y \in \mathbb{R}, \sigma(\begin{bmatrix} x \\ y \end{bmatrix}) &= \sigma(x \begin{bmatrix} 1 \\ 0 \end{bmatrix}) + \sigma(y \begin{bmatrix} 0 \\ 1 \end{bmatrix}) \\ &= x\sigma(\begin{bmatrix} 1 \\ 0 \end{bmatrix}) + y\sigma(\begin{bmatrix} 0 \\ 1 \end{bmatrix}) \\ &= x \begin{bmatrix} a \\ c \end{bmatrix} + y \begin{bmatrix} b \\ d \end{bmatrix} \\ &= \begin{bmatrix} ax + by \\ cx + dy \end{bmatrix} \\ &= \begin{bmatrix} a & b \\ c & d \end{bmatrix} \begin{bmatrix} x \\ y \end{bmatrix} \\ &= f_{\begin{bmatrix} a & b \\ c & d \end{bmatrix}}(\begin{bmatrix} x \\ y \end{bmatrix}) \end{aligned}$$

这当然是线性代数中的经典结论。今天我们从环同构的角度去理解它。

理想的概念

在群论中，我们有正规子群，正规子群可以诱导商群。那么在环论中，有没有类似的概念？
在群中，一个经典的正规子群是群同态的核。在环中，我们也从同态的核开始引入对应的概念，即**理想**。
考虑$R \to S$的环同态f. 记

$$Ker(f) := \{x \in R : f(x) = 0\}$$

由环的定义和核的基本性质，我们有$Ker(f)$是$(R, +)$的子群。然而，**子群**的结论仅仅考虑了环上**加法**的性质。其实，对于环上的**乘法**，$Ker(f)$也有良好的性质：

$$\forall a, b \in Ker(f), f(ab) = f(a)f(b) = 00 = 0, f(ba) = f(b)f(a) = 00 = 0$$

事实上，很容易看出这个结论可以加强：a, b中只要有一个是$Ker(f)$的元素即可。
将这个核的概念做一步抽象，我们就得到了**理想**的概念：

对于环$(R, +, \cdot)$, I是$(R, +)$的子群。若有：

$$\forall a \in I, b \in R, ba \in I, ab \in I$$

则称I是$(R, +, \cdot)$的理想。
由上面的结论，我们可以看出环同态的核就是一个理想。
注意：交换群的子群一定是正规子群。因为一定有

$$aI = Ia, \forall a \in R$$

> 和正规子群诱导商群类似，理想也能够诱导商环。这正是**理想**这一概念的重要之处。

例子：整数环的理想

我们熟知，整数加群的子群具有如下的形式:

$$\{bq : q \in \mathbb{Z}\}，\text{其中} b \in \mathbb{Z}$$

根据理想的定义，容易看出整数加群的子群都是整数环的理想。

另一个对理想的定义的理解

对于群$(G, \cdot)$以及G的正规子群H诱导的商群$(G/H, \cdot)$，有很好的运算性质：

$$\forall a, b \in G, (aH) \cdot (bH) = (ab)H$$

这里的重点在于，所谓**代表元无关**的性质。这是什么意思呢？
我们知道，商群的每个元素都是一个**等价类**。在这里，表示出这个等价类，我们就不得不借助这个等价类中的一个元素，也就是**代表元**。我们把aH表示为aH，这里a就是**代表元**。既然一个等价类可能有多个元素，那么我们当然可以用aH中的另一个元素$a' \in aH$来将aH表示为$a'H$. 同样，bH也可以写成$b'H$，其中$b' \in bH$.
说到这里，还没什么问题。问题出现在我们将要进行的运算上。既然有

$$aH = a'H, bH = b'H$$

那么aH和bH, $a'H$和$b'H$相乘的结果应该是一致的。根据上述定理，也就是应该有

$$(ab)H = (a'b')H$$

这就是说，对于同样的陪集，无论选取怎样的代表元，运算得到的结果总是一致的。这就是**代表元无关**。但是我们知道，这个结论，对于一般的子群H未必是成立的，但是对于**正规子群**H一定是成立的。这就是为什么一般的子群H得到的商集G/H无法构成群，也正是为什么我们要将H限制为**正规子群**，或者说，为什么**正规子群**在群论中是重要的。
在使用代表元来定义运算时，我们总是要注意这种运算是不是**代表元无关**的，以检验这个定义是否合理(well-defined)。

在群论中，我们有**商群**这一良好的结构。那么在环上，我们自然也希望找到**类似的结构**。这个结构应当也是一个**环**，因此，我们自然要先尝试去定义这个环的**乘法**。
正如**正规子群**确保了陪集运算的代表元无关性质，进而得以诱导**商群**；**理想**也在**环**上确保了类似的**代表元无关**性质，从而得以诱导**商环**。

对于我们希望在R/I上定义的乘法，一个自然的想法是将它定义为：

$$(u+I)*(v+I) = uv+I$$

注：当用符号+表示群运算时，习惯上也将陪集uI写作$u+I$
和上面在**商群**中提到的问题一样，需要注意，运算的结果$uv+I$是一个陪集，但是它是由代表元u, v表示的。当代表元不同时，运算的结果是否能保持相同呢？也就是说，这个运算是否是**well-defined**的？形式化地说，当

$$u+I = x+I, v+I = y+I$$

成立时，是否有

$$uv+I = xy+I$$

成立呢？
事实上，当I是一个**理想**时，我们就能保证这种良定性。我们接下来给出证明。

设I是一个理想，则对

$$u, v, x, y \in R, u+I = x+I, v+I = y+I$$

总有

$$xy+I = uv+I$$

证明：由条件，存在$a, b \in I$使得$x = u+a$,$y = v+b$. 则有

$$xy = (u+a)(v+b) = ub + a(v+b) + uv$$

由理想的定义，$b \in I$, $a \in I$，有$ub \in I, a(v+b) \in I$（**注意，这里理想的定义，两边都用到了**），从而$ub + a(v+b) \in I$，从而$xy \in uv+I$，于是$xy+I = uv+I$.

事实上，不仅**理想**可以使得上述的定义合理，并且上述定义如果合理，则也可保证I是理想。也就是说：

> 从**商环**的角度，**理想**的概念是充分且必要的。

商环

命题

设R是环，I是R的理想，在R/I上定义二元运算$+$和$*$：

$$\forall u, v \in R, (u+I)+(v+I)=(u+v)+I$$

$$\forall u, v \in R, (u+I)*(v+I)=uv+I$$

则$(R/I, +, *)$构成环。并且当R有乘法幺元1_R时，1_R+I是该商环的乘法幺元。

证明

这种运算定义的合理性，我们已经论证过，不再赘述。接下来验证环公理：

- $(G/I, +)$构成交换群。这由$(R, +)$构成交换群直接保证。
- $*$的结合律。这由$(R, \cdot)$的结合律直接保证。
- 分配律：

  $$\forall u, v, w \in R, (u+I)*((v+I)+(w+I))=(u+I)*((v+w)+I)=u(v+w)+I=(uv+uw)+$$

  又有：

  $$(uv+uw)+I=(uv+I)+(uw+I)=((u+I)*(v+I))+((u+I)*(w+I))$$

  故左分配律成立。右分配律的验证也是类似的。

当R有乘法幺元时，有

$$(1_R+I)*(u+I)=(1_R u)+I=u+I$$

同理，右乘也是一样。

环的同态定理

在群同态的研究中，我们知道，可以将一个一般的群同态，借助其核诱导的商群，"升级"为一个单同态。并且依据像集的性质，可能可以进一步得到同构。在环中，是否会有类似的可能性呢？

环到其商环的自然同态

设R是环，I是R的理想，如下定义$f: R \to R/I$：

$$\forall x \in R, f(x) := x + I$$

则f是环同态。并且$Ker(f) = I$,$Im(f) = R/I$

证明

我们已经知道，f是$(R, +)$到$(R/I, +)$的同态。这个结论在群到商群的自然同态处已经得到证明。
接下来证明f保持乘法。我们有：

$$\forall u, v \in R, f(uv) = uv + I, f(u) * f(v) = (u + I) * (v + I) = uv + I$$

因此

$$f(uv) = f(u) * f(v)$$

即f保持乘法。另外容易验证I是$(R/I, +)$的幺元，并且

$$Ker(f) = \{u \in R : f(u) = u + I = I\}$$

又熟知

$$u + I = I \iff u \in I$$

因此

$$Ker(f) = I$$

最后，

$$Im(f) = R/I$$

是显然的。

环的同态定理

设R,S是环，$\phi : R \to S$是环同态。$I = Ker(\phi)$，则有：

1. I是R的理想。
2. 如下定义$g : R/I \to S$:

$$\forall u \in R, g(u + I) = \phi(u)$$

   则g是**well-defined**的，并且g是商环R/I到S的单同态。

证明

事实上，由群的同态定理，很多结论已经无须验证。但是此处为完整起见，我们依然全部重新证明。
(1)
$Ker(\phi) = \{u \in R : \phi(u) = 0\}$

我们有：

$$\forall u,v\in I,有\phi(u+v)=\phi(u)+\phi(v)=0+0=0$$
$$\phi(-u)=-\phi(u)=-0=0$$

因此，I是R的加法子群。又有

$$\phi(ab)=\phi(a)\phi(b)=0\phi(b)=0,即ab\in I,\forall a\in I,\forall b\in R.同理ba\in I$$

故I确实是R的理想。
(2)
我们要说明，g的像是代表元无关的。也就是要断言：

$$\forall u,v\in R,u+I=v+I\iff\phi(u)=\phi(v)$$

断言的证明：

$$u+I=v+I\implies v\in u+I\implies 存在b\in I使得v=u+b$$

从而

$$\phi(v)=\phi(u+b)=\phi(u)+\phi(b)=\phi(u)+0=\phi(u)$$

又有

$$\phi(v)=\phi(u)\implies\phi(v-u)=\phi(v)-\phi(u)=0\implies v-u\in I,即v+I=u+I$$

故断言是成立的。这个断言和**群的同态定理**中的完全一致。
由这个断言，g就是well-defined. 接下来验证g的同态性质。

$$g(u+I)+g(v+I)=\phi(u)+\phi(v)=\phi(u+v)=g((u+v)+I)=g((u+I)+(v+I))$$
$$g(u+I)g(v+I)=\phi(u)\phi(v)=\phi(uv)=g(uv+I)=g((u+I)*(v+I))$$

因此g是同态。单同态由前面的断言保证。

推论

记号同上。若有

$$Im(\phi)=S$$

那么

$$R/Ker(\phi)\cong S$$

即像集对核的商环与像集同构。

这是当然的，条件

$$Im(\phi)=S$$

正好保证了上面定义的g是一个满同态。又已经证明g是一个单同态，那么自然是同构。

我们如何理解同态定理

简单来说，同态定理确保我们能做这样一件事：把一个已知的同态，通过变换其原像集，“升级”为一个**单同态**。并且在像集比较好的情况下，得到一个同构。
这里，原来的同态是$\phi : R \to S$，变换后的像集为R/I, “升级”得到的单同态是$g : R/I \to S$. 在$Im(\phi)$充满S时，g就是一个同构。

那么，这个“升级”是怎么做到的呢？既然我们希望得到一个**单同态**，那么就不能有R的元素被映到同一个像上。而世界如此美好，恰好就有一种自然的方法，把R中所有映射到同一个像的元素聚在一起，那就是让R对这个同态的**核**做**商结构**。注意：

- 在**群同态**中，**群同态的核**是原像集的**正规子群**，因此可以做**商群**。
- 在**环同态**中，**环同态的核**是原像集的**理想**，因此可以做**商环**。
  这个**商结构**中的每个元素，恰好是原像集中的一个**等价类**，这个等价类中的元素都被ϕ映射到像集的同一个元素，并且被映射到该元素的原像都在该等价类中。

上述的**同态的核诱导的商结构**的良好性质，intuitively speaking, 或许可以说是一种同态的像对于其核的”平移不变性“。为什么我这么说呢？对于$u, v \in R$, 我们已经证明，$\phi(u) = \phi(v)$等价于u, v在核I诱导的同一陪集中。也就是说，u, v可以通过加或减去I中的某一元素，互相得到，而不影响映射后的取值。

例子

考虑$n \in \mathbb{Z}, n \geq 2$，那么$\mathbb{Z}_n$对模$n$的加法与乘法构成环。考虑映射$f : \mathbb{Z} \to \mathbb{Z}_n, f(m) = m \mod n$.
这当然是一个环同态.
显然有

$$Ker(f) = n\mathbb{Z}$$

那么由同态定理就有

$$\mathbb{Z}/n\mathbb{Z} \cong \mathbb{Z}_n$$

这当然是我们熟知的同构。

多项式环

$$f = a_0 + a_1 x + a_2 x^2 + \ldots + a_n x^n, a_i \in \mathbb{R}$$

环上多项式的定义

设$(R,+,\cdot)$是有乘法幺元的环。x是未定元。则一个表达式

$$f=a_0+a_1x+a_2x^2+...+a_nx^n, n\in\mathbb{N}, a_i\in R, \forall 0\le a_i\le n$$

称为R上的一个多项式。R上的多项式全体记为$R[x]$.

考虑结构$(R[x],+,\cdot)$，其中$+$和$\cdot$如下定义：
对于

$$f=a_0+a_1x+a_2x^2+...+a_nx^n$$

$$
g=b_0+b_1x+b_2x^2+...+b_nx^n

定义$$f+g := f=(a_0+b_0)+(a_1+b_1)x+(a_2+b_2)x^2+...+(a_n+b_n)x^n$$注意，上面的系数是可以

由环上的分配律，这个定义是自然的。容易看出，$(R[x],+,\cdot)$构成环，它称为R上的一元多项式环。
加法幺元为零多项式，逆元为各个系数取负数，乘法幺元同R的乘法幺元。

在计算机科学中，有更快的计算多项式乘积的算法。

多项式的另一个定义

我们给出一个更**形式化**的定义：
给定R是有乘法幺元的环。记

$$T := \{(a_0,a_1,a_2,...,a_n,...)|a_i\in R, \forall i\in\mathbb{N}\}$$

（当然，T也可理解为所有$\mathbb{N}$到R的映射全体）
基于此，**多项式全体的集合**T_1定义为T的子集，满足对于每个元素，至多有有限个$a_i\neq 0$.
我们在T上定义加法和乘法，从而T_1继承T上的加法和乘法（需要注意，继承来的加法和乘法在$R[x]$上是**封闭**的）

$$\text{对于}\alpha = (a_0, a_1, a_2, \dots, a_n, \dots) \in T, \beta = (b_0, b_1, b_2, \dots, b_n, \dots) \in T$$
$$\text{定义}: \alpha + \beta := (a_0 + b_0, a_1 + b_1, \dots, a_n + b_n, \dots)$$
$$\alpha \cdot \beta := (c_0, c_1, \dots, c_n, \dots)$$
$$\text{其中}: \forall c \in \mathbb{N}, c_n = \sum_{i=0}^{n} a_i b_{n-i} = \sum_{i,j \in \mathbb{N}, i+j=n} a_i$$

我们容易验证$(T, +, \cdot)$构成环。这个环称为R上的幂级数环。这个环，熟悉组合数学的母函数方法的同学应当感到熟悉。其中，加法幺元为

$$(0, 0, \dots, 0, \dots)$$

乘法幺元为

$$(1, 0, 0, \dots 0, \dots)$$

继承这里的$+$和$\cdot$的定义，我们仍然得到同样的多项式环$(T_1, +, \cdot)$.
这个定义的好处在于，我们避免了上述定义中**未说明的**未定元x. 具体而言:

$$x = (0, 1, 0, 0, \dots, 0, \dots) \in T, T_1$$

(即T中仅第一个分量为1的元素。)
我们将T_1记作$R[x]$. 可以理解为，将x**添加**进R后(添加后，由封闭性，就得到x的所有的有限幂次，进而与T中的元素进行种种运算组合)，就得到T_1.

对于$R[x]$中的每个元素，可以定义它的次数:

$$\text{对}\alpha = (a_0, a_1, a_2, \dots, a_n, \dots)\text{，定义} \deg \alpha = \max\{n \in \mathbb{N} | a_n \neq 0\}$$

这个定义是有意义的，因为由$R[x]$的定义$\{n \in \mathbb{N} | a_n \neq 0\}$一定是有限集。

域

回顾：域的概念

$(F, +, \cdot)$是域，是指它是有乘法幺元的交换环。并且

$$\forall a \in F, a \neq 0, \text{存在} b \in F \text{使得} ab = 1_F$$

命题——域仅有“平凡理想”

域$(F, +, \cdot)$仅有$\{0\}$和F.

证明

设I是F的理想，$I \neq \{0\}$. 下证$I = F$. 有条件，可取$a \in I, a \neq 0$.
由F是域，存在$b \in F$使得$ab = 1_F$. 那么由理想的定义，$1_F = ab \in I$.

那么，对任意的$c \in F$, 有$c = c1_F \in I$，故$I = F$.

可以看到，证明的关键在于域上**每个非零元素都由乘法逆。**

逆命题

设R是有幺元的交换环，且R仅有平凡理想，则R是域。
这个命题也是真的。读者可以自己证明。

- 代数基本定理：n次多项式f在$\mathbb{R}$上至多有n个根（计重数），在$\mathbb{C}$在恰好有n个根（计重数）。
- 奇数次多项式在$\mathbb{R}$上一定有实根 + Sylow定理可以证明上述定理。

在计算机科学中，一个快速判断非标准形式的（之所以不写成标准形式，是因为比较大的计算开销）多项式是否是零多项式的方法如下：
取充分大的有限域F，使得$|F| >> n$，随机$c \in F$，计算$f(c)$.
显然，取到f的零点的概率不高于$\frac{n}{|F|}$, 进行若干次迭代，若都由$f(c) = 0$, 那么f有极大概率是零多项式。

多项式的带余除法

回顾整数的带余除法：

$$\text{对}a \in \mathbb{Z}^+, b \in \mathbb{Z}, \text{则存在}q, r \in \mathbb{Z}, \text{使得}b = qa + r, 0 \leq r \leq a - 1$$

对于多项式，也有类似的结论：

$$\text{对多项式}f(\text{非零}), g, \text{存在多项式}q, r\text{使得}g = qf + r. \text{其中}\deg r < \deg f$$

其中，$\deg f$表示多项式f的次数

带余除法的例子

$$g = x^4 + 2x^3 + 5x + 1, f = x^2 + x + 1$$

显然，可以用f消去g的最高此项：

$$g - x^2 f = x^3 - x^2 + 5x + 1$$

接着，我们还可以用f消去$g - x^2 f$的最高次项：

$$h := g - x^2 f - xf = -2x^2 + 4x + 1$$

现在还有办法用f消去h的最高次项：

$$h+2f=6x+3$$

现在f已经消不了$h+2f$的最高次项了。因为f的次数已经高于$h+2f$.

最后的一个式子，就是：

$$g-x^2f-xf+2f=6x+3$$

亦即：

$$g=(x^2+x-2)f+(6x+3)$$

在上述定义的记号中，就有

$$q=x^2+x-2, r=6x+3$$