近世代数之六

陈小伍
中国科学技术大学

xwchen@mail.ustc.edu.cn

内容梗概

1. 一元多项式环
2. 主理想整环PID
3. 不可约多项式
4. 添根构造

多项式

设R为环，x为字母（形式符号）

1. R上关于x的多项式

$$f(x) = a_n x^n + \cdots + a_2 x^2 + a_1 x + a_0$$

系数$a_i \in R$，其中的$a_i x^i$为单项式

2. 两多项式相等 $\Leftrightarrow$ 对应系数相等
3. 若$a_n \neq 0_R$，则称$a_n x^n$为**首项**，a_n为**首项系数**，定义**次数**$\deg(f) = n$；a_0 为常数项
4. 约定：$0_R x^i$可以略去，$1_R x^i$简记为x^i
5. 多项式$f(x)$称为**首一**的(monic)，若$a_n = 1_R$

一元多项式环

1. $R[x]$自然成为环。
2. 零多项式0_R，不定义次数；其他常值多项式a的次数定义为0
3. 有典范环嵌入$R \hookrightarrow R[x],\ a \mapsto a$
4. $x \in R[x]$，于是，单项式x^i恰等于x的第i次幂

$R[x]$的“另类定义”：考虑

$$\bar{R} = \{(a_0, a_1, \cdots) \mid a_i \in R, a_i = 0_R \text{ when } i \gg 0\}$$

可以定义其上的加法和乘法使得

$$R[x] \simeq \bar{R}, \quad x \mapsto (0_R, 1_R, 0_R, \cdots)$$

整环

命题

若R为整环，则$R[x]$亦为整环。特别地，若k为域，$k[x]$为整环。

注：$R[x]$绝不是域，因为$U(R[x]) \simeq U(R)$。

泛性质

命题

设R为环。对于任给的环同态$\psi\colon R \to S$以及$s \in S$，则唯一存在环同态

$$\tilde{\psi}\colon R[x] \longrightarrow S$$

使得$\tilde{\psi}|_R = \psi$且$\psi(x) = s$.

例子

考虑$\mathrm{Id}_R\colon R \to R$以及$a \in R$。则$a$处的**赋值同态**

$$\mathrm{ev}_a\colon R[x] \longrightarrow R$$

使得$f(x) \mapsto f(a)$，称为多项式$f(x)$在a处的**取值**。(强调：这只是形象的说法，不确切；因为$f(x)$不是函数，故，不能取值!)

例子，续

例子

设$f(x) \in R[x]$。则多项式$f(x)$给出**多项式函数**

$$f\colon R \longrightarrow R, \quad a \mapsto f(a)$$

即，$f \in \mathrm{Map}(R, R)$。强调：函数f在a处（真的可以）取值！

定义函数环$\mathrm{Map}(R, R)$以及**赋值同态**

$$\mathrm{ev}\colon R[x] \longrightarrow \mathrm{Map}(R, R), \quad f(x) \mapsto f.$$

该映射一般不是单射。

不能混淆$f(x)$以及f，它们根本不在同一集合里！

带余除法

回顾：初等数论的基石 — $\mathbb{Z}$上的带余除法

从现在开始，k为域。（**首一化**: $f(x) = a \cdot \bar{f}(x)$，其中$a$为首项系数，$\bar{f}(x)$为首一多项式）

定理

给定多项式$f(x)$以及非零多项式$h(x)$。则存在多项式$q(x), r(x) \in k[x]$使得

$$f(x) = q(x) \cdot h(x) + r(x)$$

且$r(x) = 0$或$\deg(r) < \deg(h)$。这样的$q(x)$与$r(x)$是唯一的。

注：$h(x)|f(x)$ 当且仅当$r(x) = 0$。

余数定理

定理

给定多项式$f(x)$以及$a \in k$。则唯一存在多项式$q(x) \in k[x]$使得

$$f(x) = q(x) \cdot (x - a) + f(a).$$

特别地，$(x - a) | f(x)$ 当且仅当$f(a) = 0_k$。

展望：**解集** $\mathrm{Root}_k(f) = \{a \in k \mid f(a) = 0_k\}$本质上是$f(x)$的“线性因子”。

主理想整环PID

定义

整环R称为**PID**，若其任何理想均为主理想。

注：按定义，域为PID。但，我们仅考虑非域的PID。

定理

$\mathbb{Z}$以及$k[x]$均为PID。

证明：利用带余除法。数的绝对值vs多项式的次数!

PID的基本性质

设R为整环。利用整除关系，定义最大公因子$\gcd(a,b)$（不一定存在）。

PID满足如下：

1. 任何非零元素a,b，存在$\gcd(a,b)$
2. 存在Bezout等式
3. 素元=不可约元
4. 任何非零素理想均极大。故，$\mathrm{Spec}(R)=\{0\}\cup\mathrm{Max}(R)$。

最大公因式与不可约多项式

在$k[x]$，我们可以约定：仅考虑首一多项式

例如：多项式$f(x), g(x) \in k[x]$，其**最大公因式**是指**首一**多项式$h(x)$满足：$h|f, h|g$，且若$a(x)|f, a(x)|g$，总有$h|a(x)$。

例如：$k[x]$中不可约元称为**域k上的不可约多项式**，故

$$\mathrm{Max}(k[x]) \longleftrightarrow \{k\text{上首一不可约多项式}\}$$

特别地，$k \hookrightarrow \mathrm{Max}(k[x]), \quad \lambda \mapsto (x - \lambda)$。

域扩张

设有域的包含关系$k \subseteq K$。则$f(x) \in k[x]$可视为$K[x]$中元素。

1. $\mathrm{Root}_k(f) \subseteq \mathrm{Root}_K(f)$
2. $f(x) \in k[x]$不可约 $\nRightarrow$ $f(x) \in K[x]$不可约
3. 设$f(x), g(x) \in k[x]$。但，总有$\gcd_{k[x]}(f,g) = \gcd_{K[x]}(f,g)$

思考：若域扩张$\theta\colon k \hookrightarrow K$（域同态一定是单的），相应的结果呢？

添根构造

设k为域，$f(x) \in k[x]$为首一不可约多项式。注意：若$\deg(f) \geq 2$，则$\mathrm{Root}_k(f) = \emptyset$。

构造

考虑典范同态

$$\theta\colon k \xrightarrow{\text{can}} k[x] \xrightarrow{\text{can}} k[x]/(f(x)) = K$$

仍记$\theta(\lambda) = \lambda + (f(x))$为$\lambda$，于是，我们有$k \subseteq K$（危险否？）

记$u = x + (f(x)) \in K$，务必忘记上面的符号x，被$u \in K$取代！

视$f(x) \in K[x]$，有重要观察:$u \in \mathrm{Root}_K(f)$，即，$f(u) = 0_K$。

$$f(x) = (x - u) \cdot g(x)$$

其中$g(x) \in K[x]$，次数降低。探究k-线性空间K的维数，基。

泛性质

考虑$\theta\colon k \hookrightarrow K = k[x]/(f(x))$如上。

定理

任给域同态$\delta\colon k \to F$，以及$\alpha \in F$满足$\delta(f)(\alpha) = 0_F$。则唯一存在域同态

$$\delta'\colon K \longrightarrow F$$

使得$\delta = \delta' \circ \theta$以及$\delta'(u) = \alpha$。

注：$\delta(f) \in F[x]$; 等式$\delta = \delta' \circ \theta$意味着$\delta'$**延拓**$\delta$。

例子

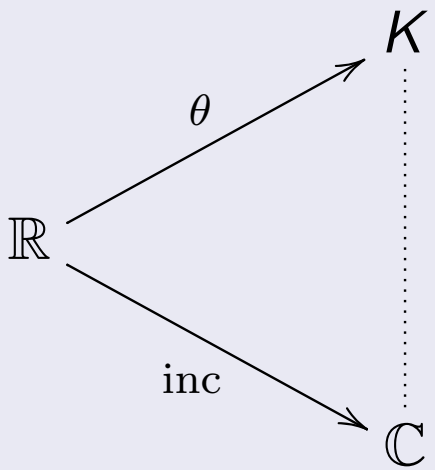
例子

考虑不可约多项式$x^2+1 \in \mathbb{R}[x]$，以及域嵌入

$$\theta\colon \mathbb{R} \longrightarrow \mathbb{R}[x]/(x^2+1) = K$$

记$u = x + (x^2+1) \in K$。则K中元素为$a+bu$，其中$a, b \in \mathbb{R}$。

探求：K与$\mathbb{C}$的关系，更确切的，两同态的关系



四元域

记$\mathbb{F}_2 = \{\bar{0}, \bar{1}\}$。

例子

考虑不可约多项式$x^2 + x + \bar{1} \in \mathbb{F}_2[x]$，以及域同态

$$\mathbb{F}_2 \hookrightarrow \mathbb{F}_2[x]/(x^2 + x + \bar{1}) = \mathbb{F}_4$$

记$u = x + (x^2 + x + \bar{1}) \in \mathbb{F}_4$（$\mathbb{F}_4$中，没有$x$，只有$u!!!$）。

探求：$\mathbb{F}_4$的加法表与乘法表。

解方程：在$\mathbb{F}_4$中解方程$x^2 + x + \bar{1} = \bar{0}$。

比较：$\mathbb{F}_4$与$\mathbb{Z}_4$

九元域

记$\mathbb{F}_3 = \{\bar{0}, \bar{1}, \bar{2}\}$。

例子

考虑不可约多项式$x^2 + \bar{1} \in \mathbb{F}_3[x]$，以及域同态

$$\mathbb{F}_3 \hookrightarrow \mathbb{F}_3[x]/(x^2 + \bar{1}) = \mathbb{F}_9$$

记$v = x + (x^2 + \bar{1}) \in \mathbb{F}_9$（$\mathbb{F}_9$中，没有$x$，只有$v$!!!）。

探求：$\mathbb{F}_9$的加法表与乘法表。

解方程：在$\mathbb{F}_9$中解$x^2 + \bar{1} = \bar{0}$。

比较：$\mathbb{F}_4$与$\mathbb{Z}_9$