抽象代数学

我们最熟悉整数环 $\mathbb{Z}$ 和域 $\mathbb{Q}$，它们的关系将被推广到整环与分式域的关系.

定义 设 R 是一个整环，$a\neq 0\in R$，若存在 $m\in\mathbb{N}$，$ma=0$ 则 a 是周期元，若 m 是使 $ka=0$，$k\in\mathbb{N}$ 的最小自然数 则 m 是 a 的周期.

定理 设 R 是一个整环，若存在一个周期元，则存在素数 p，$\forall r\neq 0\in R$，$pr=0$. p 称为 R 的特征 (记作 $\mathrm{char}R=p$)

证明：设 a 是一个周期元，$\exists m\in\mathbb{N}$，$ma=0$

$\forall b\in R$，$0=(ma)b=a(mb)\Rightarrow mb=0$（无零因子）

假设 m 是 a 的周期，若 $m=m_1m_2$ $m_1<m_2<m$，

则 $m_1a=0$ 或 $m_2a=0$，否则 $m_2a\neq 0$，$m_1(m_2a)=0$

$\forall b\in R$，$m_1b=0$，这与 m 的最小性矛盾. 因此 m 是一个素数 p.

例：p 素数，$\mathbb{Z}_p$ 是一个域，特征 $=p$. 记作 $\mathrm{char}\,\mathbb{Z}_p=p$

$\mathbb{Q}$ 有理数域，无有限特征. $\mathrm{char}\,\mathbb{Q}=0$

例：若整环 R 含幺元，则幺元在加法群中的阶

就是R的特征

证明：设$1\in R$，若$o(1)=+\infty$，则R特征$=+\infty$

若$o(1)=n>0$，则$\forall a\in R$，$na=(n\cdot 1)a=0$

n是素数，否则$n=n_1n_2$　　$n_1n_2\cdot 1=n_1(n_2\cdot 1)=0=(n_1\cdot 1)\cdot(n_2\cdot 1)$

$\Rightarrow n_1\cdot 1=0$或$n_2\cdot 1=0$

例　设R是整环，$a,b\in R$，$na=nb$，$n\in N$

(1) 若$\mathrm{char}R=$ ，则$a=b$；

(2) 若$\mathrm{char}R=r$，且r与n互素，则$a=b$

证明：$n(a-b)=0$　若$a\neq b$，则由定理$\mathrm{char}R<\infty$

设$\mathrm{char}R=r$，$(r,n)=d$，$n=qr+r_0$

$\Rightarrow r_0(a-b)=0\Rightarrow r_0=0$　即$r\mid n$

定理　设F是一个域，且不含非零真子域，则

(1) $\mathrm{char}F=0$，则$F\cong\mathbb{Q}$

(2) $\mathrm{char}F=p$，则$F\cong\mathbb{Z}_p$

证明：(1) 若$\mathrm{char}F=0$，$1\in F$　定义$\Delta=\{(n\cdot 1)\cdot(m\cdot 1)^{-1}\mid m,n\in\mathbb{Z},$

$m\neq 0\}$，$\Delta\subseteq F$，且Δ是个域　则$\Delta=F$

$$\begin{aligned}\Delta &\longrightarrow \mathbb{Q}\\ (n\cdot 1)\cdot(m\cdot 1)^{-1} &\longmapsto \frac{n}{m}\end{aligned}$$

(2) $\mathrm{char}F=p$，令 $\Delta=\{0,1,2\cdot 1,\cdots,(p-1)\cdot 1\}$

Δ 是一个域：$\forall m\cdot 1$ $0\le m<p$，$\Rightarrow (m,p)=1$ $\exists u,v$

$um+vp=1$ $(um+vp)\cdot 1=(um)\cdot 1=(u\cdot 1)\cdot(m\cdot 1)=1$.

$$\begin{aligned}\Delta &\longrightarrow \mathbb{Z}_p\\ m\cdot 1 &\longmapsto \overline{m}\end{aligned}$$

问题：如何从 $\mathbb{Z}$ 诱导出 $\mathbb{Q}$ 的构造.

$\mathbb{Q}=\{\frac{n}{m}\mid n,m\in\mathbb{Z},m\neq 0\}\longleftrightarrow\{(n,m)\mid n,m\in\mathbb{Z},m\neq 0\}$

$=\mathbb{Z}\times\mathbb{Z}^*$ $\mathbb{Z}^*=\mathbb{Z}\setminus\{0\}$

一般地，设 R 是含幺交换整环（称为整区 domain 或 integral domain）

$R\times R^*=\{(a,b)\mid a,b\in R,b\in R^*\}$

定义一个等价：$(a,b)\sim(c,d)\Leftrightarrow ad=bc$

它是一个等价关系. 令 (a,b) 的等价类为 $\frac{a}{b}=\overline{(a,b)}$

F 是等价类的集合. 定义

加法：$\overline{(a,b)}+\overline{(c,d)}=\overline{(ad+bc,bd)}$

乘法：$\overline{(a,b)}\cdot\overline{(c,d)}=\overline{(ac,bd)}$

这是定义合理的. 例如加法合理性

$\overline{(a,b)}=\overline{(a',b')}$，$\overline{(c,d)}=\overline{(c',d')}$

则 $ab'=ba'$，$cd'=dc'$

$\overline{(a,b)}+\overline{(c,d)}=\overline{(ad+bc,bd)}$

$\overline{(a',b')}+\overline{(c',d')}=\overline{(a'd'+b'c',b'd')}$

因为 $(ad+bc)b'd'=ab'dd'+bb'cd'=a'bdd'+bb'c'd$

$(a'd'+b'c')bd=a'd'bd+b'c'bd$ $\overset{\text{ⅱ}}{=}$

$\Rightarrow$ 定义合理.

性质：F关于以上加法、乘法构成一个域，包含R

证明：F的零元：$\overline{(0,m)}$ $m\in R^*$

F的幺元：$\overline{(m,m)}$ $m\in R^*$

$\forall\ \overline{(a,b)}\in F$，它的逆元 $\overline{(b,a)}$

$a\neq 0$

$$\begin{array}{ccc} R & \xrightarrow{f} & F \\ r & \longmapsto & \overline{(r,1)} \end{array}$$

这是单环同态：$f(r)=0\in F$

则 $\overline{(r,1)}=0\Rightarrow r=0$

F称为R的分式域（the field of fractions）

定理（F的泛性）设R整区，F是其分式域，$f:R\to F$ 是以上嵌入，设 $g:R\to F'$ 是R到域F'的单同态，且 $g(1)=1$，则 $\exists!\, h:F\to F'$，使得 $h\circ f=g$

证明：定义 $h: F \to F'$　$h(\frac{a}{b}) = g(a)[g(b)]^{-1}$

这是定义合理的：若 $\frac{a}{b} = \frac{a'}{b'}$　则 $ab' = a'b$

$g(a)g(b') = g(a')g(b) \Rightarrow g(a)[g(b)]^{-1} = g(a')[g(b')]^{-1}$

（注：$b, b' \neq 0 \Rightarrow g(b), g(b') \neq 0$）

即 $h(\frac{a}{b}) = h(\frac{a'}{b'})$

h 保持加法：$h(\frac{a}{b} + \frac{c}{d}) = h(\frac{ad+bc}{bd}) = g(ad+bc) \cdot g(bd)^{-1}$

$h(\frac{a}{b}) + h(\frac{c}{d}) = g(a)g(b)^{-1} + g(c)g(d)^{-1}$ $//$

$\Rightarrow h(\frac{a}{b} + \frac{c}{d}) = h(\frac{a}{b}) + h(\frac{c}{d})$

h 保持乘法：$h(\frac{a}{b} \cdot \frac{c}{d}) = h(\frac{ac}{bd}) = g(ac)g(bd)^{-1}$

$= g(a)g(b)^{-1}g(c)g(d)^{-1} = h(\frac{a}{b})h(\frac{c}{d})$

$\Rightarrow h$ 是环同态　且 $h \circ f = g$

h 是唯一的：若 $h': F \to F'$ 环同态，满足 $h' \circ f = g$

即 $\forall a \in R$，$(h-h')[f(a)] = 0$，$\ker(h-h')$ 是 F 的理想，

则 $\ker(h-h') = \{0\}$ 或 F，若 $\ker(h-h') = \{0\}$ 则 $f(a) = 0$

由 f 单 $\Rightarrow a = 0$，矛盾。因此 $h - h' = 0$

例 若 $R = \mathbb{Z}$，分式域 $= \mathbb{Q}$

若 $R = \mathbb{F}[x]$　$\mathbb{F}$ 是一个域，则 ~~再~~ R 的分式域 F

则 $F=\left\{\frac{f(x)}{g(x)} \middle| f(x),g(x)\in\mathbb{F}[x],\ g(x)\neq 0\right\}=\mathbb{F}(x)$

例 $\mathbb{Z}[i]=\{a+bi \mid a,b\in\mathbb{Z}\}$ 整区，它的分式域

是 $\mathbb{Q}[i]=\{x+yi \mid x,y\in\mathbb{Q}\}$

的确 $\frac{a+bi}{c+di}=\frac{(a+bi)(c-di)}{c^2+d^2}=\frac{ac+bd}{c^2+d^2}+\frac{bc-ad}{c^2+d^2}i$

反之 $\frac{q}{p}+\frac{t}{s}i=\frac{qs+pti}{ps}$

例 $\mathbb{Q}[x,y]/(x^2+y^2-1)=R$ 求它的分式域

x^2+y^2-1 是不可约多项式，R 是一个整区

$$R \xrightarrow{\varphi} \mathbb{Q}(t)=\left\{\frac{f(t)}{g(t)} \middle| f(t),g(t)\in\mathbb{Q}[t],\ g(t)\neq 0\right\}$$

$$\bar{x} \longmapsto \frac{2t}{1+t^2}$$

$$\bar{y} \longmapsto \frac{1-t^2}{1+t^2}$$

φ 是一个环同态，这是一个单同态，则 R 的分式域 F 到

$\mathbb{Q}(t)$ 有一个环同态，这是一个同构.

$\mathbb{Q}\left[\frac{2t}{1+t^2},\frac{1-t^2}{1+t^2}\right]=\mathbb{Q}\left[\frac{1}{1+t^2},\frac{t}{1+t^2}\right]$ 的分式域是 $\mathbb{Q}(t)$

$\mathbb{Q}[x,y]\longrightarrow\mathbb{Q}\left[\frac{2t}{1+t^2},\frac{1-t^2}{1+t^2}\right]$ 的核 $=(x^2+y^2-1)$

或者 $F\xrightarrow{h}\mathbb{Q}(t)$ $\quad h\left(\frac{\bar{x}}{\bar{y}+1}\right)=t$，$h$ 是满射，从而

h 单.

例 设 R 含幺交换整环，S 是 R 的含幺子环

则 $\mathrm{Frac}\,S = \mathrm{Frac}\,R \Longleftrightarrow \forall x \in R, \exists t \neq 0 \in S, tx \in S$

这里 $\mathrm{Frac}\,S$ 是 S 的分式域.

作业：Page 98, 1, 3, 6, 8, 9, 10, 11