可逆元

设G为幺半群，称$a \in G$是G的可逆元，如果

$$\text{存在} b \in G\text{，使得} ab = ba = 1_G$$

例子

$(\mathbb{Z}, \cdot)$的可逆元只有1和-1.
域F上的多项式环$F[x]$的可逆元仅有$\{a \in F, a \neq 0\}$. 这是因为，设$f \in F[x]$是$F[x]$的可逆元，则存在$g \in F[x]$使得$fg = 1_F$. 那么$0 = \deg(fg) = \deg f + \deg g$，则有$\deg f = \deg g = 0$. 从而$f \in F, f \neq 0$.

也就是说，$F[x]$上的可逆元全体就是F中的所有非零元素，即$F[x]$上的所有0次多项式。

整数环与域上多项式环

整除

整数环上的整除

对$a, b \in \mathbb{Z}$，定义$a \mid b \iff$ 存在$q \in \mathbb{Z}$使得$b = qa$.

一些基本的性质：
对于$a, b, c \in \mathbb{Z}$, 有：

1. $c \mid 0$. 当$0 \mid c$时，一定有$c = 0$.
2. $a \mid a$.
3. $a \mid b, b \mid a \implies b = a$或$b = -a$.
4. $a \mid b, b \mid c \implies a \mid c$.
5. $a \mid b, a \mid c \implies a \mid (ma + nb), \forall m, n \in \mathbb{Z}$.
   以上的性质，根据整除的定义，很容易证明。

多项式环上的整除

设F为域。定义

$$f, g \in F[x], f \mid g \iff \text{存在} h \in F[x] \text{使得} g = hf$$

对应地，一些基本的性质有：
对于$f, g, h \in F[x]$，有：

1. $h \mid 0$. 并且$0 \mid h \implies h = 0$.

2. $f \mid f$.
3. $f \mid g, g \mid f \implies$ 存在$a \in F, a \neq 0,$使得$g = af$.
4. $f \mid g, g \mid h \implies f \mid h$.
5. $f \mid g, f \mid h \implies f \mid (g+h), f \mid (g-h)$.

   只给出第三条的证明：

$$f \mid g \implies \text{存在} h_1 \in F[x] \text{使得} g = h_1 f$$

$$g \mid f \implies \text{存在} h_2 \in F[x] \text{使得} f = h_2 g$$

   则有

$$f = h_2 g = h_1 h_2 f$$

   若有$f = 0$，则由$0 \mid g$有$g = 0$. 命题成立。
   若有$f \neq 0$，则由

$$f = h_2 h_1 f \implies (1_F - h_1 h_2) f = 0$$

   及$f \neq 0$，就推出$1_F - h_1 h_2 = 0$，即$h_2 h_1 = 1_F$. 由前面提到的可逆元的性质，有

$$\text{存在} a \in F - \{0\}，h_1 = a$$

   因此原命题成立。

注：多项式中也有消去律：

$$f \neq 0, fg = fh \implies g = h$$

带余除法

整数的带余除法

设$a \in \mathbb{Z}^+, b \in \mathbb{Z}$，则存唯一一对$q, r \in \mathbb{Z}$，使得

$$b = qa + r，\text{并且} 0 \leq r \leq a - 1$$

多项式的带余除法

给定域F, 设$f, g \in F[x], f \neq 0$，则存在唯一一对$q, r \in F[x]$，使得

$$g = qf + r, \text{并且} \deg r \leq \deg f - 1$$

从这里可以看出多项式的次数是一个重要的性质，它类似于整数中的大小。
很多环都有整数的性质，但是有带余除法性质的环就很少了。

最大公因数

整数

设$a, b \in \mathbb{Z}$

1. 设$c \in \mathbb{Z}$, $c \mid a, c \mid b$，则称c是a和b的公因数.
2. 设$d \in \mathbb{N}$, 且d是a和b的公因数，若对任意的$c \in \mathbb{Z}$, c是a和b的公因数，都由$c \mid d$，则称d是a和b的最大公因数. 记作$d = \gcd(a, b)$.

多项式

给定域F, 设$f, g \in F[x]$. f, g不全为0.

1. 设$h \in F[x]$, 若有$h \mid f, h \mid g$则称h是f和g的公因式.
2. 对f, g的公因式d, 若d的首项系数为1_F, 且对任意a, b的公因式h都有$h \mid d$, 则称d是f, g的最大公因式. 记作$\gcd(f, g) = d$.
   这两个定义本身并不保证最大公因数/最大公因式的存在性和唯一性。在上周的课程中我们已经证明了它的存在性。下面给出唯一性的证明：

证明

设d_1, d_2都是f, g的最大公因式，则由最大公因式的定义有

$$d_1 \mid d_2, d_2 \mid d_1$$

从而由多项式整除的性质有

$$\text{存在} a \in F, a \neq 0, \text{使得} d_2 = a d_1$$

又由d_1, d_2的首项系数都为1, 则有$a = 1_F$, 即$d_1 = d_2$.

互素

整数

对$a, b \in \mathbb{Z}$，称a, b互素，若a, b的公因数只有$1, -1$.
这等价于存在$u, v \in \mathbb{Z}$，使得$au + bv = 1$.

若干基本性质

对于$a, b, c \in \mathbb{Z}$:

1. 若a, b互素，则$a \mid bc \implies a \mid c$.
2. 若a, b互素，则$a \mid c, b \mid c \implies ab \mid c$.

多项式

给定域F，对$f, g \in F[x]$，称f, g互素，若f, g的公因式只有零次多项式（即F中的非零元）。
这等价于存在$u, v \in F[x]$，使得$fu + gv = 1_F$.

证明

设存在$u, v \in F[x]$，使得$fu + gv = 1_F$. 任取$h \in F[x]$，$h \mid f, h \mid g$，则有$h \mid (fu + gv)$，即$h \mid 1$. 于是$\deg h = 0$.
设f, g不全为0，且它们的公因式仅有零次多项式，则它们的最大公因式为1_F. 于是由Week12的结论知存在$u, v \in F[x]$，使得$fu + gv = 1_F$.

若干基本性质

对$f, g, h \in F[x]$:

1. 若f, g互素，则$f \mid gh \implies f \mid h$.
2. 若f, g互素，则$f \mid h, g \mid h \implies fg \mid h$.

第一条性质的证明：
由f, g互素，有

$$\text{存在}u, v \in F[x]，\text{使得}fu + gv = 1_F$$

从而

$$hfu + hgv = h$$

又显然有

$$f \mid hfu, f \mid gh \implies f \mid hgv$$

从而

$$f \mid (hfu + hgv)，\text{即}f \mid h$$

子群性质

我们熟知：

$$H \leq (\mathbb{Z}, +) \iff \text{存在}d \in \mathbb{N}，\text{使得}H = \{dq \mid q \in \mathbb{Z}\}$$

并且，所有这些子群也是整数环的所有理想。

在多项式环上，我们也有类似的重要定理：
给定域F, 则I是$F[x]$的理想当且仅当

$$\text{存在}d \in F[x]，\text{使得}I = \{du \mid u \in F[x]\} = \{f \in F[x] : d \mid f\}$$

证明

若有$d \in F[x]$，使得

$$I = \{du \mid u \in F[x]\}$$

则显然I对于加法、加法逆和乘法都是封闭的。于是I是理想。

反过来，如果I是$F[x]$的理想，若$I=\{0\}$，则命题显然成立。下设I中含非零多项式。记d是$I-\{0\}$中次数最小的多项式。我们证明

$$I=\{du \mid u\in F[x]\}$$

对任意的$u\in F[x]$，由$d\in I$，I是理想，则由理想的定义有$du\in I$.
对任意的$g\in I$，由带余除法，存在$q,r\in F[x]$，使得

$$g=qd+r,\text{ 其中}\deg r<\deg d$$

由于$d\in I$，因此$qd\in I$（理想的定义），又$g\in I$，所以$r=g-qd\in I$.
又$\deg r<\deg d$，但是已经定义d是$I-\{0\}$中次数最小的多项式，因此只能有$r=0$. 从而$g=qd$.

素数与不可约多项式

定义

设$g\in F[x],\deg g\geq 1$. 若g的因式只有a和$ag, a\in F$的因式，则称g是F上的不可约多项式。也就是说

$$\forall f\in F[x], 1\leq \deg f\leq \deg g-1, \text{都有} f\nmid g$$

$a, ag, a\in F$一定是g的因式，这是因为

$$g=a(a^{-1}g)=a^{-1}(ag)$$

注意：可约与不可约是对于具体的**域**而言的。在某一域上不可约的多项式，可能在一个更大的域上是可约的。在$\mathbb{C}$上，$\mathbb{R}$中所有的不低于二次的多项式都是可约的，即使它在$\mathbb{R}$中不可约。

事实

以下的p均表示素数。设$a\in\mathbb{Z}$，则下面两个情况之一成立：

1. $p\mid a$.
2. $p\nmid a$，$\gcd(p,a)=1$，从而存在$u,v\in\mathbb{Z}$，使得$au+pv=1$.

类似地，在多项式中，我们有：
设$g\in F[x]$是F上的不可约多项式，$h\in F[x]$是F上的任意多项式，则下面两个情况之一成立：

1. $g\mid h$.
2. $g\nmid h, \gcd(g,h)=1_F$，从而存在$u,v\in F[x]$，使得$gu+hv=1_F$.

证明

记$d=\gcd(g,h)$. 由于$d\mid g$，而g不可约，因此根据不可约的定义，存在$a\in F-\{0_F\}$，使得

$$d=a\text{或}d=ag$$

若$d=ag$, 则由$d\mid h$，知$ag\mid h$，又$a\neq 0$，知$g\mid h$，情况1成立；
若$d=a$, 则有$\gcd(g,h)=1_F$(注意由定义，最大公因式的首项系数为1_F). 最后的部分是Week12的结论。

另一个事实

设p是素数，$a,b\in\mathbb{Z}$，$p\mid ab$，则$p\mid a$或$p\mid b$.

类似地，在多项式中，我们有：
设g是$F[x]$上的不可约多项式，$f,h\in F[x],g\mid fh$，则或者$g\mid f$，或者$g\mid h$.

证明

假设$g\nmid h$，下证$g\mid f$. 由假设知$\gcd(g,h)=1_F$，$g\mid fh$，有$g\mid h$（上节课的结果）

算术基本定理

设$m\in\mathbb{Z}^+$, 则存在素数$p_1\leq p_2\leq\ldots\leq p_s$，使得$m=p_1p_2\ldots p_s$. 若还有素数$q_1\leq q_2\leq\ldots\leq q_t$，使得$m=q_1q_2\ldots q_t$，则有$s=t$，并且$\{p_i\}_{i=1}^s$是$\{q_i\}_{i=1}^t$的一个排列.

在多项式中，也有类似的“唯一分解定理”：
设$h\in F[x],h\neq 0$，首项系数为a. 则存在F上首项系数为1_F的非常数不可约多项式

$$g_1,g_2,\ldots,g_s$$

使得

$$h=ag_1g_2\ldots g_s$$

若还有F上的首项系数为1_F的非常数不可约多项式

$$f_1,f_2,\ldots,f_t$$

使得

$$h=af_1f_2\ldots f_t$$

则有

$$s=t\text{，并且}\{g_i\}_{i=1}^s\text{是}\{f_i\}_{i=1}^s\text{的一个排列}$$

证明

不妨设$\deg h\geq 1$.
先证存在性。若h自身不可约，则命题自然成立。下设h可约。则由定义，存在
$f\in F[x],1\leq\deg f\leq\deg h-1$，使得$f\mid h$.

记$h=qf$. 则有$1\le \deg q=\deg h-\deg f<\deg h$. 这样就降低了待分解多项式的次数。直接对多项式次数用第二数学归纳法即可。
再证存在性。沿用定理叙述中的记号，我们有

$$g_1g_2\dots g_s=f_1f_2\dots f_t$$

则有

$$g_s\mid f_1f_2\dots f_t$$

于是存在$1\le j\le t$，使得$g_s|f_j$. 不妨设为$f_j=f_t$. 又f_t为F上的不可约多项式，其因式只有a和af_t，其中$a\in F-\{0\}$. 而$\deg g_s\ge 1$，故$g_s=af_t$. 又它们首项系数都为1_F, 因此$a=1_F$，即$g_s=f_t$. 这样就消去了一个因式，后续的过程可由归纳法完成（大致了解证明思路即可）

商环

我们知道，$F[x]$的全体理想形如

$$I=\{gq:q\in F[x]\}\text{，其中}g\in F[x]$$

那么对应的商环$F[x]/I$长什么样呢?

当$g=0$时，$I=\{0\},F[x]/I\cong F[x]$
当$g=a\in F-\{0\}$时，$I=F[x],F[x]/I=\{F[x]\}$
当$g\in F[x],\deg g\ge 1$时，$I=\{gq:q\in F[x]\}$.

$$F[x]/I=\{f+I:f\in F[x]\}$$

事实上，我们有

$$\forall f\in F[x]\text{，存在唯一的}r\in F[x]\text{，}\deg r\le \deg g-1\text{，使得}f+I=r+I$$

这个结论是由带余除法直接给出的。由带余除法，存在唯一的一对$q,r\in F[x],\deg r\le\deg g-1$，使得$f=qg+r$，由$qg\in I$，有$f\in r+I$，即$f+I=r+I$. 假设还存在$\tilde r\in F[x]$，$\deg\tilde r\le\deg g-1$，使得$\tilde r+I=f+I$，则存在$q\in F[x]$，使得$f=\tilde qg+\tilde r$，于是由带余除法的唯一性知$q=\tilde q,r=\tilde r$. 即上述的$r$是唯一的。

命题

给定

$$g\in F[x],\deg g\ge 1,I=\{qg:q\in F[x]\},H=\{r\in F[x]:\deg r\le\deg g-1\}$$

则有
(1) $F[x]/I$的表示：

$$F[x]/I=\{r+I:r\in H\}$$

并且这种表示是不重复的，即

$$r_1 + I = r_2 + I \implies r_1 = r_2$$

(2) 加法性质：

$$(r_1 + I) + (r_2 + I) = (r_1 + r_2) + I, \text{ 并且} r_1 + r_2 \in H$$

(3) 乘法性质：$\forall r_1, r_2 \in H$，$r_1 r_2$对g做带余除法

$$r_1 r_2 = qg + \phi, \phi \in H$$

则有

$$(r_1 + I)(r_2 + I) = (r_1 r_2) + I = \phi + I$$

(4) 幺元：$F[x]/I$的乘法幺元为$1_F + I$.
(5) 进一步地，如果g在F上不可约，则$F[x]/I$是一个域！
(6) 如果g在F上可约，则$F[x]/I$中存在两个乘积为0的非零元。