最大公约数

2023 年 11 月 5 日

目录

1 最大公约数

现在我们可以看到在第一章数论中对Z的几乎所有定理的证明都在$k[x]$中有一些类似多项式的性质。其中k是域；这意味着我们还可以把数论中的定理证明变为多项式的定理证明。

对域中多项式带有的系数的除法表明长除法可能是成立的。

$$s_nx^n + s_{n-1}x^{n-1} + \cdots \quad \begin{array}{l} s_n^{-1}t_mx^{m-n} + \cdots \\ \hline)t_mx^m + t_{m-1}x^{m-1} + \cdots \end{array}$$

1.1 定义：首项

若$f(x) = s_nx^n + \cdots + s_1x + s_0$是n次多项式，则其首项(leading term)是

$$\mathrm{LT}(f) = s_nx^n$$

令k是域和$f(x) = s_nx^n + \cdots + s_1x + s_0$和$g(x) = t_mx^m + \cdots + t_1x + t_0$都是$k[x]$中的多项式，并且$\deg(f) \leq \deg(g)$，因此$n \leq m$，由于$k$是域，则$s_n^{-1} \in k$且

$$\frac{\mathrm{LT}(g)}{\mathrm{LT}(f)} = s_n^{-1}t_mx^{m-n} \in k[x]$$

因此$\mathrm{LT}(f) \mid \mathrm{LT}(g)$

1.2 除法算式

令R是交换环，并令$f(x), g(x) \in R[x]$和$f(x)$其首系数是R中的单位，则

1. 存在一些多项式$q(x), r(x) \in R[x]$使得

$$g(x) = q(x)f(x) + r(x)$$

   其中$r(x) = 0$或者$\deg(r) < \deg(f)$

2. 若R是整环，则多项式$q(x)$和$r(x)$在上述条件1中是唯一的。

注意： 若R是域，则假设$f(x)$的首系数是单位相当于$f(x) \neq 0$

证明： 我们证明$q(x), r(x) \in R[x]$的存在如我们声称的：若$f \mid g$，则$g = qf$对某个q成立，只要定义余数$r = 0$则最简单的情况就证明就完了。其次，若$f \not| g$，则考虑像q在$R[x]$中变化而得到的全部非零形如$g - qf$的非零多项式。最小整数公理证明了存在一个次数最小的多项式$r = g - qf$。因此$g = qf + r$，它满足$\deg(r) < \deg(f)$。我们记$f(x) = s_n x^n + \cdots + s_1 x + s_0$和$r(x) = t_m x^m + \cdots + t_1 x + t_0$。由假设可得$s_n$是单位，那么存在$s_n^{-1} \in k$。若$\deg(r) \geq \deg(f)$，定义

$$h(x) = r(x) - t_m s_n^{-1} x^{m-n} f(x)$$

所以，$h = r - [\mathrm{LT(r)}/\mathrm{LT(f)}]\, f$，注意的是，存在$h = 0$或者$\deg(g) < \deg(r)$这种情况，若$h = 0$，则$r = [\mathrm{LT}(r)/\mathrm{LT}(f)]f$且

$$g = qf + r = qf + \frac{\mathrm{LT}(r)}{\mathrm{LT}(f)} f = \left[q + \frac{\mathrm{LT}(r)}{\mathrm{LT}(f)}\right] f$$

和我们的假设$f \nmid g$矛盾。

其次，若$h \neq 0$，则$\deg(h) < \deg(r)$且

$$g - qf = r = h + \frac{\mathrm{LT}(r)}{\mathrm{LT}(f)} f$$

那么我们就可以得到$h = g - (qf + r) = g - [q + \frac{\mathrm{LT}(r)}{\mathrm{LT}(f)}]f$，但根据我们的假设，最小具备$g - qf$的形式的多项式是$r$，这是一个矛盾，因此$\deg(r) < \deg(f)$

证明2： 为了证明q, r是唯一的，我们设$g = q'f + r'$，其中$\deg(r') < \deg(f)$，则

$$(q - q')f = r' - r$$

若$r' \neq r$，则两边都是有次数的。但$\deg(q - q')f = \deg(q - q') + \deg(f) \geq \deg(f)$，其次$\deg(r' - r) \leq \max\{\deg(r'), \deg(r)\} < \deg(f)$。我们得到了一个矛盾，左边的式子次数小于右边的。因此$r' = r$和$(q - q')f = 0$。由于$R[x]$是整环，我们有$q = q'$成立。

1.3 定义：商式和余式

若$f(x)$和$g(x)$是$k[x]$中多项式，其中k是数域，则通过被$f(x)$除的$g(x)$得到的多项式$q(x), r(x)$被我们称作商式和余式。

1.4 命题

对每个正整数n，割圆多项式$\Phi_n(x)$是一个所有系数都是整数的首一多项式。

证明： 割圆多项式就是每个根都位于单位圆上的式子，我们采用归纳的方式证明，对基本步骤有$\Phi_1(x) = x - 1$是成立的，现在，我们假设$\Phi_d(x)$是带有整系数的首一多项式，利用等式$x^n - 1 = \Pi_d \Phi_d(x)$，我们得到

$$x^n - 1 = \Phi_n(x)f(x)$$

其中$f(x)$是$\Phi_d(x)$的所有乘积且$d \mid n$和$d < n$。由归纳假设，$f(x)$是首一多项式且带有整系数。因为$f(x)$是首一的，且$x^n - 1$也是整系数多项式，那么$\frac{x^n-1}{f(x)} = \Phi_n(x)$也是首一多项式。

1.5 定义：数域上的根

若$f(x) \in k[x]$，其中k是域，那么在k中$f(x)$的根是指元素$a \in k$使得$f(a) = 0$

注意： 多项式$f(x) = x^2 - 2$拥有的是Q上的系数。即使$\sqrt{2} \notin Q$，但我们经常说$\sqrt{2}$是$f(x)$的一个根。

在等一下我们将看到，对于多项式$f(x) \in k[x]$，都存在一个更大的域E包含k作为子域且包含$f(x)$的所有根。

1.6 引理

令$f(x) \in k[x]$，其中k是域并令$a \in k$，则存在一个$q(x) \in k[x]$带有

$$f(x) = q(x)(x - a) + f(a)$$

证明： 利用多项式除法，我们有

$$f(x) = q(x)(x - a) + r$$

由于$\deg(x - a) = 1$，因此$\deg r < 1 = 0$，所以r是某个常数。现在我们知道赋值映射$e_a : k[x] \to k$ 是一个环同态。

$$e_a(f) = e_a(q)e_a(x-a) + e_a(r)$$

因此，$f(a) = q(a)(a-a) + r$，所以$r = f(a)$

1.7 命题

若$f(x) \in k[x]$其中k是域，则$a \in k$是$f(x)$在$k[x]$中的根当且仅当$x-a$整除$f(x)$且对$k[x]$封闭。

证明： 若a是$f(x)$的根，则$f(a) = 0$，由命题有$f(x) = q(x)(x-a)$。反过来若$f(x) = q(x)(x-a)$，那么我们就有$f(a) = q(a)(a-a) = 0$

1.8 定理:因式分解定理

令k是域且$f(x) \in k[x]$

1. 若$f(x)$是n次的，则$f(x)$有至多n个根在k中

2. 若$f(x)$是n次的且$a_1, a_2, \cdots, a_n \in k$是$f(x)$在$k$中不同的根，则存在$c \in k$和一个因式分解使得

$$f(x) = c(x-a_1)(x-a_2)\cdots(x-a_n)$$

证明： 我们对$n \geq 0$进行归纳，若$n = 0$，则$f(x)$是非零常数，现在令$n > 0$，若$f(x)$不存在k中的根，那么我们的证明就结束了，再看看另一种情况，若存在$a \in k$是$f(x)$的根，那么利用命题1.7，就有

$$f(x) = q(x)(x-a)$$

且$q(x) \in k[x]$是具备次数为$n-1$的多项式，若$b \in k$是另一个不同的根，则

$$0 = f(b) = q(b)(b-a)$$

由于$b - a \neq 0$，那么我们只有得到$q(b) = 0$的结论，所以由归纳假设$q(x)$只有至多$n-1$个根，因此$f(x)$至多有n个根在k中。

证明2： 利用归纳法和命题1.7即可。

1.8.1 例子

定理1.8会在交换环上失效，例如$x^2-[1]\in I_8[x]$，满足的根只有$[1],[3],[5],[7]$四个根。

1.9 推论

令k是无限域且令$f(x)$和$g(x)$是$k[x]$中的多项式，若$f(x)$和$g(x)$是多项式函数，即对每个$a\in k$有$f^b(a)=g^b(a)$，则$f(x)=g(x)$

证明： 若$f(x)\neq g(x)$ 则多项式$f(x)-g(x)$是非零的多项式，我们假设他们的次数为n。现在，每个k中的元素都是$f(x)-g(x)$的根，由于k是无限的，而n次多项式最多只有n个根，这是一个矛盾。

1.10 推论

令k是任意域（可能有限）令$f(x),g(x)\in k[x]$且$n=\max\{\deg(f),\deg(g)\}$。若这里存在$n+1$个不同的元素$a\in k$且$f(a)=g(a)$，则$f(x)=g(x)$

证明： 若$f(x)\neq g(x)$，令$h(x)=f(x)-g(x)\neq 0$，有

$$\deg(h)\leq \max\{\deg(f),\deg(g)\}=n$$

由假设，若存在$n+1$个元素$a\in k$使得$h(a)=f(a)-g(a)=0$这与根的存在性定理矛盾，因此$h(x)=0$可得$f(x)=g(x)$

1.11 推论：拉格朗日插值定理

令k是一个域，并令$u_0,\cdots,u_n$是k中不同的元素，给定任意列$y_0,\cdots,y_n\in k$，则这里存在唯一的次数$\leq n$的$f(x)\in k[x]$ 带有$f(u_i)=y_i$对所有$i=0,\cdots,n$成立，实际上：

$$f(x)=\sum_{i=0}^{n}y_i\frac{(x-u_0)\cdots(x-u_i)\cdots(x-u_n)}{(u_i-u_0)\cdots(u_i-u_i)\cdots(u_i-u_n)}$$

1.12 定义：公因子

若k是一个域，且$f(x),g(x)\in k[x]$，则公因子是多项式$c(x)\in k[x]$使得$c(x)\mid f(x)$和$c(x)\mid g(x)$

若$f(x)=0=g(x)$，则它们的最大公因子记为gcd且也被定义为0.若至少有一个非零多项式，那么$f(x),g(x)$的最大公因式被定义为(f,g)的首一多项式$d(x)\in k[x]$且$\deg(c)\leq\deg(d)$对每个公因式$c(x)$成立。

1.13 引理

令$f(x)$是$k[x]$中的非零多项式，其中k是域，若$h(x)=a_nx^n+\cdots+a_0\in k[x]$是$f(x)$的因式，则$a_n^{-1}h(x)$是$f(x)$的首一因子且与$h(x)$有一样的次数。

证明： 由于k是域，$a_n\in k$非零则意味着存在逆$a_n^{-1}\in k[x]$，若$f(x)=c(x)h(x)$，则$f(x)=[a_nc(x)][a_n^{-1}h(x)]$，所以$\deg(a_n^{-1}h)=\deg(h)$

1.14 命题

若k是域，则对每对$f(x),g(x)\in k[x]$都存在一个最大公因式。

证明： 若$f(x),g(x)=0$，则结果是显然的，我们假设至少有一个非零多项式，那么$f(x)$的次数保证了g,f的公因子次数上界。设$d(x)$是次数最大的，由于k是域，则$\deg(a_m^{-1}d(x))=\deg(d(x))$。所以根据引理1.13，$d(x)$也可以是首一的并且$d(x)$是最大公因式。

1.15 定理：线性组合

若k是域且$f(x),g(x)\in k[x]$，则最大公因式是$f(x)$和$g(x)$的线性组合。

注意： 定理的意思是有$sf+tg$形式的线性组合，其中$s=s(x),t=t(x)$是$k[x]$中的多项式。

证明： 我们假设至少有一个多项式f,g是非零的（公因子是0的也除外）考虑由所有线性组合构成的集合I：

$$I=\{s(x)f(x)+t(x)g(x):s(x),t(x)\in k[x]\}$$

令$s=1,t=0$可以验证$f,g\in I$。现在，构造另一个集合$N=\{n\in N:n=\deg(f),f(x)\in I\}$，容易验证$N$是非空的，由最小数原理可知$N$存在一个最小数，我们设为$n$，这说明对应一个$d(x)\in I$中使得$\deg(d)=n$，由引理1.13我们可以设$d(x)$是首一的，现在我们说$d(x)=(f,g)$，这是因为

$d \in I$说明是一个f和g的线性组合

$$d = sf + tg$$

现在用d去除f, g，由除法算式可得$f = qd + r$，其中$r = 0$或者$\deg(r) < \deg(d)$，若$r \neq 0$，则

$$r = f - qd = f - q(sf + tg) = (1 - qs)f - qtg \in I$$

这与我们假设$d(x)$是最小次数矛盾，因此$r = 0$有$d \mid f$和$d \mid g$

最后，若c也是一个f, g的公因子，那么c整除$d = sf + tg$，但$c \mid d$意味着$\deg(c) \leq \deg(d)$，因此d是f和g的最大的公因子

1.16 引理

令k是域，且$f(x), g(x) \in k[x]$那么

1. 首一公因子$d(x)$是最大公因子当且仅当$d(x)$可以被每个公因子整除
2. 每两个多项式f, g都有一个唯一的公因子。

1.17 定义：最大公因子

若R是整环且$a, b \in R$，则公共因子是元$c \in R$使得$c \mid a$和$c \mid b$成立。若$a = 0 = b$，则最大公因子定义为0，记为gcd，若至少有一个非零，则最大公因子记为(a, b)且说明有一个公因子$d \in R$使得对每个公因子$c \in R$都有$c \mid d$

1.18 定理

若k是域，则每个$k[x]$中的理想I是主理想。更多的，若$I \neq \{0\}$，则有一个首一多项式生成I

证明： 若$I = 0$，只需要取$d = 0$。现在我们假设有一些非零多项式在I中，最小数公理告诉我们存在$d(x) \in I$拥有最小次数。接着我们还是假设$d(x)$是首一的。

我们说每个I中的f是d的倍数，则除法算式告诉了我们存在q, r使得$f = qd + r$，其中$r = 0$或者$\deg(r) < \deg(d)$。现在我们有$d \in I$可知$qd \in I$满

足理想的第三个条件，其次$r = f - qd \in I$满足第二个条件，若$r \neq 0$，则有$\deg(r) < \deg(d)$与我们假设矛盾，因此d是I中的最小次数多项式。所以$r = 0$且f是d的倍数。

1.19 定义：主理想整环（PID）

一个交换环R被称为是主理想整环的，若其在整环中的每个理想都是主理想。通常我们缩写为PID

1.19.1 例子

1. 环Z是PID
2. 每个域都是PID
3. 利用定理1.18可知若k是域，则$k[x]$是PID

1.19.2 例子

若J, I是交换环R上的理想，我们现在来证明$I \cap J$也是R中的理想。由于$0 \in I$和$0 \in J$，则$0 \in I \cap J$，若$a, b \in I \cap J$，则$a - b \in J$且$a - b \in I$，因此$a - b \in I \cap J$，最后若$a \in I \cap J$且$r \in R$，则$ra \in I$也有$ra \in J$可知$ra \in I \cap J$，因此$I \cap J$是理想。我们也可以用差不多的方法证明无限理想族的交集也是一个理想。

1.20 定义：公倍数

若$f(x), g(x) \in k[x]$，其中k是域，则公倍数指的是多项式$m(x) \in k[x]$使得$f(x) \mid m(x)$和$g(x) \mid m(x)$

若多项式都是非零的，我们记最小公倍数为lcm，指的是其最小度量的倍数，若$f(x)$或者$g(x) = 0$，定义公倍数为$\mathrm{lcm} = 0$，并且我们经常把公倍数记为

$$[f(x), g(x)]$$

1.21 命题

设k是域且$f(x), g(x) \in k[x]$是非零的，则

1. $[f(x), g(x)]$是$(f(x) \cap g(x))$的首一生成元。
2. 令$m(x)$是$f(x)$和$g(x)$的首一公倍数。则$m(x) = [f(x), g(x)]$
3. 每对多项式$f(x), g(x)$都有唯一的公倍数

证明： 由于$f, g \neq 0$，那么理想$(f) \cap (g)$是理想且非空，那么利用引理1.18可知$(f) \cap (g) = (m)$，其中m是一个在$(f) \cap (g)$中的最小次多项式。由于$m \in (f)$，那么$m = qf$对某个$q(x) \in k[x]$成立。因此$f \mid m$，同样的方法我们可以得到$g \mid f$，因此m是f, g的公倍数。若M是其他的公倍数，则$M \in (f)$且$M \in (g)$，所以$M \in (f) \cap (g) = (m)$可知$m \mid M$，我们有$\deg(m) \leq \deg(M)$，得到$m = [f, g]$

证明2： 在刚才我们已经证明了$[f, g]$整除f和g的所有公倍数M。反之，我们设m'是整除每个公倍数的首一的公倍数利用第一部分的定理，且存在一个单位$u(x) \in k[x]$[1] 使得$m' \in u(x)m(x)$，而$u(x)$是单位说明了其是一非零常数，又因为m', m是首一的，则$m(x) = m'(x)$

证明3： 若l, l'是f, g的lcm，则利用第二部分的定理可知它们整除彼此，且有$l = l'$

[1]这里需要用到一个命题：设R是一个整环，$f(x)$是$R[x]$中的单位当且仅当$f(x)$是非零常数和单位

证明：设$f(x) \in R[x]$是单位，则存在$u(x) \in R[x]$使得$u(x)f(x) = 1$，现在我们对两边比较次数，设$\deg(u) = s, \deg(f) = t$，其中$s, t \geq 0$而1的次数是0，$s + t = 0$当且仅当$s = 0$和$t = 0$这意味着$u(x)$是常数或者$f(x)$是常数。且可以得到$u(x)$也是一个单位。反之，若$f(x)$是常数和单位，则有$ff^{-1} = 1$可知$f \in R[x]$也是一个单位。

1.22 定义：不可约

我们说交换环R中的元素p是不可约的，这指的是p既不是0也不是单位。且对R中的任意因式分解$p = ab$，要求a或者b是单位。

例如Z中的元素$\pm p$，其中p是素数就是一个不可约的元素。

1.23 命题：

若k是域，则非常数多项式$p(x) \in k[x]$是不可约的当且仅当$p(x)$在$k[x]$中没有形如$p(x) = f(x)g(x)$的因式分解，其中$\deg(f), \deg(g) < \deg(p)$

证明： 若$p(x)$是不可约的，利用命题1.21的证明，$k[x]$中的单位是常数，因此由定义可得$p(x)$是非常数多项式。

假设$p(x) = f(x)g(x) \in k[x]$则两个因子的次数都小于$\deg(p)$得到$f(x), g(x)$的次数实际上也不等于0，所以f, g不是$k[x]$中的单位，这是一个矛盾。

反之，若$p(x)$不能分解为更小次数的多项式，则它有唯一形如a或者$ap(x)$的因子，其中a是非零常数。由于k是域，非零常数是单位，所以$p(x)$不可约。

若R不是域，则不可约多项式的特性不适合环$R[x]$，例如在$Q[x]$中，多项式$f(x) = 2x + 2 = 2(x + 1)$是不可约的，这里2是$Q[x]$中的单位，但在$Z[x]$中，这并不是不可约的，因为2和$x + 1$都不是$Z[x]$中的单位。

并且，多项式的不可约性依赖交换环$k[x]$甚至依赖于域k。例如：$p(x) = x^2 - 2$在$Q[x]$中是不可约的，但在$R[x]$中则可以因式分解为$(x - \sqrt{2})(x + \sqrt{2})$

1.24 命题

令k是域且$f(x) \in k[x]$是二次或者三次方程，则$f(x)$在$k[x]$中不可约当且仅当$f(x)$在k中不存在根。

证明： 若$f(x)$在k中存在根，那么由因式分解定理可知其是可约多项式。

反之我们设$f(x)$是可约的，则这里有一个因式分解$f(x) = g(x)h(x)$，其中$\deg(g), \deg(h) < \deg(f)$。而$\deg(f) = \deg(g) + \deg(h)$，由于$\deg(f) = 2, 3$，则有一个$\deg(g)$或者$\deg(h)$的次数必定为1。因此，$f(x)$存在一个根在$k$中。

但对于定理有一个比较致命的缺陷，对于次数大的多项式可能不适合，例如：

$$x^4+2x^2+1=(x^2+1)^2$$

是一个因式分解，但在R中无根。

1.25 命题

若k是域，则每个非常数多项式$f(x)\in k[x]$都有因式分解

$$f(x)=ap_1(x)\cdots p_t(x)$$

其中a是非零常数而$p_i(x)$是首一多项式。

证明： 我们对多项式$f(x)$通过$\deg(f)\geq 1$利用第二归纳来证明。若$\deg(f)=1$，则$f(x)=ax+c=a(x+a^{-1}c)$是线性多项式，$x+a^{-1}c$是不可约的，所以它是不可约的乘积。现在我们设$\deg(f)\geq 1$，若$f(x)$是不可约的且首系数为a，我们记$f(x)=a(a^{-1}f(x))$，则证明完了。

不妨假设$f(x)$是可约多项式，则$f(x)=g(x)h(x)$，其中$\deg(g),\deg(h)<\deg(f)$，由归纳假设我们有$g(x)=bp_1(x)\cdots p_m(x)$和$h(x)=cq_1(x)\cdots q_n(x)$，其中$g,h$是首一的不可约分解，则$f(x)=(bc)p_1\cdots p_m q_1\cdots q_m$，证毕。

1.26 引理

令k是一个域，并令$p(x),f(x)\in k[x]$，且令$d(x)=(p,f)$是gcd，是首一不可约的，则

$$d(x)=\begin{cases}1 & p(x)\nmid f(x)\\ p(x) & p(x)\mid f(x)\end{cases}$$

证明： 唯一的因子只有$p(x)$和1，若$p(x)\mid f(x)$，则$p(x)$是首一的。若$p(x)\nmid f(x)$，则$\gcd=1$是首一的。

1.27 欧拉定理

令k是域且$f(x),g(x)\in k[x]$，若$p(x)$是$k[x]$中的不可约多项式，并且有$p(x)\mid f(x)g(x)$，则$p(x)\mid f(x)$或者$p(x)\mid g(x)$。更一般的，如果$p(x)\mid f_1(x)\cdots f_n(x)$，则$p(x)\mid f_i(x)$对某个$i$成立

证明： 若$p \mid f$，定理自然成立。若$p \nmid f$，则$\gcd(p, f) = 1$意味着有$s(x), t(x)$的存在使得$1 = sp + tf$，并且

$$g = spg + tfg$$

由于$p \mid fg$，上述式子说明了$p \mid g$。而对于第二个声明，只需要利用归纳法对$n \geq 2$归纳即可。

1.28 定义：互素

两个多项式$f, g \in k[x]$是互素的，其中k是域。我们称其是互素的当且它们的$\gcd = 1$

1.29 引理

令$f(x), g(x), h(x) \in k[x]$，其中$k$是域，并令$h(x), f(x)$是互素的。若$h(x) \mid f(x)g(x)$，则$h(x) \mid g(x)$

证明： 由我们的假设，$fg = hq$对某个$q(x) \in k[x]$成立。则有一些多项式s, t使得$1 = sf + th$，所以$g = sfg + thg = shq + thg = h(sq + tg)$有$h \mid g$

1.30 定义：既约形式

若k是域，则有理函数$f(x)/g(x) \in k[x]$是既约形式指的是$f(x), g(x)$互素。

1.31 命题

令k是域，每个非零多项式$f(x)/g(x) \in k[x]$都可以是既约的。

证明： $d = (f, g)$，则$f = df'$和$g = dg'$其次，f', g'是互素的。我们假设f', g'不是互素的，这说明存在一个f', g'的公因子h，它会令hd是一个比d次数还大的因子，这与我们的假设矛盾。而现在$f/g = df'/dg' = f'/g'$是既约形式。

1.32 欧几里得算法

若k是域且$f(x), g(x) \in k[x]$，则欧几里得算法是一个计算$\gcd(f(x), g(x))$的方法，并且可以寻找一堆多项式$s(x), t(x)$使得$(f, g) = sf + tg$

证明： 这个证明是重复欧拉算法在Z上的除法算法的迭代应用。

$$\begin{array}{ll} g = q_0 f + r_1 & \deg(r_1) < \deg(f) \\ f = q_1 r_1 + r_2 & \deg(r_2) < \deg(r_1) \\ \vdots & \end{array}$$

剩下的最后一个非零余数是一个公因子，可以被每个公约数整除。由于余数可能不是首一的，所以我们可以通过乘一个逆元使得其是首一多项式。

1.32.1 例子

在$Q[x]$中可以用欧几里得算法球$\gcd(x^5 + 1, x^3 + 1)$

$$\begin{aligned} x^5 + 1 =& x^2(x^3 + 1) - x^2 + 1 \\ x^3 + 1 =& (-x)(-x^2 + 1) + (x + 1) \\ -x^2 + 1 =& (-x + 1)(x + 1) \end{aligned}$$

所以，$x + 1$是gcd

1.33 推论

若k是域K的子域，则$k[x]$是$K[x]$的子环。若$f(x), g(x) \in k[x]$，则在$k[x]$的gcd等于在$K[x]$中的gcd

证明： 利用$K[x]$中的除法我们有

$$g(x) = Q(x)f(x) + R(x)$$

其中$Q(x), R(x) \in K[x]$并且$R(x)$要么是0，要么是$\deg(R) < \deg(f)$，由于$f, g \in k[x]$，则在$k[x]$中我们可以得到另一个除法算式

$$g(x) = q(x)f(x) + r(x)$$

其中$q, r \in k[x]$且r的情况同上R的情况一样。但等式$g(x) = q(x)f(x) + r(x)$在$K[x]$是一定的，因为$k[x] \subseteq K[x]$使得在$K[x]$中的商和余数是唯一的。则$Q(x) = q(x)$和$R(x) = r(x)$都在$k[x]$中。因此欧几里得算法得到的方程组在和较小环中得到的方程组完全相同，因此存在相同的gcd

2 欧几里得环

我们讲的东西和Z或者$k[x]$这些环有一些区别，因为这些环上有除法算式定义。特别的，我们给出一个商和余数不是唯一的环。不过首先我们来推广一些Z和$k[x]$上有的东西

2.1 定义：欧几里得环

一个交换环R称为欧几里得环，这是再说它是一个整环且带有函数

$$\partial : R^{\times} \to N$$

∂是次数函数，而$R^{\times}$是R所有非零元素组成。次数函数满足

1. $\partial(f) \leq \partial(fg)$对所有$f, g \in R^{\times}$成立

2. 对所有$f, g \in R$其中$f \in R^{\times}$，则存在$q, r \in R$使得

$$g = qf + r$$

   其中r要么是0要么$\partial(r) < \partial(f)$

2.1.1 命题

每个欧几里得环是PID，特别的，高斯整环$Z[i]$是PID

证明： 我们改写定理1.18的证明，我们要证明其每个理想都是主理想。

首先，我们取高斯整环中理想I，它的元素是形如$a + bi$，其中$a, b \in Z$的。当选取$a = b = 0$的时候，我们就得到$0 \in Z$成立。其次，对于$Z[i]$的任意两个元素我们可以得到q, r使得$b = qa + r$，其中$a, b \in I$，借此得到$r = b - qa \in I$而 $r = 0$或者$\deg(r) < \deg(a)$。由于Z是整数，不妨假设a是最小值，若$r = 0$，则证明结束，$b = qa$说明是主理想，若$r \neq 0$，那么$\deg(r) < \deg(a)$和$r = b - qa$与我们得到的假设矛盾，因此$r = 0$且$Z[i]$是PID

2.1.2 例子

在代数数论中，我们证明了环

$$R = \{a + b\alpha\, a, b \in Z\}$$

是一个PID，其中$\alpha = \frac{1}{2}(1 + \sqrt{-19})$，但他不是欧几里得环。这说明命题2.1.1的逆定理是不成立的。但证明这个的数学家发现了如下一些性质：

2.2 定义：通用侧因子

一个整环R中的元u是通用侧因子，这是在说u不是单位且对每个$x \in R$有$u \mid x$或者存在单位$z \in R$使得$u \mid (x + z)$

2.3 命题

若R是欧几里得环但不是域，则R有一个通用侧因子

证明： 定义

$$S = \{\partial(v) : v \neq 0, v\text{不是单位}\}$$

其中∂是R的次数函数。由于R不是域，则存在一些$v \in R^{\times}$不是单位，所以S是非空的且是自然数集的一个子集，那么由最小数原理，存在$R^{\times}$的一个非单位u使得$\partial(u)$是S中的最小元。我们说u是通用侧因子，若$x \in R$这里有元q和r使得$x = qu + r$。其中$r = 0$或者$\deg(r) < \deg(u)$，若$r = 0$，则$u \mid x$，若$r \neq 0$，则r必须是单位，否则它的存在和我们的假设，$\partial(u)$是最小次数矛盾。而单位不在S中，只能是单位。

2.4 命题

令R是PID，则

1. 每个$\alpha, \beta \in R$都有$\gcd, \delta$，使得有一线性组合，即存在$\delta, \tau \in R$有

$$\delta = \sigma\alpha + \tau\beta$$

2. 若有不可约元素$\pi \in R$整除$\alpha\beta$，则$\pi \mid \alpha$或者$\pi \mid \beta$

证明： 我们假设α,β至少有一个非零。则考虑由所有线性组合构成的集合I

$$I=\{\sigma\alpha+\tau\beta\}$$

容易验证I是理想，那么由于R是PID，那么就存在$\delta\in I$有$I=(\delta)$是真理想，我们假设δ是α,β的最大公因子。

由于$\alpha\in I=(\delta)$，那么有$\alpha=\rho\delta$对某个$\rho\in R$成立，所以δ是α的一个因子。类似的，对β的证明也可以由此得到。因此δ就是那个公因子。

由于$\delta\in I$，则存在一些线性组合使得

$$\delta=\sigma\alpha+\tau\beta$$

最后，若γ也是一个公因子，则$\alpha=\gamma\alpha'$，而$\beta=\gamma\beta'$。得到γ是δ的一个因子。因此δ是最大的公因子。

证明2： 若$\pi\mid\alpha$，证明完毕，若$\pi\nmid\alpha$，则1是π和α的gcd，因此存在$\sigma,\tau\in R$使得

$$1=\sigma\pi+\tau\alpha$$

有

$$\beta=\beta(\sigma\pi+\tau\alpha)$$

可知$\pi\mid\beta$，因此若$\pi\mid\alpha\beta$，则$\pi\mid\beta$

2.5 引理

若p是素数且$p\equiv 1 \mod 4$，则存在一个整数m使得

$$m^2\equiv -1 \mod p$$

证明： 若$G=F_p^{\times}$，则它是一个F_p中非零元素组成的乘法群。由题设，$p\equiv 1 \mod 4$，则有$\mid G\mid=p-1\equiv 0 \mod 4$是成立的。所以存在一个4阶的群$S$。并且$I_p^{\times}$是阿贝尔群，所以，要么$a^2=1$对所有$S$的元素成立，要么$S$是循环群。由于$F_p$是域，但$x^2-1$在域中不可能包含4个根，所以$S$是循环群。$S=<[m]>$，其中$[m]$是$m \mod 4$的同余类，则$[m^4]=[1]$，那么$[m^2]\neq[1]$，最后，$S$中阶为2的元素只有$[-1]$，所以阶为2的元$[m^2]=[-1]$。因此$m^2\equiv -1 \mod p$

2.6 定理：费马二平方定理

一个奇素数p可以表示为两个数的平方和。

$$p = a^2 + b^2$$

当且仅当$p = 1 \mod 4$且其中a, b是整数

证明： 对每个整数a，我们有$a \equiv r \mod 4$，其中$r = 1, 2, 3, 0$.则$a^2 \equiv r^2 \equiv 4$，但 $\mod 4$的话，我们带入r的情况会得到

$$0^2 \equiv 0,\ 1^2 \equiv 1,\ 2^2 = 4 \equiv 0,\ \ 3^2 = 9 \equiv 1$$

因此$a^2 \equiv 0$或者$1 \mod 4$，所以，若$p = a^2 + b^2$，其中a, b是整数，则$a^2 + b^2 \equiv 3 \mod 4$，而题设说$p$是奇数，那么$p \equiv 1 \mod 4$或$p \equiv 3 \mod 4$，但后一种情况已经被我们证明是不可能的，所以$p \equiv 1 \mod 4$

反过来，若$p \equiv 1 \mod 4$，在欧几里得环$Z[i]$中，则存在一些整数m使得

$$p \mid (m^2 + 1)$$

由于$Z[i]$中有一个因式分解$m^2+1 = (m+i)(m-i)$，所以$p \mid (m+i)(m-i)$。因此，若$p \mid m+i$，则有整数u, v使得$m+i = p(u+iv)$。取复共轭，则$m-i = p(u-iv)$所以$p \mid m-i$。那么可以得到$p \mid m+i-(m-i) = 2i$。利用欧几里得度量，我们知道$\partial(p) = p^2 > \partial(2i) = 4$，因此，我们断言$p$不是不可约元素，因为不满足命题2.4，那么由于$Z[i]$是PID，则存在因式分解

$$p = \alpha\beta$$

其中$\alpha = a + ib$，$\beta = c + id$都不是单位，则$\partial(\alpha) \neq 1$且$\partial(\beta) \neq 1$。那么利用范数就有

$$\begin{aligned} p^2 =& \partial(p) \\ =& \partial(\alpha\beta) \\ =& \partial(\alpha)\partial(\beta) \\ =& (a^2 + b^2)(c^2 + d^2) \end{aligned}$$

且有$p \mid a^2 + b^2 \neq 1$或者$p \mid c^2 + d^2 \neq 1$，因此$p = a^2 + b^2$(且$p = c^2 + d^2$)

3 习题

> 找出x^2-x-2和x^3-7x+6在$F_5[x]$中的最大公因式。且表示为线性组合。

3.1 解：

为了求出公因式，它肯定是某个域中的根，满足$x^2-x-2=[0]\in F_5[x]$的解是5的倍数，有$x^2-x-2=(x-2)(x+1)\in F_5[x]$，而对于另一个则有分解$(x-1)(x-2)(x+3)\in F_5[x]$，所以公因式就是$x-2$

> 若R是整环且$f(x)\in R[x]$是次数为n的多项式，证明$f(x)$最多只有n个根在R中

证明： 我们定义一个R上的分式域$F(R)$，利用整环中$ab=1$的元素，则$ab\neq 0$有$b=a^{-1}=a/a^{-1}\in F(R)$。那么我们就可以在环上定义带余除法。然后利用推论1.33，我们设$f(x),f(x)$，则它们自身的公因子等于在分式域中的公因子，由此可知在R中的根在分式域中不会发生变化。那么

设a是$f(x)$的一个根，那么$f(a)=0$成立。那么$f(x)=q(x)(x-a)+r(x)$成立，其中$\deg(r)<\deg(x-a)$成立。但$\deg(x-a)=1$，因此$r(x)$的次数为0，现在，由于R是整环，则$1\neq 0$。a我们有$f(a)=r(a)$，但$f(a)=0$有$r(a)=0$可知$(x-a)\mid f(x)$。现在不妨假设$f(x)$在整环上存在$n+1$个根，那么由归纳法可知n次多项式$f(x)$至多可以分解为n个次数为1形如$x-a$，其中a是根的多项式相乘，这与我们的假设矛盾，为此n次多项式$f(x)$至多有n个根。