Content

Chapter 1 : Unique Factorization

The notion of prime number is fundamental in number theory. The first part of this chapter is devoted to proving that every integer can be written as a product of primes in an essentially unique way.

After that, we shall prove an analogous theorem in the ring of polynomials over a field.

On a more abstract plane, the general idea of unique factorization is treated for principal ideal domains.

Finally, returning from the abstract to the concrete, the general theory is applied tv two special rings that will be important later in the book.

§1 $\mathbb{Z}$的唯一因数分解

作为第一近似,数论可以被定义为对于自然数$1,2,3,\cdots,L$的研究.Kronecker曾经说过(泛指数学),上帝创造了自然数,其余的都是人类的工作.尽管自然数在某种意义上构成了最基本的数学体系,但对于自然数性质的研究给一代又一代的数学家带来了具有无穷魅力的问题.

对于两个自然数a,b若存在一个自然数c使得$b=ac$则说a整除b.若a整除b,我们使用符号$a\mid b$来表示.举个例子$2\mid 8,3\mid 15$但是$6\nmid 21$.若我们给定一个数,我们很容易把它一遍又一遍的分解,直到无法再分解.举个例子$180=18\times 10=2\times 9\times 2\times 5=2\times 3\times 3\times 2\times 5$.这些不能被进一步分解的数称为素数(primes).更精确的说,若一个数p只能被1和p整除,我们就说它是素数.素数非常重要,因为每个数字都可以写为素数的乘积.此外,素数之所以引起人们的极大兴趣,是因为素数的许多问题很容易表述但是很难证明.事实上,许多关于素数的老问题至今无法得到解决.

排在最前边的几个素数是$2,3,5,7,11,13,17,19,23,29,31,37,41,43,\cdots$.有人可能会问素数是否是无穷多个的.回答是肯定的.Euclid在距今2000多年前给出了一个优雅的证明.我们将在第二章给出他和其他几个人的证明.令$\pi(x)$为在1到x之间的素数个数.$\pi(x)$有什么有趣的性质呢?几位数学家通过试验发现,当x较大时,函数$\pi(x)$近似等于$\frac{x}{\ln x}$.这个论断被称为素数定理,在19世纪末由J. Hadamard证明,并且由Ch-J. de la Vallé Poussin.更准确的说,他们证明了

$$\lim_{x\to\infty}\frac{\pi(x)}{x/\ln x}=1$$

即使从一个很小的素数列表中,人们也可以注意到它们具有成对出现的趋势,例如3和5,5和7,11和13,17和19.是否存在无穷的素数对?这是至今无法回答的问题.

另一个著名的未解之谜是Goldbach(C.G.Goldbach)猜想.每个偶数都可以写为两个素数之和吗?Goldbach通过实验得出这个猜想.如今,电子计算机可以使用非常大的数字进行实验.Goldbach猜想的反例从未被发现过.I.M. Vinogradov和L.Schnirelmann在校对方面取得了很大的进展.1937年Vinogradov证明了每一个足够大的数都是三个奇素数之和.

在本书中,将不会深入研究素数分布或关于它们"可加性"的问题.相反,我们关注的是素数如何进入数字的乘法结构.这些主要的定理可以追溯到Euclid年代.它就是唯一分解定理(unique factorization).这个定理有时也被称为算术基本定理(fundamental theorem of arithmetic),这是当之无愧的.某种程度上,我们将要讨论的几乎所有结果都取决于它.该定理指出,任何一个数字都可以以唯一的方式分解为质数的乘积.下面将解释唯一性的含义.

以数字180为例.我们知道$180=2\times 2\times 3\times 3\times 5=2^2\times 3^2\times 5$.在这种情况下,唯一性指的是能够整除180的素数只有$2,3,5$.其指数$2,2,1$是唯一由180所确定的.

$\mathbb{Z}$表示整数环,即集合$0,\pm 1,\pm 2,\pm 3,\cdots$,加法与乘法定义为最常见的加法与乘法.用$\mathbb{Z}$来操作要比使用正整数方便得多.整除的概念可以毫不费力的扩张到$\mathbb{Z}$上.若p为一个正素数,则$-p$也是一个素数.我们不将$1,-1$考虑为素数即使它们确实符合定义.这只是一个有用的约定.注意到,$1.-1$是唯二拥有整除所有数这一性质的整数.它们被称为$\mathbb{Z}$的单位.注意到每一个非零数都可以整除0.依照惯例,0不作为被除数.

除法有一些简单的性质,我们将简单列出.

1. $a\mid a,a\neq 0$
2. 若$a\mid b$且$b\mid a$则$a=\pm b$.
3. 若$a\mid b$且$b\mid c$则$a\mid c$
4. 若$a\mid b$且$a\mid c$则$a\mid b+c$.

令$n\in\mathbb{Z}$且p为一个素数.则若n非零,就存在一个非负整数a使得$p^a\mid n$且$p^{a+1}\nmid n$(a可以等于0).很容易看出若p和n都是正的,那么p的幂会不断增大,直至超过n.其他的情况也很容易被归结到这种结果上.数字a称为p的n阶并使用$\mathrm{ord}_p n$表示.粗略的说,$\mathrm{ord}_p n$是n能被p所整除的次数.若$n=0$我们设置$\mathrm{ord}_p n=\infty$注意到$\mathrm{ord}_p n=0$当且仅当$p\nmid n$.

引理 1 每一个非零整数都可以写为素数的乘积.

[证明]

假设整数使其不能写为素数的乘积

我们取N为这样的整数中的最小正整数(由于正整数集有下界,因此若上述假设成立,必然存在一个最小的符合上述特征的正整数).则显然其不为一个素数,所以必然存在一个m使其不为素数且可以整除N因此得到$N=mn$其中$1<m,n<N$然而对于m,n都有其小于N,因此其可以写为素数的乘积,即N也可以写为素数的乘积,这与N是最小的不能写成素数的乘积的正整数相矛盾.

也可以使用数学归纳法进行更精确的证明,我们只需要证明对于正整数的情况成立即可.

首先对于2有2为素数自然可以写为素数的乘积,接下来假设$2 < N$,然后对于任意的$2 \leq m < N$均可以写为素数的乘积,对于N,若N为素数,则自然可以写为素数的乘积,若N不为素数,则存在m使得$N = mn$其中$1 < m, n < N$因此可以证明N可以写为素数的乘积.□

不难发现我们可以写为$n = p_1^{a_1} p_2^{a_2} \cdots p_m^{a_m}$的形式.其中$p_i$是素数且$a_i$是非负整数.我们将使用下述记号

$$n = (-1)^{\varepsilon(n)} \prod_p p^{a(p)}$$

其中$\varepsilon(n) = 0, 1$取决于n是否是一个正数,可以理解为一个sgn函数.指数$a(p)$是非负整数,当然除了有限个素数以外都有$a(p) = 0$.

我们现在就可以证明核心的定理了.

定理 1 所有非负整数n都存在一个指数由n唯一确定的因数分解.

$$n = (-1)^{\varepsilon(n)} \prod_p p^{a(p)}$$

事实上,我们有$a(p) = \mathrm{ord}_p n$.

这个定理的证明没有看上去那么简单.我们将在确定了一些初步结果之后对其进行证明.

引理 2 若$a, b \in \mathbb{Z}$且$b > 0$,则存在$q, r \in \mathbb{Z}$使得$a = qb + r$且$0 \leq r < b$.

[证明]

考虑所有$a - xb, x \in \mathbb{Z}$形式的整数.这个集合至少包含一个正整数.令$r = a - qb$为这个集合中的最小正整数.我们断言$0 \leq r < b$,若不成立,则$r = a - qb \geq b$即$0 < a - (q+1)b \leq r$这与r是$a - xb$中最小的正整数相矛盾.□

定义: 若$a_1, a_2, \cdots, a_n \in \mathbb{Z}$,我们定义$(a_1, a_2, \cdots, a_n)$为所有形如$a_1x_1 + a_2x_2 + \cdots + a_nx_n$其中$x_1, x_2, \cdots, x_n \in \mathbb{Z}$的整数所构成的集合.令$A = (a_1, a_2, \cdots, a_n)$.注意到$A$中任意两个元素的和与差仍然在$A$中(即$A$对于加法构成群).且对于任意的$a \in A, r \in \mathbb{Z}$有$ra \in A$,于是得到$rA \subset A$因此$A$是$\mathbb{Z}$的一个理想.

引理3 若$a, b \in \mathbb{Z}$则有一个$d \in \mathbb{Z}$使得$(a, b) = (d)$

[证明]

我们假设a, b不全为0.于是在(a, b)中必然存在正元素.令d为(a, b)中最小的正元素.显然有$(d) \subset (a, b)$接下来我们需要证明反向包含也是成立的.

对于任意的$c \in (a, b)$,根据引理2可以得到存在q, r使得$c = qd + r$.且无论是c还是d都在(a, b)中,也就是说$r = c - qd$也属于(a, b).由于$0 \leq r < d$而d是(a, b)中最小的正元素,于是得到$r = 0$因此$d \mid c$即$c \in (d)$.□

定义 : 对于$a, b \in \mathbb{Z}$.若有一个整数d使得d同时整除a和b且对于其他所有a和b的公因子c都有$c \mid d$则d称为a和b的最大公因子(greatest common divisor).注意到,若存在c也是a和b的最大公因子,则$c \mid d$且$d \mid c$即$c = \pm d$.因此,两个数的最大公因子,若存在,则由符号函数sign所决定.

举个例子,我们可以检验14是42和196的最大公因子.下面的引理将保证最大公因子的存在性,但是不会给出计算它的方法.在Exercise中,我们将概述一种行之有效的计算方法,称为Euclid算法.

引理4 若$a, b \in \mathbb{Z}$且$(a, b) = (d)$则d是a和b的最大公因子.

[证明]

由于$a, b \in (a, b) = (d)$因此可以得到d确实是a, b的公因子.对于a, b的某个公因子c,有c可以整除任意$ax + by$形式的整数,其中$x, y \in \mathbb{Z}$,因此得到$c \mid d$.□

定义 : 我们说整数a和b是互素的若其最大公因子只有± 1即单位.

虽然我们定义(a, b)是一个集合,但是由于$(a, b) = (d)$且d是一个最大公因子,因此使用(a, b)表示a和b的最大公因子是相当标准的.使用(a, b)表示两种含义不会太混乱.因此a, b互素当且仅当$(a, b) = 1$.

命题1.1.1 假设$a \mid bc$且$(a, b) = 1$则$a \mid c$.

[证明]

因为$(a, b) = 1$因此存在$r, s \in \mathbb{Z}$使得$ra + sb = 1$因此$rac + sbc = c$,由于$a \mid bc$因此存在e使得$ea = bc$于是得到$rac + sea = c$即$(rc + se)a = c$因此$a \mid c$.□

当$(a, b) \neq 1$时,命题是错误的.举个例子$6 \mid 24$但是$6 \nmid 3$且$6 \nmid 8$.

推论1 若p是一个素数且$p \mid bc$则要么有$p \mid b$要么有$p \mid c$.

[证明]

由于p的因子只有± 1和$\pm p$因此$(p, b) = 1$或p,若$(p, b) = p$则$p \mid b$,若$(p, b) = 1$则由于$p \mid bc$得到$p \mid c$.□

我们可以用一种稍微不同的形式来表述这个推论,这种形式通常是有用的:若p是一个素数且$p \nmid b, p \nmid c$则$p \nmid bc$.

推论2 若p是一个素数且$a, b \in \mathbb{Z}$则$\mathrm{ord}_p ab = \mathrm{ord}_p a + \mathrm{ord}_p b$.

[证明]

令$\alpha = \mathrm{ord}_p a$,$\beta = \mathrm{ord}_p b$于是得到$a = p^\alpha c$,$b = p^\beta d$其中$p \nmid c$且$p \nmid d$因此得到$ab = p^{\alpha+\beta} cd$由于$p \nmid c$且$p \nmid d$于是有$p \nmid cd$因此$\mathrm{ord}_p ab = \alpha + \beta = \mathrm{ord}_p a + \mathrm{ord}_p b$.□

现在,我们来证明定理1.

回顾等式

$$n = (-1)^{\varepsilon(n)} \prod_p p^{a(p)}$$

对于两侧同时作用一个函数ord_q得到

$$\mathrm{ord}_q n = \varepsilon(n)\mathrm{ord}_q(-1) + \sum_p a(p)\mathrm{ord}_q p$$

$p \neq q$时由于$\mathrm{ord}_q(-1) = \mathrm{ord}_q p = 0$因此得到$\mathrm{ord}_q n = 0$.

而$p = q$时有$\mathrm{ord}_q n = a(q)$.这就是我们想要证明的.

需要强调的是,证明的关键步骤是推论1也就是说若$p \mid ab$则$p \mid a$或$p \mid b$.证明中的所有难点都集中在这个事实上.

> 这是因为若$q \mid n$则有$q \mid (-1)^{\varepsilon(n)}$或$q \mid \prod_p p^{a(p)}$
>
> 若$q \mid (-1)$则$q^{\varepsilon(n)} \mid (-1)^{\varepsilon(n)}$若$q \mid p$则$q^{a(p)} \mid p^{a(p)}$,再根据推论2将乘法转化为加法得到
>
> $$\mathrm{ord}_q n = \varepsilon(n)\mathrm{ord}_q(-1) + \sum_p a(p)\mathrm{ord}_q p$$

§ 2　$k[x]$上的唯一因式分解

唯一分解定理可以在比 § 1更一般的情况下表述和证明.在本节中,我们将考虑系数在域$\Bbbk$中的多项式环$k[x]$.在 § 3中我们将考虑主理想域.事实证明,这些情况的分析将对于整数的研究有益.

若$f, g \in k[x]$,若存在$h \in k[x]$使得$g = fh$则称f整除g.

若使用$\deg f$来表示f的度(即最高次非零项的次数),我们有$\deg fg = \deg f + \deg g$.同理,当且仅当$f$为一个非零常数时有$\deg f = 0$.这也说明$f \mid g$且$g \mid f$当且仅当$g = cf$其中$c$是一个非零常数.它还可以得出,可以整除所有其他多项式的唯一多项式是一个非零常数.这些非零常数就是$k[x]$的单位.若$q \mid p$可以推出q是一个常数或q是p的常数倍,那么常系数多项式p是不可约的(irreducible).不可约多项式是素数的类似物.

引理1 每个非常数的多项式都可以写为若干个不可约多项式的乘积.

[证明]

通过对于度进行归纳来证明引理.

不难发现当多项式的度为1时多项式是不可约的(根据$\deg fg = \deg f + \deg g$得到若$\deg fg = 1$且其可约,则$f$和$g$必然一个的度为1一个的度为0,假设$f$的度为1则有$g$为非零常数,即$fg$是不可约的).

现在假设我们已经对于所有的度小于n的多项式证明了上述引理,则考虑$\deg f = n$若f为不可约多项式,则f自然可以写为自身与1的乘积,也就是说可以写为不可约多项式的乘积.若f可约则存在$f = gh$使得$1 \leq \deg g, \deg h < n$因此根据前文假设可以得知$g$和$h$都可以写为若干个不可约多项式的乘积,也就是说$f$可以写为不可约多项式的乘积.□

很自然地,可以引出首一多项式(monic polynomial)的定义.对于多项式f,若其第一个(非零)系数为1则称其为一个首一多项式.举个例子,$x^2 + x - 3$以及$x^3 - x^2 + 3x + 17$都是首一的,但是$2x^3 - 5$以及$3x^4 + 2x^2 - 1$就不是首一的.每一个非零多项式都是某个首一多项式的常数倍.

令p为一个首一不可约多项式.我们定义$\mathrm{ord}_p f$为一个满足$p^a \mid f$且$p^{a+1} \nmid f$的整数.由于p^a将越来越大,因此这样的整数a必然存在.注意到$\mathrm{ord}_p f = 0$当且仅当$p \nmid f$.

定理2 令$f \in k[x]$与是我们可以得到

$$f = c \prod_p p^{a(p)}$$

其中乘积为所有的不可约多项式,且c为常数.常数c和指数$a(p)$由f唯一确定.事实上,$a(p) = \mathrm{ord}_p f$.

这种乘积的存在性可以直接从引理1推导出来.和先前一样,唯一性的证明较为困难,我们将先推导出一些数学工具来辅助证明

引理 2 令$f, g \in k[x]$若$g \neq 0$则存在多项式$h, r \in k[x]$使得$f = hg + r$其中r要么为0要么$\deg r < \deg g$.

[证明]

若$g \mid f$则$f = hg$即$r = 0$.

若$g \nmid f$则令r为$f - lg$其中$l \in k[x]$的多项式中度数最小的多项式.我们断言$\deg r < \deg g$否则设r的第一项为ax^d而g的第一项为bx^m.于是得到
$r - ab^{-1}x^{d-m}g = f - (h + ab^{-1}x^{d-m}g)$其度数比$\deg r$小,造成矛盾.□

> 构建$ab^{-1}x^{d-m}g$的原因在于其第一项为ax^d,可以保证$r - ab^{-1}x^{d-m}g$的度数比r小.

定义 若$f_1, f_2, \cdots, f_n \in k[x]$则$(f_1, f_2, \cdots, f_n)$是所有形如$f_1h_1 + f_2h_2 + \cdots + f_nh_n$的多项式构成的集合其中$h_1, h_2, \cdots, h_n \in k[x]$.

使用环理论语言来说$(f_1, f_2, \cdots, f_n)$无非是由$f_1, f_2, \cdots, f_n$生成的理想.

引理3 给定$f, g \in k[x]$存在一个$d \in k[x]$使得$(f, g) = (d)$

[证明]

令d为(f, g)中具有最小度的多项式.必然有$(d) \subset (f, g)$并且我们打算证明反向的包含也是成立的.

令$c \in (f, g)$则$\deg c \geq \deg d$.若$d \nmid c$则根据引理2可知存在$h, r \in k[x]$使得$c = hd + r$,其中$\deg r < \deg d$由于(f, g)是理想

因此$r = c - hd \in (f, g)$而$\deg r < \deg d$

这与d是(f, g)中具有最小度的多项式相矛盾.

因此r必然为0也就是说对于任意的$c \in (f, g)$都有$c \in (d)$.□

定义 令$f, g \in k[x]$,若有d同时作为f和g的公因子且对于f和g的其他公因子c都有$c \mid d$则d为f和g的最大公因子.

注意到两个多项式的最大公因子之间相差常数倍.若我们要求它是首一的,则它就是唯一确定的,我们一般特指其为最大公因子.

引理4 令$f, g \in k[x]$通过引理3可以得到有一个$d \in k[x]$使得$(f, g) = (d)$.d是f和g的最大公因子.

[证明]

因为$f \in (d)$且$g \in (d)$因此d是f和g的公因子,接下来对于任意的c也为f和g的公因子,有$d = h_1 f + h_2 g$其中$h_1, h_2 \in k[x]$于是有$c \mid d$因此d是最大公因子.□

定义: 两个多项式f和g的最大公因子为常数时,称(f, g)是互素的,有$(f, g) = (1)$

命题1.2.1 若f和g是互素的,则$f \mid gh$可以推出$f \mid h$.

[证明]

若f和g是互素的,我们有$(f, g) = (1)$因此存在两个多项式l, r使得$1 = lf + rg$因此$lfh + rgh = h$由于$f \mid gh$因此得到$f \mid h$.□.

推论1 若p是不可约多项式且$p \mid fg$则$p \mid f$或$p \mid g$.

[证明]

因为p是不可约多项式,因此对于任意的$f \in k[x]$都有$p \mid f$或者$(p, f) = (1)$.若$p \mid f$则得到推论成立,若$(p, f) = (1)$则根据前文命题得到$p \mid g$.□

推论2 若p是一个首一不可约多项式且$f, g \in k[x]$就得到$\mathrm{ord}_p fg = \mathrm{ord}_p f + \mathrm{ord}_p g$.

[证明]

令$\alpha = \mathrm{ord}_p f$且$\beta = \mathrm{ord}_p g$则$f = p^\alpha c$,$g = p^\beta d$, $c, d \in k[x]$且$(p, c) = (p, d) = (1)$于是$p \nmid cd$.因此$fg = p^{\alpha+\beta} cd$得到$\mathrm{ord}_p fg = \mathrm{ord}_p f + \mathrm{ord}_p g$.□

依照 § 1中的证明方式,我们在

$$f = c \prod_p p^{a(p)}$$

等式两侧都应用函数ord_q得到

$$\mathrm{ord}_q f = \mathrm{ord}_q c + \sum_p a(p) \mathrm{ord}_q p$$

仿照 § 1中的讨论得到$q \neq p$时,$\mathrm{ord}_q f = 0$而$q = p$时有$\mathrm{ord}_q f = a(p)$.

§ 3　主理想域上的唯一因式分解

读者不会没有注意到 § 1和 § 2的证明方法存在巨大性的相似.在本节中,我们将证明一个抽象定理,它将前面的结果作为一个特例从而包含在内.

在本节中,R表示一个整环.

定义1 对于R若存在一个函数λ将R中的非零元映射到集合$\{0, 1, 2, 3, \cdots\}$上使得对于$a, b \in R$且$b \neq 0$存在$c, d \in R$且具有特性:$a = cb + d$其中d要么为0要么有$\lambda(d) < \lambda(b)$.则称R为一个欧几里得整环(Euclidean domain).

环$\mathbb{Z}$与$k[x]$都是欧几里得整环.在$\mathbb{Z}$上我们可以令绝对值为函数λ;在环$k[x]$上可以将多项式的度视为λ来达成目的.

命题1.3.1 若R是一个欧几里得整环且$I \subset R$为一个理想,则存在一个元素$a \in R$使得$I = Ra = \{ra : r \in R\}$.

[证明]

考虑非负整数$\{\lambda(b) : b \in I, b \neq 0\}$所构成的集合.由于每个非负整数所构成的集合均存在一个最小元,此处为一个$a \in I, a \neq 0$且$\lambda(a) \leq \lambda(b)$对于所有的$b \in I, b \neq 0$成立.

我们断言$I = Ra$.由于I是一个理想,且$a \in I$,显然有$Ra \subset I$,取$b \in I$可以得到存在$c, d \in R$使得$b = ac + d$其中d要么为0要么有$\lambda(d) < \lambda(a)$.由于I是一个理想,于是可以得到$b - ca \in I$即$d \in I$若有$d \neq 0$则d与$\lambda(a) = \inf\{\lambda(b) : b \in I, b \neq 0\}$矛盾.

因此得到$I \subset Ra$.□

对于元素$a_1, a_2, \cdots, a_n \in R$,定义$(a_1, a_2, \cdots, a_n) = Ra_1 + Ra_2 + \cdots + Ra_n = \{\sum_{i=1}^{n} r_i a_i : r_i \in R\}$.$(a_1, a_2, \cdots, a_n)$是一个理想.若一个理想$I$等于$(a_1, a_2, \cdots, a_n)$其中$a_i \in I$则说$I$是有限生成的(finitely generated).若$I = (a)$对于某个$a \in I$成立,我们就说I是一个主理想.

定义2 若每一个R中的理想都是主理想,则R为一个主理想环(principal ideal domian (PID)).

命题1.3.1断言每个欧几里得整环都是一个PID.虽然我们很难提供一个真实例子,但是这种说法反过来是错误的.

本节剩下的讨论是关于PID的.欧几里得整环的概念是非常有用的,在实践中,人们可以通过先确定一个环时欧几里得整环而后来证明环是PID的.我们将在§4中给出两个更具体的例子.

我们引入更多的术语.

若$a, b \in R$且$b \neq 0$,若对于某个$c \in R$有$a = bc$我们称,b整除a.记为$b \mid a$.

一个元素$u \in R$整除1则称u为单位.

两个元素$a, b \in R$若对于某个单位u有$a = bu$则称a和b是关联的(associates).

对于一个元素$p \in R$若对于$a \mid p$都有a是一个单位或者与p关联则称p是不可约的.

若一个非单位元$p \in R$,有$p \mid ab$推出$p \mid a$或$p \mid b$则p称为一个素元.

不可约元和素元的定义是新的,但是一般来说,这两个概念并不是一致的.正如我们所见,在$\mathbb{Z}$和$k[x]$中它们是一致的,我们将很快证明在所有的PID中它们都一致.

一些我们讨论的概念可以翻译为理想的语言

$a \mid b$当且仅当$(b) \subset (a)$.

> 由于$a \mid b$因此存在c使得$b = ac$即$b \in Ra$即$(b) \subset (a)$

u是R的单位当且仅当$R = (u)$.

> 若u是R的单位,由于$u \mid 1$因此$(1) \subset (u)$,此外由于$(1) = R$因此得到$R \subset (u) \subset R$因此$(u) = R$

a和b是关联的当且仅当$(a) = (b)$.

> 若$a = bu$则$b \mid a$,得到$(a) \subset (b)$,且$(a) = (bu) = buR$
>
> 由于$(u) = R$因此得到R中存在元素u'使得$uu' = 1$因此得到$b = buu' \in (bu) = (a)$
>
> 因此$(b) \subset (a)$即$(b) = (a)$

p是一个素元当且仅当$ab \in (p) \Rightarrow a \in (p) \vee b \in (p)$.

> 由于$p \mid ab \Rightarrow p \mid a \vee p \mid b$
>
> 因此得到若$ab \in (p)$则$p \mid ab$,即$p \mid a \vee p \mid b$
>
> 因此自然可以得到$a \in (p) \vee b \in (p)$

定义 若$a, b \in R$且$d \in R$,d称为a, b之间的最大公因子(greatest common divisor(gcd)在不引起矛盾的时候使用gcd)若

(a) $d \mid a$且$d \mid b$

(b) $d' \mid a$且$d' \mid b$则$d' \mid d$.

不难发现若d和d'均为a与b的gcd,则d与d'关联.

一般环中两个元素的gcd不一定存在.然而

命题1.3.2 令R为一个PID且$a, b \in R$.则a与b有一个最大公因子d且$(a, b) = (d)$

[证明]

由于R是一个PID因此R中的所有理想均为主理想,也就是说必然存在一个$d \in R$使得$(a, b) = (d)$.因为$(a) \subset (d)$且$(b) \subset (d)$我们可以得到$d \mid a$且$d \mid b$.因此d是一个a, b的公因子.接下来证明d是gcd.

若有$d' \mid a$且$d' \mid b$则有$(a) \subset (d')$且$(b) \subset (d')$因此得到$(d) = (a, b) \subset (d')$即$d' \mid d$因此根据定义得到$d$确实是一个gcd.□

对于两个元素a,b若它们的公因子是单位u,则a和b互素.

推论1 若R是一个PID且$a,b\in R$是互素的,则$(a,b)=R$

[证明]

由于$(a,b)=(u)=R$直接得到结果□

推论2 若R是一个PID且$p\in R$是不可约的,则p是一个素元.

[证明]

假设$p\mid ab$且$p\nmid a$.因此有$(ab)\subset(p)$但是$a\notin(p)$.于是由于p是不可约的,有a与p互素.因此$(a,p)=R$

从而有$(ab,pb)=(b)$.因为$p\mid ab$因此$ab\in(p)$且$pb\in(p)$于是得到$(ab,pb)\subset(p)$因此得到$(b)\subset(p)$即$p\mid b$即p是一个素元.□

从现在起R将会是一个PID且我们将交替的使用素元和不可约元来表述.

我们打算证明R中每一个非零元均可写为不可约元素的乘积.证明分为两步.第一步证明若$a\in R$且$a\neq 0$则存在一个不可约元整除a,紧接着我们就可以将a写为不可约元的乘积.

引理 1 令$(a_1)\subset(a_2)\subset(a_3)\subset\cdots$为一条不断上升的理想链.则存在一个整数$k$使得$(a_k)=(a_{k+l})$其中$l=0,1,2,\cdots$换句话说,链条将在有限步内断裂.

[证明]

令$I=\bigcup_{i=1}^{\infty}(a_i)$则显然对于任意的$k\in\mathbb{N}$有$(a_k)\subset I$

不难发现I是一个理想(对于任意的$a\in I$都存在一个k使得$a\in(a_k)$因此有$aR\subset(a_k)$因此$aR\subset I$,且I显然是一个加法子群)

但是由于R是一个PID因此得知$I=(a)$对于某个$a\in R$成立.

因此存在k使得$a\in(a_k)$,即$I=(a)\subset(a_k)\subset(a_{k+1})\subset\cdots\subset I$.□

命题1.3.3 每一个R中的非零非单位元都可以写为不可约元的乘积.

[证明]

令$a\in R$且$a\neq 0$且a不是单位.

我们首先要证明a可以被一个不可约元素整除.若a是不可约元,则自然成立.

否则a可约,即存在a_1,b_1使得$a=a_1b_1$其中a_1和b_1均不是单位.

若a_1不可约,则我们就证明了命题,若a_1可约,则有$a_1=a_2b_2$其中a_2,b_2均不为单位.

若a_2不可约,则证明命题,若a_2可约则继续得到a_3

由于它们之间都具有整除关系,因此

$(a)\subset(a_1)\subset(a_2)\subset\cdots$最终得到存在某个$k$使得$(a_k)=(a_{k+l})$因此得知$a_k$为不可约元(不可约元的定义)

接下来再证明a可以写为不可约元的乘积.若a是不可约的,则证毕

若a可约,则根据前文推导可知存在p_1使得$p_1\mid a$且p_1是不可约元.

那么有$a=p_1c_1$若c_1是单位元,则证毕.

若c_1不是单位元且可约,则存在$p_2\mid c_1$使得$a=p_1p_2c_2$.

不难发现$(a)\subset(c_1)\subset(c_2)\subset\cdots$根据引理1可知总是存在一个$c_k$使得$c_k$是单位,由于$p_kc_k$是不可约的,因此$a=p_1p_2\cdots p_kc_k$,即$a$可以写为不可约元的乘积.□

现在我们打算像在§1和§2一样定义一个ord函数.

引理2 令p为一个素元且$a\neq 0$.则存在一个整数n使得$p^n\mid a$且$p^{n+1}\nmid a$

[证明]

假设不存在这样一个n,那么对于任意的$m>0$都有$p^m\mid a$也就是说存在b_m使得$a=p^mb_m$则有$pb_{m+1}=b_m$因此得到$b_{m+1}\mid b_m$即$(b_m)\subset(b_{m+1})$

那么我们可以得知$(b_1)\subset(b_2)\subset(b_3)\subset\cdots$

根据引理1得知这个链条将会断裂.因此必然存在一个b_m使得$a=p^mb_m$且$(b_m)=(b_{m+1})$

由于p是一个素元,因此$(pb_m)\neq(b_m)$因此造成矛盾.□

由于n只由p和a决定,因此可以令$n=\operatorname{ord}_pa$.

引理3 若$a,b\in R$且$a,b\neq 0$则$\operatorname{ord}_pab=\operatorname{ord}_pa+\operatorname{ord}_pb$

[证明]

令$\alpha=\operatorname{ord}_pa$且$\beta=\operatorname{ord}_pb$则有$a=p^\alpha c$且$b=p^\beta d$且有$p\nmid c$且$p\nmid d$.,

由于p是一个素元,因此$p\nmid cd$

$ab=p^{\alpha+\beta}cd$因此有$\mathrm{ord}_pab=\mathrm{ord}_pa+\mathrm{ord}_pb$.□

现在我们就可以表述并证明这一节的主要定理了.

令S为R的素元所构成的集合,且具有以下两种特性:

(a) R中每一个素元均与S中某一个素元相关联.

(b) S中任意两个素元都是不相关联的.

为了得到这样一个集合,从每一类关联素元某种选择一个素元(即代表元).这样的选择显然具有很大的随意性.在$\mathbb{Z}$和$k[x]$中有一种比较自然的方式供我们选择.在$\mathbb{Z}$中我们将正素数的集合作为S,在$k[x]$中我们将首一不可约多项式构成的集合记为S.一般来说,没有哦简单的方法来做出选择,这偶尔会导致复杂的情况(见Chapter 9)

定理3 令R为一个PID且S为素元所构成的满足前文所述条件的集合,则若$a\in R$且$a\neq 0$则我们可以写成

$$a=u\prod_p p^{e(p)}$$

其中u是单位且有$p\in S$.单位u和$e(p)$完全由a所决定.事实上,$e(p)=\mathrm{ord}_pa$.

[证明]

存在性前文已经证明.

照例引入ord_q函数且$q\in S$

根据引理3可以得到

$$\mathrm{ord}_qa=\mathrm{ord}_qu+\sum_p e(p)\mathrm{ord}_qp$$

显然有$\mathrm{ord}_qu=0$.

接下来由于S中的素元两两不相关联,因此若$q\neq p$则有$\mathrm{ord}_qp=0$若$q=p$则$\mathrm{ord}_qp=1$

因此得到$\mathrm{ord}_qa=e(q)$□

§4　环$\mathbb{Z}[i]$与$\mathbb{Z}[\omega]$

作为第三章结果的应用,我们将考虑两个例子,它们在后续的Chapter中是有用的.

令$i=\sqrt{-1}$并且考虑由复数所构成的集合$\mathbb{Z}[i]:=\{a+bi:a,b\in\mathbb{Z}\}$.这个集合对于加减法显然是封闭的.此外,若$a+bi,c+di\in\mathbb{Z}[i]$则$(a+bi)(c+di)=(ac-bd)+(ad+bc)i\in\mathbb{Z}[i]$因此$\mathbb{Z}[i]$对于乘法是封闭的.因此$\mathbb{Z}[i]$可以构成一个环.由于$\mathbb{Z}[i]$包含在复数域(无零因子)中,因此它是一个整环.

命题1.4.1 $\mathbb{Z}[i]$是一个欧几里得整环.

[证明]

对于$a+bi\in\mathbb{Z}[i]$定义$\lambda(a+bi)=a^2+b^2$.

令$\alpha=a+bi$,$\gamma=c+di$并且假设$\gamma\neq 0$.$\alpha/\gamma=r+si$其中r和s均为实数(事实上它们都是有理数).

选择整数$m,n\in\mathbb{Z}$使得$|r-m|\leq\frac{1}{2}$且$|s-n|\leq\frac{1}{2}$.

令$\delta=m+ni$.则$\delta\in\mathbb{Z}[i]$.有$\lambda((\alpha/\gamma)-\delta)=(r-m)^2+(s-n)^2n\leq\frac{1}{4}+\frac{1}{4}=\frac{1}{2}$.

令$\rho=\alpha-\gamma\delta$则$\rho\in\mathbb{Z}[i]$且有$\rho=0$或$\lambda(\rho)=\lambda(\gamma(\alpha/\gamma-\delta))=\lambda(\gamma)\lambda(\alpha/\gamma-\delta)\leq\frac{1}{2}\lambda(\gamma)\leq\lambda(\gamma)$

因此得到$\mathbb{Z}[i]$是一个欧几里得整环.□

这个环被称为ring of Gaussian integers即Gaussian整数环,以C.F. Gauss的名字命名,这是因为Gauss首先详细地研究了它的算术性质.

数字$\pm1,\pm i$都是$x^4=1$在复数域上的根.考虑等式$x^3=1$.由于$x^3-1=(x-1)(x^2+x+1)$得到等式的根为$1,\frac{-1\pm\sqrt{-3}}{2}$.令$\omega=\frac{-1+\sqrt{-3}}{2}$得到$\omega^2=\frac{-1-\sqrt{-3}}{2}$从而可以发现$1+\omega+\omega^2=0$.

考虑集合$\mathbb{Z}[\omega]=\{a+b\omega:a,b\in\mathbb{Z}\}$.得到$\mathbb{Z}[\omega]$在加减法下是封闭的.且$(a+b\omega)(c+d\omega)=ac+bd\omega^2+(ad+bc)\omega=ac-bd(1+\omega)+(ad+bc)\omega$ $=(ac-bd)+(ad+bc-bd)\omega$.因此$\mathbb{Z}[\omega]$对于乘法封闭.因此$\mathbb{Z}[\omega]$是一个环.由于$\mathbb{Z}[\omega]$在复数域中,因此其是一个整环.

我们注意到$\mathbb{Z}[\omega]$在复共轭下是封闭的.事实上,因为$\overline{\sqrt{-3}}=\overline{\sqrt{3}i}=-\sqrt{3}i=-\sqrt{-3}$我们得到了$\overline{\omega}=\omega^2$.因此若$\alpha=a+b\omega\in\mathbb{Z}[\omega]$则有$\overline{\alpha}=a+b\overline{\omega}=a+b\omega^2=a-b-b\omega\in\mathbb{Z}[\omega]$.

命题1.4.2 $\mathbb{Z}[\omega]$是一个欧几里得整环.

[证明]

令$\alpha=a+b\omega\in\mathbb{Z}[\omega]$且令$\lambda(\alpha)=a^2-ab+b^2$.通过简单的计算可以得知$\lambda(\alpha)=\overline{\alpha}\alpha$.

现在,令$\alpha,\beta\in\mathbb{Z}[\omega]$且假设$\beta\neq 0$于是有$\alpha/\beta=\alpha\overline{\beta}/\beta\overline{\beta}=r+s\omega$其中$r,s$为实数(事实上是有理数).不难发现有$\beta\overline{\beta}=\lambda(\beta)$且$\alpha\overline{\beta}\in\mathbb{Z}[\omega]$.

可以找到两个整数m,n使得$|r-m|\leq\frac{1}{2}$且$|s-n|\leq\frac{1}{2}$,接着令$\gamma=m+n\omega$可以得到$\lambda(\alpha/\beta-\gamma)=(r-m)^2-(r-m)(s-n)+(s-n)^2\leq\frac{1}{4}+\frac{1}{4}+\frac{1}{4}<1$.

令$\rho=\alpha-\gamma\beta$得到$\rho=0$或$\lambda(\rho)=\lambda(\beta(\alpha/\beta-\gamma))=\lambda(\beta)\lambda(\alpha/\beta-\gamma)<\lambda(\beta)$.

因此得知$\mathbb{Z}[\omega]$是一个欧几里得整环.□

由于$\mathbb{Z}[i]$和$\mathbb{Z}[\omega]$均为欧几里得整环,因此它们都是PID.也就是说唯一因式分解在它们上均成立.为了进一步分析这些环,我们必须研究其上的单位和素元.在Exercise中有一些这种性质的结果.

Notes（太多了, 此处并非重点, 暂时不译）

支持唯一分解定理的环称为唯一因子分解整环(unique factorization domains(UFD)).事实上Euclid已经悄然证明了$\mathbb{Z}$是一个唯一因子分解整环,但是第一个明确而清晰的结果似乎是在C.F.Gauss的*Disquisitiones Arithmeticae*中被记载.Zermelo通过归谬法给出了一个巧妙的证明.

Exercises

1. 令a,b为非负整数.我们可以找到非负整数q,r使得$a=qb+r$其中$0\le r<b$.证明$(a,b)=(b,r)$

   由于$a-qb=r$因此有$r\in(a,b)$,因此任意的$k\in(b,r)$都可以写为$k=s_1b+s_2r=s_1b+s_2(a-qb)=(s_1-s_2q)b+s_2a\in(a,b)$,其中$s_1,s_2\in\mathbb{Z}$且$q$为非负整数.

   因此得知$(b,r)\subset(a,b)$.

   同理证明$(a,b)\subset(b,r)$

   因此有$(a,b)=(b,r)$

2. (延续上问) 若$r\neq 0$且我们可以找到q_1和r_1使得$b=q_1r+r_1$且$0\le r_1<r$.证明$(a,b)=(r,r_1)$.这个过程是可以重复的.证明它必然在有限步后停止.证明最后一个非零余数必然等于(a,b).这个过程看起来像

$$\begin{array}{rcll} a & = & qb+r, & 0\le r<b \\ b & = & q_1r+r_1, & 0\le r_1<r \\ r & = & q_2r_1+r_2, & 0\le r_2<r_1 \\ \vdots & & & \\ r_{k-1} & = & q_{k+1}r_k+r_{k+1}, & 0\le r_{k+1}<r_k \\ r_k & = & q_{k+2}r_{k+1} & \end{array}$$

   则$r_{k+1}=(a,b)$.这个寻找(a,b)的过程称为Euclidean algorithm.

   首先证明$(a,b)=(r,r_1)$由于$(a,b)=(b,r)$而$(b,r)=(r,r_1)$因此得知$(a,b)=(r,r_1)$.

   接下来证明这个过程在持续有限步后必然停止.

   假设这个过程可以无限重复下去,那么对于任意的正整数n都有$0<r_{n+1}<r_n$,且r_n和r_{n+1}均为整数.

   由于b是一个整数,而$0\le r_{n+1}<r_n<\cdots<r<b$

   也就是说在经过b步后必然有$r_b=q_br_{b-1}=0$.

   即存在k使得$r_{k+2}=0$且$r_{k+1}>0$.

   因此得到这个步骤必然在有限步后停止.

   接下来由于$(a,b)=(b,r)=(r,r_1)=\cdots=(r_{k-1},r_k)=(r_k,r_{k+1})=(r_{k+1},r_{k+2})=(r_{k+1},0)=r_{k+1}x+0=(r_{k+1})$因

   因此$r_{k+1}=(a,b)$.

3. 计算$(187,221),(6188,4709),(314,159)$

   读者自行计算即可

   $221=187+34$

   $187=5\times 34+17$

   $34=2\times 17$

   因此$17=(187,221)$

   $6188=4709+1479$

   $4709=3\times 1479+272$

   $1479=5\times 272+119$

   $272=2\times 119+34$

   $119=3\times 34+17$

   $34=2\times 17$

   因此$17=(6188,4709)$

   $314=159+155$

$159=155+4$
$155=38\times 4+3$
$4=3+1$
$3=3\times 1$
因此$1=(314,159)$

4. 令$d=(a,b)$使用$\mathrm{Euclidean\ algorithm}$找到整数$m,n$使得$am+bn=d.$

   反过来使用$\mathrm{Euclidean\ algorithm}$,令最后个非零元$r_{k+1}=d.$
   因此有$r_k=q_{k+2}d,$
   那么$r_{k-1}=q_{k+1}q_{k+2}d+d$
   $r_{k-2}=q_k(q_{k+1}q_{k+2}d+d)+q_{k+2}d=q_kq_{k+1}q_{k+2}d+q_kd+q_{k+2}d$
   $r_{k-3}=q_{k-1}(q_kq_{k+1}q_{k+2}d+q_kd+q_{k+1}d)+q_{k+1}q_{k+2}d+d=(q_{k-1}q_kq_{k+1}q_{k+2}+q_{k-1}q_k+q_{k-1}q_{k+1}+q_{k+1}+q_{k+2}+1)d$
   以此类推可以得知m与n的值.

5. 计算3中给出数的m,n
   读者当自强
   自己算吧

6. 令$a,b,c\in\mathbb{Z}$.证明等式$ax+by=c$有整数解当且仅当$(a,b)\mid c.$

   $(\Leftarrow)$ 若$(a,b)\mid c$则有$c\in(a,b)$因此存在$x,y\in\mathbb{Z}$使得$ax+by=c.$
   $(\Rightarrow)$ 若$ax+by=c$有整数解,即$c\in(a,b)$因此自然有$(a,b)\mid c$

7. 令$d=(a,b)$且$a=da'$以及$b=db'$,证明$(a',b')=1.$

   由于$d=(a,b)$因此对于任意的$c\mid a$且$c\mid b$有$c\mid d.$
   若$(a',b')\neq 1$即存在c使得$(a',b')=c$则有$c\mid a'$且$c\mid b'.$
   因此得到$a=da'=dca''$其中$a'=ca''$,$b=db'=dcb''.$
   由于d,c均为整数,有$dc>d$且$dc\mid a$,$dc\mid b$.因此有$dc\mid d$造成矛盾.
   于是有$c=1$即$(a',b')=1.$

8. 令x_0,y_0为$ax+by=c$的解.证明所有这样的解都形如$x=x_0+t(b/d)$,$y=y_0-t(a/d)$其中$d=(a,b)$且$t\in\mathbb{Z}.$

   由于$d=(a,b)$因此有$(a/d,b/d)=1.$
   由于$ax+by=c$有解的条件为$(a,b)\mid c$因此有c/d为一个整数
   令$a/d=a',b/d=b',c/d=c'$有$(a',b')=1$
   且$ax+by=c$的解即为$a'x+b'y=c'$的解.
   由于$(a',b')=1$因此$\frac{a'}{b'}$必然不为整数.
   由于$y=\frac{c'-a'x}{b'}=\frac{c'-a'x_0+a'x_0-a'x}{b'}=y_0+\frac{a'x_0-a'x}{b'}=y_0+a'\frac{x_0-x}{b'}$
   得到x必然形如x_0-tb'的形式.

9. 假设$u,v\in\mathbb{Z}$且$(u,v)=1$.若$u\mid n$且$v\mid n$证明$uv\mid n$.并且证明若$(u,v)\neq 1$则不成立

   由于$(u,v)=1$因此存在$s,r\in\mathbb{Z}$使得$us+vr=1.$
   因为$u\mid n$因此存在t使得$n=ut$,我们需要证明$v\mid t$
   由于$v\mid n=ut$且$v\nmid u$,$(v,u)=1$因此有$v\mid t$(命题1.1.1).
   因此得到$uv\mid n.$

   若$(u,v)\neq 1$则无$us+vr=1.$
   则无$ust+vrt=t$即$v(es+rt)=t$因此无$v\mid t$即无法得到$uv\mid n$

10. 假设$(u,v)=1$则$(u+v,u-v)$要么为1要么为2

    因$(u+v)+(u-v)=2u$且$(u+v)-(u-v)=2v$
    因$(u,v)=1$因此存在s,r使得$su+rv=1$
    若对于$(u+v,u-v)=x_1(u+v)+x_2(u-v)=u(x_1+x_2)+v(x_1-x_2)$不存在$x_1,x_2$使得$x_1+x_2=s$且$x_1-x_2=r$则$(u+v,u-v)\neq 1$

但是因$2u,2v\in(u+v,u-v)$于是有$2su+2rv=2\in(u+v,u-v)$
因此$(u+v,u-v)$要么为1要么为2

11. 证明$(a,a+k)\mid k$

    即证$k\in(a,a+k)=x_1a+x_2(a+k)$其中$x_1,x_2\in\mathbb{Z}$取$x_1=-1,x_2=1$即可

12. 假设我们将正多边形复制了几次,并试图在一个公共顶点上均匀地摆放它们.证明唯一可能是6个等边三角形,4个正方形和3个六边形.

    问题其实可以转化为问满足内角可以整除2π的正n边形有什么?
    根据正n边形的内角和为$(n-2)\pi$得到正n边形的每一个内角均为$(n-2)\pi/n$.
    因此问题转化为求能够整除2的所有$(n-2)/n=1-2/n$即$\frac{2n}{n-2}$且n为整数的情况.
    显然有$n=3,4,6$满足情况,
    对于其他的n,n为奇数时,$n-2$为奇数而$2n$为偶数,因此不成立.
    当n为大于6的偶数时,$n=2k(k>3)$那么$\frac{2n}{n-2}=\frac{4k}{2(k-1)}=\frac{2k}{k-1}$由于$k-1>2$因此得到$\frac{2n}{n-2}$均不为整数.

13. 令$n_1,n_2,\cdots,n_s\in\mathbb{Z}$.定义$n_1,n_2,\cdots,n_s$的最大公因子$d$证明存在整数$m_1,m_2,\cdots,m_s$使得$m_1n_1+m_2n_2+\cdots+m_sn_s=d$.

    $(\Leftarrow)$根据题意显然有$d\in(n_1,n_2,\cdots,n_s)$.因此有$(d)\subset(n_1,n_2,\cdots,n_s)$
    接下来证明反向包含也成立.
    任取$c\in(n_1,n_2,\cdots,n_s)$由于d是$n_1,n_2,\cdots,n_s$的公因子,必然有$d\mid c$因此$c\in(d)$.
    因此有$(d)=(n_1,n_2,\cdots,n_s)$
    则此时d确实为$n_1,n_2,\cdots,n_s$的最大公因子.

    $(\Rightarrow)$接下来设d为最大公因子.
    那么对于任意的公因子c都有$c\mid d$.且对于任意的n_i均有$d\mid n_i$.
    由于d是最大公因子,因此取$n_i=dn_i'$.
    我们断言$(n_1',n_2',\cdots,n_s')=1$不然存在一个公因子$c$使得$dc>d$且$dc\mid n_i$对于任意的$n_i$均成立.
    因此得到$(n_1',n_2',\cdots,n_s')=(1)$即存在$m_1,m_2,\cdots,m_s$使得$m_1n_1'+m_2n_2'+\cdots+m_sn_s'=1$因此得到
    $m_1n_1+m_2n_2+\cdots+m_sn_s=d$.

14. 讨论$a_1x_1+a_2x_2+\cdots+a_rx_r=c$的解的性质.

    若$a_1x_1+a_2x_2+\cdots+a_rx_r=c$有解,则$c\in(a_1,a_2,\cdots,a_r)$
    因此得到$(a_1,a_2,\cdots,a_r)\mid c$

15. 证明$a\in\mathbb{Z}$是某个整数的平方当且仅当对于所有的素数p都有ord_pa是偶数.

    若a是某个数b的平方,则对于b进行唯一因式分解得到

    $$b=(-1)^{\varepsilon(n)}\prod_p p^{a(p)}$$

    因此有$a=b^2$即$\mathrm{ord}_pa=\mathrm{ord}_pb^2=2\mathrm{ord}_pb$必然是一个偶数(0也是偶数)

    若ord_pa是一个偶数,则$\frac{1}{2}\mathrm{ord}_pa$是一个整数,因此令$a'(p)=\frac{1}{2}\mathrm{ord}_pa$从而构建一个唯一因式分解

    $$b'=\prod_p p^{a'(p)}$$

    有$b^2=a$

16. 若$(u,v)=1$且$uv=a^2$则u和v均为某个整数的平方.

    不难得到$\mathrm{ord}_puv=\mathrm{ord}_pu+\mathrm{ord}_pv$是偶数.
    因$(u,v)=1$因此对于任意的素数p都有若$p\mid u$则$p\nmid v$.
    因此得到ord_pu和ord_pv在同一个p下至多只有一个非零.
    因此得到对于每一个p都有ord_pu和ord_pv是偶数.
    因此根据15得到u和v均为某个整数的平方.

17. 证明2的平方根是无理数,也就是说没有有理数$r=a/b$使得$r^2=2$.

由于2为素数,因此2的唯一因式分解中$\mathrm{ord}_2 2=1$为奇数.

因此2不为整数的平方.

接下来证明2也不为有理数的平方.

对于有理数a/b有a,b均为整数,因此我们可以对于a,b分别进行唯一因式分解得到:

$$\begin{aligned} a &= (-1)^{\varepsilon(a)}\prod_p p^{a(p)} \\ b &= (-1)^{\varepsilon(b)}\prod_p p^{b(p)} \end{aligned}$$

因此得到了$a/b=(-1)^{\varepsilon(a)-\varepsilon(b)}\prod_p p^{a(p)-b(p)}$

其中$a(p)-b(p)$也是整数.

若$r^2=2$则$2(a(2)-b(2))=1$这与$a(p)-b(p)$为整数这一事实相矛盾,因此$\sqrt{2}$是无理数

18. 证明$\sqrt[n]{m}$在m不为一个整数的n次方时是无理数.

仍然假设$\sqrt[n]{m}$是一个有理数,即存在a/b使得$\sqrt[n]{m}=a/b$

由于m不为一个整数的n次方,于是存在p使得对于$\mathrm{ord}_p m$有$n\nmid \mathrm{ord}_p m$.

仍然对于a,b进行唯一因式分解

而后得到在素数p上有$a(p)-b(p)$是一个整数.

那么因为$m=(a/b)^n$,则有$n\nmid n(a(p)-b(p))$这与$a(p)-b(p)$为整数相矛盾.

因此m必然是一个无理数

19. 定义两个整数a,b的最小公倍数为一个整数m满足$a\mid m$且$b\mid m$且m可以整除a和b的任意公倍数.证明m是存在的,我们将使用$[a,b]$来标记它.

考虑正整数的情况,容易扩充到$\mathbb{Z}$上.

首先由于a,b为整数,因此总是存在一个整数m使得$a\mid m$且$b\mid m$(考虑ab)

接下来证明所有的公倍数中总是存在一个最小公倍数

我们任取一个公倍数m_0,使得存在一个公倍数$m_1\mid m_0$,

然后对于m_1重复如上操作.

我们就可以得到一个不断上升的链$(m_0)\subset(m_1)\subset(m_2)\subset\cdots$

我们证明这条链在有限步之内会断开.

由于显然有$m_1<m_0$,且m_1为一个公倍数

因此经过$m_0-\sup\{a,b\}$步后必然有$m_{m_0-\sup\{a,b\}}=m_{m_0-\sup\{a,b\}+1}$不然$m_{m_0-\sup\{a,b\}+1}<\sup\{a,b\}$这与其为一个最小公倍数矛盾.

因此最小公倍数必然存在

20. 证明下述结果:

$(\mathrm{a})\mathrm{ord}_p[a,b]=\max(\mathrm{ord}_p a,\mathrm{ord}_p b)$

$(\mathrm{b})(a,b)[a,b]=ab$

$(\mathrm{c})(a+b,[a,b])=(a,b)$

(a)

不难发现$\mathrm{ord}_p[a,b]\geq\max(\mathrm{ord}_p a,\mathrm{ord}_p b)$这是由$a\mid[a,b]$且$b\mid[a,b]$导出的.

若有$\mathrm{ord}_p[a,b]>\max(\mathrm{ord}_p a,\mathrm{ord}_p b)$则$\mathrm{ord}_p[a,b]\geq\max(\mathrm{ord}_p a,\mathrm{ord}_p b)+1$.那么我们取$m=(-1)^\varepsilon\prod_p p^{\max(\mathrm{ord}_p a,\mathrm{ord}_p b)}$可以得到$a\mid m$且$b\mid m$此外还有$m\mid[a,b]$

因此$\mathrm{ord}_p[a,b]=\max(\mathrm{ord}_p a,\mathrm{ord}_p b)$

(b)

不难发现$\mathrm{ord}_p(a,b)=\min(\mathrm{ord}_p a,\mathrm{ord}_p b)$因此可以得到$\mathrm{ord}_p(a,b)[a,b]=\mathrm{ord}_p a+\mathrm{ord}_p b=\mathrm{ord}_p ab$.由于$(a,b)$的符号默认为正,因此可以得到$[a,b]$的正负号与$ab$相同.

因此根据唯一因式分解定理得到$(a,b)[a,b]=ab$

(c)

首先由于$(a,b)\mid a$且$(a,b)\mid b$因此有$(a,b)\mid(a+b)$

因此可以得到$(a,b)\mid(a+b,[a,b])$

剩下内容结合21使用唯一因式分解进行证明就行了

21. 证明$\mathrm{ord}_p(a+b)\geq\min(\mathrm{ord}_p a,\mathrm{ord}_p b)$当$\mathrm{ord}_p a\neq\mathrm{ord}_p b$时等式成立

使用唯一因数分解可以轻松得到不等式

而$\mathrm{ord}_2 a = \mathrm{ord}_2 b \neq 0$时$\mathrm{ord}_2(a+b) = 1 + \mathrm{ord}_p a$

22. 若我们考虑环$k[x]$而不是环$\mathbb{Z}$时,前面几乎所有的练习仍然有效.事实上,在大多是情况下,我们考虑任何的欧几里得整环.本题的目的是让你相信这个事实,不过简单起见,我们将继续使用$\mathbb{Z}$.

23. 假设$a^2+b^2=c^2$且$a,b,c\in\mathbb{Z}$.举个例子,$3^2+4^2=5^2$以及$5^2+12^2=13^2$.假设$(a,b)=(b,c)=(c,a)=1$.证明存在整数u,v使得$c-b=2u^2$且$c+b=2v^2$且有$(u,v)=1$(不失一般性,可以假设b,c为奇数且a为偶数)因此$a=2uv,b=v^2-u^2,c=v^2+u^2$.反过来说明若$u,v$已知,那么由这些公式所给出的三个数$a,b,c$满足$a^2+b^2=c^2$.

    先证明反向

    若存在u,v满足上式则有$a^2+b^2=4u^2v^2+v^4-2v^2u^2+u^4=(u^2+v^2)^2$.于是确实有$c=v^2+u^2$.

    由于$(u,v)=1$因此有$[u,v]=uv$.有$(2uv,u^2-v^2)=(2uv,u^2+v^2)=(u^2-v^2,u^2+v^2)=1$.

    再证明正向

    由于$a^2+b^2=c^2$于是有$a^2=(c-b)(c+b)$由于$(b,c)=1$有$(b-c,b+c)=1$或2.由于我们假设了b,c均为奇数于是有$(b-c,b+c)=2$,且有$2\mid a$

    因此得到$\frac{a}{2},\frac{c-b}{2}$和$\frac{c+b}{2}$是一个整数.

    因此可以得到$(\frac{a}{2})^2=\frac{c-b}{2}\frac{c+b}{2}$且$(\frac{b-c}{2},\frac{b+c}{2})=1$.

    因此根据16得知存在u,v使得$u^2=\frac{c-b}{2},v^2=\frac{b+c}{2}$.

    由于$(u^2,v^2)=1$因此可以得到$(u,v)=1$.

24. 证明恒等式

    (a)$x^n-y^n=(x-y)(x^{n-1}+x^{n-2}y+\cdots+y^{n-1})$

    (b)若n是奇数,则$x^n+y^n=(x+y)(x^{n-1}-x^{n-2}y+x^{n-3}y^2-\cdots+y^{n-1})$

    两问均可在等式两侧同时除以y^n转化为等比数列求和得到,读者自行证明即可

25. 若a^n-1是一个素数,证明$a=2$且n是一个素数.形如2^p-1的素数称为Mersenne素数.比如说$2^3-1=7$以及$2^5-1=31$现在暂且不知晓Mersenne素数是否是无穷多个的.

    $a^n-1=(a-1)(a^{n-1}+a^{n-2}+\cdots+1)$为一个素数,所以有$a=2$,

    而若n不为素数,则存在p,q使得$n=pq$,而$2^n-1=2^{pq}-1=(2^p)^q-1=(2^p-1)(2^{p(q-1)}+\cdots+1)$不为素数

26. 若a^n+1是一个素数,证明a是偶数且n是2的幂.形如$2^{2^t}+1$的素数称为Fermat素数.举个例子$2^{2^1}+1=5$以及$2^{2^2}+1=17$现在暂且不知晓Fermat素数是否是无穷多个的.

    若n为奇数则a^n+1不为素数,因此n必然为偶数.

    而奇数的幂为奇数,于是a必然为偶数.

    若n不为2的幂,且n为偶数,则有$n=2^mk$其中k为奇数,m为一个整数.

    因此我们可以得到$x^n+1=x^{2^mk}+1=(x^{2m})^k+1$就可以按照24进行分解了

27. 证明对于所有的奇数n有$8\mid n^2-1$若$3\nmid n$则$6\mid n^2-1$

    $n=1$时有$n^2-1=0$满足条件.

    对于$n\geq 3$时$n=2k+1,k\geq 1$则有$n^2-1=(n-1)(n+1)=(2k+2)2k=4(k+1)k$由于$k+1$和$k$中必然有一个是偶数

    因此得到$8\mid n^2-1$

    若$3\nmid n$则$n=1$时有$6\mid 0$

    由于$3\nmid n$因此有$n\neq 3k$即$n^2-1\neq(3k-1)(3k+1)$.

    因此有$6\mid n^2-1$

28. 证明对于所有的n有$30\mid n^5-n$且$42\mid n^7-n$

    $n^5-n=n(n^4-1)=n(n^2+1)(n+1)(n-1)$而$30=6\times 5=2\times 3\times 5=(2-1)2(2+1)(2^2+1)$

    因此得到$30\mid n^5-n$

    同理证明42的情况

29. 假设$a,b,c,d\subset\mathbb{Z}$且$(a,b)=(c,d)=1$若$(a/b)+(c/d)$等于一个整数证明$b=\pm d$

由于$(a/b)+(c/d)$为一个整数,由于$(a,b)=(c,d)=1$因此a/b和c/d均为既约分数,因此自然有$b=\pm d$

30. 证明$\frac{1}{2}+\frac{1}{3}+\cdots+\frac{1}{n}$不是一个整数

    由于$(1,i)=1, i\in\mathbb{Z}_{\geq 1}$因此根据29得知其不为一个整数

31. 证明在$\mathbb{Z}[i]$中有2被$(1+i)^2$整除.

    $(1+i)^2=2i$有$2=2i\times(-i)$因此$(1+i)^2\mid 2$

32. 对于$\alpha=a+bi\in\mathbb{Z}[i]$我们定义$\lambda(\alpha)=a^2+b^2$根据λ的性质证明$(a^2+b^2)(c^2+d^2)=(ac-bd)^2+(ad-bc)^2$

    由于$(a+bi)(c+di)=(ac-bd)+(ad-bc)i$因此$(a^2+b^2)(c^2+d^2)=\lambda(a+bi)\lambda(c+di)=\lambda((a+bi)(c+di))=(ac-bd)^2+(ad-bc)^2$

33. 证明$\alpha\in\mathbb{Z}[i]$是一个单位当且仅当$\lambda(\alpha)=1$.这诱导了$1,-1,i,-i$是$\mathbb{Z}[i]$上的单位.

    若α是一个单位,则$(\alpha)=\mathbb{Z}[i]$,也就是说有$\alpha\mid 1$,即$1=t\alpha+0$由于$1\mid\alpha$于是得到t也为一个单位,因此得到$\lambda(t)\lambda(\alpha)=\lambda(t\alpha)=\lambda(1)=1$.由于λ的特性可知$\lambda(t)=\lambda(1)=\lambda(\alpha)=1$

34. 证明3可以被$\mathbb{Z}[\omega]$的$(1-\omega)^2$整除.

    $(1-\omega)^2=1-2\omega+\omega^2=-3\omega$因此得到$3=(1-\omega)^2(-3\omega^2)=(1-\omega)^2(-3(1-\omega))$因此$(1-\omega)^2\mid 3$.

35. 类似于33读者自证即可

36. 定义$\mathbb{Z}[\sqrt{-2}]$是所有形如$a+b\sqrt{-2}$的复数所构成的集合,其中$a,b\in\mathbb{Z}$.证明$\mathbb{Z}[\sqrt{-2}]$构成一个环.定义$\lambda(\alpha)=a^2+2b^2$其中$\alpha=a+b\sqrt{-2}$.使用λ证明$\mathbb{Z}[\sqrt{-2}]$是一个欧几里得整环

    不难验证$\mathbb{Z}[\sqrt{-2}]$对于加减法封闭.对于乘法有$(a+b\sqrt{-2})(c+d\sqrt{-2})=(a-2bd)+(bc+ad)\sqrt{-2}\in\mathbb{Z}[\sqrt{-2}]$因此$\mathbb{Z}[\sqrt{-2}]$确实构成环.
    接下来验证构成欧几里得整环.
    考虑$\alpha=a+b\sqrt{-2}$且$\beta=c+d\sqrt{-2}\neq 0$得到$\delta=\alpha/\beta=r+s\sqrt{-2}$.
    其中r,s均为实数
    我们可以得到两个整数m,n使得$|r-m|<1/2$且$|s-n|<1/2$
    令$\rho=\alpha-\beta\delta$得到$\rho=0$或$\lambda(\rho)=\lambda(\beta)\lambda(\alpha/\beta-\delta)=\lambda(\beta)\lambda(m-r+(n-s)\sqrt{-2})<\lambda(\beta)(1/4+1/2)<\lambda(\beta)$
    因此确实构成一个欧几里得整环

37. 证明$\mathbb{Z}[\sqrt{-2}]$的单位只有$1,-1$

    $\lambda(\alpha)=1$

38. 假设$\pi\in\mathbb{Z}[i]$且$\lambda(\pi)=p$为$\mathbb{Z}$上的一个素数.证明π是$\mathbb{Z}[i]$上的一个素元.且证明相同的结果在$\mathbb{Z}[\omega]$和$\mathbb{Z}[\sqrt{-2}]$上成立

    由于$\lambda(\pi)=p$因此对于$\alpha=a+bi$,$\beta=c+di$有$p\mid\lambda(\alpha\beta)\Leftrightarrow p\mid\lambda(\alpha)\vee p\mid\lambda(\beta)$
    因此我们有$\lambda(\pi)\mid\lambda(\alpha\beta)\Leftrightarrow\lambda(\pi)\mid\lambda(\alpha)\vee\lambda(\pi)\mid\lambda(\beta)$
    得到$\alpha\beta=k_1\pi+0\Leftrightarrow\alpha=k\pi+0\vee\beta=t\pi+0$
    因此得到π是$\mathbb{Z}[i]$上的一个素元

39. 证明在任意整环上有素元是不可约元.

    若整环R上的素元p可约,则有$p=qr$其中$q,r\in R$且不为单位
    于是有$p\mid qr$因此$p\mid q$或$p\mid r$又因为$q\mid p$且$r\mid p$于是得到其中必有一个单位元.与假设矛盾.