初等数论笔记

副标题

Zhang Liang

2025 年 3 月 2 日

前言标题

前言内容

2025 年 3 月 2 日

目录

第一章　唯一分解

1.1　$\mathbb{Z}$ 上的唯一分解

1.1.1　整除和素数

作为数论的基础，我们需要先研究素数。

定义 1.1.1: 整除

设 $a,b\in\mathbb{Z},\exists c\in\mathbb{Z},\text{s.t. }ac=b$，那么我们称 a 整除 b，记作 $a\mid b$；

否则，我们称 a 不整除 b，记作 $a\nmid b$

有了整除的定义，我们就可以定义素数的概念：

定义 1.1.2: 素数

设 $p\in\mathbb{N},p\geqslant 2$，如果 $a\mid p,a\in\mathbb{N}\Leftrightarrow a=1\vee a=p$

那么我们称 p 是一个素数，否则称其是个合数。

我们研究素数的第一个目的是一个比较显然的事实：所有大于 1 的整数都能写成若干素数的乘积。我们还将看到，这个分解是唯一的。

我们先引入以下概念。

定义 1.1.3: 素数的指数

设有素数 $p\in\mathbb{N}$ 和 $n\in\mathbb{Z}$

如果 $p\mid n$，那么我们记满足 $p^k\mid n$ 的最大正整数 k 为 $ord_p n$，称为 p 的指数

特别地，如果 $p\nmid n$，我们定义 $ord_p n=0$；如果 $n=0$，我们定义 $ord_p n=+\infty$

1.1.2 算数基本定理

我们先给出一个基本引理，它证明了可分解但是没有证明唯一性。

引理 1.1.1: 大于 1 的正整数的可分解性

每一个大于 1 的正整数都可以写成有限个素数的乘积。

证明: 假设命题不成立。于是一定有一个 N 为不满足此性质的最小正整数。

首先，N 不可能是素数，否则它就可以写成自身，与假设矛盾。

于是，一定 $\exists m, n, 1 < m < N, 1 < n < N$，满足 $mn = N$

那么，m, n 也不能满足命题所说的性质，否则 N 也就有了这一性质，与假设矛盾。

但是，这样 N 就不再是最小的满足此性质的正整数了。与假设矛盾，命题得证 □

接下来我们证明唯一性。为了证明这一部分，我们将提出一系列全新概念，包括互素、最大公因数等。

定义 1.1.4: $\mathbb{Z}$ 上生成的子模

我们定义：

$\mathbb{Z}\text{-span}(a_1, \cdots, a_n) := \{a_1 \cdot q_1 + \cdots + a_n \cdot q_n | q_i \in \mathbb{Z}\}$

称为 $\mathbb{Z}$ 上由 $a_1, \cdots, a_n$ 生成的子模

我们先证明一个引理：由两个数在整数集上生成的子模，其实也可以只由一个数生成。

引理 1.1.2

对于 $\mathbb{Z}\text{-span}(a, b), \exists c \in \mathbb{Z}, \text{s.t. } \mathbb{Z}\text{-span}(a, b) = \mathbb{Z}\text{-span}(c)$

证明: 如果 $a = b = 0$，那么命题是平凡的。

如果 a, b 中至少有一者不为 0，那么一定能找到 $\mathbb{Z}\text{-span}(a, b)$ 的最小正元素 c。

由定义易知，$\mathbb{Z}\text{-span}(c) \subseteq \mathbb{Z}\text{-span}(a, b)$

现在取 $\forall d \in \mathbb{Z}\text{-span}(a, b)$，那么一定 $\exists q, r \in \mathbb{Z}, 0 \leqslant r \leqslant c, d = qc + r$

那么 $r = d - qc$，因为 $c, d \in \mathbb{Z}\text{-span}(a, b)$，于是 $r \in \mathbb{Z}\text{-span}(a, b)$

于是一定有 $r = 0$ 因为我们已经假设 c 是 $\mathbb{Z}\text{-span}(a, b)$ 最小的正整数，而 $0 \leqslant r$。

那么 $d = qc \in \mathbb{Z}\text{-span}(a, b)$，于是 $\mathbb{Z}\text{-span}(a, b) \subseteq \mathbb{Z}\text{-span}(c)$，于是命题得证。 □

这个数实际上就是两个数的最大公因数，我们先给出定义，随后给出证明

定义 1.1.5: 公因数

于 $a, b \in \mathbb{Z}$，如果 $c \in \mathbb{Z}$ 满足 $c \mid a, c \mid b$，那么称 c 是 a, b 的最大公因数。

如果又有：对于任何 a, b 的公因数 $d, d \mid c$，那么称 c 是 a, b 的最大公因数，记作 (a, b)

引理 1.1.3

如果 $\mathbb{Z}\text{-span}(a, b) = \mathbb{Z}\text{-span}(c)$，那么 c 是 a, b 的最大公因数

证明: 取 a, b 的一个公因数 $d \mid a, d \mid b$，由 $\mathbb{Z}\text{-span}(a, b)$ 的定义可知，$\forall e \in \mathbb{Z}\text{-span}(a, b), d \mid e$

那么 $\forall e \in \mathbb{Z}\text{-span}(c), d \mid e$，那么 $d \mid c$，命题得证。 □

最大公因数是 1 的情况比较特别，我们称之为互素

定义 1.1.6: 互素

如果 a, b 的公因数仅有 $1, -1$，那么我们称 a, b 互素，记作 $(a, b) = 1$

互素有以下显然的性质：

引理 1.1.4

$(a, b) = 1 \Leftrightarrow \exists r, q \in \mathbb{Z}, \text{s.t. } ra + qb = 1$

证明: 只需注意到 $(a, b) = 1 \Leftrightarrow \mathbb{Z}\text{-span}(a, b) = \mathbb{Z}\text{-span}(1)$，于是命题得证。 □

引理 1.1.5

若 $a \mid bc, (a, b) = 1$，那么 $a \mid c$

证明: 因为 $(a, b) = 1$，所以 $\exists r, q \in \mathbb{Z}, \text{s,t. } ra + qb = 1$

所以 $rac + qbc = c$，但是我们知道 $a \mid rac, a \mid qbc$，于是 $a \mid c$ □

引理 1.1.6

如果 p 是一个素数，$p \mid bc$，那么 $p \mid b, p \mid c$ 至少有一者成立。

证明: 因为 p 是一个素数，所以 (p, b) 或者为 1，或者为 p。

如果 $(p, b) = p$ 那么一定有 $p \mid b$，命题成立；

如果 $(p, b) = 1$，那么 p, b 的公因数仅有 $1, -1$，那么必定有 $p \mid c$ □

最后，为了指出唯一分解中素数的指数，我们给出最后一个引理。

引理 1.1.7

如果 p 为素数，$a, b \in \mathbb{Z}$，那么 $ord_p ab = ord_p a + ord_p b$

证明： 首先处理一些特殊情形：

如果 a, b 中至少一者为 0，不妨假设 $a = 0$，那么有 $+\infty = +\infty + ord_p b$，因为 $ord_p b$ 或者有限，或者为正无穷，于是命题成立；

如果 $p \nmid ab, p \nmid a, p \nmid b$，那么有 $0 = 0 + 0$，命题成立；

如果 $p \mid ab$，但是 $p \mid a$ 和 $p \mid b$ 仅一者成立，那么不妨假设 $p \nmid a$，于是依上面的引理，有 $p \mid b$

假设 $ord_p b = n$，于是 $\exists c, b = c \cdot p^n, p \nmid c$

代入得:$ab = p^n \cdot (ac)$,但是 $p \nmid a, p \nmid c$,那么 $p \nmid ac$,即 $ord_p ab = n$,于是 $ord_p ab = 0 + ord_p b$,命题成立。

最后假设 $p \mid ab, p \mid a, p \mid b$，设 $ord_p a = m, ord_p b = n$，于是 $\exists c, d, a = c \cdot p^m, b = d \cdot p^n, p \nmid c, p \nmid d$

那么 $ab = (cd) \cdot p^{m+n}$，但是 $p \nmid cd$，于是有 $ord_p ab = ord_p a + ord_p b$，命题成立。 □

至此，我们可以开始证明算数基本定理了。

定理 1.1.8: 算数基本定理

$\forall n \in \mathbb{Z}, n \neq 0$

$$n = (\text{sgn } n) \prod_p p^{ord_p |n|} \tag{1.1}$$

其中求积下标 p 对全体素数求积

证明： 先对 $n > 1$ 考虑，此时有 $n = \prod_p p^{a_p}$, 其中 a_p 是未知的。

取任意一个素数 q，那么有 $ord_q n = \sum\limits_p a_p \cdot ord_q(p)$

只需注意到如果 $q \neq p, ord_q(p) = 0$，即得 $a_q = ord_p(q)$，于是此情形下命题成立。

对于 $n = 1$ 的情形，$ord_p(1) = 0$ 恒成立，于是命题也成立。

$n < 0$ 的情形，在已经证明了上述事实后是显然的。 □

1.2 $K[x]$ 上的唯一分解

1.3 主理想整环上的唯一分解

1.3.1 主理想整环

定义 1.3.1: 主理想整环

设 R 是一个交换环，如果它的任何一个理想 $I \subseteq R$ 都是主理想，即

$\exists c, I = (c) = \{rc|c \in R\}$

那么我们称 R 是一个主理想整环

在初等数论中，我们更多考虑的所谓欧几里得环

定义 1.3.2: 欧几里得环

设 R 是一个交换环，如果 $\exists\lambda : R - 0_R \to \mathbb{N}$，称为欧几里得函数，满足

$\forall a, b \in R, \exists c, d \in R, a = cb + d$，$d$ 满足 $d = 0$ 或者 $\lambda(d) < \lambda(b)$

那么称 R 是一个交换环

本节中我们把主要精力放在主理想整环上，我们接下来定义主理想整环上的一系列概念

定义 1.3.3: 整除

设 R 是一个主理想整环，$a, b \in R$，如果 $\exists c \in R, ac = b$，那么称 a 整除 b，记作 $a \mid b$

否则，称 a 不整除 b，记作 $a \nmid b$

这个定义也可以写成一个等价形式：$(b) \subseteq (a)$

定义 1.3.4: 不可约元

主理想整环 R 中的元素 a 如果满足：

如果 $b \mid a$，那么或者 b 可逆，或者 a 与 b 相伴，那么我们称 a 是 R 中的不可约元

定义 1.3.5: 素元

主理想整环 R 中的元素 p 如果满足

$p \mid ab \Rightarrow p \mid a \vee n \mid b$,

那么称 p 是 R 上的素元

定义 1.3.6: 公因子

主理想整环 R 中的元素 a, b，如果 $c \in R$ 满足 $c \mid a, c \mid b$，那么称 c 是 a, b 的公因子；如果还满足：任意 a, b 的公因子 $d, d \mid c$，那么称 c 是 a, b 的最大公因子，记作 $(a, b) = c$

定义 1.3.7: 互素

如果 $(a, b) = c \Leftrightarrow c$可逆，那么称 a, b 互素。

1.3.2 主理想整环的唯一分解定理

命题 1.3.1. *任何一个欧几里得环都是主理想子环*

证明: 设 R 是一个欧几里得环，取 R 上的任意一个理想 $I \subseteq R$

考虑集合 $S = \{\lambda(k) | k \in I, k \neq 0\}$，取其中的元素 a 满足 $\forall b \in S, \lambda(a) \leqslant \lambda(b)$。

因为 $a \in I$，按照理想的定义一定有 $(a) \subseteq I$，我们接下来证明相反方向的式子。

再取 $b \in I$，那么 $\exists c, d \in I, b = ca + d$

现在假设 $d = 0$，那么有 $b = ca$，$I \subseteq (a)$ 自然成立

如果 $d \neq 0$，那么就有 $\lambda(d) < \lambda(a)$，但是我们本来就假设 $\lambda(a)$ 应该是所有 $\lambda(k), k \neq 0$ 中最小的，矛盾。

于是命题得证 □

命题 1.3.2. *主理想整环中的任何两个元素 $a, b \in R$，*
$c = (a, b)$ 都存在，并且有 $R\text{-}span(a, b) = (c)$

证明: 显然，R-span(a, b) 也是 R 的一个理想，于是 $\exists c \in R, \text{s.t. } R\text{-span}(a, b) = (c)$

那么有 $(a) \subseteq (c), (b) \subseteq (c)$，于是 $c \mid a, c \mid b$，即 c 是 a, b 的公因数

现在假设 $d \mid a, d \mid b$，那么 $(a) \subseteq (d), (b) \subseteq (d)$

于是一定有 R-span$(a, b) \subseteq (d)$，即 $(c) \subseteq (d)$，那么 $d \mid c$，于是命题得证。 □

推论 1.3.1

如果 a, b 互素，那么 $R\text{-span}(a, b) = R$

证明: 如果 a, b 互素，那么 $(a, b) = 1$，但是 $(1) = R$，于是命题得证。 □

推论 1.3.2

不可约元 p 同时也是素元

证明: 只需证明 $p \mid ab, p \nmid a \Rightarrow p \mid b$

因为 p 不可约，所以 p 仅有可逆元以及与 p 相伴的元素为因子

但是 $p \nmid a$，那么一定有 $R\text{-span}(p, a) = 1$，于是 $R\text{-span}(pb, ab) = (b)$

又因为 $p \mid pb, p \mid ab$，所以 $(pb) \subseteq (p), (ab) \subseteq (p)$

$\Rightarrow R\text{-span}(pb, ab) \subseteq (p) \Rightarrow (b) \subseteq (p) \Rightarrow p \mid b$，于是命题得证 □

引理 1.3.3

取一个主理想链 $(a_1) \subseteq (a_2) \subseteq \cdots \subseteq (a_i) \subseteq \cdots$

那么，一定 $\exists k, \forall i \in \mathbb{N}, (a_k) = (a_{k+i})$，也就是说这个链在某一元素开始到达极限

证明: 设 $I = \bigcup_{i=1}^{\infty}(a_i)$，那么 $\exists a, I = (a)$

于是一定能找到一个 $k, a \in (a_k)$，于是一定有 $(a) \subseteq (a_k) \Rightarrow I \subseteq (a_k)$，那么命题得证 □

命题 1.3.3. 主理想整环 R 中的每一个非零不可逆元素都可以写成一系列不可约元的乘积

证明: 取 $a \in R$，a 非零且不可逆。我们首先证明 a 可被不可约元整除。

假设 a 不可约，那证明完毕；如果可约，那么有 $a = a_1 b_1$，我们如此拆分 $a_i = a_{i+1} b_{i+1}$，如果有一步中 a_n 不可约，那么证明完毕

如果找不到这样的一不，那么按照整除的定义，有 $(a) \subseteq (a_1) \subseteq \cdots \subseteq (a_k) \subseteq \cdots$，按照前面的引理，

一定有一个 k，$\forall i \in \mathbb{N}, (a_k) = (a_{k+i})$，那么其实 a_k 就不可约，这样证明就完成了。

现在证明它可以写成一系列不可约元的乘积。

如果 a 不可约，那么命题成立；如果并非，有 $a = p_1 c_1$，其中 p_1 不可约，我们如此不断拆分 $c_i = p_{i+1} c_{i+1}$，如果有一步中 c_n 不可约，那么命题成立

如果找不到这样的一步，那么按照整除的定义，有 $(a) \subseteq (c_1) \subseteq \cdots \subseteq (c_k) \subseteq \cdots$，按照前面的引理，

一定有一个 k，$\forall i \in \mathbb{N}, (c_k) = (c_{k+i})$，那么其实 c_k 就不可约，这样证明就完成了。 □

引理 1.3.4

设 $p \in R$ 是一个素元，$a \in R, a \neq 0$，那么 $\exists n \in \mathbb{N}, p^n \mid a, p^{n+1} \nmid a$

证明： 假设命题不成立，那么对于 $\forall m \in N, p^m \mid a$。

即，$\exists b_m, a = p^m b_m$

因为 $a = p^m b_m = p^{m+1} b_m$，所以 $pb_{m+1} = b_m$，于是有 $(b_0) \subseteq \cdots \subseteq (b_k) \subseteq \cdots$，

按照引理，一定有一个 k，$\forall i \in \mathbb{N}, (b_k) = (b_{k+i})$，这和 p 是素元的前提矛盾，于是命题得证。 □

引理 1.3.5

如果 p 为素元，$a, b \in R$，那么 $ord_p ab = ord_p a + ord_p b$

证明： 首先处理一些特殊情形：

如果 a, b 中至少一者为 0，不妨假设 $a = 0$，那么有 $+\infty = +\infty + ord_p b$，因为 $ord_p b$ 或者有限，或者为正无穷，于是命题成立；

如果 $p \nmid ab, p \nmid a, p \nmid b$，那么有 $0 = 0 + 0$，命题成立；

如果 $p \mid ab$，但是 $p \mid a$ 和 $p \mid b$ 仅一者成立，那么不妨假设 $p \nmid a$，于是依上面的引理，有 $p \mid b$

假设 $ord_p b = n$，于是 $\exists c, b = c \cdot p^n, p \nmid c$

代入得:$ab = p^n \cdot (ac)$,但是 $p \nmid a, p \nmid c$,那么 $p \nmid ac$,即 $ord_p ab = n$,于是 $ord_p ab = 0 + ord_p b$,命题成立。

最后假设 $p \mid ab, p \mid a, p \mid b$，设 $ord_p a = m, ord_p b = n$，于是 $\exists c, d, a = c \cdot p^m, b = d \cdot p^n, p \nmid c, p \nmid d$

那么 $ab = (cd) \cdot p^{m+n}$，但是 $p \nmid cd$，于是有 $ord_p ab = ord_p a + ord_p b$，命题成立。 □

最后，我们证明唯一分解定理

定理 1.3.6: 主理想整环的唯一分解定理

设 R 是一个主理想子环，那么 $\forall n \in R, n \neq 0$

$$n = u \prod_p p^{ord_p n} \tag{1.2}$$

其中 u 是 R 中的可逆元，求积符号对全体不可约元求积

证明: 先对 n 不可逆考虑，此时有 $n = \prod_p p^{a_p}$, 其中 a_p 是未知的。

取任意一个素元 q，那么有 $ord_q n = \sum_p a_p \cdot ord_q(p)$

只需注意到如果 $q \neq p, ord_q(p) = 0$，即得 $a_q = ord_p(q)$，于是此情形下命题成立。

对于 n 可逆的情形，$ord_p(n) = 0$ 恒成立，于是命题也成立。 □

第二章　一致收敛性、函数项级数与函数族的基本运算

在之前章节的讨论中，曾经涉及了级数一般项是函数的级数，也就是所谓的函数项级数。

在此之前，我们利用了所谓“逐点收敛”，即对每一变量取值收敛。但是，一些例子中我们发现这种收敛性并不具备很好的性质。

我们提出一致收敛性这一全新的收敛性，这一性质可以允许级数仅仅需要少量条件就可以拥有微分、积分上的良好性质

2.1　逐点收敛性和一致收敛性

2.1.1　逐点收敛性

定义 2.1.1: 逐点收敛性

考虑函数列 $f_n: X \to \mathbb{R}$. 如果在点 $x \in X$，$\{f_n(x), n \in\}$ 收敛，则称 $\{f_n(x), n \in \mathbb{N}\}$ 在点 x 收敛

使得 $\{f_n(x), n \in \mathbb{N}\}$ 收敛的点的集合称为收敛集。

$\{f_n(x), n \in \mathbb{N}\}$ 在其收敛集上产生的极限 $f(x) = \lim\limits_{n\to\infty} f_n(x)$ 称为极限函数，同时称 $\{f_n(x), n \in \mathbb{N}\}$ 逐点收敛于 $f(x)$

第三章　附录

这一部分中，对于正文中因为逻辑结构无法提及的部分，进行补充。包括特殊函数，有趣的数学概念，一些命题的全新解法，以及难以推导的公式证明可能使用复分析、实分析、泛函等超纲内容

3.1　原函数初等性的判定方法

3.1.1　切比雪夫定理

定理 3.1.1: 切比雪夫定理

设 $m, n, p \in \mathbb{Q} - \{0\}$，那么以下积分

$$\int x^m (a + bx^n)^p \mathrm{d}x \tag{3.1}$$

初等的充要条件是：$p, \frac{m+1}{n}, \frac{m+1}{n} + p$ 中至少有一个为整数

3.1.2　刘维尔定理

在介绍刘维尔定理前，需要先介绍一些微分代数的概念：

首先我们扩展微分的概念。我们将满足类似乘法、除法微分性质的泛函也称为微分。

先引入微分域及其常数域

1. 微分域

定义 3.1.1: 微分域

一个由函数组成的域 F 及其上的一个算子 $\delta : F \to F$，如果 $\forall f, g \in F$ 有：

$\neg\delta(f+g) = \delta(f) + \delta(g)$

$\delta(fg) = \delta(f) \cdot g + f \cdot \delta(g)$

那么称 (F, δ) 是一个微分域

容易验证 δ 是线性算子，于是我们有时简记 $\delta(f)$ 为 δf

定义 3.1.2: 微分域的常数域

微分域 (F, δ) 的常数域定义为：

$Con(F, \delta) = \{f \in F | \delta f = 0\}$

同时定义域的扩张：

定义 3.1.3: 域的扩张

设 F, K 是两个域，并且 K 是满足 $F \subseteq K$ 且包含 $h \subseteq K$ 的最小域（即 K 是任何满足上述条件的域的子域），记作 $K = F(h)$

作为接下来内容的预备，我们先验证那些显然的微分性质：

命题 3.1.1. $\delta C = 0$，其中 C 为常数

证明: 只需要验证 $\delta 1 = 0$

那么有：$\delta(1 \cdot 1) = \delta 1 \cdot 1 + 1 \cdot \delta 1 = 2\delta 1$

于是有 $\delta 1 = 0$，利用微分的线性即得证。 □

命题 3.1.2. $\delta\left(\frac{f}{g}\right) = \frac{\delta f \cdot g - f\delta g}{g^2}$

证明: 首先推导 $\delta\left(\frac{1}{g}\right)$

$\because \delta 1 = \delta\left(g \cdot \frac{1}{g}\right) = 0$

$\Rightarrow \delta g \frac{1}{g} + g\delta\left(\frac{1}{g}\right) = 0$

$\Rightarrow \delta\left(\frac{1}{g}\right) = -\frac{\delta g}{g^2}$

于是 $\delta\left(\frac{f}{g}\right) = \delta\left(f \cdot \frac{1}{g}\right)$

$= \delta f \frac{1}{g} - f\frac{\delta g}{g^2} = \frac{\delta f \cdot g - f\delta g}{g^2}$ □

2. 微分域的初等扩张 接下来讨论什么是“初等”的函数。

定义 3.1.4: 微分域的初等扩张

设 $(F,\delta),(K,\delta)$ 是两个微分域，$h \in K$ 并且 $K = F(h)$，那么：

¬ 如果存在 F 中的一个多项式 $p(x) \in F[x]$，有 $p(h) = 0$，那么称 h 是 F 的一个代数元素，$K = F(h)$ 是 F 的单代数扩张

如果存在 F 中的一个函数 f，使得 $\delta h = \frac{\delta f}{f}$，那么称 $K = F(h)$ 是 F 的单对数扩张

如果存在 F 中的一个函数 f，使得 $\frac{\delta h}{h} = \delta f$，那么称 $K = F(h)$ 是 F 的单指数扩张。

单对数扩张和单指数扩张统称为单超越扩张，其对应的 h 称为 F 的超越元素；以上三种扩张统称为单初等扩张

有限次初等扩张的复合称为初等扩张

我们也可以在此以另外的方式定义出初等函数：

定义 3.1.5: 初等函数

如果函数 f 处于微分域 $\left(C(x), \frac{\mathrm{d}}{\mathrm{d}x}\right)$ 的某个初等扩张中，那么称 f 是一个初等函数

接下来就可以给出刘维尔定理了。

3. 刘维尔定理

定理 3.1.2: 刘维尔定理

$(F,\delta),(K,\delta)$ 是两个微分域，K 是 F 的初等扩张，并且 $Con(F,\delta) = Con(K,\delta)$，且 $\forall f \in F, \exists g \in K, s.t. \delta g = f$

那么一定 $\exists c_1, \cdots, c_n \in Con(F,\delta), u_1, \cdots, u_n, v \in F$，使得

$$g = \sum_{i=1}^{n} c_i \ln(u_i) + v \tag{3.2}$$

3.2 一些超越积分的特殊解法

3.2.1 Direchlet 积分