从二次互反律到类域论

——代数数论的发展历史

目录

0. 序言

本文主要分为 9 个章节，依此介绍了二次互反律、复数在数论中引入、代数数和代数整数的历史、高斯关于型的理论、抽象的群、环、域的理论及其在数论中的应用、p-进域的构造、ζ函数和L-函数以及整体类域论的经典结果。其中第 5，6，7，8 章都可以看作是为最终叙述类域论做的准备。

本文简要介绍了代数数论发展中的一些著名的工作，除了叙述历史，还对一些核心的定义做了解释说明，对一些核心的定理做了简单的论证。代数数论的历史悠久且深邃，限于篇幅和本人水平，本文只包括了其中的一小部分。如果有读者因为这篇文章而对数论产生兴趣，我将感到无比荣幸。

1. 二次互反律

1.1 二次互反律的发现

18 世纪中数论的最富于首创精神、引发最多成果的发现是二次互反律。它用到了二次剩余的概念，[1]这个概念被欧拉在 1754 年或 1755 年的一篇论文引入，后来高斯给了它现在的说法：如果存在一个 x，使得x^2-p能被q整除，那么就称 p 是 q 的二次剩余；如果这样的 x 不存在，那么就说 p 是 q 的二次非剩余。

勒让德（1808）发明了一个记号，即 Legendre symbol，现在用于表示上面提到的两种情况中的任意一种。这个记号是$(\frac{p}{q})$，它的意义如下：对于任意数 p 和任意素数 q，

$$\left(\frac{p}{q}\right)=\begin{cases}1,\text{当 p 是 q 的二次剩余时，}\\-1\text{ 当 p 是 q 的二次非剩余时}\end{cases}$$

还可以认为，如果 p 恰好能被 q 乘除，则 $\left(\frac{p}{q}\right)=0$。

在这种记号下，二次互反律说的时，当 p 和 q 是不同的奇素数是，那么

$$\left(\frac{p}{q}\right)\ \left(\frac{q}{p}\right)=(-1)^{\frac{(p-1)(q-1)}{4}}$$

对于偶素数的情况，有：对于奇素数 p，我们有

$$\left(\frac{2}{p}\right)=(-1)^{\frac{p^2-1}{8}}$$

[1] Morris Kline: Mathematical Thought from Ancient to Modern Times II ,page 191.

稍微将公式变形：

$$\left(\frac{\mathrm{p}}{\mathrm{q}}\right) = \left(\frac{\mathrm{q}}{\mathrm{p}}\right) \cdot (-1)^{\frac{(p-1)(q-1)}{4}}$$

我们可以看出，如果固定某个奇素数 p，那么奇素数 p 是否是奇素数 q 的二次剩余由 q 模 4p 的余数决定。这是个非常深刻的结果。它最直接的应用就是迅速地判断一个数是不是另一个数的二次剩余。例如，由公式，我们有

$$\left(\frac{5}{\mathrm{p}}\right) = \left(\frac{\mathrm{p}}{5}\right)$$

其中 p 是否是 5 的二次剩余非常好判断（对于一个明确的素数 p

这个深刻的结果最终被高斯所证明，但它在高斯之前就被发现了。[2]欧拉在 1783 年的一篇论文中给出了四条定理和第五总结性的定理，非常清楚地叙述了二次互反律。克罗内克（Leopold Kronecker）在 1875 年注意到，这条定理的叙述实际上已经包含在欧拉很早以前写的文章当中。但是欧拉并没有严格地证明这些定理，他的“证明”是建立在计算的基础上的。1785 年勒让德在他关于这个课题的论文中独立地宣布了这一定律，但他引用了欧拉在《短论》的同一卷的另一篇文章。勒让德的证明是不完全的。勒让德在他所著的《数论》中再次叙述了这一定律，并给出了另外一个证明，但是

[2] Morris Kline: *Mathematical Thought from Ancient to Modern Times* //,page 191.

这一证明仍然是不完全的，因为他在证明中假定了在某一算术级数中存在无穷多个素数。

1.2 分圆域的威力：用高斯和证明二次互反律

二次互反律第一个严格的证明是由高斯在 1796 年作出的，随后他又发现了另外七个不同的证明。高斯在他所著的《算术研究》中将二次互反律称为“基石”。[3]在此我将展示高斯的一个利用分圆域的一个证明。在之后的数学家的研究中表明分圆域是数论中极其重要的对象。ζ

引理：设ζ是一个本原 p 次单位根，其中 p 是一个奇素数。令

$$S = \sum_{a} \left(\frac{a}{p}\right) \zeta^{a}$$

其中对 a 的求和取遍模 p 的非零剩余类。则有

$$S^2 = \left(\frac{-1}{p}\right) \cdot p$$

证明：由求和恒等式得

$$S^2 = \sum_{a,b} \left(\frac{ab}{p}\right) \zeta^{a+b}$$

其中 a，b 取遍模 p 的非 0 剩余类。 用 ab 替换 a，得

$$S^2 = \sum_{a,b} \left(\frac{ab^2}{p}\right) \zeta^{b(a+1)}$$

$$= \sum_{a,b} \left(\frac{a}{p}\right) \zeta^{b(a+1)}$$

[3] Serge Lang: *Algebraic Number Theory,* page 76~78

$$= \sum_{b} \left(\frac{-1}{p}\right) \zeta^{0} + \sum_{a \neq -1} \left(\frac{a}{p}\right) \zeta^{b(a+1)}$$

注意到对于固定的$a \neq -1$，有

$$\sum_{b \neq 0} \zeta^{b(a+1)} = \sum_{b \neq 0} \zeta^{b} = -1$$

从而有

$$S^2 = \left(\frac{-1}{p}\right)(p-1) + (-1) \sum_{a \neq -1} \zeta^{a}$$

$$= \left(\frac{-1}{p}\right) p$$

除此之外，我们还有两个简单的结果：

$$\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}}$$

和

$$\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} \ (mod p)$$

这些均可由F_p^*是循环群得出。

现在我们来证明二次互反律。设 p，q 是不同的奇素数。

一方面，我们有

$$S^q = S(S^2)^{\frac{q-1}{2}} = S(-1)^{\frac{p-1}{2}\frac{q-1}{2}} p^{\frac{q-1}{2}}$$

$$\equiv S(-1)^{\frac{p-1}{2}\frac{q-1}{2}} \left(\frac{p}{q}\right) \pmod{q}$$

另一方面，我们有

$$S^q \equiv \sum_{a=1}^{p-1} \left(\frac{a}{p}\right) \zeta^{aq} \pmod{q}$$

$$\equiv \left(\frac{q}{p}\right)\sum_{a=1}^{p-1}\left(\frac{aq}{p}\right)\zeta^{aq} \pmod{q}$$

$$\equiv \left(\frac{q}{p}\right)S \qquad \pmod{q}$$

因此我们得到了

$$S(-1)^{\frac{p-1}{2}\frac{q-1}{2}}\left(\frac{p}{q}\right) \equiv \left(\frac{q}{p}\right)S \pmod{q}$$

两边同时乘以 S，再由引理，即可得到

$$(-1)^{\frac{p-1}{2}\frac{q-1}{2}}\left(\frac{p}{q}\right) = \left(\frac{q}{p}\right)$$

对偶素数的情形，仍可以用类似的方法证明。

在证明中，我们实际上是在分圆域Q（ζ）中考虑问题，这里模 q 实际上是模Q（ζ）的代数整数环Z[ζ]中 q 生成的理想（ideal）。在之后的章节中我们可以看到分圆扩张是类域论中极其重要的一个研究对象。

2. 复数在数论中的引入

2.1 同余

虽然同余的概念不是从高斯开始的，它出现在欧拉、拉格朗日和勒让德的著作中，但是高斯在《探讨》的第一节引进了同余的记号，并在此后系统地应用了它。

如果整数 a，b 除以非 0 整数 m 的余数相同，那么我们将这一事实记作

$$\mathrm{a} \equiv \mathrm{b} \bmod \mathrm{m}$$

我们可以考虑一个整系数多项式在模 m 下的解，具体来说，考虑方程

$$a_n x^n + \ldots + a_1 x + a_0 \equiv 0 \; mod \; m$$

的解。拉格朗日证明了，n 次同余方程

$$a_{\mathrm{n}} x^n + \ldots + a_1 x + a_0 \equiv 0 \; mod \; p \text{，} \; p \text{是素数}$$

最多只有n个解（在 mod p 意义下）。同余方程是数论中重要的研究对象，其中二次剩余的概念可以用同余方程重新陈述。我们称 a 是模 p 的一个二次剩余，如果 a 不被 p 整除，且同余方程

$$\mathrm{x}^2 \equiv \mathrm{a} \bmod \mathrm{p}$$

有整数解。

2.2 高斯整环

考察同余方程

$$x^4 \equiv q \bmod p$$

如果存在一个整数满足这个方程，则称 q 是 p 的双二次剩余。高斯经过研究，得到了双二次互反律和三次互反律。为了使他的三次和双二次剩余的理论优美而简单，高斯使用了复数。在高斯关于双二次剩余的著作中，他将形如 4n+1 的素数 p 分解成了两个形如 a+bi（a，b 都是整数）的乘积，这种整数称为高斯整数，他们构成一个环$Z[i]$，称为高斯整环。早在欧拉和拉格朗日时期就已经将这种整数引入了数论，但高斯进一步地研究了他们。

高斯证明了高斯整数和普通的整数一样，具有唯一分解的性质。这个事实依赖于$Z[i]$是一个欧式环。具体来说，对$Z[i]$中的$a+bi$赋予一个模N，$N(a+bi) := (a+bi)(a-bi) = a^2 + b^2$。可以证明，对于任何的高斯整数 B 和任意的非 0 高斯整数 A，存在唯一的高斯整数 q 和高斯整数 r，使得

$$B = Aq + r, N(r) < N(A)$$

依赖于这个性质，我们可以得知高斯整环是一个主理想环，更是一个唯一分解环。

通过复数，高斯得到了双二次互反律的一个美妙的叙述。将不能被$1+i$整除的整数定义为非偶整数。定义准素非偶整数

为那些a +bi满足a是偶数，b是奇数。双二次互反律可以叙述为：如果α和β是两个准素非偶素数，A和B是他们的模，则

$$\left(\frac{\alpha}{\beta}\right)_4 = (-1)^{\frac{(A-1)(B-1)}{16}}\left(\frac{\beta}{\alpha}\right)_4$$

其中符号$\left(\frac{\alpha}{\beta}\right)_4$具有下述意义：如果 p 是任意一个复素数，k 是任何一个不能被 p 整除的双二次剩余，则$\left(\frac{k}{p}\right)_4$是i的幂$i^e$,它满足同余式

$$k^{\frac{Np-1}{4}} \equiv 1 \, mod \, p$$

这个定律等价于下列说法：两个准素非偶素数之间的两个双二次特征是相同的，也就是$\left(\frac{\alpha}{\beta}\right)_4 = \left(\frac{\beta}{\alpha}\right)_4$，只要每个素数模 4 余 1；但如果没有一个素数满足这个同余条件，则这两个双二次特征就互反，即$\left(\frac{\alpha}{\beta}\right)_4 = -\left(\frac{\beta}{\alpha}\right)_4$。

高斯陈述了这一互反性定理，但没有发表他的证明。定理的证明是雅可比于 1836 年到 1837 年在科尼斯堡的演讲中给出的。艾森斯坦（Eisenstein）是高斯的学生，他先后发表了这一定理的 5 个证明。

2.3 艾森斯坦整环和三次互反律

高斯发现，对于三次互反性他能得到一个运用“整数”a +bω的一个机会，其中ω是方程$x^2 + x + 1 = 0$的一个根，a,b 都是整数。但是高斯没有发表他对三次互反律的结果，直到高斯去世，人们整理他的手稿时才发现。

环Z[ω]称为艾森斯坦整环，可以证明，它也是一个欧几里得整环，从而具有唯一分解的性质。三次互反律的证明将在Z[ω]上进行。

设π是一个Z[ω]中的素元，满足$N(\pi) \neq 3$。Z[ω]中元素 a 模π的三次剩余特征记为$\left(\frac{a}{\pi}\right)_3$,它的定义为当π|a时，$\left(\frac{a}{\pi}\right)_3 = 0$，当π不整除a时，

$$\left(\frac{a}{\pi}\right)_3 = \begin{cases} 1，若 a^{\frac{N(\pi)-1}{3}} \equiv 1\ (mod\ \pi) \\ \omega，若 a^{\frac{N(\pi)-1}{3}} \equiv \omega\ (mod\ \pi) \\ \omega^2，若 a^{\frac{N(\pi)-1}{3}} \equiv \omega^2\ (mod\ \pi) \end{cases}$$

三次互反律：设π_1，π_2是Z[ω]中本原的素元且$N(\pi_1), N(\pi_2) \neq 3$，$N(\pi_1) \neq N(\pi_2)$。则

$$\left(\frac{\pi_1}{\pi_2}\right)_3 = \left(\frac{\pi_2}{\pi_1}\right)_3$$

三次互反律的证明比二次互反律的证明困难不少。我们可以定义三次的高斯和，它在证明中起关键作用。

设素数$p \equiv 1\ (\mathrm{mod}\ 3)$，记

$$G = \sum_{i=1}^{p} e^{\frac{2\pi i k^3}{3}}$$

为三次高斯和。则G的极小多项式是$x^3 - 3px - Ap$,其中A,B是方程$4p = A^2 + 27B^2, A \equiv 1(mod\ 3), B > 0$的唯一解

3. 代数数和代数整数

3.1 库默尔的理想数

费马大定理叙述简洁但证明起来却极其困难，历史上无数的数学家试图证明它，却最终以失败告终。但在尝试的过程中，数学家们发展出了许多强有力的新的理论，大大促进了数论的发展。其中，库默尔的理想数便是对费马大定理探索中的产物。它是理想（ideal）的前身，揭示了代数整环的某种深刻性质。

我们在上一章提到了欧拉、拉格朗日等数学家将复数引入数论，高斯将这一理论发扬光大，这本质上是对有理数域作代数扩张，在扩张后的域中考虑问题。这一想法在证明费马大定理的过程中变得逐渐清晰。

费马大定理：方程

$$\mathrm{x}^{\mathrm{n}} + y^n = z^n$$

在$\mathrm{n} > 2$时没有正整数解。

欧拉证明当$\mathrm{n} = 3$时的情形，费马证明了$\mathrm{n} = 4$的情形，勒让

德证明了$n=5$的情形。高斯试图证明$n=7$的情形，但失败了。[4]他在 1816 年给奥伯斯（Heinrich W.M. Olbers,1758-1840）的一封信中说：“我的确承认，费马定理作为一个孤立的命题对我而言没有多少兴趣，因为可以容易地立出许多那样的命题，人们既不能证明它们也不能否定它们。” $n=7$ 的情形由拉梅（Gabriel Lame）于 1837 年证明。

这个问题由库默尔（Ernst Eduard Kummer, 1810-1893）持续下来。库默尔从神学转向数学，并做了高斯和狄利克雷的学生，后来在布雷斯劳（Breslau）和柏林做教授。他把x^p+y^p(p为奇素数)分解成

$$(x+y)(x+\alpha y)\ldots(x+\alpha^{p-1}y)$$

这里α是一个p次本原单位根，即α满足

$$\alpha^{p-1}+\alpha^{p-2}+\ldots+\alpha+1=0$$

这启发库默尔将高斯的负整数理论推广到形如

$$f(\alpha)=a_0+a_1\alpha+\ldots+a_{p-2}\alpha^{p-2}$$

的数，其中a_i是通常的整数。库默尔将这样的数称为复整数。

在 1843 年，库默尔对他的这类数，仿照整数定义了什么是整除，什么是素元等等。然而，库默尔想当然地认为他的这类数，即环$Z[\alpha]$,具有唯一分解的性质，这是不对的。在 1843 年，库默尔将他的手稿寄给狄利克雷，狄利克雷告诉他，唯一分解的性质仅仅对一部分素数p成立。[5]事实上，对代数整数环假定

[4] Morris Kline: Mathematical Thought from Ancient to Modern Times Ⅲ,page 6.
[5] Morris Kline: Mathematical Thought from Ancient to Modern Times Ⅲ,page 6.

唯一因子分解，柯西和拉梅也犯了同样的错误。在 1844 年，库默尔认识到了狄利克雷的批评是正确的。

为了在一般的代数整数环上建立唯一分解理论，库默尔在 1844 年开始的一系列论文中创立了理想数的理论。为了理解库默尔的理想数，我们考虑一个简单的例子：$Z[\sqrt{-5}]$。这是数域$Q(\sqrt{-5})$对应的代数整数环。这个环并不是唯一分解整环（UFD），因为

$$6 = 2 \cdot 3 = （1 + \sqrt{-5}）（1 - \sqrt{-5}）$$

容易证明，$2,3,1+\sqrt{-5},1-\sqrt{-5}$都是不可约元素。

我们引入理想数$\alpha = \sqrt{2}, \beta_1 = \frac{1+\sqrt{-5}}{\sqrt{2}}, \beta_2 = \frac{1-\sqrt{-5}}{\sqrt{2}}$。我们看到，$6 = \alpha^2\beta_1\beta_2$。这样，6 现在唯一地被表示成了四个因子的乘积，就环$Z[\sqrt{-5}]$而言，这四个因子全是理想数。通过这些理想数和其他不可约元素，这个环的因子分解是唯一的。

我们注意到，库默尔的理想数虽是普通的数，但是不属于他所引进的代数数类。而且，理想数也不是以一般方式定义的。尽管这个理论看起来有那么一点奇怪，但它在解决费马猜想上展现出惊人的力量：库默尔用这一理论成果证明了费马大定理对 1~100 中 37，59 和 67 以外的其他整数全部成立。然后，库默尔在 1857 年的一篇论文中将他的结果扩展到这 3 个例外的整数上。日内瓦大学的教授米里马诺夫（Dimitry Mirimanoff, 1861—1945）进一步完善了库默尔的方法，证明了对于直到 256 的每一个n，费马大定理成立，只要x,y,z与指数n互素。

3.2 戴德金的理想

这里的理想不是“理想抱负”的意思，而是一个代数学对象。在介绍理想的概念之前，我们先介绍戴德金的代数数理论。戴德金的代数数理论是高斯的复整数和库默尔的代数数的一般化，但这个一般化和高斯的复整数有些许差别。

若一个数r是某个不可约n次首一有理系数多项式的根，那么称r是n次代数数，这个不可约多项式称作r的极小多项式（minimal polynomial）。如果这个多项式是整系数的，那么称r是一个代数整数。戴德金引进了域（field）的概念。这是一个实数或复数的集合 F，它含有单位元 1，并且对加减法以及乘法封闭，且非 0 的元素存在乘法逆元。可以证明，所有代数数形成一个域。如果 a 是一个代数数，考虑

$$Q[a]:=\{f(a)\,|\,f(x)\in Q[x]\}$$

可以证明，$Q[a]$是一个域，因此$Q[a]=Q(a)$，其中$Q(a)$表示$Q[a]$生成的域。

戴德金还引进了环（ring）的概念，一个交换环R是一个集合，上面有加法和乘法，乘法满足交换律，同时还含有乘法单位 1。我们可以证明，所有代数整数构成一个环。

我们还可以定义什么叫做数域 (number field)。一个数域 K 是一个域使得K/Q是有限扩张。在K中考察整数环Z的整闭包（integral closure）,我们会发现它构成一个环，记作O_K，叫做数

域K的整数环（ring of integer of K)。代数数论的一个非常基本的问题便是确定某个数域的整数环。对于最简单的二次数域$K = Q[\sqrt{d}]$,其中 d 是某个不含平方因子的非零整数，我们有

$$O_K = \begin{cases} Z[\sqrt{d}], & d \equiv 2,3\ (mod\ 4) \\ Z\left[\dfrac{(1+\sqrt{d})}{2}\right], & d \equiv 1\ (mod\ 4) \end{cases}$$

一个经典问题便是问有哪些二次的代数整数环具有唯一分解的性质。对于d是负整数的情形，人们证明只有有限个这样的d。对于d是正整数的情形，目前仍然是开放的问题。

有了这些铺垫，我们回到戴德金关于理想的定义上。将代数数的概念一般化之后，戴德金用了一个不同于库默尔的方案去建立代数整数环O_K的唯一分解理论：戴德金考虑了用数定义的“类”。早在欧拉之前，人们就开始对整数作同余运算，即对于一个给定的整数n，考虑所有被n整除的数，而不是n。两个n整除的数作整数的线性组合仍然是被n整除的数。这个对象是整数环Z的一个理想（ideal)。更一般地，对于一个交换环R，我们定义它的一个理想I是这样一个集合，它满足对任意$x,y \in I, a \in R$,有$ax + by \in I$。我们可以I定义R上模I的剩余类：两个数属于同一个剩余类当且仅当它们的差在I中。我们注意到，这样定义出来的剩余类之间可以定义自然的乘法，从而所有这样的剩余类构成的集合拥有一个环结构，这个环记作R/I。我们看出，这种定义方法跟整数上的剩余类非常相似。戴德金注意到理想对于一个环是非常本质的对象，人们可以通过研究一个环上的理想去了

解这个环。

为了建立理想的唯一分解理论，我们首先要定义一个环中的两个理想的乘积。对环R的两个理想I_1,I_2,定义它们的积I_1I_2为所有形如$ab\ (a \in I_1, b \in I_2)$的元素的R-系数线性组合。容易验证，$I_1I_2$还是一个理想。理想中有一种理想在戴德金的理论中扮演唯一分解中的素元的地位，它便是素理想（prime ideal）。一个素理想是一个理想p使得R/p是一个整环。同时我们可以定义环R的极大理想：唯一真包含它的理想是R。容易证明，理想m是极大理想当且仅当R/m是一个域。

现在我们可以叙述戴德金的伟大发现了。戴德金发现并证明了O_K的每一个非零理想都可以唯一地表示成素理想的乘积（单位理想看成素理想的 0 次幂）。当然，不是所有环都具有这样的性质。O_K其实属于某一类具有特殊性质的环，这类环被称作戴德金整环（Dedekind domain），具有理想的唯一分解性质。

定义（戴德金整环）：一个环被称作戴德金整环，如果它是诺特整环且整数闭，并且任何非零素理想都是极大理想。

3.3 理想类群

对于一个戴德金整环R，我们还可以定义它的分式理想（fractional ideal），具体定义不在此赘述，简单来说它是理想的一种推广，构造出了素理想在乘法下的逆元。所有的分式理想

在乘法意义下构成一个群I，由唯一分解性知这是一个由所有素理想生成的自由阿贝尔群（free abelian group）。同时我们可以考虑所有主理想生成的群P,知P是I的子群。商群I/P被称作戴德金环R的理想类群（ideal class group）。商群I/P的元素个数被称作是戴德金环R的类数（class number）。对于代数整数环O_K,它的类数我们也可以称作是数域K的类数，记作h_K

根据定义，一个戴德金整环是主理想整环当且仅当它的理想类群是平凡群，或者说，它的类数是 1。同时，可以证明，一个戴德金整环是唯一分解整环当且仅当它是主理想整环。所以，一个戴德金整环是唯一分解整环当且仅当它的类数是 1。

对于一个一般的戴德金整环，它的类数不一定是有限的。然而，对于任意数域K，戴德金证明了它的类数是有限的——这是一个非常不平凡的事实。代数数论中的一个基本问题便是确定一个数域K的理想类群和类数。

有了理想类群的概念，我们便可以欣赏库默尔对费马大定理取得的结果。

(Kummer) 费马大定理对大于 2 的正则素数（regular prime）p成立。

这个定理还有一个较弱的形式:

（Kummer）如果奇素数p满足p不整除$Q(\zeta_p)$的类数，那么费马大定理对$n = p$的情形成立。

4. 型的理论

这一章主要介绍型的理论。什么是型呢？考察表达式

$$f(x,y) = ax^2 + 2bxy + cy^2$$

其中a,b,c均为整数，这是一个二元型，因为它有两个变量x,y；它又是一个二次型，因为它是齐次的，且次数是 2。如果存在特殊的整数x_0,y_0，使得$f(x_0,y_0) = M$，我们便称数M可以用型f(x,y)表示。一个经典的问题便是对于某个给定的整数M，找到整数x，y使得$M = f(x,y)$。这一问题属于经典的丢番图问题。

在这些问题方面在欧拉时代已经取得了一些进展，拉格朗日却做出了关键性的观察：如果一个数能被一个型表示出，它就能被许多其他的型表示出，他称这些型是等价的。比如考察变换

$$\begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} \begin{pmatrix} x' \\ y' \end{pmatrix}$$

其中$\alpha,\beta,\gamma,\delta$是整数，满足$\det\begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} = 1$。原来的二元二次型f(x,y)通过将x,y替换成x′,y′得到了一个新的二元二次型f′(x′,y′)。这两个二元型等价。拉格朗日阐明了对于一个给定的判别式（discriminant）$b^2 - ac$，存在着有限个型，使得具有这一判别式的每一个型等价于这有限个型中的一个。从而所有具有已给判别式的型可以分成有限类。

这一结果以及由勒让德归纳出的一些结果引起了高斯的注意。高斯从拉格朗日的著作中抽象出了型的等价的概念，并系统化并扩展了型的理论。高斯定义了型的等价。设用之前的线性变换把型

$$F = ax^2 + 2bxy + cy^2$$

变换为型

$$F' = a'x^2 + 2b'xy + c'y^2$$

那么

$$b'^2 - a'c' = (b^2 - ac)(\alpha\delta - \beta\gamma)^2$$

如果$(\alpha\delta - \beta\gamma)^2 = 1$，那么这两个型的判别式相等。如果$\alpha\delta - \beta\gamma = 1$，F和F′称为固有等价；如果$\alpha\delta - \beta\gamma = -1$，则F和F′称为非固有等价。

高斯证明了一系列有关型的等价的命题。例如，如果F和F′等价，F′和F′′等价，则F和F′′等价。又比如，高斯说明了如果F和F′等价，那么一个整数M能被F表示当且仅当它能被F′表示，且表示的方法数是相同的。他还说明了在F和F′等价的条件下，如何去寻找从F变换F′的所有变换。在x和y的值是互素的情况，他也找到了已知数M被型F表示出的一切表示。

由定义不难推出两个等价的型的判别式$D = b^2 - ac$有相同的值，但判别式相同的型不一定是等价的。判别式为D的型尽管有无穷多个，但高斯证明了判别式为某个固定整数D的型可以按照是否彼此固有等价分成有限个等价类，这是一个不平凡的结

果。高斯称$x^2 - D$所属的固有等价类为以D为判别式的型的*主要类*。

高斯还研究了型的复合（乘积）。如果型

$$F = AX^2 + 2BXY + CY^2,$$

在替换 $X = p_1xx' + p_2xy' + p_3x'y + p_4yy'$,

$$Y = q_1xx' + q_2xy' + q_3x'y + q_4yy'$$

之下变换为两个型

$$f = ax^2 + 2bxy + cy^2 \text{和} f' = a'x'^2 + 2b'x'y + c'y'^2$$

的乘积，那么就称F可被变换为ff'。进一步，如果六个数

$$p_1q_2 - q_1p_2, p_1q_3 - q_1p_3, p_1q_4 - q_1p_4,$$

$$p_2q_3 - q_2p_3, p_2q_4 - q_2p_4, p_3q_4 - q_3p_4$$

没有公约数，则称F是型f和型f'的复合。

高斯证明了一个重要的定理：如果f和g属于同一类，而f'和g'属于同一类，则由f和f'所复合的型与由g和g'所复合的型属于同一类。于是我们可以谈论由两个（或两个以上）给定的型的类所复合的型的类。在这种类的复合中，主要类起到了乘法单元的作用，即任何类K和主要类相复合，得到的类仍然是K。

除了二元二次型，高斯还考察了三元二次型：

$$Ax^2 + 2Bxy + Cy^2 + 2Dxz + 2Eyz + Fz^2$$

这里的系数A~F均是整数。高斯将一部分的二元型的理论推广到三元型当中。

研究型的初衷便是解决一些整数的表示的问题。高斯应用

型的理论解决了一大类整数表示的问题，其中包括许多早已被欧拉和拉格朗日等人证明过的定理。例如，高斯证明了任何形如$4n+1$的素数可以唯一地表示成两个正整数的平方和；任何形如$8n+1$或$8n+3$的素数可以唯一地表示成型x^2+2y^2，其中x和y是正整数。高斯阐明了如何去找一个已知数M在给定型$ax^2+2bxy+cy^2$下的所有表示，这里假定判别式D是一个正的非平方数（不然解是有限的）。更进一步，如果K是一个基本型，即a,b,c三个数互素），带有判别式D，并且p是一个能整除D的素数，那么不能被p整除而能被F表示出的诸数要么都是p的二次剩余，要么都是p的二次非剩余。

此外，高斯利用三元二次型的理论证明了每一个正整数可以表示成三个三角数的和。所谓三角数，便是形如$\frac{n(n+1)}{2}, n \in N$的整数。他还重新证明了拉格朗日四平方和定理：任何正整数可以表示为四个平方数的和。

在 19 世纪的数论中，型的理论成为一个主要的课题。希尔伯特在 1900 年提出的 23 个问题中的第 11 个问题便是关于一般数域的二次型理论。关于这个问题，德国数学家哈赛（Hasse）和西格尔（Siegel）在 20 世纪 20 年代取得了重要成果。在 20 世纪 60 年代，法国数学家韦伊（A.Weil）取得了新进展。

5. 抽象群论和域论

5.1 19 世纪的历史背景

本章主要讲述抽象代数的历史及它的一些基本概念和结果，这对于理解之后章节中将要介绍的伽罗瓦理论（Galois theory）和类域论（class field theory）是不可或缺的。在之前的章节中已经多次出现了群、环、域的概念，它们是抽象代数中重要的研究对象。数学家们其实很早便开始研究一些具体的群、环、域，但是关于它们的抽象理论建立是相对较晚的，它们的基本概念直到 19 世纪才被确定下来。

19 世纪大量的数学研究表明了一件事：代数能够处理的不一定只有实数和复数这样的具体的数。向量、四元数、矩阵、二次型如$ax^2+2bxy+cy^2$、各种形式的超复数、变换、替换或置换等都可以用代数来研究，这些对象在各自集合所特有的运算和运算规律下联系起来。

我们可以用运算的特性来区别不同类型的对象。我们引进的群、环、理想、域等概念，以及子群、不变子群、域扩张这样一些从属的概念，是为了“识别”各种集合。然而，19 世纪关

于各种代数的著作，大多是讨论上述的具体对象，比如研究具体的有限群、具体的数域等。直到 19 世纪的最后 10 年，数学家们才意识到，从许多不同的具体的代数对象抽象出一些关键的性质进行研究，可以更加地接近问题的本质，并且能大大提高研究的效率。这是一种“一劳永逸”的研究，因为如果我们研究清楚了某一类抽象结构，之后遇到具有这种抽象结构的具体数学对象，便可以套用抽象结构下的结果。比如，置换群，二次型组成的群，加法的超复数系，通过一下的说法，它们就可以在统一的形式下进行探讨：它们都是一些元素或对象组成的集合，集合上面有某种运算关系，这种运算的特性仅仅由某些抽象性质来决定，其中最为关键的是任何两个元素g_1,g_2，在运算的作用下唯一决定了一个元素，我们记为g_1g_2。对于一些更为复杂的代数对象，比如环，模等，相较于群，它上面有更多的运算关系，但我们依然可以将它们抽象出来，仅仅在集合和运算的层面上定义某一类对象。这种想法其实强烈依赖于集合论以及公理系统的一些事实。但在帕施、皮亚诺、希尔伯特的公理体系之前，人们便有了这种抽象集合的想法。随着公理系统的发展，人们对代数抽象方法越来越有信心。

5.2 抽象群论的建立

从古至今，数学家们研究了无数具体的群。尽管对于如今

的学习了抽象代数的数学系本科生来说，默写出群的定义并举出一些具体的例子是易如反掌的，但是从具体群的例子归纳出抽象的群的概念并不容易。群的抽象概念预伏在高斯、阿贝尔、伽罗瓦、柯西以及很多其他数学家的著作中，经过了漫长的时间最终才变成了今天的样子。

我们首先来看看如今抽象的群是如何定义的。为了定义抽象的群，我们首先要定义一个集合S上的结合法则（law of composition）。通俗来说，一个集合S上的一个结合法则是某种通过结合两个S中的元素a，b得到某个S的元素c。如果用正式的语言叙述，一个集合S上的结合法则是一个映射

$$f: S \times S \to S.$$

这里的$S \times S$意为“集合的积”，它是一个集合，包含所有有序元素对(a,b), $a \in S, b \in S$。

我们可以用$a \cdot b$表示(a,b)在f下的像。这种记号源自数的乘法，因此我们可以称一个集合上的一个结合法则为这个集合上的“乘法”。有了乘法的概念，我们可以仿照自然数或者实数，定义什么叫结合律，交换律。我们称结合法则（或乘法）是结合的（associated），如果对任意S中的任意三个元素a,b,c，有

$$(ab)c = a(bc)$$

我们称结合法则（或乘法）是交换的（commutative），如果对S中的任意两个元素a，b，有

$$ab = ba$$

我们习惯用符号“＋”表示一个交换的法则，即我们习惯记$f(a,b)=a+b$。

事实上，结合律是个比交换律更加基本的性质。其中一个理由是集合之间的映射在复合（composition）下是满足结合律的。具体来说，设T是一个集合，设g和f都是T到T的映射，我们便可以定义g和f的复合，记作$g\circ f$它也是一个T到T的映射，将任何的$t\in T$映到$g(f(t))$。记S为所有从T到T的映射构成的集合，我们可以通过复合定义S上的一个乘法：

$$(g,f)\to g\circ f$$

根据集合之间的映射的定义，这个乘法是结合的，即对于任意$f,g,h\in S$，有

$$(h\circ g)\circ f=h\circ(g\circ f)$$

我们还可以定义乘法的单位元e（或记作1）。如果一个集合S上有一个乘法，那么一个S中的元素e称作是单位元（unit），如果对任意$a\in S$，有

$$ea=a=ae$$

我们可以证明，单位元如果存在，那便是唯一的：假设e_1, e_2都是S中的单位元，根据定义，

$$e_1=e_1e_2=e_2$$

有了前面的一些铺垫，我们终于可以定义什么是一个抽象的群。一个群G是一个集合G，G上有一个乘法，满足

- 乘法交换律：对任何$a,b,c\in G$，有

$$(ab)c = a(bc)$$

- G含有单位元1：对任何$a \in G$，有

$$1 \cdot a = a = a \cdot 1$$

- 每一个G中的元素a都有乘法逆元：存在$b \in G$，使得

$$ab = ba = 1$$

抽象群的概念及其性质是逐渐地被揭示出来的。凯莱(Caley)曾经在 1849 年提出过抽象群，但这个概念的价值在当时并没有被认识到。戴德金在 1858 年给有限群下了一个抽象的定义，这个群是他从置换群引导出来的。他又在 1877 年注意到，他的"代数数模"（即对模中任意两个元素$a,b, a+b,a-b$仍属于这个模）可以推广到元素不限于代数数而且运算可以普遍化，但必须要求每一元素拥有一个逆元素，并且这运算是可交换的。这样他就提出了一个抽象的有限交换群。此外，之前也提到了理想的概念是戴德金提出的。戴德金对这些抽象结构的认识是超越时代的，他是抽象代数的重要创始人。

克罗内克从库默尔的理想数的工作出发，也给出了一个相当于有限交换群的抽象定义，这个概念于凯莱在 1849 年提出的概念。在这个结构中，克罗内克规定了抽象的元素和抽象的运算，运算的封闭性、结合性、交换性，以及每一个元素的逆元素的存在和唯一。他证明了这个结构G（有限交换群G）的一些结果。例如，对G中任一元素a，存在正整数n，使得$a^n = 1$。如

果称满足条件的最小正整数n为a的阶，用$ord(a)$表示，则对任意满足$a^n = 1$的正整数n，有$ord(a)|n$。克罗内克证明了，如果$a,b \in G, gcd(ord(a), ord(b)) = 1$，则$ord(ab) = ord(a)ord(b)$。克罗内克还证明了所谓的基定理（basis theorem），即存在有限多个元素$a_1, a_2, \ldots a_k$,构成的“基”，使得乘积

$$a_1^{h_1} a_2^{h_2} \ldots a_k^{h_k}, h_i = 1,2,\ldots,n_i$$

表示群中全部元素，并且表示是唯一的。其中$n_i = ord(a_i)$，且$n_{i+1}|n_i$。这个定理即有限阿贝尔群的结构定理：有限阿贝尔群G同构于群$Z/n_1Z \oplus Z/n_2Z \oplus \cdots Z/n_kZ$。

1878 年凯莱写了四篇关于有限抽象群的文章。跟他在 1849 年和 1854 年的文章一样，他强调一个群可以看作一个普遍的概念，无须只限于置换群（即某个S_n的子群）；但他同时指出，每个有限群都可以看作是一个置换群，这就是群论中的凯莱定理（Cayley theorem）：一个n阶有限群同构于S_n的一个子群。

弗罗贝尼乌斯（Frobenius）和施蒂克贝格（Ludwig Stickelberger,1850-1936）合作的一篇文章把认识又推进了一步，他们认为抽象群的概念应当包含同余，高斯的二次型合成以及伽罗瓦的置换群。他们认为仅仅考虑有限的群是不够的，抽象群应当可以包含无穷多个元素。

到了 1880 年年，关于群的新概念引起了人们的注意。在若尔的（Jordan）关于置换群的著作的影响下，克莱因在他的埃尔兰根纲领中指出，无限的变换群可以用来对几何对象进行分类。

所谓变换群，便是由几何变换构成的群，例如考虑三维空间中绕某一个轴的旋转变换，一个旋转变换由旋转的角度θ唯一确定，由于θ可以在全体实数中取值，故这是一个由无穷多元素组成的群。

群论有三个主要来源——方程的理论、数论和无限变换群。迪克（Walther von Dyck,1856—1934）将这三种群的共同特点抽象出来，定义了抽象群。在 1882 年和 1883 年他发表了关于抽象群的文章，定义一个抽象群为一个由元素组成的集合，一种满足封闭性的运算，运算满足结合律，每个元素都有一个逆元。我们可以看到，这便是今天抽象群的定义。在这个定义下，无论是伽罗瓦群，置换群，还是几何变换群等，都被囊括其中。这一定义是数学家们智慧的结晶。

5.3　域的理论和伽罗瓦理论

伽罗瓦的故事耳熟能详：他运用创建群和域扩张的理论，证明了一般的五次方程不存在根式解，却为情所困，死于一场决斗之中。用现在的观点来看，伽罗瓦理论的价值远远地超出证明五次方程无根式解，这个理论发现了群和域的某种深刻联系，是研究数域的极为有力的工具，可以说若是没有它现代数论就无从说起。

首先我们来看域（field）的定义。在伽罗瓦的著作中，由n

个量$a_1,a_2,...,a_n$生成的域R，是指这些量经过加、减、乘和除（除数不为0）得到的一切量所构成的集合，扩域（field extension）是指将一个域R加上一个新元素α得到得新的域，或者说是由R和α生成的域。伽罗瓦考虑的域主要是方程系数生成的域，他考虑的域扩张主要是添加方程的根得到的域。

域的抽象理论是从海因里希·韦伯（Heinrich·Friedrich·Weber）开始的。韦伯是抽象群概念的拥护者。在 1893 年他给伽罗瓦理论进行了抽象的阐述，他将一个域定义成一个由元素组成的集合，这个集合上面有两种运算，叫做加法和乘法，都满足封闭性、结合律、交换律和分配律。且所有元素在加法下构成一个群，所有元素去掉加法单位元0后在乘法下构成一个群。海因里希·韦伯强调群和域是代数的两个重要的基本概念。

有了群和域扩张的基本定义，我们便可以陈述（有限扩张的）伽罗瓦理论。在这之前，我们介绍两类基本的域扩张。

可分扩张（separable extension）

F是一个域。给定$p(x) \in F[x]$。多项式$p(x)$称为可分的，如果它在$\bar{F}$中没有重根。否则称$p(x)$是不可分的。

对于一个代数扩张K/F，一个元素$u \in K$称为可分的，如果它在域F上的极小多项式没有重根。代数扩张K/F称为可分的，如果任意K中的元素都是可分的。

正规扩张（normal extension）

域扩张$F \subseteq K \subseteq \bar{F}$称为是正规的，如果满足条件: 对每一个$F[x]$中的不可约多项式$p(x)$，如果它在$K$中有一个根$u$，那么它所有根都在$K$中。

有了这两个定义，我们便可以定义伽罗瓦扩张:

一个有限扩张被称作是伽罗瓦扩张（Galois extension）如果它既是可分扩张又是正规扩张。我们可以定义一个伽罗瓦扩张K/F的伽罗瓦群为

$$Gal(K/F) = \{\varphi \in Aut(K) | \varphi(x) = x, \forall x \in F\}$$

对于一个$Aut(K)$的有限子群H，在H的所有元素作用下的元素构成K的一个子域，称作是群H的固定域（fixed field）,记作K^H。

我们便可以叙述重要的伽罗瓦对应（Galois correspondence）:

如果K/F是有限伽罗瓦扩张，则有一个一一对应:

$$\{Gal(K/F)\text{的子群}\} \leftrightarrow \{K \text{ 包含 } F \text{ 的子域 } E\}$$

具体由

$$H \longmapsto K^H$$

$$Gal(K/E) \longmapsto E$$

给出。

在所有这些伽罗瓦扩张中，我们了解的比较深入的是阿贝尔扩张，也就是那些伽罗瓦群是阿贝尔群的扩张。类域论证明了一系列数域阿贝尔扩张的性质，对于非阿贝尔的情形我们仍

然知之甚少。

6. 环的理论

6.1 环和理想的抽象定义

虽然环和理想的构造早在戴德金和克罗内克关于代数数的著作中出现过,但关于它们的抽象理论却完全是20世纪的产物。在克罗内克的著作将环称作“序”（order），环（ring）一词实际上是由希尔伯特引进的。

我们现在来定义什么叫做含单位元的交换环（commutative ring with an identity element）:一个含幺交换环R是一个集合，上面有两个运算$+,\times$，分别称作加法和乘法，满足以下性质:

(a) 在加法运算$+$下，R是一个阿贝尔群。我们将这个阿贝尔群记作R^+，它的加法单元记作0。

(b) 乘法$\times$满足结合律和交换律，它有一个乘法单位元，记作1。

(c) 加法和乘法满足分配律：对任意$a,b,c \in R$, $(a+b)c = ac + bc$。

由于在数论中，我们主要关心的环都是含单位元的交换环，所以之后出现的环都是含单位元的交换环。

我们再来定义环的理想：一个环R的理想I是R的一个非空子集，满足以下性质:

(a) I在加法下封闭。

(b) 如果$s \in I, r \in R$，则$rs \in R$。

此外，我们还可以定义什么叫环之间的同态：一个映射$\phi:R_1 \to R_2$称为是一个从R_1到R_2的同态，如果它满足对任意$a,b \in R$，有$\phi(a+b)=\phi(a)+\phi(b), \phi(ab)=\phi(a)\phi(b)$，此外还必须满足$\phi(1)=1$。

6.2 素理想在戴德金整环中的扩张

在数论中，我们非常关心的代数整数环是一种戴德金整环。它具有的许多优秀性质在一般的戴德金整环中也成立。我们接下来介绍一点素理想在戴德金整环中的扩张的理论。

设A是一个戴德金整环，$K=\mathrm{Frac}(A)$是 A 的分式域。设L/K是一个有限可分扩张，B为A在L中的整闭包。可以证明，B也是一个戴德金整环。对于A中的一个非零素理想p，它在B中生成的理想pB称作是p在B中的扩张。由戴德金整环的性质，pB可以唯一地表示为B的一些非零素理想的乘积：

$$pB = P_1^{e_1} P_2^{e_2} \ldots P_r^{e_r}$$

其中$P_1, P_2, \ldots, P_r$是两两不同的素理想，$e_1, e_2, \ldots, e_r$为正整数。称这些素理想是p上的素理想（prime ideal above p）。称这些e_i称作是素理想P_i的分歧数（ramification index），记为$e(P_i/p)$。

由环的嵌入映射A→B可以诱导出一个域的嵌入映射：

$$A/p \to B/P_i$$

可以证明，$[B/P_i : A/p]$是有限的，将其记为$\mathrm{f_i} = f(P_i/p)$，称作是素理想$\mathrm{P_i}$的"惯性度"（inertia degree）。

称素理想$\mathrm{P_i}$是非分歧的（unramified），如果$\mathrm{e}(\mathrm{P_i}/p) = 1$。如果所有p上的素理想都是非分歧的，即对任意i有$\mathrm{e}(\mathrm{P_i}/p) = 1$，则称p是非分歧的。如果$\mathrm{r} = 1, \mathrm{f} = 1$, 则称素理想p是完全分歧的（totally ramified）。

一个不平凡的结果是，这些 ramification index 和 index degree 之间有一个美妙的等式:

$$\sum_{i=1}^{r} e_i f_i = [L:K]$$

当$\mathrm{L/K}$进一步是伽罗瓦扩张时，可以证明，$\mathrm{Gal(L/K)}$在p上的素理想构成的集合上的作用是可迁的，即对于任意两个p上的素理想$\mathrm{P_1}, P_2$,存在$\sigma \in \mathrm{Gal(L/K)}$，使得$\sigma(\mathrm{P_1}) = P_2$。由此可见，对于$\mathrm{L/K}$是伽罗瓦扩张的情形，所有p上的素理想的 ramification index 和 inertia degree 都相等。此时有$\mathrm{efr} = [\mathrm{L:K}]$。

在伽罗瓦扩张的情形下，我们可以定义某个p上素理想P的 decomposition group $\mathrm{G_P} = \{\sigma \in Gal(L/K) | \ \sigma(P) = P\}$。我们考虑$\mathrm{G_P}$的固定域$\mathrm{L}^{\mathrm{G_P}}$，它称作是素理想P的 decomposition field。记B^{P}为A在$\mathrm{L}^{\mathrm{G_P}}$中的整闭包，设$\mathrm{P} \cap \mathrm{B}^{\mathrm{P}} = O$。则根据伽罗瓦群在O上的素理想的作用是可迁的知，P是唯一一个O上的素理想。

任何一个G_P中的元素σ可以诱导一个B/P到自身的同构映射。注意到这个自同构固定了子域A/p，因此这是$Gal((B/P)/(A/p))$中的一个元素。（这里我们假定了A/p是完美的（perfect），也就是说假设它的任何代数扩张都是可分的。在具体的应用中，我们考虑的A大多是代数整环，因此A/p是一个有限域，而有限域是完美的。我们可以证明扩张$(B/P)/(A/p)$是正规的，因此$(B/P)/(A/p)$是伽罗瓦扩张。）这样我们便定义了一个从G_P到$Gal((B/P)/(A/p))$的映射，这是一个群同态，且我们可以证明这个同态是满的。我们称这个满同态的核为素理想P的 inertia group，记作I_P。它的固定域L^{I_P}称为 inertia field。

注意到对于两个不同的p上的素理想P_1,P_2，存在$\tau \in Gal(L/K)$，使得$\tau(P_1) = P_2$。则它们的 decomposition group 满足关系

$$G_{P_1} = \tau^{-1} G_{P_2} \tau$$

如果此时L/K是一个阿贝尔扩张，即$Gal(L/K)$是一个阿贝尔群，则有$G_{P_1} = G_{P_2}$。因此 decomposition group 不依赖于p上素数的选取，此时我们可以记$G_{P_1} = G_{P_2} = G_p$

以上我们介绍了一些关于素理想在戴德金整环中扩张的概念及性质，它们在数域的阿贝尔扩张的研究中是基本的。

7. p 进数——域的完备化

在数论中，p进域的发现是革命性的。在 19 世纪已经知道的域已经有有理数域、实数域、复数域、代数数域和一个或多个变数的有理函数域等。亨泽尔（Hensel）发现了一种新的域，叫做p进域，在代数数论方面开辟了新的天地。Hensel 首先观察到每个普通的非负整数D可以唯一地表示成一个素数p的方幂的和，即

$$\mathrm{D} = \mathrm{d}_0 + d_1 p + d_2 p^2 + \ldots + d_k p^k$$

其中$\mathrm{d_i}$是整数且$0 \le \mathrm{d_i} \le p-1$。对于一般的整数，比如负整数，我们同样可以将它写成这种幂和，只不过这回需要无穷多项，比如

$$-1 = (\mathrm{p}-1) + (\mathrm{p}-1)\mathrm{p} + (\mathrm{p}-1)\mathrm{p}^2 + \ldots = \sum_{k=0}^{\infty} (p-1)p^k$$

对于一般的有理数q，我们首先可以将它写成$\mathrm{q} = \frac{\mathrm{a}}{\mathrm{b}} \cdot p^k$的形式，其中a,b为与p互素的整数，k为整数。再将$\frac{\mathrm{a}}{\mathrm{b}}$展开成无穷幂级数，具体来说，存在唯一一个$\mathrm{a}_0 \in \{0,1,\ldots,p-1\}$使得$\frac{\mathrm{a}}{\mathrm{b}} - a_0$的既约分

数形式的分子被p整除。再考虑$\left(\frac{\mathrm{a}}{\mathrm{b}}-a_0\right)\cdot p^{-1}$，同理，存在唯一一个$\mathrm{a}_1\in\{0,1,\ldots,p-1\}$使得$\left(\frac{\mathrm{a}}{\mathrm{b}}-a_0\right)\cdot p^{-1}-a_1$的既约分数的分子被p整除。再考虑$\left(\left(\frac{\mathrm{a}}{\mathrm{b}}-a_0\right)\cdot p^{-1}-a_1\right)\cdot p^{-1}$。如此下去，我们得到了一连串的$\mathrm{a}_0,a_1,a_2\ldots$。我们有

$$\frac{a}{b}=\sum_{i=0}^{\infty}a_i p^i$$

$$\mathrm{q}=\frac{\mathrm{a}}{\mathrm{b}}\cdot p^k=\sum_{i=0}^{\infty}a_i p^{i-k}$$

Hensel 定义的p进域$\mathrm{Q_p}$在*集合层面上*等于

$$\mathrm{Q_p}=\left\{\sum_{k=-n}^{\infty}a_k p^k\middle|\, n\in\mathbb{N},\, a_k\in\{0,1,\ldots,p-1\}\right\}$$

这个集合中的两个元素之间的加法和乘法并不是简单的逐项加减，也就是说，我们不能定义$\mathrm{a}=\sum_{k=-n}^{\infty}a_k p^k$和$\mathrm{b}=\sum_{k=-n}^{\infty}b_k p^k$的和为$\sum_{k=-n}^{\infty}c_k p^k$,其中$\mathrm{c_k}\equiv a+b\ (mod\ p),\ c_k\in\{0,1,\ldots,p-1\}$。不能这样做的原因非常简单：如果a和b的级数表示中只有有限多项，那么这样定义出的加法于整数的加法不符，换言之，我们就没有办法把整数环当成$\mathrm{Q_p}$的一个自环——这样定义出来的$\mathrm{Q_p}$就不是很好。我们应该意识到，$\mathrm{a+b}=\sum_{k=-n}^{\infty}c_k p^k$中的$\sum_{k=-n}^{m}c_k p^k$作为整数应当等于$\sum_{k=-n}^{m}(a_k+b_k)p^k$。

我们发现，这样定义两个数的加法或乘法非常的繁琐。我们在此介绍一个一般性的理论彻底地解决这个问题，并进一步阐述什么是$\mathrm{Q_p}$。

首先我们有一个概念叫做域上的绝对值（absolute value）。具体来说，一个域K上的绝对值$|\cdot|$是一个映射

$$|\cdot|:\mathrm{K}\to\mathbb{R}_{\geq 0},\ x\mapsto|x|$$

使得（1）$|\mathrm{x}|=0\Leftrightarrow\mathrm{x}=0$

(2) $|\mathrm{xy}|=|\mathrm{x}|\cdot|\mathrm{y}|$

(3) $\forall\mathrm{x},\mathrm{y}\in\mathrm{K},|\mathrm{x}+\mathrm{y}|\leq|\mathrm{x}|+|\mathrm{y}|(triangular\ inequality)$

$(\mathrm{K},|\cdot|)$称为一个赋值域（valued field）。

域上的绝对值给出了域上的一个度量：$\mathrm{d}(\mathrm{x},\mathrm{y})=|\mathrm{x}-\mathrm{y}|$,这个度量诱导了K上的一个拓扑。我们域K上两个绝对值是等价的，如果它们诱导了相同的拓扑。一个重要的结论是，两个绝对值$|\cdot|_1$,$|\cdot|_2$是等价的当且仅当存在$\lambda>0$使得对任意$\mathrm{x}\in\mathrm{K}$，有$|\mathrm{x}|_1=|x|_2^{\lambda}$。一个域上的所有绝对值在等价的定义下分成了若干等价类，其中每一个等价类称为一个位（place）。

我们称一个绝对值是非阿基米德的，如果$\forall\mathrm{x},\mathrm{y}\in\mathrm{K},|\mathrm{x}+\mathrm{y}|\leq\max\{|\mathrm{x}|,|\mathrm{y}|\}$。否则就称它是阿基米德的。与非阿基米德的绝对值对偶的一个概念叫做赋值（valuation）。域K上的一个赋值v是一个函数$\mathrm{v}:\mathrm{K}\setminus\{0\}\to\mathbb{R}$,满足：

(1) $\mathrm{v}(\mathrm{ab})=\mathrm{v}(\mathrm{a})+\mathrm{v}(\mathrm{b})$

(2) $\mathrm{v}(\mathrm{a}+\mathrm{b})\geq\min\{\mathrm{v}(\mathrm{a}),\mathrm{v}(\mathrm{b})\}$

对任意一个绝对值$|\cdot|$，我们都可以定义一个赋值：

$$\mathrm{v}(\mathrm{x}):=-\log_{\mathrm{a}}|x|,\forall x\in K$$

其中$\mathrm{a}>1$是一个实数。反过来，对于任何一个赋值 v，我们都

可以定义一个非阿基米德绝对值:

$$|\mathrm{x}|:=\mathrm{a}^{-\mathrm{v}(\mathrm{x})}, \forall x \in K$$

其中$\mathrm{a}>1$是一个实数。不难看出，对于不同的a，所定义出的绝对值是两两等价的。

有了这些概念，我们不仅想要考察一个具体的域，比如说有理数域$\mathbb{Q}$上有哪些绝对值。显然，有理数域上的将负数变正数的函数是一个绝对值。同时，对每个素数p，$\mathbb{Q}$上有一个非常自然的赋值：$\mathbb{Q} \setminus \{0\}$中每个数$\mathrm{x}$都可以写成$\mathrm{p}^{\mathrm{k}} \cdot \frac{a}{b}$的形式，其中$\gcd(\mathrm{ab},\mathrm{p})=1$。我们令$\mathrm{v}_{\mathrm{p}}(x)=k$。由这个赋值可以定义一个$\mathbb{Q}$上的绝对值$|\cdot|_p$，$|x|_p=\mathrm{p}^{-\mathrm{v}(\mathrm{x})}=p^{-k}$。这样，每一个素数$\mathrm{p}$都对应了一个$\mathbb{Q}$上的非阿基米德的 place。事实上，$\mathbb{Q}$上的 place 只有我们列举出来的这些。

我们知道，一个域K上的一个绝对值会诱导一个度量。如果我们将这个度量空间做完备化，得到的完备度量空间$\hat{K}$仍然具有一个绝对值，且可以将K视为$\hat{K}$的一个子域，$\hat{K}$上的绝对值限制在K上得到K上原本的绝对值。有了这个定义，我们便把$\mathbb{Q}_{\mathrm{p}}$定义成$(\mathbb{Q},|\cdot|_p)$的完备化。

对每一个离散赋值环（DVR）A都可以定义它的分式域K上的一个赋值，具体来说，取A的一个 uniformizer π,则K的每个非零元素x都可以唯一表示成$\mathrm{u} \cdot \pi^{\mathrm{n}}$的形式，其中$\mathrm{u}$是$\mathrm{A}$中的一个单位，$\mathrm{n}$是一个整数。定义$\mathrm{v}(\mathrm{x})=\mathrm{n}$。对于这种值域是$\mathbb{R}$中的一个离散子群的赋值，我们称它为离散赋值。在这种情形下，我们实

际上可以具体地描述$\hat{K}$中的元素。令$\hat{A}=\{\mathrm{x}\in\hat{K}\,|\,v(x)\geq 0\}=\{x\in\hat{K}\,|\,|x|\geq 1\}$。$\hat{A}$是一个DVR。我们有自然的*同构*:

$$\mathrm{A/m^n}\to\hat{A}/\hat{m}^n$$

$$\hat{A}\to\varprojlim_{n}\hat{A}/\hat{m}^n$$

其中$\mathrm{m}=\pi\mathrm{A},\hat{m}=\pi\hat{A}$，$\pi$是A的 uniformizer。我们称域$\mathrm{A/m}=\hat{A}/\hat{m}$为剩余类域（residue field）。如果对$\mathrm{A/m}$的每个类都在A中选取一个代表元，这些代表元组成一个集合S。那么$\hat{A}$中的每个元素都可以唯一地表示为一个无穷的幂级数:

$$\sum_{n=0}^{\infty}a_n\pi^n$$

其中$\mathrm{a_i}\in S$。读者可能会好奇这个幂级数的收敛情况，答案是肯定的。可以证明，在一个非阿基米德的域中，一个级数收敛等价于每一项组成的数列收敛。在这里，幂级数收敛等价于$\mathrm{a_n}\pi^n\to 0,n\to\infty$，而后者是显然的。

我们最后来讨论一般数域上的 place。对于数域K的一个绝对值，它限制在$\mathbb{Q}$上，会得到$\mathbb{Q}$上的一个 place。我们不禁问：如果两个K上的 place 限制在$\mathbb{Q}$上得到的 place 相同，那这两个 place 是否相同？事实上，这是不对的。一个$\mathbb{Q}$上的 place 可以延拓出多个K上的 place。然而对于完备域上绝对值的延拓，这确实是唯一的。我们可以证明，对于一个完备的域$(\mathrm{K},|\cdot|_K)$，若L/K是一个代数扩张，则可以唯一地将$|\cdot|_K$延拓到L上，得到(L,

$|\cdot|_L$)（若此时L/K是一个有限扩张，则$(L,|\cdot|_L)$是完备的）。同时，对任意$\alpha \in L$，我们有

$$|\alpha|_L = \sqrt[n]{N_{M/K}(\alpha)}$$

其中$\alpha \in M \subseteq L$，M/K是一个有限扩张，$[M:K] = n$。

我们再考虑一个一般域上绝对值的延拓。设$(K,|\cdot|_K)$是一个赋值域，L/K是一个有限可分扩张。设$|\cdot|_1,|\cdot|_2,\ldots,|\cdot|_g$是$|\cdot|_K$到L的延拓。设$L_i$为在L关于绝对值$|\cdot|_i$的完备化。则有一个 canonical 的同构:

$$L \otimes_K \hat{K} \cong \prod_{i=1}^{g} L_i$$

由于戴德金整环在一个非零素理想处的局部化是一个离散赋值环，所以戴德金整环的每一个素理想都可以给出它的分式域的一个非阿基米德赋值。由于代数整环O_K是戴德金整环，所以代数整环的每一个非零素理想都可以给出K上的非阿基米德赋值。可以证明，$p \in \mathbb{Z}$对应得 place 在K上得延拓与p上的素理想一一对应。K上的每一个阿基米德的 place 都是$\mathbb{Q}$上唯一的那个阿基米德 place 的延拓，$\mathbb{Q}$上阿基米德的 place 的完备化就是实数域$\mathbb{R}$（这就是定义实数的一种方式）。我们有下面的交换图:

$$\begin{array}{ccc} K & \rightarrow & \hat{K} \\ \uparrow & & \uparrow \\ \mathbb{Q} & \rightarrow & \mathbb{R} \end{array}$$

我们知$\hat{K}$是$\mathbb{R}$的一个代数扩张。但由于复数域$\mathbb{C}$是一个代数闭域，

$\mathbb{C}/\mathbb{R}$是一个二次扩张，所以$\hat{K}=\mathbb{C}$或$\mathbb{R}$。其中$\hat{K}=\mathbb{R}$的情况我们称这个K的 place 为一个 real place，否则就称它是一个 complex place。

根据以上的讨论，我们可以定义什么叫做数域K上的一个 cycle。一个 cycle $\mathfrak{c}$是一个形式的乘积

$$\prod_{\upsilon\ place\ of\ K} \upsilon^{m(\upsilon)}, \mathrm{m}(\upsilon)\in\mathbb{Z}_{\geq 0}$$

使得（1）只有有限个υ使得$\mathrm{m}(\upsilon)>0$（2）若υ是 complex place，则$\mathrm{m}(\upsilon)=0$ （3）若υ是 real place，则$\mathrm{m}(\upsilon)\leq 1$

我们知道，如果υ是非阿基米德的，那么它对应一个K中的非零素理想，此时我们可以用素理想$\mathfrak{P}$来表υ，令$\mathrm{m}(\mathfrak{P})=\mathrm{m}(\upsilon)$。将$\mathfrak{c}$中非阿基米德的部分拿出来，得到

$$\mathfrak{c}_0=\prod\mathfrak{P}^{m(\mathfrak{P})}$$

$\mathfrak{c}_0$称为是$\mathfrak{c}$的有限部分（finite part）。

以上概念在整体类域论（global class field theory）的叙述中会出现。

8. ζ函数和L-函数

8.1 黎曼ζ函数和戴德金ζ函数

黎曼ζ函数最开始完全是一个分析学研究的对象。它最早被定义成

$$\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s}$$

其中s是一个大于1的实数。后来数学的发展表明，这个函数在数论方面有及其重要的应用，或者说它后来变成了一个数论家研究的重要对象。

黎曼ζ函数最早可以追溯到 1350 年，当时的尼克尔·奥里斯姆（Nicole Oresme）发现了调和级数

$$1 + \frac{1}{2} + \frac{1}{3} + \frac{1}{4} + \cdots$$

是发散的。之后欧拉对调和级数做了研究，发现它是呈对数发散的。同时，欧拉还在 1735 年给出了著名的巴塞尔问题的解答，

证明了$\sum_{n=1}^{\infty}\frac{1}{n^2}=\frac{\pi^2}{6}$。此外，他还证明了欧拉乘积公式：

$$\zeta(s)=\prod_p\left(1+p^{-s}+p^{-2s}+\ldots\right)=\prod_p\frac{1}{1-p^{-s}},\ s>1$$

其中p取遍所有素数。这个公式揭示了它的一些和数论之间的联系。

实际上，利用复数的收敛的概念，ζ函数的定义域可以扩展到$\mathrm{Re}(s)>1$，这是一个重要的进展，但并不是最惊人的。黎曼天才的工作表明，定义在$\mathrm{Re}(s)>1$上的解析函数$\zeta(s)$可以解析延拓成$\mathbb{C}$上的一个亚纯函数（meromorphic function），它在$s=1$处有唯一的单极点（simple pole），留数是1。

利用欧拉乘积公式，我们得到

$$\begin{aligned}\log(\zeta)(s)&=-\sum_p\log\left(1-p^{-s}\right)\\&=\sum_{n\geq 1,\ p}\frac{1}{np^{ns}}\\&=\sum_{n\geq 2,\ p}\frac{1}{np^{ns}}+\sum_p\frac{1}{p^s}\end{aligned}$$

可以证明，级数$\sum_{n\geq 2,\ p}\frac{1}{pnp^{ns}}$在$\mathrm{Re}(s)>\frac{1}{2}$上绝对收敛。所以它是$\mathrm{Re}(s)>\frac{1}{2}$上的一个解析函数。因此有

$$\log(\zeta)(s)\sim\sum_p\frac{1}{p^s}\sim\log\left(\frac{1}{s-1}\right)$$

其中$f\sim g$在这里表示$f-g$是$s=1$附近的解析函数，即f和g在$s=1$处的奇异部分（singular part）相同。

戴德金将黎曼ζ函数推广到了一般的数域上。

（戴德金ζ函数）设K是一个数域，定义数域K的戴德金ζ函数为

$$\zeta_{\mathrm{K}}(s)=\sum_{\mathfrak{a}\subseteq\mathcal{O}_K}\frac{1}{(N\mathfrak{a})^s},\ \mathrm{Re(s)}>1$$

其中$\mathfrak{a}$取遍代数整数环$\mathcal{O}_{\mathrm{K}}$中所有非零理想。对于戴德金ζ函数，注意到$\mathcal{O}_{\mathrm{K}}$有理想的唯一分解，因此有欧拉乘积公式：

$$\zeta_{\mathrm{K}}(s)=\sum_{\mathfrak{a}\subseteq\mathcal{O}_K}\frac{1}{(N\mathfrak{a})^s}=\prod_{\mathfrak{p}\subseteq\mathcal{O}_K}\frac{1}{1-(N\mathfrak{p})^{-s}}$$

进而有

$$\log\left(\zeta_{\mathrm{K}}\right)(s)=-\sum_{\mathfrak{p}}\log\left(1-(N\mathfrak{p})^{-s}\right)$$

$$=\sum_{n\geq 1,\ \mathfrak{p}}\frac{1}{n(N\mathfrak{p})^{ns}}$$

$$\sim\sum_{\mathfrak{p}}\frac{1}{(N\mathfrak{p})^s}$$

事实上，我们可以进一步说明

$$\sum_{\mathfrak{p}}\frac{1}{(N\mathfrak{p})^s}\sim\sum_{\mathfrak{p},f(\mathfrak{p}/p)=1}\frac{1}{(N\mathfrak{p})^s}$$

其中$(\mathrm{p})=\mathfrak{p}\cap\mathbb{Z}$,p为素数。

下面我们来简要说明$\zeta_{\mathrm{K}}(s)$在$\mathrm{s}=1$处有一个单极点，并给出它的留数。我们将$\zeta_{\mathrm{K}}(s)$求和的理想按照它们在K的理想类群中的类进行分类，具体来说，我们令

$$\zeta_{\mathrm{K}}([\mathfrak{b}],s)=\sum_{\substack{\mathfrak{a}\subseteq\mathcal{O}_K\\ [\mathfrak{a}]=[\mathfrak{b}]}}\frac{1}{(N\mathfrak{a})^s}$$

其中[𝔞],[𝔟]表示理想𝔞,𝔟在理想类群$\mathrm{Cl_K} = I/P$中的的所在类。

从而我们有

$$\zeta_{\mathrm{K}}(s) = \sum_{[\mathfrak{b}] \in I/P} \zeta_K([\mathfrak{b}],s)$$

而

$$\zeta_{\mathrm{K}}([\mathfrak{b}],s) = \sum_{n \geq 1} \frac{a_n([\mathfrak{b}])}{n^s},$$

其中 $a_n([\mathfrak{b}]) = \#\{\mathfrak{a} \subseteq \mathcal{O}_K | [\mathfrak{a}] = [\mathfrak{b}], \text{且} N\mathfrak{a} = n$

我们有

$$\mathrm{A_n}([\mathfrak{b}]) := \sum_{k=1}^{n} a_k([\mathfrak{b}]) = \#\{\mathfrak{a} \subseteq \mathcal{O}_K | [\mathfrak{a}] = [\mathfrak{b}], N\mathfrak{a} \leq n\}$$

$$= \rho \mathrm{n} + \mathrm{o}(\mathrm{n}^{1-1/\mathrm{N}})$$

其中 $\rho = \frac{2^{\mathrm{r}_1}(2\pi)^{r_2} R_K}{\omega_K \sqrt{|DiscK|}}$，$\mathrm{N} = [\mathrm{K}:\mathbb{Q}]$，$\mathrm{r}_1, r_2$分别是K的 real place 和 complex place 的个数，$\mathrm{R_K}$是K的regulator，$\omega_{\mathrm{K}} = \#\mathcal{O}_K(torsion)$

由此，我们可以将$\zeta_{\mathrm{K}}([\mathfrak{b}],s)$延拓到$\mathrm{Re(s)} > 1 - \frac{1}{\mathrm{N}}$，在$\mathrm{s} = 1$处有一个单极点，留数为$\rho$。

从而，我们有

定理：$\zeta_{\mathrm{K}}(s)$可以延拓成$\mathrm{Re(s)} > 1 - \frac{1}{\mathrm{N}}$上的一个亚纯函数，它在$\mathrm{s} = 1$处有一个单极点，留数为

$$\rho = \frac{2^{\mathrm{r}_1}(2\pi)^{r_2} R_K h_K}{\omega_K \sqrt{|DiscK|}}$$

从而我们有

$$\zeta_{\mathrm{K}}(s)\sim\sum_{\mathfrak{p}}\frac{1}{(N\mathfrak{p})^{s}}\sim\log\left(\frac{1}{s-1}\right)$$

对于任意K中的 cycle $\mathfrak{c}$，我们可以定义：

.$\mathrm{I}(\mathfrak{c})=\{\mathrm{K}\text{ 中与}\mathfrak{c}_0\text{互素的分式理想}\}$

.$\mathrm{K}_{\mathfrak{c}}=\{x\in K^{\times},s.t\ x\equiv 1\ mod\mathfrak{c}$

.$\mathrm{P}_{\mathfrak{c}}=\{(x)\,|\,x\in K_{\mathfrak{c}}\}\subseteq\mathrm{I}(\mathfrak{c})$

我们可以证明$\mathrm{I}(\mathfrak{c})/\mathrm{P}_{\mathfrak{c}}$是一个有限群，称为$\mathfrak{c}$-ideal class group。

利用 cycle 的概念，我们可以进一步将戴德金ζ函数推广。我们对任何K中的 cycle $\mathfrak{c}$，都可以定义

$$\zeta_{\mathrm{K},\mathfrak{c}}(\mathrm{s})=\sum_{\substack{\mathfrak{a}\subseteq\mathcal{O}_K\\(\mathfrak{a},\mathfrak{c}_0)=1}}\frac{1}{(N\mathfrak{a})^{s}}=\prod_{\substack{\mathfrak{p}\subseteq\mathcal{O}_K\\(\mathfrak{p},\mathfrak{c}_0)=1}}\frac{1}{1-(N\mathfrak{p})^{-s}}$$

$$=\prod_{\mathfrak{p}|\mathfrak{c}_0}(1-N\mathfrak{p}^{-s})\cdot\zeta_{\mathrm{K}}(s)$$

因此我们有

$$\log\left(\zeta_{\mathrm{K},\mathfrak{c}}\right)(s)\sim\sum_{\mathfrak{p}}\frac{1}{(N\mathfrak{p})^{s}}$$

$$\sim\log\left(\frac{1}{\mathrm{s}-1}\right)$$

8.2 狄利克雷L-函数

狄利克雷定义了他的L-函数，这是戴德金ζ函数的推广。

定义：给定一个数域K和它的一个 cycle $\mathfrak{c}$.，令

$$\chi \in \widehat{I(\mathfrak{c})/P_{\mathfrak{c}}} = \{\phi : I(\mathfrak{c})/P_{\mathfrak{c}} \to \mathbb{C}^{\times} \text{群同态}\}$$

为$\mathfrak{c}$-ideal class group 上的一个特征（character）。定义L-函数为

$$L_{\mathfrak{c}}(\chi, s) = \sum_{(\mathfrak{a}, \mathfrak{c}_0) = 1} \frac{\chi([\mathfrak{a}])}{N\mathfrak{a}^s} = \prod_{(\mathfrak{p}, \mathfrak{c}_0) = 1} \left(1 - \frac{\chi([\mathfrak{p}])}{N\mathfrak{p}^s}\right)^{-1}$$

如果按$I(\mathfrak{c})/P_{\mathfrak{c}}$中的类进行分类，我们有

$$\sum_{(\mathfrak{a}, \mathfrak{c}_0) = 1} \frac{\chi([\mathfrak{a}])}{N\mathfrak{a}^s} = \sum_{[\mathfrak{b}] \in I(\mathfrak{c})/P_{\mathfrak{c}}} \chi([b]) \cdot \zeta_{K,\mathfrak{c}}([\mathfrak{b}], s)$$

我们看出，当χ为$\widehat{I(\mathfrak{c})/P_{\mathfrak{c}}}$中的单位元时，狄利克雷L-函数就是戴德金$\zeta$函数。

下面是关于狄利克雷 L-函数的一个重要性质。

定理：如果$\chi \neq 1$，则$L_{\mathfrak{c}}(\chi, s)$可以解析延拓到$\mathrm{Re}(s) > 1 - \frac{1}{N}$。更精确地说，序列$L_{\mathfrak{c}}(\chi, s) = \sum_{(\mathfrak{a}, \mathfrak{c}_0) = 1} \frac{\chi([\mathfrak{a}])}{N\mathfrak{a}^s}$在$\mathrm{Re}(s) > 1 - \frac{1}{N}$上的任何一个紧子集上面一致绝对收敛。

利用L-函数，[6]我们可以证明

定理（Universal index inequality）设$\mathfrak{c}$是一个K的 cycle，L/K是一个数域之间的有限伽罗瓦扩张，则

$$\#（I(\mathfrak{c})/P_{\mathfrak{c}}\mathcal{N}(\mathfrak{c})) \leq [L:K]$$

其中$\mathcal{N}(\mathfrak{c}) = \{N_{L/K}(I) | I\text{是L中与}\mathfrak{c}_0\text{互素的分式理想}\}$

定理（Weber's inequality）设L/K是一个有限的数域之间的伽罗瓦扩张，设$\mathfrak{c}$是K的一个 cycle。设H是$I(\mathfrak{c})$的一个子群，满足$I(\mathfrak{c})$

[6] Serge Lang, Algebraic Number Theory, p164-165.s

$\supseteq \mathrm{H} \supseteq \mathrm{P}_{\mathfrak{c}}$（这样的H被称为是一个$\mathfrak{c}$-ideal group。

假设H包含$\{\mathfrak{p} \subseteq \mathcal{O}_{\mathrm{K}}$ 素理想 $|\mathfrak{p}$在 L 中完全分裂$\}$在相差一个狄利克雷密度为 0 的集合意义下。则

(1) $\#(\mathrm{I}(\mathfrak{c})/\mathrm{H}) \leq [\mathrm{L}:\mathrm{K}]$

(2)$\forall \chi:\mathrm{I}(\mathfrak{c})/\mathrm{H} \to \mathbb{C}^{\times}, \chi \neq 1, \mathrm{L}_{\mathfrak{c}}(\chi,1) \neq 0$

(3)如果$\{\mathfrak{p} \in \mathrm{H},\mathfrak{p}$是素理想$\} = \{\mathfrak{p} \subseteq \mathcal{O}_{\mathrm{K}}$ 在L/K中分裂$\}$在相差一个狄利克雷密度为 0 的集合的意义下相等，那么$\#(\mathrm{I}(\mathfrak{c})/\mathrm{H}) = [\mathrm{L}:\mathrm{K}]$

9. 类域论初步

类域论是描述整体域（数域）和局部域（$\mathbb{Q}_{\mathrm{p}}$的有限扩张）的阿贝尔扩张的理论。19 世纪末有三个数论中的主题最终导致了类域论的产生，它们分别是阿贝尔扩张和理想类群的联系、素数的密度定理和L-函数，还有互反律。本章将介绍什么是类域，并且称述整体类域论的结果。

由 Universal norm index inequality 的结果，我们不禁会问以下问题：

(1) Universal norm index inequality 中的不等号什么时候会变成等号，也就是说，对于怎样的伽罗瓦扩张L/K，有

$$\#\left(\mathrm{I}(\mathfrak{c})/\mathcal{N}(\mathfrak{c})\mathrm{P}_{\mathfrak{c}}\right) = [L:K] = \#Gal(L/K)$$

(2) 当等号成立时，群$\mathrm{I}(\mathfrak{c})/\mathcal{N}(\mathfrak{c})\mathrm{P}_{\mathfrak{c}}$和群$\mathrm{Gal}(\mathrm{L}/\mathrm{K})$是否是同构的？

(3) 如果（2）成立，能否构造这两个群之间的一个 canonical 的

同构?

(4) 如果H是K的一个$\mathfrak{c}$-ideal group，什么时候存在伽罗瓦扩张L/K，使得$\mathrm{H}=\mathcal{N}(\mathfrak{c})\mathrm{P}_{\mathfrak{c}}$

(5) （4）中的L是否是唯一的？（固定一个$\mathbb{Q}$的代数闭包$\overline{\mathbb{Q}}$，$\mathbb{Q}\subseteq\mathrm{K}\subseteq\mathrm{L}\subseteq\overline{\mathbb{Q}}$）

我们一一地回答以上问题:

(1) 等式成立当且仅当L/K是阿贝尔扩张且$\mathfrak{c}$是一个 admissible cycle（这是一种满足某种性质的 cycle，它的定义需要用到ideles的理论）

(2) 是的

(3) 是的，它们之间 canonical 的同构由 Artin map 得到:

$$\mathrm{Art}_{\mathrm{L}/\mathrm{K}}\colon \mathrm{I}(\mathfrak{c})/\mathrm{P}_{\mathfrak{c}}\mathcal{N}(\mathfrak{c})\xrightarrow{\sim} Gal(L/K)$$

$$[\mathfrak{p}]\longmapsto \mathrm{Frob}_{\mathfrak{p}}$$

(4) 存在阿贝尔扩张L/K满足$\mathfrak{c}$是 admissible cycle，且$\mathcal{N}(\mathfrak{c})\mathrm{P}_{\mathfrak{c}}=H$

(5) 是的，（4）中给出的L就是唯一满足要求的那个。

我们该从哪里开始回答这些问题呢？跟着 Weber，我们考虑分裂的素数。首先我们定义什么叫做狄利克雷密度（Dirichlet density）。

设L/K是数域间的伽罗瓦扩张，如果$\mathrm{S}\subseteq\{\text{素理想}\mathfrak{p}\subseteq\mathcal{O}_{\mathrm{K}}\}$，$\mathrm{S}$的狄利克雷密度（如果存在）定义为

$$\lim_{s \to 1^+} \frac{\sum_{\mathfrak{p} \in S} \frac{1}{N\mathfrak{p}^s}}{\log\left(\frac{1}{s-1}\right)}$$

定义$S_{L/K} = \{\mathfrak{p} \subseteq \mathcal{O}_K$ 素理想 s.t.$\mathfrak{p}$ 在 L/K上完全分裂$\}$

如果$S_1, S_2 \subseteq \{$素理想$\mathfrak{p} \subseteq \mathcal{O}_K\}$, 我们用$S_1 \prec S_2$表示$S_1 \subseteq S_2$（在误差小于一个狄利克雷密度为 0 的集合的意义下）用$S_1 \sim S_2$表示$S_1 \prec S_2$ 且$S_2 \prec S_1$。Weber 证明了以下定理:

(1) 如果L/K是有限伽罗瓦扩张，则$S_{L/K}$的狄利克雷密度为$\frac{1}{[L:K]}$

(2) 如果L_1/K是有限伽罗瓦扩张，L_2/K是有限扩张，那么

$$L_2 \subseteq L_1 \Leftrightarrow S_{L_1/K} \prec S_{L_2/K}$$

Weber 在 1897 年给出了类域（class field）的定义:

设K是一个数域，$\mathfrak{c}$是K的一个 cycle。设H是一个$\mathfrak{c}$-ideal group。

我们说一个有限伽罗瓦扩张L/K是K关于H的类域，如果

$$\{\text{素理想}\mathfrak{p} \in H\} \sim S_{L/K}$$

由之前 Weber 的定理，我们可以得到类域的比较定理（comparison theorem for class fields）:

定理（比较定理）：设H_1, H_2是两个$\mathfrak{c}$-ideal groups。假设存在它们对应的类域L_1, L_2。则$L_1 \subseteq L_2 \Leftrightarrow H_2 \subseteq H_1$。

Takagi 在 1920 年证明了类域的存在性。

定理（Existence theorem）设K是一个数域，$\mathfrak{c}$是K的一个 cycle。

设H是一个$\mathfrak{c}$-ideal group。则K关于H的类域L存在。进一步，$\mathfrak{c}$是L/K的 admissible cycle，且有$\mathfrak{p}$在L/K中分歧$\Longrightarrow \mathfrak{p}|\mathfrak{c}$

设L是K关于H的类域，由第 8 章的 Weber's inequality，有$\#Gal(L/K) = [L:K] = \#(I(\mathfrak{c})/H)$。 Takagi 证明了存在从$Gal(L/K)$到$I(\mathfrak{c})/H$的同构，但没能给出具体的 canonical 的映射。Artin 在 1927 年证明了 Artin 互反律（Artin reciprocity law），给出了一个 canonical 的同构。

定理（Artin, 1927）设K是一个数域，L/K是一个有限阿贝尔扩张，$\mathfrak{c}$是这个扩张的一个 admissible cycle。有 Artin map

$$Art_{L/K}: I(\mathfrak{c}) \to Gal(L/K)$$

$$\mathfrak{p} \mapsto (\mathfrak{p}, L/K) = Frob_{\mathfrak{p}}$$

这个映射的核恰好是$P_{\mathfrak{c}}\mathcal{N}(\mathfrak{c})$。

将我们已知的结果综合起来，我们得到：

定理：设K是一个数域，$\mathfrak{c}$是K的一个 cycle。我们在

(1) $\mathfrak{c}$-ideal groups H

(2) 有限阿贝尔扩张L/K使得$\mathfrak{c}$是 admissible cycle。

之间有一个双射，其中$(1)\to(2)$的存在唯一性由 Existence theorem 给出，$(2)\to(1)$由$L/K \mapsto H = P_{\mathfrak{c}}\mathcal{N}(\mathfrak{c})$给出。

这个对应非常的美妙，但不足之处在于它的叙述中出现了K的 cycle。实际上，用 idele 的语言可以避免这一情况。在此我们不

对术语进行解释，仅仅展示这一美妙结果：

定理（idelic class field theorem）：映射$\mathrm{L/K}\mapsto \mathrm{H}=\mathrm{K}^{\times}N_{L/K}(\mathbb{A}_L^{\times})$是一个

$$\{\mathrm{L/K}\text{有限阿贝尔扩张}\}$$

和

$$\{\mathbb{A}_K^{\times}\text{中包含}\mathrm{K}^{\times}\text{的开子群}\}$$

之间的双射。Artin map

$$\mathrm{Art_{L/K}}\colon \mathbb{A}_K^{\times}\to Gal(L/K)$$

的核恰为$\mathrm{K}^{\times}N_{L/K}(\mathbb{A}_L^{\times})$。

类域论除了整体类域论，还有局部类域论（local class field theory），最早由 Hasse 证明。此外，类域论早期的证明用到了很多分析学的内容，比如L-函数，但类域论的叙述却是纯代数的。Chevalley 第一个给出了类域论的纯代数证明。他引进了 ideles 的语言，将类域论推广到了无穷阿贝尔扩张。限于篇幅，这之后的进展就不在此讨论了。

参考文献

[1][美]莫里斯·克莱因（Morris Kline）,古今数学思想第二册，石生明，万伟勋，孙树本等译，上海：上海科学技术出版社，2014

[2][美]莫里斯·克莱因（Morris Kline）,古今数学思想第三册，邓东皋，张恭庆等译，上海：上海科学技术出版社，2014

[3]S.Lang, *Algebraic Number Theory*, Springer-Verlag, New York, 1994

[4]J.S.Milne *Algebraic Number Theory*, Lecture notes,www.jmilne.org/math/.

[5][美]阿廷（Artin,M.）,代数，北京：机械工业出版社，2011