

# 谈谈代数数论

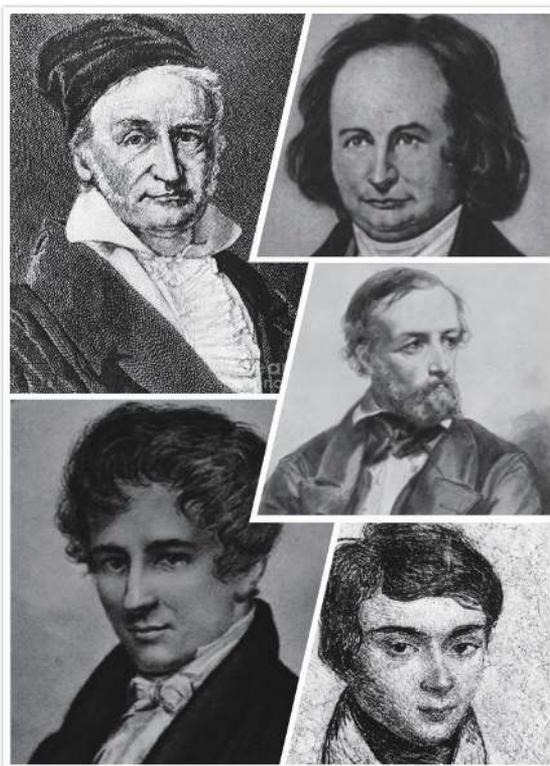
## ——代数数论百年历史回顾及分期初探

黎景辉

内容简述：我们把代数数论过去一百多年的历史作非常简单的描述，藉此探讨如何把整个发展作分期，和展望未来。我们不会在文中谈概念的详细定义和定理的证明，我们只打算谈一些主题和方法，希望对同学和科研管理员有点用，也许亦会让同行加以讨论。

### 第一部 序幕

本文简单地讲讲代数数论的历史，希望简单的讲就比较容易看见全貌，这样就方便把整个历史分期及对整个过程分析。至于文中所讨论的是否属于“代数数论”的范围？大家都会有不同的意见。例如：当 $\mathbb{Z}$ 是整数环时，有人会认为研究 $K_n(\mathbb{Z})$ 是代数拓扑学。有人会说 $K_n(\mathbb{Q}_p(\sqrt{-d}))$ 的研究是属于代数数论，但如果 $F$ 是域， $K_n(F)$ 是 $K$ 理论。我不想为此花时间争议。不管是用代数、分析、几何、拓扑方法，我相信基本上什么是代数数论大家有相当共识的，还有一些题目我没有谈到而有专家认为是代数数论的范围。例如代数数论数值算法、代数数有理逼近、代数域上的解析数论、组合与概率代数数论、函数域上超越数论、不定方程与丢番图几何等，只好请大家行文畅述了。我国数学家在代数数论有非凡的成就，我认为需要专文介绍，这里没有谈到的，请大家原谅。当然要畅顺地阅读本文是需要一点代数知识的，比如你最少要知（群、环、域）这三件事。对学生来说，不必要看明白也可以看下去，因为这样你最少知道还有什么可以学的。



	雅可比
高斯	狄利克雷
阿贝尔	伽罗瓦

注：本文首发于《数学通报》（2013年/第52卷第5期，1-5页；2013年/第52卷第6期，1-4页）。本刊转载时，黎景辉教授对多处内容进行了修改与补充。

## 奠基时代

我不打算为代数数论下个定义，因为这样便把代数数论限死了。我首先说说代数数论里几个重要的概念。

1. 我以 $\mathbb{Q}$ 记有理数域。设 $X$ 为变元，以 $\mathbb{Q}(X)$ 记有理函数域。当 $a$ 是一个复数时，以 $a$ 代 $X$ 从 $\mathbb{Q}(X)$ 得出的域记为 $\mathbb{Q}(a)$ 。
2. 域扩张，就是一个域 $E$ 包含另一个域 $F$ 。若 $E$ 包含有理数域 $\mathbb{Q}$ 我便称 $E$ 为数域。最重要的数域是二次扩张 $\mathbb{Q}(\sqrt{d})$ ，其中 $d$ 是整数， $\sqrt{d}$ 不是有理数。
3. 设有域扩张 $E \supset F$ ，考虑自同构 $\alpha: E \rightarrow E$ 满足条件：对所有 $x \in F$ ，有 $\alpha(x) = x$ 。由所有这样的自同构 $\alpha$ 所组成的集合记作 $Aut(E/F)$ 。当 $E/F$ 是Galois时， $Aut(E/F)$ 记为 $Gal(E/F)$ 并称为 $E/F$ 的伽罗瓦群。当 $Gal(E/F)$ 为交换群时则称 $E/F$ 为交换扩张。
4. 最简单的二次型便是多项式 $x^2 + y^2 + z^2$ 。
5. 在 $\mathbb{Q}$ 上的椭圆曲线是指以 $y^2 = 4x^3 - g_2x - g_3$ 所定义的曲线，其中 $g_2, g_3$ 为有理数并且 $\Delta = g_2^3 - 27g_3^2 \neq 0$ 。最著名的椭圆曲线是 $y^2 = x(x - a^\ell)(x - c^\ell)$ ，其中 $\ell$ 为 $\geq 5$ 的素数并要求有非零整数 $a, b, c$ 满足费马方程 $a^\ell + b^\ell = c^\ell$ 。
6. 对实部大于1的复数 $s$ 定义黎曼zeta函数为

$$\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s} = \prod_{p \text{ 是素数}} \frac{1}{1 - p^{-s}},$$

这是数论里常见的 $L$ 函数的祖先。注意这个等式是等价于整数的基本性质：任一整数必可写成素数乘积的唯一分解。

7. 平常的绝对值 $|x|$ 在有理数域 $\mathbb{Q}$ 上定义一个度量。按此度量把 $\mathbb{Q}$ 完备化便得实数域 $\mathbb{R}$ 。我们说一个度量空间是完备是指这空间具有下述性质：空间中的任何柯西序列都收敛在该空间之内。现固定素数 $p$ 。设整数 $a$ 有因子分解 $a = p^n d$ ，其中 $d$ 与 $p$ 没有公因子，则以 $v(a)$ 记 $n$ 。定义分数的 $p$ -绝对值

$$\left| \frac{a}{b} \right|_p = p^{v(b) - v(a)},$$

把有理数域 $\mathbb{Q}$ 对 $p$ -绝对值完备化便得 $p$ -进数域 $\mathbb{Q}_p$ 。

以下是代数数论的主要的奠基工作。

1. 高斯 (Carl Friedrich Gauss, 1777-1855)：二次型，二次域扩张，二次互反律，带复乘的椭圆曲线
2. 阿贝尔 (Niels Henrik Abel, 1802-1829)：阿贝尔积分，五次方程没有一般根号解公式
3. 雅可比 (Carl Jacob Jacobi, 1804-1851)：椭圆函数， $\theta$ 函数
4. 狄利克雷 (Peter Dirichlet, 1805-1859)： $L$ 函数，类数公式，算术序列中的素数
5. 库默尔 (Ernst Kummer, 1810-1893)：交换扩张
6. 伽罗瓦 (Évariste Galois, 1811-1832)：群论在域扩张的应用
7. 魏尔斯特拉斯 (Karl Weierstrass, 1815-1897)：椭圆函数
8. 埃尔米特 (Charles Hermite, 1822-1901)：复数域上的二次型理论
9. 埃森斯坦 (F. G. M. Eisenstein, 1823-1852)：模形式，埃森斯坦级数
10. 克罗内克 (Leopold Kronecker, 1823-1891)：有理数域的交换扩张
11. 戴德金 (Richard Dedekind, 1831-1916)： $\zeta$ 函数，理想
12. 弗罗贝尼乌斯 (Ferdinand Georg Frobenius, 1849-1917)：无分歧域扩张
13. 庞加莱 (Henri Poincaré, 1854-1912)：模形式
14. 亨泽尔 (Kurt Hensel, 1861-1941)： $p$ -进数

这些工作是在十九世纪完成的。一本很好快速介绍这些成果的书是塞尔 (Jean-Pierre Serre) 的《数论教程》，冯克勤译。一本讲 $L$ 函数的经典著作是达文波特 (Harold Davenport) 的 *Multiplicative Number Theory*。

开始主题之前，我为大家介绍模形式。已知三角函数

$$f(x) = \sin 2\pi x$$

有以下性质：对任意整数  $n$  有

$$f(n + x) = f(x),$$

我们称整数  $n$  为函数  $f(x)$  的周期。整数群  $\mathbb{Z}$  为  $f(x)$  的周期群。

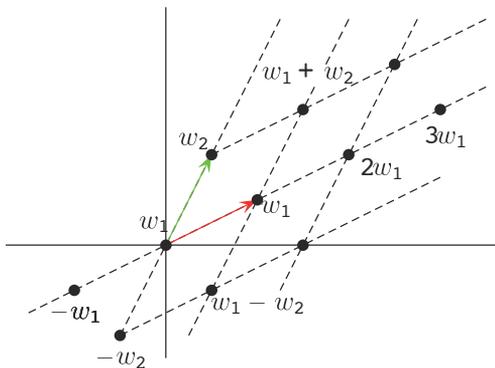
我们可以问：是否存在一些函数  $f$ ，它的周期群比整数群  $\mathbb{Z}$  更复杂。当然先问什么群比  $\mathbb{Z}$  复杂。第一个情形便是由整数对  $(n, m)$  所组成的群  $\mathbb{Z} \times \mathbb{Z}$ 。这个群的加法是这样定义的：

$$(n, m) + (n_1, m_1) = (n + n_1, m + m_1).$$

我们可以使用复数把这个群  $\mathbb{Z} \times \mathbb{Z}$  推广一点。取两个复数  $w_1, w_2$  使得  $\frac{w_1}{w_2}$  不是实数。则复数集合

$$\Gamma = \{w = n_1 w_1 + n_2 w_2 : n_1, n_2 \in \mathbb{Z}\}$$

是复平面的一组格点。



上图表示了  $\Gamma$  是由  $w_1$  和  $w_2$  生成的

用复数的加法， $\Gamma$  便是一个群。 $\Gamma$  实际上是与  $\mathbb{Z} \times \mathbb{Z}$  同构的。

现在我们可以问：是否存在复变函数  $f(z)$  使得  $\Gamma$  是  $f(z)$  的周期群？即是说，对任意  $w \in \Gamma$ ，以下公式成立：

$$f(w + z) = f(z).$$

这样的函数  $f(z)$  我们称为椭圆函数。

**例子：**已给群  $\Gamma$ ，则我们用无穷级数

$$f(z) = \sum_{w \in \Gamma} \frac{1}{(z-w)^3}$$

所定义的  $f(z)$  是一个椭圆函数。

我们要指出  $\mathbb{Z}$  和  $\mathbb{Z} \times \mathbb{Z}$  都是交换群。最简单的非交换群是  $SL_2(\mathbb{Z})$ ，它的元素是  $2 \times 2$  矩阵

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix},$$

其中  $a, b, c, d$  是整数，并且行列式  $ad - bc = 1$ ，这是用矩阵乘法来定义的一个非交换群。

我们以  $H$  记上半复平面： $H = \{z = x + iy : y > 0\}$ 。若  $z \in H$ ，

$$\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(\mathbb{Z}),$$

则设

$$\gamma(z) = \frac{az+b}{cz+d}.$$

如此我们说  $SL_2(\mathbb{Z})$  作用在  $H$  上。

我们可以问：是否存在函数  $f(z)$  在  $SL_2(\mathbb{Z})$  这个作用下不变，即是说

$$f(\gamma(z)) = f(z).$$

在  $SL_2(\mathbb{Z})$  里有元素

$$\gamma = \begin{pmatrix} 1 & n \\ 0 & 1 \end{pmatrix},$$

其中  $n$  是任意整数，这时

$$\gamma(z) = \frac{z+n}{0z+1} = z+n,$$

于是对所有  $\gamma \in SL_2(\mathbb{Z})$  成立的条件

$$f(\gamma(z)) = f(z)$$

是包括要求

$$f(z+n) = f(z),$$

即是包括要求整数群  $\mathbb{Z}$  是  $f$  的周期，从这个角度来看，我们所寻求满足条件

$$f(\gamma(z)) = f(z)$$

的函数  $f(z)$  是三角函数的推广。但是，是否有这样的函数呢？

引进符号：若

$$\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix},$$

则设  $j(\gamma, z) = cz + d$ 。因为几何的考量我们把条件

$$f(\gamma(z)) = f(z)$$

推广一点。固定一整数  $k \geq 0$ 。我们考虑定义在上半复平面  $H$  上的解析函数  $f(z)$ ，并要求对任意  $\gamma \in \Gamma$ ，以下等式成立

$$j(\gamma, z)^{-k} f(\gamma(z)) = f(z).$$

我们称这样的  $f(z)$  为模形式。例子：设  $k$  为大于等于 4 的偶数，由以下埃森斯坦级数所定义的函数  $G_k(z)$  为模形式：

$$G_k(z) = \sum_{m, n \in \mathbb{Z}} (mz + n)^{-k}$$

在和  $(m, n) \neq (0, 0)$ 。

在二十世纪的代数数论里模形式扮演一个完全意想不到的角色！我介绍一本关于模形式的书——Diamond & Shurman, *A First Course in Modular Forms*。

## 第二部 主题

以下我把二十世纪的代数数论分为五波来讲。

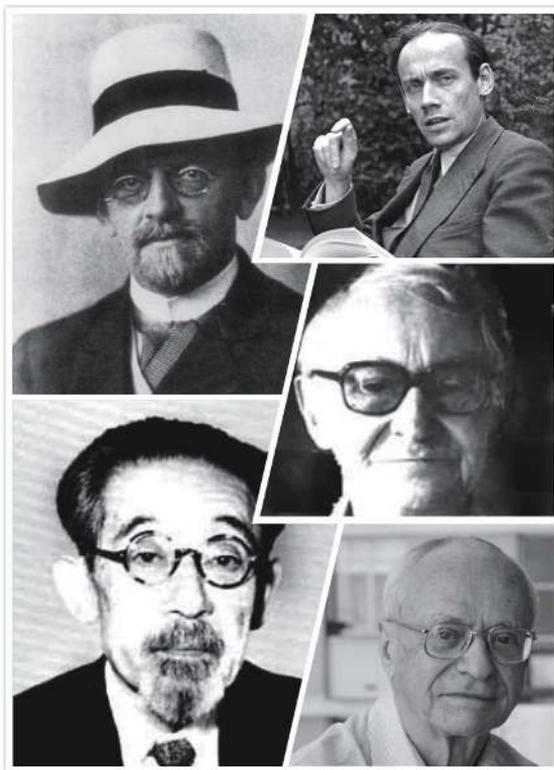
1. 交换类域论
2. 岩泽理论
3. 朗兰兹对应
4. 格罗滕迪克代数几何学在代数数论的应用
5. 同伦代数几何学在代数数论的应用

	阿廷
希尔伯特	
	谢瓦莱
高木贞治	
	塞尔

### 第一波

奠基之后的第一波是从十九世纪末到二十世中叶，由下面诸位开拓：

1. 希尔伯特 (David Hilbert, 1862-1943)
2. 高木贞治 (Takagi, 1875-1960)
3. 阿廷 (Emil Artin, 1898-1962)
4. 谢瓦莱 (Claude Chevalley, 1909-1984, 1941 年柯尔奖)
5. 中山正 (Nakayama)
6. 泰特 (John Tate, 1956 年柯尔奖, 2010 年阿贝尔奖)



7. 塞尔 (1954 年菲尔兹奖, 2003 年阿贝尔奖)。后者完成了交换扩张的伽罗瓦群的表示之上同调理论，即交换类域论。

好的参考书有下面的几本：

1. 高木贞治，代数的整数论，岩波书店（等待中文版）；
2. 岩泽健吉，局部类域论，冯克勤译，科学出版社；
3. 塞尔，*Local Field*；
4. 阿廷与泰特合著，*Class Field Theory*。

类域论的一个核心定理是互反律。高斯的二次互反律是互反律的鼻祖。让我们用拓扑群的语言介绍交换互反律。设  $G$  为拓扑群，由所有连续同态  $G \rightarrow \mathbb{C}^\times$  所组成的集合记为  $G^*$ 。设  $F$  为数域， $F^{ab}$  为  $F$  的最大交换扩张， $A^\times$  为  $F$  的 idele 群，则交换互反律是指存在单同态

$$\rho : (\text{Gal}(F^{ab}/F))^* \hookrightarrow (A^\times/F^\times)^*$$

满足  $L$  函数条件

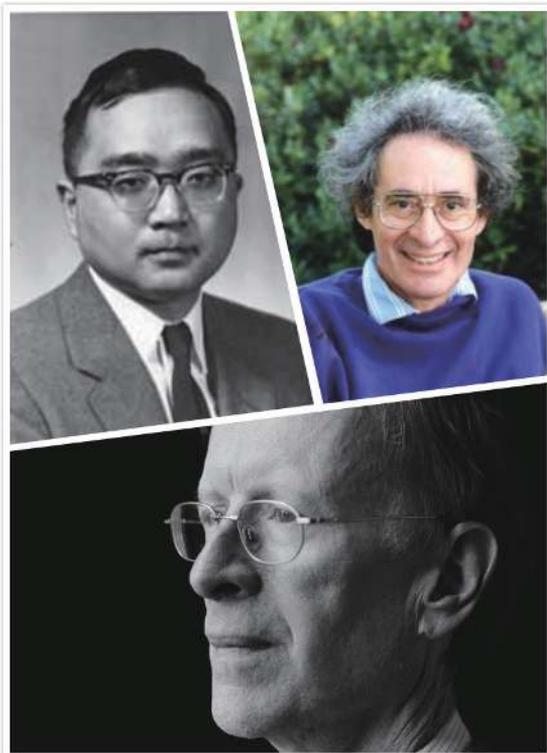
$$L_F^{\text{Artin}}(\chi, s) = L_F^{\text{Hecke}}(\rho(\chi), s).$$

在这里应推介高维局部域的互反律。这方面最早的工作是加藤和也（Kazuya Kato）的硕士论文<sup>1</sup>以及参考文献 [2]。

### 3 第二波

我想先说什么是类数。设有数域  $K$ 。则  $K$  的分式理想以乘法为群  $I$ 。  $K$  的每一个非零元生成一个主理想，以  $P$  记由主理想所组成的群。  $K$  的理想类群  $C_K$  是指商群  $I/P$ 。称  $C_K$  的元素个数为  $K$  的类数，记作  $h_K$ 。域  $K$  的元素有唯一素元乘积分解的充要条件是  $h_K = 1$ 。所以我们说  $h_K$  是数域  $K$  的一个重要算术参数。设  $p$  为素数， $\zeta_p$  为  $p$  次单位原根。以  $h_p$  记  $\mathbb{Q}(\zeta_p)$  的最大实子域类数。Vandiver 猜想： $p$  不除尽  $h_p$ ；这是代数数论的一个重要的猜想。

岩泽健吉 (Iwasawa Kenkichi, 1917-1998, 1962 年柯尔奖) 二十世中叶岩泽提出传统类域论之外的一个新方向——交换岩泽理论 (*On the  $\Gamma$  extensions of algebraic number fields*, Bull. AMS 65 (1959) 183-226)。岩泽健吉是弥永昌吉的学生，弥永昌吉 (Shokichi Iyanaga) 是高



岩泽健吉 | 马祖尔  
怀尔斯

木贞治的学生，高木贞治是希尔伯特的学生。

考虑下述例子：取素数  $p \neq 2$ ，研究以下数域所组成的塔：

$$K_0 \subset K_1 \subset \dots \subset K_n \subset \dots \subset K_\infty = \bigcup K_n,$$

其中  $\text{Gal}(K_n/K_0) \cong \mathbb{Z}/p^n\mathbb{Z}$ 。则

$$\text{Gal}(K_\infty/K_0) = \lim_{n \rightarrow \infty} (\mathbb{Z}/p^n\mathbb{Z}) = \mathbb{Z}_p,$$

常称  $K_\infty/K_0$  为  $\mathbb{Z}_p$  扩张。

岩泽认为：当代数数论中某些数域所成的塔的伽罗瓦群同构于  $p$  进整数  $\mathbb{Z}_p$  的加法群的时候，岩泽建议把这些数域所成的塔的理想类群 (class group) 看作  $\mathbb{Z}_p$  模研究。理想类群  $\mathbb{Z}_p$  模的特征理想可以用久保田富雄 (Kubota Tomio) 和里奥博特 (Heinrich-Wolfgang Leopoldt) 在 1960 年定义的  $p$  进  $L$ -函数的特殊值算出——“岩泽主猜想”。这个猜想在有理