Reciprocity Law

Jiahai Wang

2024 年 9 月 4 日

Beauty is the first test:there is no permanment place in the world for ugly mathematics——G.H.Hardy

Wir müssen wissen. Wir werden wissen. ——-David Hilbert

目录

目录 **2**

0 Preface **4**

1 Quadratic Reciprocity Law **5**

1.1 Gauss lemma——初等方法 5

1.2 高斯和 7

1.3 分圆域——更高角度 7

1.4 类域论的证明 8

2 三、四次互反率 **10**

2.1 Cubic Reciprocity Law 10

2.2 Quartic Reciprocity Law 10

3 Eisenstein's Reciprocity Law **11**

3.1 m 次剩余符号的定义及其性质 11

3.1.1 m 次剩余符号 11

3.1.2 高斯和 12

3.1.3 m 次互反律的介绍 13

3.2 Stickelberger 关系 13

3.2.1 域自同构在元素和理想上的作用 13

3.2.2 Stickelberger 关系 14

3.3 Eisenstein 互反律的证明 14

4 Kummer's Reciprocity Law **16**

5 Hasse' s Reciprocity law **17**

6 Hilbert's Reciprocity Law **18**

6.1 Local 18

6.2 global 19

7 Artin's Reciprocity Law **21**

7.1 Artin 符号 21

7.2 Artin 互反律 21

8 附录 I-galois **23**

参考文献 **24**

Wir müssen wissen. Wir werden wissen. ——-David Hilbert

Chapter 0

Preface

互反律在数论中具有深远的重要性，是理解许多数论问题的关键工具。它们不仅为判断二次、三次及更高次的同余方程的可解性提供了有效的手段，也为类域论和代数数论的发展奠定了基础。互反律的广泛应用不仅在数论本身，还在代数几何、模形式、表示论等领域得到了展现。它们为许多复杂问题的解决提供了基本框架，展现了数学中不同领域之间的深刻联系。

首先，二次互反律，尤其是高斯通过初等方法和高斯和给出的证明，揭示了模 p 的二次剩余性与模 q 的二次剩余性之间的深刻联系。这一律表明，在对称的情况下，同余方程的解的性质可以通过较小的素数来决定，从而极大地简化了数论问题的处理。

在更高次的背景下，分圆域提供了一种观察二次互反律的更高角度，进一步推进了对这些现象的理解。例如，通过类域论方法，二次互反律与域的扩张和群的表示之间的关系得到了更清晰的阐述。

除了二次互反律，三次和四次互反律等更高次的互反律也起到了重要作用。这些律为模高次幂的剩余性提供了准则，并且在代数数论中引入了更加复杂的结构。

Eisenstein, Kummer, Hilbert 和 Artin 的互反律 Eisenstein 和 Kummer 的互反律在推广二次互反律的基础上，处理了更高次幂的剩余性问题。Kummer 特别是在处理分圆域和高次方程方面做出了贡献。

Hilbert 的互反律更加系统化了这些概念，将其推广到一般数域中，并且引入了局部域和全局域的观念。这一律是现代类域论的重要组成部分，对代数数论中的很多重要结果奠定了基础。

Artin 的互反律则进一步将 Hilbert 的思想推广到伽罗瓦扩张的情形，确立了伽罗瓦群的表示与类域论之间的深刻联系。这一律不仅在理论上有极高的价值，而且在实际应用中也起到了关键作用。

本文主要是整理了一些重要的互反率，仅供参考

Chapter 1

Quadratic Reciprocity Law

Theorem 1.1 (Quadratic Reciprocity Law)**.** *Let $p, q \in \mathbb{N}$ be different odd primes; then*

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

Moreover, we have

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

these are called the first and the second supplementary law, respectively.

那么，什么是互反律呢？Euler 说的是，$a \bmod p$ 的二次特征仅取决于 $p \bmod 4a$ 的剩余类。对于 Legendre（他首先提出了“互反”这一术语）来说，互反律表明一个奇素数 p 是模另一个奇素数 q 的二次剩余，当且仅当 q 是模 p 的二次剩余，除非 $p \equiv q \equiv 3 \bmod 4$。更准确地说，Legendre 为奇素数 q 定义了一个符号 (p/q)，取值在 $\{-1, +1\}$ 中，要求 $(p/q) \equiv p^{(q-1)/2} \bmod q$。高斯把二次互反律誉为算术理论中的宝石这里不再介绍 Legendre 符号下面围绕四种证明感受二次互反率的美妙

1.1 Gauss lemma——初等方法

我们先给出广为人知的证明方法，大部分初等数论书都是这样证明的

Lemma 1.2 (Gauss)**.** *设 p 为奇素数，则设 $1 \cdot a, 2 \cdot a, \cdots, \frac{p-1}{2} \cdot a$ 除以 p 的余数落在 $\{\frac{p+1}{2}, \cdots, p-1\}$ 中的次数为 m，则 $\left(\frac{a}{p}\right) = (-1)^m$.*

对于 $k = 1, 2, \cdots, \frac{p-1}{2}$，设 $ka \equiv r_k \mod p$ $(1 \le r_k \le p-1)$

并且令 $s_k = \begin{cases} r_k, & r_k < \frac{p}{2} \\ p - r_k, & r_k > \frac{p}{2} \end{cases}$ 对于 $\forall k, l \in \{1, 2, \cdots, \frac{p-1}{2}\}$，由于 $1 < k + l \le p - 1$，

因此 $(k+l,p)=1$, 因此 $a(k+l)\neq 0 \mod p$, 因此我们容易得到：$\{s_1,s_2,\cdots,s_{\frac{p-1}{2}}\}=\{1,2,\cdots,\frac{p-1}{2}\}$
于是 $s_1s_2\cdots s_{\frac{p-1}{2}}=(\frac{p-1}{2})!$
因此 $(1\cdot a)(2\cdot a)\cdots(\frac{p-1}{2}\cdot a)=(\frac{p-1}{2})!a^{\frac{p-1}{2}}\equiv\left(\frac{a}{p}\right)(\frac{p-1}{2})! \mod p$

与此同时 $(1\cdot a)(2\cdot a)\cdots(\frac{p-1}{2}\cdot a)\equiv r_1r_2\cdots r_{\frac{p-1}{2}}=(-1)^m s_1s_2\cdots s_{\frac{p-1}{2}}=(-1)^m(\frac{p-1}{2})! \mod p$
于是我们就得到：$\left(\frac{a}{p}\right)=(-1)^m$

回到二次互反律的证明（需要用到三角函数的倍角公式）
$\frac{\sin 2\pi qx}{\sin 2\pi x}=(-4)^{\frac{q-1}{2}}\prod\limits_{i=1}^{\frac{q-1}{2}}(\sin^2 2\pi x-\sin^2 2\pi\frac{l}{q})$
（补充一个引理：

Lemma 1.3.

$$\frac{f(qz)}{f(z)}=\prod_{k=1}^{\frac{q-1}{2}}f(z+\frac{k}{q})\prod_{k=\frac{q+1}{2}}^{q}f(z-\frac{q-k}{q})=\prod_{k=1}^{\frac{q-1}{2}}f(z+\frac{k}{q})f(z-\frac{k}{q}) \tag{1.1}$$

证明. 假设 $f(x)=e^{2\pi ix}-e^{-2\pi ix}$, $\zeta=e^{\frac{2\pi i}{n}}$. 由于恒等式 $x^q-y^q=\prod\limits_{k=0}^{q-1}(x-\zeta^k y)$

由于 q 为奇素数，因此 $-2,-4,\cdots,-2(q-1)$ 构成了模 q 的一组完全剩余系，于是

$$x^q-y^q=\prod_{k=1}^{q-1}(x-\zeta^{-2k}y) \tag{1.2}$$

$$=\zeta^{(-1-2-\cdots-(q-1))}\prod_{k=1}^{q-1}(\zeta^k x-\zeta^{-k}y) \tag{1.3}$$

$$=\prod_{k=1}^{q-1}(\zeta^k x-\zeta^{-k}y) \tag{1.4}$$

于是，令 $x=e^{2\pi ix}$, $y=e^{-2\pi ix}$ 得到：$f(qz)=\prod\limits_{k=0}^{q-1}f(z+\frac{k}{q})$
注意到 $f(z+\frac{k}{q})=f(z+\frac{k}{q}-1)=f(z-\frac{q-k}{q})$, 于是

代入得证 □

由于 $\prod\limits_{k=1}^{\frac{p-1}{2}}\sin 2\pi\frac{ka}{p}=\prod\limits_{k=1}^{\frac{p-1}{2}}\sin 2\pi\frac{r_k}{p}=(-1)^m\prod\limits_{k=1}^{\frac{p-1}{2}}\sin 2\pi\frac{s_k}{p}=\left(\frac{a}{p}\right)\prod\limits_{k=1}^{\frac{p-1}{2}}\sin 2\pi\frac{k}{p}$

于是令 $a=q$ 得

$$\left(\frac{q}{p}\right)=\frac{\prod\limits_{k=1}^{\frac{p-1}{2}}\sin 2\pi\frac{kq}{p}}{\prod\limits_{k=1}^{\frac{p-1}{2}}\sin 2\pi\frac{k}{p}}=(-4)^{\frac{p-1}{2}\frac{q-1}{2}}\prod_{k=1}^{\frac{p-1}{2}}\prod_{l=1}^{\frac{q-1}{2}}(\sin^2\frac{k}{p}-\sin^2\frac{l}{q}) \tag{1.5}$$

$$=(-4)^{\frac{p-1}{2}\frac{q-1}{2}}(-1)^{\frac{p-1}{2}\frac{q-1}{2}}\prod_{k=1}^{\frac{q-1}{2}}\prod_{l=1}^{\frac{p-1}{2}}(\sin^2\frac{l}{q}-\sin^2\frac{k}{p})=(-1)^{\frac{p-1}{2}\frac{q-1}{2}}\left(\frac{p}{q}\right) \tag{1.6}$$

（注：上面的恒等变换利用了 $\prod\limits_{k=1}^{\frac{p-1}{2}}\prod\limits_{l=1}^{\frac{q-1}{2}}(\sin^2\frac{k}{p}-\sin^2\frac{l}{q})$ 关于 p,q 的对称性）

总结：除了最后处理用了对称性，整个证明非常奇怪，下面给出更好的理解

1.2 高斯和

假设 p 为奇素数，p 次单位根 $\zeta_p=e^{\frac{2\pi i}{p}}$，则定义 Gauss 和为：$g=\sum\limits_{k=0}^{p-1}\left(\frac{k}{p}\right)\zeta_p^k\in\mathbb{Z}[\zeta_p]\subset\mathbb{Q}(\zeta_p)$

我们首先需要证明引理：$g^2=\left(\frac{-1}{p}\right)p.$

证明. $g^2=\sum\limits_{0\le x,y\le p}\left(\frac{xy}{p}\right)\zeta_p^{x+y}=\sum\limits_{0\le x,y\le p}\left(\frac{z}{p}\right)\zeta_p^{y(z+1)}=\sum\limits_{z=0}^{p}\left(\frac{z}{p}\right)\sum\limits_{y=0}^{p}\zeta_p^{y(z+1)}$

注意到 $\sum\limits_{y\in\mathbb{F}_p^\times}\zeta_p^{y(z+1)}=\begin{cases}p, p\mid z+1\\ 0, p\nmid z+1\end{cases}$

因此 $g^2=\left(\frac{-1}{p}\right)p.$ □

下面我们利用这一结论来证明二次互反律。假设 q 是一个与 p 不等的奇素数，下用两种不同的方法来计算 g^q 的值：

$$g^q=(g^2)^{\frac{q-1}{2}}\cdot g=(\left(\frac{-1}{p}\right)p)^{\frac{q-1}{2}}g \tag{1.7}$$

$$=(-1)^{\frac{p-1}{2}\frac{q-1}{2}}p^{\frac{q-1}{2}}g\equiv(-1)^{\frac{p-1}{2}\frac{q-1}{2}}\left(\frac{p}{q}\right)g \mod q \tag{1.8}$$

1.3 分圆域——更高角度

我们考虑 $p^*=(-1)^{\frac{p-1}{2}}p$ 利用 Gauss 和的方法我们可以证明 $\tau=\sqrt{p^*}\in\mathbb{Q}(\zeta_p)$.

Wir müssen wissen. Wir werden wissen. ——-David Hilbert

设 q 是一个与 p 互异的奇素数，考虑同构 $\sigma_q:\zeta_p\to\zeta_p^q$，由于 $\mathbb{Q}(\tau)$ 被 $\mathbb{Q}(\zeta_p)$ 的 Galois 群 G 的指数为 2 的子群 H 所固定，因此当 $\sigma_q\in H$ 时，$\sigma_q(\tau)=\tau$，当 $\sigma_q\notin H$ 时，$\sigma_q(\tau)=-\tau$.

注意到 $G\simeq U(\mathbb{Z}/p\mathbb{Z})$ 因此当且仅当 q 为模 p 的二次剩余时，$\sigma_q\in H$，即有 $\sigma_q(\tau)=\left(\frac{q}{p}\right)\tau$

另一方面，设 Q 是一个包含 q 的素理想，则根据性质 2.6 得 $\sigma_q(\tau)\equiv\tau^q \pmod Q$

于是 $\left(\frac{q}{p}\right)\equiv\tau^{q-1}=(p^*)^{\frac{q-1}{2}}\equiv\left(\frac{p^*}{q}\right)=(-1)^{\frac{p-1}{2}\frac{q-1}{2}}\left(\frac{p}{q}\right) \pmod Q$

于是就得到了 $\left(\frac{q}{p}\right)=(-1)^{\frac{p-1}{2}\frac{q-1}{2}}\left(\frac{p}{q}\right)$

1.4 类域论的证明

Theorem 1.4. *设 m,N 如上，且 p 为素数. (1) p 在 $\mathbb{Q}(\sqrt{m})$ 中分歧 $\Leftrightarrow p|N$. (2) 当 p 不除尽 N 时，在 $\mathbb{Q}(\sqrt{m})$ 的整数环中 $\chi_m(p)=1\Leftrightarrow(p)$ 为相异的两个素数的乘积 $\chi_m(p)=-1\Leftrightarrow(p)$ 为素理想.*

Lemma 1.5. *设 L 为一个二次域, L=$Q(\sqrt{m})$, 其中m 为不被1 以外的平方数除尽的整数. 又设p 为不除尽m 的奇素数. 于是在$\mathbb{Q}(\sqrt{m})$ 中有*
$\left(\frac{m}{p}\right)=1\Longleftrightarrow(p)$ 为两个相异的素数的乘识,
$\left(\frac{m}{p}\right)=-1\Longleftrightarrow(p)$ 为素理想.

证明. 令L=Q($\sqrt{m}$). 根据交换代数的理论知,
O_L 中包含了p 的素理想$\overset{1:1}{\to}O_L/pO_L$ 的素理想 O_L/pO_L 的方式来研究在 O_L 中 p 的分解情形. 因为 O_L 或者等于 $\mathbb{Z}[\sqrt{m}]$ 或者等于 $\mathbb{Z}\left[\frac{1}{+}\sqrt{m}2\right]$, 故商群 $O_L/\mathbb{Z}[\sqrt{m}]$ 的阶数或为 1 或为 2. 由此以及 p 为奇数的事实，我们得到

$$O_L/pO_L\cong\mathbb{Z}[\sqrt{m}]/p\mathbb{Z}[\sqrt{m}].$$

$$O_L/pO_L\cong\mathbb{F}_p[x]/(x^2-m).$$

因为 $\mathbb{Z}[\sqrt{m}]\cong\mathbb{Z}[x]/(x^2-m)$, 则 $\left(\frac{m}{p}\right)=-1$ 的情形. 因为在 $\mathbb{F}_p$ 中没有 m 的平方根，故 x^2-m 在 $\mathbb{F}_p$ 上为不可约，从而 $\mathbb{F}_p[x]/(x^2-m)$ 为域. 因此 O_L/pO_L 为域，从而 pO_L 为素理想 $\left(\frac{m}{n}\right)=1$ 的情形. 取使 $a^2-m\equiv 0 \bmod p$ 的 $a\in\mathbb{Z}$, 于是在 $\mathbb{F}_p$ 上 $x^2-m=(x-a)(x+a)$, 故 $\mathbb{F}_p[x]/(x^2-m)$ 具有两个素理想 $(x-a)$ 和 $(x+a)$. 因此在 O_L 中存在两个包含 p 的素理想.(从而，它们是 $(p,\sqrt{m}-a)$ 与 $(p,\sqrt{m}+a)$.) 令这些素理想为 $\boldsymbol{p},\boldsymbol{q}$, 因为 (p) 被 $\boldsymbol{p},\boldsymbol{q}$ 除尽，故 $\boldsymbol{pq}\supset(p)$. 另一方面，由于 $(x-a)(x+a)$ 在 $\mathbb{F}_p[x]/(x^2-m)$ 中等于 0, 故 $\boldsymbol{pq}\subset(p)$, 从而 $(p)=\boldsymbol{pq}$.

□

由定理并使用引理可以按下面的方式推导出二次剩余的互反律. 设 m,N 如在小节中所设. 当取 p 为不能除尽 m 的奇素数时，根据引理我们有 p 在 $\mathbb{Q}(\sqrt{m})$ 中完全分解

$\Leftrightarrow \left(\frac{m}{p}\right) = 1$. 另一方面，定理说的是 (5.5) p 在 $\mathbb{Q}(\sqrt{m})$ 中完全分解 $\Leftrightarrow p \bmod N$ 属于 $\chi_m : (\mathbb{Z}/N\mathbb{Z})^\times \to \{\pm 1\}$ 的核得到了

$$\left(\frac{m}{p}\right) = \chi_m(p).$$

在中将 m 取为不同于 p 的奇素数 q, 按照 χ_q 的定义我们有 $\chi_q(p) = \left(\frac{p}{a}\right) = \theta_q(p) = \left(\frac{p}{q}\right)(-1)^{\frac{p-1}{2}\frac{q-1}{2}}$, 故而得到了二次剩余的互反律

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

Wir müssen wissen. Wir werden wissen. ——-David Hilbert

Chapter 2

三、四次互反率

三次之前讨论班做过了，四次是类似的，放在最后有时间处理

2.1 Cubic Reciprocity Law

etc

2.2 Quartic Reciprocity Law

Theorem 2.1. *Quartic Reciprocity Law Let*$\pi, \lambda \in \mathbb{Z}[i]$ *be different primary primes, i.e assume that* $\pi \equiv \lambda \equiv 1$ *mod* $(2+2i)$; *then*

$$\left[\frac{\pi}{\lambda}\right] = (-1)^{\frac{N\pi-1}{4} \cdot \frac{N\lambda-1}{4}} \left[\frac{\lambda}{\pi}\right].$$

etc

Chapter 3

Eisenstein's Reciprocity Law

Theorem 3.1 (Eisenstein's Reciprocity Law)**.** *Let ℓ be an odd prime and suppose that $\alpha \in \mathbb{Z}[\zeta_\ell]$ is primary,i.e. congruent to a rational integer modulo $(1-\zeta_\ell)^2$.*

Then

$$\left(\frac{\alpha}{a}\right)_\ell = \left(\frac{a}{\alpha}\right)_\ell$$

for all integers $a \in \mathbb{Z}$ prime to ℓ .

介绍一下历史背景，爱森斯坦是 19 世纪数学家，他和高斯有过交流，高斯对他评价很高，亲自为其论文集做序，称之为未来可以成为像牛顿那样的人物，不过后来在 29 岁英年早逝。

爱森斯坦的主要研究方向是高次互反律，椭圆函数，他是第一个发表三次，4 次互反律证明的人。同时也在椭圆函数课上当过黎曼的老师。爱森斯坦最著名的成就之一就是爱森斯坦互反律。它是高斯的二次互反律，以及三次互反律，四次互反律的推广形态。我们这里将给出证明。

我们这里给出的证明不同于爱森斯坦的证明，实际上是绝大部分书上的证明，因为它依赖于一个很强的定理，The Stickelberger Relation，但这是一个相对比较简洁的证明。

3.1 m 次剩余符号的定义及其性质

3.1.1 m 次剩余符号

在介绍二次互反律的时候，我们引入了二次剩余符号 $\left(\frac{\cdot}{p}\right)$ 。现在我们试图将其推广到 m 次剩余符号。在分圆域 $K=\mathbb{Q}(\zeta_m)$ 中考虑问题，于是对于 K 的代数整数环 D_m 上的任一不包含 m 的素理想 P 来说，记其范数 $q=N(P)=|D_m/P|$ ，于是根据我们之前对分圆域的讨论，得知 $1,\zeta_m,\zeta_m^2,\cdots,\zeta_m^{m-1}$ 在 D_m/P 中属于互不相同的陪集，并且 $q\equiv 1 \pmod m$ 。

我们可以证明，对于任一 $\alpha \in D_m$ 且 $\alpha \notin P$ ，都能找到一个 m 次单位根，使得其与 $\alpha^{\frac{q-1}{m}}$ 在 D_m/P 中属于同一个陪集。

Proposition 3.2. *设 $\alpha \in D_m$ 且 $\alpha \notin P$ ，则存在唯一的 $i \in \mathbb{Z}/m\mathbb{Z}$ 使得*

$$\alpha^{\frac{q-1}{m}} \equiv \zeta_m^i \pmod P.$$

证明. 由于 $|D_m/P| = q$ ，于是对任一 $\alpha \notin P$ 有 $\alpha^q \equiv 1 \pmod P$ 。于是

$$\prod_{i=1}^{m}(\alpha^{\frac{q-1}{m}} - \zeta_i) \equiv 0 \pmod P.$$

由于 P 是素理想，于是存在一个唯一的整数 i ，使得 $\alpha^{\frac{q-1}{m}} \equiv \zeta_m^i \pmod P$ 。 □

Definition 3.3. 对于 $\alpha \in D_m$ 以及一个不包含 m 的素理想 P，定义 m 次剩余符号 $\left(\frac{\alpha}{P}\right)_m$ 为

$$\left(\frac{\alpha}{P}\right)_m = \begin{cases} 0, & \text{如果}\alpha \in P, \\ \zeta_m^i, & \text{满足}\zeta_m^i \equiv \alpha^{\frac{N(P)-1}{m}} \pmod P. \end{cases}$$

显然，m 次剩余符号继承了许多二次剩余符号的性质。

Proposition 3.4. *1. $\left(\frac{\alpha}{P}\right)_m = 1$ 等价于 $x^m \equiv \alpha \pmod P$ 在 D_m 内有解;*

2. $\left(\frac{\alpha\beta}{P}\right)_m = \left(\frac{\alpha}{P}\right)_m \left(\frac{\beta}{P}\right)_m$;

3. 若 $\alpha \equiv \beta \pmod P$ ，则 $\left(\frac{\alpha}{P}\right)_m = \left(\frac{\beta}{P}\right)_m$ 。

类似于将 Legendre 符号推广为 Jacobi 符号，我们可以在任一理想的剩余类域中引入 m 次剩余符号：设 $A \subset D_m$ 是一个与 m 互素的理想，设 $A = P_1P_2\cdots P_g$ 为 A 的素理想分解，则定义

$$\left(\frac{\alpha}{A}\right)_m = \left(\frac{\alpha}{P_1}\right)_m \left(\frac{\alpha}{P_2}\right)_m \cdots \left(\frac{\alpha}{P_g}\right)_m.$$

3.1.2 高斯和

有了 m 次剩余符号的定义，在代数整数环 D_m 上我们可以定义特征标 $\chi_P = \left(\frac{\cdot}{P}\right)_m$ ，进而可以引入高斯和：给定素数 $p \nmid m$ 以及 (p) 的一个素理想因子 P，我们可以定义如下的高斯和

$$g(P) = \sum_{\alpha \in D_m/P} \overline{\chi_P(\alpha)} \zeta_p^{\mathrm{tr}(\alpha)},$$

其中 $\mathrm{tr}(\alpha) = \alpha + \alpha^p + \cdots + \alpha^{p^{f-1}}$ （f 为 p 的剩余类域指数）。

这里稍微解释一下为什么 $\mathrm{tr}(\alpha)$ 可以写到指数上去：由于 $\mathrm{tr}(\alpha)^p = \alpha^p + \alpha^{p^2} + \cdots + \alpha^{p^n} = \alpha + \alpha^p + \cdots + \alpha^{p^{n-1}} = \mathrm{tr}(\alpha)$ ，于是 $\mathrm{tr}(\alpha)$ 属于某个 p 元有限域（与 $\mathbb{Z}/p\mathbb{Z}$ 同构），因此 $\mathrm{tr}(\alpha) \in \mathbb{Z}/p\mathbb{Z}$ 。

显然我们可以知道 $g(P) \in \mathbb{Q}(\zeta_m, \zeta_p)$ ，同时 $g(P)$ 还满足以下性质：

Proposition 3.5. *1.* $|g(P)|^2 = p^f$ *;*

2. 记 $\Phi(P) = g(P)^m$ ，则 $\Phi(P) \in \mathbb{Q}(\zeta_m)$ 。

3.1.3 m 次互反律的介绍

与介绍三次、四次互反律的时候相同，我们在讨论 m 次互反律的时候也需要讨论合规元素的概念。先讨论 m 为奇素数 l 的情形。在 D_l 中的合规元素定义如下：若 α 不是单位元，与 l 互素，并且满足 $\alpha \equiv n \pmod{(1-\zeta_l)^2} (n \in \mathbb{Z})$ ，则称 α 为合规元素。

下面我们就可以介绍艾森斯坦 m 次互反律了：

Theorem 3.6. 设 l 是一个奇素数，$a \in \mathbb{Z}$ 与 l 互素，而 $\alpha \in D_l$ 是一个合规元并与 a 互素，则

$$\left(\frac{\alpha}{a}\right)_l = \left(\frac{a}{\alpha}\right)_l.$$

定理的证明我们将在第三节讨论。

3.2 Stickelberger 关系

3.2.1 域自同构在元素和理想上的作用

假设域扩张 $\mathbb{Q}(\zeta_m)/\mathbb{Q}$ 的 Galois 群为 G ，则对于任一 $\sigma \in G$ 以及 $\alpha \in \mathbb{Q}(\zeta_m)$ ，我们将 $\sigma(\alpha)$ 写成 α^σ 。类似的，若 A 是一个理想，则我们将 $\sigma(A)$ 写成 A^σ 。我们将证明，这些写在指数项的自同构对于 m 次剩余符号具有如下性质：

Proposition 3.7. 设 A 是一个与 m 互素的理想，则

$$\left(\frac{\alpha}{A}\right)_m^\sigma = \left(\frac{\alpha^\sigma}{A^\sigma}\right)_m.$$

证明. 由于 m 次剩余符号的可乘性以及素理想唯一分解定理，显然只需证明对于素理想 P ，有

$$\left(\frac{\alpha}{P}\right)_m^\sigma = \left(\frac{\alpha^\sigma}{P^\sigma}\right)_m.$$

这是由于范数的性质：显然 $N(P) = N(P^\sigma)$ 。另一方面，由于 m 次剩余符号的定义，对 P 有

$$\left(\frac{\alpha}{P}\right)_m^\sigma = (\zeta_m^i)^\sigma = \zeta_m^{i\sigma}.$$

而由于 ζ_m^σ 仍然是某个 m 次单位根，因此假设 $\zeta_m^\sigma = \zeta_m^j$ ，于是

$$\left(\frac{\alpha^\sigma}{P^\sigma}\right)_m = \zeta_m^j.$$

显然由于自同构的定义，$i=j$ ，从而有

$$\left(\frac{\alpha}{P}\right)_m^{\sigma}=\left(\frac{\alpha^{\sigma}}{P^{\sigma}}\right)_m.$$

□

3.2.2 Stickelberger 关系

由于 D_m 不一定是唯一分解整环，因此 $\Phi(P)$ 不一定能够唯一分解为不可约元的乘积。但是我们对于 $\Phi(P)$ 生成的主理想有如下美妙的结果：

Theorem 3.8 (Stickelberger 关系)**.** 设 P 是 D_m 的一个不包含 m 的素理想，则

$$(\Phi(P))=P^{\sum\limits_t t\sigma_t^{-1}},$$

其中上述的求和是对于所有与 m 互素且小于 m 的自然数进行。

3.3 Eisenstein 互反律的证明

首先根据 m 次剩余符号的可乘性，我们可以假设 $a=q\in\mathbb{Z}$ 是一个素数，其剩余类域指数为 ν。设 (α) 在 D_m 中的素理想分解为 $(\alpha)=P_1P_2\cdots P_g$。

Step 1. 我们考虑 $g(P_i)$ 的 q^{ν} 次方的两种计算方法（下面的 Q 是 (q) 的一个素理想因子）：

方法一：

$$g(P_i)^{q^{\nu}}=\left(g(P_i)^l\right)^{\frac{q^{\nu}-1}{l}}g(P_i)\equiv\left(\frac{g(P_i)^l}{Q}\right)_l g(P_i)\pmod Q$$

方法二：

$$g(P_i)^{q^{\nu}}\equiv\sum_{\beta}\chi_{P_i}(\beta)\zeta_{p_i}^{\mathrm{tr}(\beta)q^{\nu}}\equiv\left(\frac{q^{\nu}}{P_i}\right)_l g(P_i)\pmod Q$$

于是我们综合以上两种方法得到

$$\left(\frac{g(P_i)^l}{Q}\right)_l=\left(\frac{q^{\nu}}{P_i}\right)_l$$

□

Step 2. 令 $\mu=g(P_1)^lg(P_2)^l\cdots g(P_g)^l$，则根据 Stickelberger 关系可得

$$(g(P_i)^l)=P_i^{\sum\limits_{t=1}^{l-1}t\sigma_t^{-1}}$$

于是

$$(\mu) = (P_1P_2\cdots P_g)^{\sum\limits_{t=1}^{l-1} t\sigma_t^{-1}} = (\alpha^{\sum\limits_{t=1}^{l-1} t\sigma_t^{-1}})$$

于是我们可以推出 $\mu = \varepsilon \cdot \alpha^{\sum\limits_{t=1}^{l-1} t\sigma_t^{-1}}$，其中 ε 为单位根。进一步地，我们可以证明 $\varepsilon = \pm 1$。 □

Step 3. 我们来计算

$$\left(\frac{\mu}{Q}\right)_l = \left(\frac{\alpha^{\sum\limits_{t=1}^{l-1} t\sigma_t^{-1}}}{Q}\right)_l = \prod_{t=1}^{l-1}\left(\frac{\sigma_t^{-1}(\alpha)}{Q}\right)_l^t = \prod_{t=1}^{l-1}\left(\frac{\sigma_t^{-1}(\alpha)}{Q}\right)_l^{\sigma_t} \tag{3.1}$$

$$= \prod_{t=1}^{l-1}\left(\frac{\alpha}{\sigma_t(Q)}\right)_l = \left(\frac{\alpha}{N(Q)}\right)_l = \left(\frac{\alpha}{q}\right)_l^{\nu} \tag{3.2}$$

另一方面，根据 Step 1 中的结果得到

$$\left(\frac{\mu}{Q}\right)_l = \prod_{i=1}^{g}\left(\frac{g(P_i)^l}{Q}\right)_l = \prod_{i=1}^{g}\left(\frac{q^\nu}{P_i}\right)_l = \left(\frac{q^\nu}{\alpha}\right)_l = \left(\frac{q}{\alpha}\right)_l^{\nu}$$

进而结合 $\nu \equiv 1 \mod l$ 得到

$$\left(\frac{q}{\alpha}\right)_l = \left(\frac{\alpha}{q}\right)_l$$

□

Chapter 4

Kummer's Reciprocity Law

Chapter 5

Hasse’ s Reciprocity law

Chapter 6

Hilbert's Reciprocity Law

Theorem 6.1 (Hilbert's Reciprocity Law)**.** *设 $a, b \in \mathbb{Q}^\times$ 于是，除去有限个 v 外 $(a,b)_v$ 都等于 1, 且*

$$\prod_v (a,b)_v = 1.$$

在这个积中，v 遍历 ∞ 及所有的素数.

6.1 Local

Definition 6.2. 对素数 p 与 $a, b \in \mathbb{Q}^\times$, 我们来定义 Hilbert 符号 $(a,b)_p$. 记

$$a = p^i u,\ b = p^j v \quad (i, j \in \mathbb{Z},\ u, v \in (\mathbb{Z}_{(p)})^\times),$$

令 $r = (-1)^{ij} a^j b^{-i} = (-1)^{ij} u^j v^{-i} \in (\mathbb{Z}_{(p)})^\times$. 令 $(a,b)_p = \left(\frac{r \mod p}{p}\right)$

$$\text{(a,b)}_\infty = \begin{cases} 1 & a > 0\text{或}b > 0 \\ \\ -1 & a < 0\text{且}b < 0. \end{cases}$$

Proposition 6.3. *1. $(a,b)_v = (b,a)_v$。*

2. $(a,bc)_v = (a,b)_v(a,c)_v$。

3. $(a,-a)_v = 1$。若 $a \neq 1$，则 $(a, 1-a)_v = 1$。

4. 设 p 为奇素数，$a, b \in (\mathbb{Z}_{(p)})^\times$，于是成立：

(a) $(a,b)_p = 1$。

(b) $(a,pb)_p = \left(\frac{a \mod p}{p}\right)$。

5. 设 $a, b \in \mathbb{Z}_{(2)}^\times$，则成立：

$$\text{(a)}\ (a,b)_2 = \begin{cases} 1 & \text{如果} a \equiv 1 \pmod 4 \text{ 或} b \equiv 1 \pmod 4 \\ -1 & \text{如果} a \equiv b \equiv -1 \pmod 4 \end{cases}。$$

$$\text{(b)}\ (a,2b)_2 = \begin{cases} 1 & \text{如果} a \equiv 1 \pmod 8 \text{ 或} a \equiv 1-2b \pmod 8 \\ -1 & \text{其他情形} \end{cases}。$$

6.2 global

证明. 定理 6.1

对于 $(a,b)_v$ 在除去有限个 v 外都为 1 这个论断，可根据除去有限个素数 p 外都有 $a,b \in (\mathbb{Z}_{(p)})^\times$ 这个事实得到. 对于遍历所有 v 的那个积为 1 的论断，根据命题 2.4(1),(2),(3)(考虑 a,b 的素因子分解), 若能对下面的 (i)—(iii) 情形得到证明即可. (i)a,b 为相异的奇素数. (ii)a 为奇素数，b 为-1 或 2. (iii)$a=-1$, b 为-1 或 2

(i) 的情形. 根据 Proposition 6.3 有

$$(a,b)_v = \begin{cases} \left(\dfrac{b}{a}\right) & v = a \\ \left(\dfrac{a}{b}\right) & v = b \\ (-1)^{\frac{a-1}{2}\frac{b-1}{2}} & v = 2 \\ 1 & \text{其他的 } v, \end{cases}$$

结果 $\prod_v (a,b)_v = 1$ 不是别的，正是二次剩余的互反律 (定理 2.2(1)).

(ii) 的情形

$$(a,-1)_v = \begin{cases} \left(\dfrac{-1}{a}\right) & v = a \\ (-1)^{\frac{a-1}{2}} & v = 2 \\ 1 & \text{其他的 } v, \end{cases}$$

$$(a,2)_v = \begin{cases} \left(\dfrac{2}{a}\right) & v = a \\ (-1)^{\frac{a^2-1}{8}} & v = 2 \\ 1 & \text{其他的 } v, \end{cases}$$

于是 ,$\prod_v (a,b)_v = 1$ (iii) 的情形. 由计算一看就明白了:

$$(-1,-1)_v = \begin{cases} -1 & v \text{为 } 2 \text{ 或} \infty \\ 1 & \text{其他的 } v \end{cases}$$

$(-1,2)_v = 1$ 所有的 v.

Wir müssen wissen. Wir werden wissen. ——-David Hilbert

注：将二次剩余的互反律改成定理 6.1 的形式时 (由 Hilbert) , 就看出二次剩余的互反律表现了“实数的威力”与“素数的威力”的协调性

□

Exercise 6.4. 设 p 为素数. (1) 存在 $x, y \in \mathbb{Q}$ 使得 $p = x^2 + y^2$ 的充要条件是 $p \equiv 1 \mod 4$ 或者 $p = 2$.
(2) 存在 $x, y \in \mathbb{Q}$ 使得 $p = x^2 + 5y^2$ 的充要条件是 $p \equiv 1$ 或 $9 \mod 20$ 或者 $p = 5$.
(3) 存在 $x, y \in \mathbb{Q}$ 使得 $p = x^2 + 26y^2$ 的充要条件是 $p \equiv 1$ 或 $3 \mod 8$ 并且 $p \equiv (1, 3, 4, 9, 10, 12$ 中的一个$) \mod 13$.

Chapter 7

Artin's Reciprocity Law

阿廷的互反律是代数数论中的一个基础结果，构成了类域论的核心。它推广了二次互反律和其他更高次的互反律。本讲座旨在介绍阿廷互反律的基本思想和陈述，并结合一些例子和应用进行说明。

在陈述阿廷的互反律之前，我们需要介绍一些基本概念和符号。

设 K 是一个数域，即有理数域 $\mathbb{Q}$ 的有限扩张。K 的整数环，记作 $\mathcal{O}_K$，是 K 中所有满足整系数首一多项式的根的元素的集合。

在 $\mathcal{O}_K$ 中的一个理想 $\mathfrak{a}$ 是 $\mathcal{O}_K$ 的一个子集，它满足加法和被 $\mathcal{O}_K$ 元素乘法的封闭性等特定性质。K 的理想类群 $Cl(K)$ 是分式理想对主理想的商集。

7.1 Artin 符号

阿廷符号 $\left(\frac{L/K}{\mathfrak{p}}\right)$ 是阿廷互反律中的一个核心对象。它定义在伽罗瓦扩张 L/K 和 K 的素理想 $\mathfrak{p}$ 上，而 $\mathfrak{p}$ 在 L 中不分歧。

Definition 7.1 (阿廷符号)**.** 设 L/K 是伽罗瓦数域扩张，伽罗瓦群为 $\mathrm{Gal}(L/K)$。对于 $\mathcal{O}_K$ 的素理想 $\mathfrak{p}$，若在 L 中不分歧，则阿廷符号 $\left(\frac{L/K}{\mathfrak{p}}\right)$ 是 L 的一个自同构，它将每个最小多项式的根模 $\mathfrak{p}$ 映射到其 Frobenius 共轭。

7.2 Artin 互反律

阿廷的互反律将阿廷符号与数域的理想类群联系起来。

Theorem 7.2 (阿廷的互反律)**.** 设 L/K 是有限阿贝尔数域扩张。则存在一个同态

$$\phi : Cl(K) \to Gal(L/K)$$

使得对于 K 的每个在 L 中不分歧的素理想 $\mathfrak{p}$，其理想类在 ϕ 下的像是阿廷符号 $\left(\frac{L/K}{\mathfrak{p}}\right)$。

证明. □

Example 7.3. 阿廷互反律最简单的例子之一是二次互反律，它可以看作是 $K = \mathbb{Q}$ 和 $L = \mathbb{Q}(\sqrt{d})$ 的特例。

Artin 互反律是现代数论的基石之一。它在数域的算术与伽罗瓦群理论之间提供了深刻的联系。进一步研究这一领域将引向更广泛的类域论。

Chapter 8

附录 I-galois

etc

参考文献

[1] *Gtm7*

[2] *GTM84*

[3] *GTM228*

[4] 数论 *I–Fermat* 的梦想和类域论