J.-P.塞尔 著

冯克勤 译 丁石孙 校

数论教程

上海科学技术出版社

数 论 教 程

J.-P. 塞尔 著

冯克勤 译

丁石孙 校

上海科学技术出版社

A Course in Arithmetic
J.- P. Serre
Springer-Verlag New York Inc. 1973.

数 论 教 程

J.- P. 塞尔 著
冯克勤 译
丁石孙 校
上海科学技术出版社出版
(上海瑞金二路 450 号)
新华书店上海发行所发行 上海市印刷四厂印刷
开本 787×1092 1/32 印张 5 125 字数 110,000
1980 年 11 月第 1 版 1980 年 11 月第 1 次印刷
印数 1—6,500

书号: 13119·873 定价: (科四) 0.50 元

前　言

本书分两部分.

第一部分是纯代数的. 它的目标是有理数域上二次型的分类(Hasse-Minkowski 定理), 这工作在第四章完成. 前三章叙述某些预备知识: 二次互反律, p-adic 域, Hilbert 符号. 第五章是将上述结果用于判别式为 ± 1 的整二次型. 这种二次型出现在模函数、微分拓扑和有限群等各种问题中.

第二部分(第六章和第七章)采用"解析"方法(全纯函数). 第六章给出 Dirichlet "算术级数中的素数定理"的证明; 在前一部分(第三章 § 2.2)的一个关键地方曾经用过这一定理. 第七章处理模形式, 特别是 Theta 函数. 这里再次出现第五章中的某些二次型.

这两部分的材料来源于 1962 年和 1964 年国立高等学校(Ecole Normale Supérieure)大学二年级讲义. J.-J. Sansuc (第一到四章) 和 J.-P. Ramis 与 G. Ruget(第六、七章)将这些讲义作了修订, 写成了笔记. 这些笔记对我是很有益处的, 在这里我谨向这些笔记的作者表示谢意.

J.-P. 塞尔

目　录

第二部分　解析方法

第一部分

代数方法

第一章 有限域

下面所考虑的域全是可交换的.

§1. 一般结果

1.1. 有限域

设 K 是一个域, $\mathbf{Z}$ 在 K 中的象是一个整环, 从而同构于 $\mathbf{Z}$ 或者 $\mathbf{Z}/p\mathbf{Z}$, 其中 p 为素数; 它的商域同构于 $\mathbf{Q}$ 或者

$$\mathbf{Z}/p\mathbf{Z}=\mathbf{F}_p.$$

在第一种情形下, 称 K 为特征零域; 在第二种情形下, 称 K 为特征 p 域.

K 的特征记成 $\mathrm{char}(K)$. 如果 $\mathrm{char}(K)=p\neq 0$, 那末 p 也是满足 $n\cdot 1=0$ 的最小正整数 n.

引理 如果 $\mathrm{char}(K)=p$, 则映射 $\sigma: x\mapsto x^p$ 是 K 到其子域 K^p 上的同构.

证 我们有 $\sigma(xy)=\sigma(x)\sigma(y)$. 进而, 如果 $0<k<p$, 则二项式系数 $\binom{p}{k}\equiv 0(\mathrm{mod}\,p)$. 由此得到

$$\sigma(x+y)=\sigma(x)+\sigma(y);$$

从而 σ 是一个同态. 此外, σ 显然是单射.

定理 1 i) 有限域 K 的特征是素数 $p\neq 0$. 如果

$$f=[K:\mathbf{F}_p],$$

则 K 的元素个数为 $q=p^f$.

ii) 设 p 为素数, 且 $q=p^f(f\geqslant 1)$ 为 p 的方幂. 令 Ω 为特

征 p 的代数封闭域. 则 Ω 存在唯一的 q 元子域 $\mathbf{F}_q$, 它就是多项式 X^q-X 的根所构成的集合.

iii) 每个 $q=p^f$ 元有限域均同构于 $\mathbf{F}_q$.

证 如果 K 是有限的, 它不能包含域 $\mathbf{Q}$, 从而它的特征是素数 p. 如果 f 为扩张 $K/\mathbf{F}_p$ 的次数, 显然 $\mathrm{Card}(K)=p^f$, 这就得到 i).

另一方面, 如果 Ω 是特征 p 的代数封闭域, 上面的引理表明映射 $x\mapsto x^q$ ($q=p^f$, $f\geqslant 1$) 是 Ω 的自同构, 这是因为此映射是自同构 σ: $x\mapsto x^p$ 重复 f 次(注意由于 Ω 代数封闭, 从而 σ 是映上). 因此对于 $x\mapsto x^q$ 不变的元素 $x\in\Omega$ 形成 Ω 的一个子域 $\mathbf{F}_q$. 多项式 X^q-X 的微商是

$$qX^{q-1}-1=p\cdot p^{f-1}X^{q-1}-1=-1,$$

即不为零. 由于 Ω 代数封闭, 这导致 X^q-X 有 q 个不同的根, 于是 $\mathrm{Card}(\mathbf{F}_q)=q$. 反之, 如果 K 是 Ω 的 q 元子域, 则 K 内非零元素组成的乘法群 K^* 有 $q-1$ 个元素. 于是若 $x\in K^*$, 则 $x^{q-1}=1$; 若 $x\in K$, 则 $x^q=x$. 这表明 K 包含在 $\mathbf{F}_q$ 之中. 由于 $\mathrm{Card}(K)=\mathrm{Card}(\mathbf{F}_q)$, 我们有 $K=\mathbf{F}_q$, 这就完成了 ii) 的证明.

由 ii) 及每个 p^f 元域均可嵌到 Ω 中 (因为 Ω 代数封闭) 这一事实即可得到 iii).

1.2. 有限域的乘法群

设 p 为素数, f 为 $\geqslant 1$ 的整数, $q=p^f$.

定理 2 有限域 $\mathbf{F}_q$ 的乘法群 $\mathbf{F}_q^*$ 是 $q-1$ 阶循环群.

证 如果 $d\geqslant 1$ 为整数, 以 $\phi(d)$ 表示 Euler ϕ-函数, 即满足 $1\leqslant x\leqslant d$ 并且与 d 互素的整数 x 的个数 (换句话说, 即在 $\mathbf{Z}/d\mathbf{Z}$ 中的象为该群生成元的 x 的个数, $1\leqslant x\leqslant d$). 显然 d 阶

循环群的生成元个数为 $\phi(d)$.

引理 1 若 $n\geqslant 1$ 为整数，则 $n=\sum_{d|n}\phi(d)$ (注意符号 $d|n$ 表示 d 整除 n).

证 如果 $d|n$，令 C_d 表示 $\mathbf{Z}/n\mathbf{Z}$ 中唯一的 d 阶子群，而以 Φ_d 表示 C_d 的生成元集合. 由于 $\mathbf{Z}/n\mathbf{Z}$ 中每个元素均生成某个 C_d，从而群 $\mathbf{Z}/n\mathbf{Z}$ 是所有 Φ_d 的非交并集，于是我们有

$$n=\mathrm{Card}\,(\mathbf{Z}/n\mathbf{Z})=\sum_{d|n}\mathrm{Card}\,(\Phi_d)=\sum_{d|n}\phi(d).$$

引理 2 令 H 为 n 阶有限群. 假设对 n 的每个因子 d，集合 $\{x\in H\,|\,x^d=1\}$ 至多有 d 个元素. 则 H 必为循环群.

证 设 d 为 n 的因子. 如果存在 d 阶元素 $x\in H$，则由 x 生成的子群 $(x)=\{1,\ x,\ \cdots,\ x^{d-1}\}$ 是 d 阶循环群. 按照假设，使 $y^d=1$ 的每个元素 $y\in H$ 均属于 (x) (特别地，H 中所有 d 阶元素都是 (x) 的生成元)，而它们共有 $\phi(d)$ 个. 从而 H 中 d 阶元素的个数或者为零或者为 $\phi(d)$. 如果对某个 d 的值该数是零，则公式 $n=\sum_{d|n}\phi(d)$ 表明 H 中元素的个数 $<n$，这与假设相矛盾. 特别地，H 中存在着 n 阶元素 x，因而 H 即为循环群 (x).

将引理 2 用于 $H=\mathbf{F}_q^*$ 和 $n=q-1$ 即得定理 2，因为次数为 d 的方程 $x^d=1$ 在 $\mathbf{F}_q$ 中至多有 d 个解.

注 由上述证明可知更一般地，一个域的乘法群的每个有限子群都是循环群.

§2. 有限域上的方程

设 q 为素数 p 的方幂，而 K 为 q 元域.

2.1. 方幂和

引理 设 $u>0$ 为整数，则和式

$$S(X^u)=\sum_{x\in K}x^u=\begin{cases}-1, & \text{当 } u\geqslant 1 \text{ 且 } (q-1)\mid u \text{ 时},\\ 0, & \text{在相反情况下}.\end{cases}$$

(当 $u=0$ 时，即使 $x=0$，也都规定 $x^u=1$.)

证 如果 $u=0$，和式中每项均为 1，由于 K 的特征为 p，从而 $S(X^u)=q\cdot 1=0$.

如果 $u\geqslant 1$，并且 $(q-1)\mid u$，则 $o^u=0$，而当 $x\neq 0$ 时 $x^u=1$，从而 $S(X^u)=(q-1)\cdot 1=-1$.

最后，如果 $u\geqslant 1$，且 $(q-1)\nmid u$，根据定理 2，K^* 是 $q-1$ 阶循环群，从而存在 $y\in K^*$，使 $y^u\neq 1$，于是有

$$S(X^u)=\sum_{x\in K^*}x^u=\sum_{x\in K^*}y^ux^u=y^uS(X^u),$$

即 $(1-y^u)S(X^u)=0$，从而推得 $S(X^u)=0$.

(另证 利用如下事实：如果 $d\geqslant 2$，d 与 p 互素，则 d 次单位根之和为零.)

2.2. Chevalley 定理

定理 3(Chevalley-Warning) 设 $f_\alpha\in K[X_1,\cdots,X_n]$ 是 n 元多项式，$\sum_\alpha \deg f_\alpha<n$，而 V 是它们在 K^n 中的公共零点集合，我们有

$$\mathrm{Card}(V)\equiv 0 \pmod p.$$

证 令 $P=\prod_\alpha (1-f_\alpha^{q-1})$，$x\in K^n$. 如果 $x\in V$，则所有 $f_\alpha(x)$ 均为零，从而 $P(x)=1$；如果 $x\notin V$，则必有某个 $f_\alpha(x)$ 不为零，从而 $f_\alpha(x)^{q-1}=1$，于是 $P(x)=0$. 因而 P 是集合 V 的特征函数. 如果对每个多项式 f，记 $S(f)=\sum_{x\in K^n}f(x)$，我们有

$$\mathrm{Card}(V)\equiv S(P) \pmod p,$$

于是将问题归结为证明 $S(P)=0$.

现在由假设 $\sum_{\alpha}\deg f_\alpha<n$ 可知: $\deg P<n(q-1)$. 从而 P 是单项式 $X^u=X_1^{u_1}\cdots X_n^{u_n}$ 的线性组合, 其中 $\sum u_i<n(q-1)$. 只需证明对于每个这样的单项式 X^u, 有 $S(X^u)=0$, 而这一点由引理即可推出, 因为至少有一个 $u_i<q-1$.

系 1 如果 $\sum_{\alpha}\deg f_\alpha<n$, 并且每个 f_α 都没有常数项, 则 f_α 有非平凡的公共零点.

证 这是因为若 V 只是 $\{0\}$, 则 $p\nmid\mathrm{Card}(V)$.

系 1 可以用于当 f_α 都是齐次多项式的时候. 特别有

系 2 每个至少有 3 个变数的二次型在 K 上都有非平凡零点.

(用几何的话说, 就是有限域上的每个二次超曲面都有有理点.)

§3. 二次互反律

3.1. $\mathbf{F}_q$ 中平方元素

设 q 为素数 p 的方幂.

定理 4 (a) 如果 $p=2$, 则 $\mathbf{F}_q$ 中每个元素都是平方元素.

(b) 如果 $p\neq 2$, 则 $\mathbf{F}_q^*$ 的平方元素形成 $\mathbf{F}_q^*$ 的指数为 2 的子群, 这个子群是同态

$$x\mapsto x^{(q-1)/2},\quad \mathbf{F}_p^*\to\{\pm 1\}$$

的核. (换句话说, 我们有正合列

$$1\to\mathbf{F}_q^{*2}\to\mathbf{F}_q^*\to\{\pm 1\}\to 1.)$$

证 情形(a)从 $x\mapsto x^2$ 为 $\mathbf{F}_q$ 的自同构这一事实即可推出.

对于情形(b), 令 Ω 为 $\mathbf{F}_q$ 的代数闭包. 如果 $x\in\mathbf{F}_q^*$, 令 $y\in\Omega$, 使 $y^2=x$. 我们有

$$y^{q-1}=x^{\frac{q-1}{2}}=\pm 1 \quad (\text{因为 } x^{q-1}=1).$$

为了 x 是 $\mathbf{F}_q$ 中的平方元素，其充要条件是 $y\in\mathbf{F}_q^*$，即 $y^{q-1}=1$. 于是 $\mathbf{F}_q^{*2}$ 为 $x\mapsto x^{\frac{q-1}{2}}$ 的核. 进而，由于 $\mathbf{F}_q^*$ 是 $q-1$ 阶循环群，从而 $\mathbf{F}_q^{*2}$ 的指数是 2.

3.2. Legendre 符号(基本情形)

定义 设 $p\neq 2$ 为素数，$x\in\mathbf{F}_p^*$. x 的 Legendre 符号 $\left(\frac{x}{p}\right)$ 是整数 $x^{\frac{p-1}{2}}=\pm 1$.

为方便起见，令 $\left(\frac{0}{p}\right)=0$，从而将 $\left(\frac{x}{p}\right)$ 扩充到 $\mathbf{F}_p$ 的全部元素上. 并且对于 $x\in\mathbf{Z}$，若 x 有象元素 $x'\in\mathbf{F}_p$，则记作

$$\left(\frac{x}{p}\right)=\left(\frac{x'}{p}\right).$$

我们有 $\left(\frac{x}{p}\right)\left(\frac{y}{p}\right)=\left(\frac{xy}{p}\right)$：Legendre 符号是“特征”(见第六章 § 1). 正如定理 4 中所表明的，$\left(\frac{x}{p}\right)=1$ 等价于 $x\in\mathbf{F}_q^{*2}$. 如果 $x\in\mathbf{F}_p^*$，x 在 $\mathbf{F}_p$ 的代数闭包中有平方根 y，则

$$\left(\frac{x}{p}\right)=y^{p-1}.$$

对于 $x=1,\ -1,\ 2$，计算 $\left(\frac{x}{p}\right)$：

若 n 为奇整数，令 $\varepsilon(n)$，$\omega(n)$ 为 $\mathbf{Z}/2\mathbf{Z}$ 中的元素，定义为

$$\varepsilon(n)\equiv\frac{n-1}{2}(\mathrm{mod}\,2)=\begin{cases}0, & \text{如果 } n\equiv 1\ (\mathrm{mod}\,4),\\ 1, & \text{如果 } n\equiv -1\ (\mathrm{mod}\,4),\end{cases}$$

$$\omega(n)\equiv\frac{n^2-1}{8}(\mathrm{mod}\,2)=\begin{cases}0, & \text{如果 } n\equiv \pm 1\ (\mathrm{mod}\,8),\\ 1, & \text{如果 } n\equiv \pm 5\ (\mathrm{mod}\,8).\end{cases}$$

[函数 ε 是乘法群 $(\mathbf{Z}/4\mathbf{Z})^*$ 到 $\mathbf{Z}/2\mathbf{Z}$ 上的同态；类似地 ω 是

$(\mathbf{Z}/8\mathbf{Z})^*$ 到 $\mathbf{Z}/2\mathbf{Z}$ 上的同态.]

定理 5 i) $\left(\frac{1}{p}\right)=1$; ii) $\left(\frac{-1}{p}\right)=(-1)^{\varepsilon(p)}$; iii) $\left(\frac{2}{p}\right)=(-1)^{\omega(p)}$.

证 只有最后一个公式值得证明. 令 α 为 $\mathbf{F}_p$ 之代数闭包 Ω 中的一个 8 次本原单位根. 元素 $y=\alpha+\alpha^{-1}$, 满足 $y^2=2$ (因为由 $\alpha^4=-1$ 可知 $\alpha^2+\alpha^{-2}=0$). 我们有

$$y^p=\alpha^p+\alpha^{-p}.$$

若 $p\equiv\pm1 \pmod 8$, 这导致 $y^p=y$, 因此 $\left(\frac{2}{p}\right)=y^{p-1}=1$. 如果 $p\equiv\pm5 \pmod 8$, 我们发现

$$y^p=\alpha^5+\alpha^{-5}=-(\alpha+\alpha^{-1})=-y.$$

(这又是从 $\alpha^4=-1$ 推出来的.) 由此得到 $y^{p-1}=-1$, 从而证明了 iii).

注 定理 5 可以表达成下面的方式:

-1 是 mod p 平方数 $\Leftrightarrow p\equiv1 \pmod 4$.

2 是 mod p 平方数 $\Leftrightarrow p\equiv\pm1 \pmod 8$.

3.3. 二次互反律

设 l 和 p 是两个不同的奇素数.

定理 6 (Gauss) $\left(\frac{l}{p}\right)=\left(\frac{p}{l}\right)(-1)^{\varepsilon(l)\varepsilon(p)}$.

证 设 Ω 为 $\mathbf{F}_p$ 的代数闭包, $w\in\Omega$ 是 l 次本原单位根. 如果 $x\in\mathbf{F}_l$, 因为 $w^l=1$, 从而元素 w^x 是可以定义的. 于是我们可以作成 Gauss 和:

$$y=\sum_{x\in\mathbf{F}_l}\left(\frac{x}{l}\right)w^x.$$

引理 1 $y^2=(-1)^{\varepsilon(l)}l$.

（记号 l 也表示 l 在域 $\mathbf{F}_p$ 中的象.）

证　我们有

$$y^2=\sum_{x,z}\left(\frac{xz}{l}\right)w^{x+z}=\sum_{u\in\mathbf{F}_l}w^u\left(\sum_{t\in\mathbf{F}_l}\left(\frac{t(u-t)}{l}\right)\right).$$

现在若 $t\neq 0$:

$$\left(\frac{t(u-t)}{l}\right)=\left(\frac{-t^2}{l}\right)\left(\frac{1-ut^{-1}}{l}\right)=(-1)^{\varepsilon(l)}\left(\frac{1-ut^{-1}}{l}\right),$$

而

$$(-1)^{\varepsilon(l)}y^2=\sum_{u\in\mathbf{F}_l}C_uw^u,$$

其中

$$C_u=\sum_{t\in\mathbf{F}_l^*}\left(\frac{1-ut^{-1}}{l}\right).$$

如果 $u=0$, $C_0=\sum_{t\in\mathbf{F}_l^*}\left(\frac{1}{l}\right)=l-1$; 否则, $s=1-ut^{-1}$ 过 $\mathbf{F}_l-\{1\}$, 从而有

$$C_u=\sum_{s\in\mathbf{F}_l}\left(\frac{s}{l}\right)-\left(\frac{1}{l}\right)=-\left(\frac{1}{l}\right)=-1,$$

这是因为在 $\mathbf{F}_l^*$ 中平方元素和非平方元素有同样多个. 于是

$$\sum_{u\in\mathbf{F}_l}C_uw^u=l-1-\sum_{u\in\mathbf{F}_l^*}w^u=l,$$

此即证明了引理.

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

证　由于 Ω 的特征是 p, 我们有

$$y^p=\sum_{x\in\mathbf{F}_l}\left(\frac{x}{p}\right)w^{xp}=\sum_{z\in\mathbf{F}_l}\left(\frac{zp^{-1}}{l}\right)w^z=\left(\frac{p^{-1}}{l}\right)y=\left(\frac{p}{l}\right)y,$$

从而

$$y^{p-1}=\left(\frac{p}{l}\right).$$

现在可以证明定理 6. 由引理 1 和引理 2, 有

$$\left(\frac{(-1)^{\varepsilon(l)}l}{p}\right)=y^{p-1}=\left(\frac{p}{l}\right),$$

而定理 5 的第二部分表明

$$\left(\frac{(-1)^{\varepsilon(l)}}{p}\right)=(-1)^{\varepsilon(l)\varepsilon(p)}.$$

如果把 l 是 $\bmod p$ 平方数(即 l 是 $\bmod p$"二次剩余")表示成 lRp, 否则表示成 lNp. 则定理 6 可以叙述为

$lRp \Leftrightarrow pRl$, 当 p 或 $l\equiv 1 \pmod 4$ 时;

$lRp \Leftrightarrow pNl$, 当 p 和 $l\equiv -1 \pmod 4$ 时.

注 定理 6 可使我们采用逐次化简的方法计算Legendre符号. 例如

$$\left(\frac{29}{43}\right)=\left(\frac{43}{29}\right)=\left(\frac{14}{29}\right)=\left(\frac{2}{29}\right)\left(\frac{7}{29}\right)$$
$$=-\left(\frac{7}{29}\right)=-\left(\frac{29}{7}\right)=-\left(\frac{1}{7}\right)=-1.$$

附录 二次互反律的另一证明

(G. Eisenstein, J. Crelle, 29, 1845, pp. 177～184.)

i) Gauss 引理

设 p 为奇素数, S 为 $\mathbf{F}_p^*$ 的子集, 使 $\mathbf{F}_p^*$ 为 S 和 $-S$ 的非交并集. 以下我们取 $S=\left\{1, \cdots, \frac{p-1}{2}\right\}$.

如果 $s\in S$, $a\in\mathbf{F}_p^*$, 我们记成形式

$$as=e_s(a)s_a,\quad e_s(a)=\pm 1,\quad s_a\in S.$$

引理(Gauss) $\left(\frac{a}{p}\right)=\prod_{s\in S}e_s(a)$.

证 首先注意, 如果 s 和 s' 是 S 中两个不同的元素, 则 $s_a\neq s'_a$(因为否则 $s=\pm s'$, 与 S 之选取相矛盾). 这说明 $s\mapsto s_a$ 是 S 到它本身之上的一一对应. 将诸等式 $as=e_s(a)s_a$ 相乘, 得到

$$a^{\frac{(p-1)}{2}}\prod_{s\in S}s=\left(\prod_{s\in S}e_s(a)\right)\prod_{s\in S}s_a=\left(\prod_{s\in S}e_s(a)\right)\prod_{s\in S}s,$$

于是

$$a^{\frac{p-1}{2}}=\prod_{s\in S}e_s(a),$$

因为在 $\mathbf{F}_p$ 中 $\left(\frac{a}{p}\right)=a^{\frac{p-1}{2}}$, 这就证明了引理.

【例】 取 $a=2$, $S=\left\{1, \cdots, \frac{p-1}{2}\right\}$. 有

$$e_s(2)=\begin{cases} 1, & \text{如果 } 2s\leqslant\frac{p-1}{2}, \\ -1, & \text{否则.} \end{cases}$$

由此得到 $\left(\frac{2}{p}\right)=(-1)^{n(p)}$, 这里 $n(p)$ 是满足 $\frac{p-1}{4}<s\leqslant\frac{p-1}{2}$ 的整数 s 的个数. 如果 p 有形式 $1+4k$(或 $3+4k$), 则 $n(p)=k$(或 $n(p)=k+1$). 因此我们发现, 当 $p\equiv\pm1 \pmod 8$ 时, $\left(\frac{2}{p}\right)=1$; 而当 $p\equiv\pm5 \pmod 8$ 时, $\left(\frac{2}{p}\right)=-1$, 参见定理 5.

ii) 一个关于三角函数的引理

引理 设 m 为奇自然数. 则有

$$\frac{\sin mx}{\sin x}=(-4)^{\frac{m-1}{2}}\prod_{1\leqslant j\leqslant\frac{m-1}{2}}\left(\sin^2 x-\sin^2\frac{2\pi j}{m}\right).$$

证明是初等的. $\left(\text{例如, 可先证}\frac{\sin mx}{\sin x}\text{ 是对于变量 }\sin^2x\text{ 的 }\frac{m-1}{2}\text{ 次多项式, 然后注意这个多项式有根 }\sin^2\frac{2\pi j}{m}\left(1\leqslant j\leqslant\frac{m-1}{2}\right),\right.$ $\left.\text{比较 } e^{i(m-1)x}\text{ 两边的系数, 即得到因子 }(-4)^{\frac{m-1}{2}}.\right)$

iii) 二次互反律的证明

设 l 和 p 是两个不同的奇素数. 如上一样, 令

$$S=\left\{1, \cdots, \frac{p-1}{2}\right\}.$$

从 Gauss 引理得到

$$\left(\frac{l}{p}\right)=\prod_{s\in S}e_s(l).$$

现在等式 $ls=e_s(l)s_l$ 表明

$$\sin\frac{2\pi}{p}ls=e_s(l)\sin\frac{2\pi}{p}s_l.$$

将这些等式相乘, 并考虑到 $s\mapsto s_l$ 是 S 上的一一对应, 便得到

$$\left(\frac{l}{p}\right)=\prod_{s\in S}e_s(l)=\prod_{s\in S}\sin\frac{2\pi ls}{p}\Big/\sin\frac{2\pi s}{p}.$$

对于 $m=l$, 利用上面三角函数的引理, 可以将它重写为