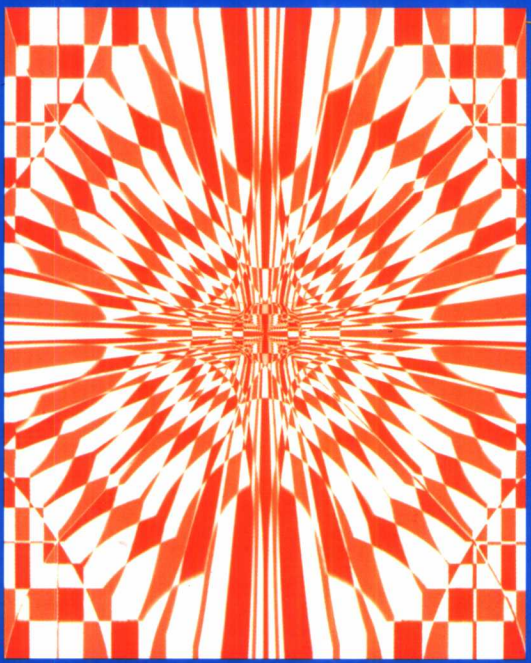
北京大学数学丛书

数论及其应用

李文卿 著



北京大学出版社

北京大学数学丛书

数论及其应用

李文卿 著

北京大学出版社
·北 京·

图书在版编目(CIP)数据

数论及其应用/李文卿著. —北京：北京大学出版社，2001.3
(北京大学数学丛书/程民德主编)
ISBN 7-301-04169-1

Ⅰ. 数… Ⅱ. 李… Ⅲ. 数论 Ⅳ. 0156

中国版本图书馆 CIP 数据核字(1999)第 17241 号

书　　名：数论及其应用
著作责任者：李文卿
责任编辑：邱淑清
标准书号：ISBN 7-301-04169-1/O・445
出 版 者：北京大学出版社
地　　址：北京市海淀区中关村北京大学校内　100871
网　　址：http://cbs.pku.edu.cn/cbs.htm
电　　话：出版部 62752015　发行部 62754140　理科编辑部 62752021
电子信箱：zpup@pup.pku.edu.cn
排 版 者：北京大学印刷厂
印 刷 者：北京大学印刷厂
发 行 者：北京大学出版社
经 销 者：新华书店
850 毫米×1168 毫米　32 开本　12.25 印张　302 千字
2001 年 3 月第一版　2001 年 3 月第一次印刷
定　　价：20.00 元

前　言

在过去的 10 年中，通过精确构造所谓的 Ramanujan 图，数论在网络通讯及计算复杂性方面有了非常重要的应用. Ramanujan 图是一些其非平凡特征值都很小的正则图 (详细说明参见本书的第九章). 到目前为止, 所有已知的 Ramanujan 图的构造都源于数论: 一种想法基于模形式的 Fourier 系数的估计，即由 Deligne 证明的 Ramanujan-Petersson 猜想；另一种想法则依赖于一些特征和的估计，这些估计可由被 Weil 证明的有限域上的代数曲线的 Riemann 猜想导出. 这两种思路的共同背景是著名的 Weil 猜想，该猜想已在 1973 年被 Deligne 所证明. 这即是我们这本书的出发点. 本书的目的是介绍与上述应用相关的数论知识，最终给出 Ramanujan 图的精确构造. 事实上，我们希望通过以这样一个简单的目标作为本书取材和论述的基础，让读者能够接触到现代数论里一些最深奥、最精美的部分.

这是一本为高年级本科生，研究生和对数论及其应用感兴趣的人写的书. 其风格是半正式的. 作者假定读者已经有了一些代数及数论的基础知识. 在此基础上，作者尽可能地保持本书的自封性. 我们的主要目的是介绍相关的基本概念和结果，同时也给出一些难度较大的定理的证明提要，以便让读者能比较完整地了解所阐述的理论体系和思想方法. 一般地，没有给出证明的论述都可以假定成立，而不影响论述的完整性. 有兴趣的读者可以从每章后的参考文献里找到所有省略的材料以及没有讨论的相关的内容. 贯穿本书，我们准备了许多习题，以便让读者有机会练习，其中，有些习题将用于定理的证明.

全书的内容安排如下：在第一章复习了有限域的基本概念之后，第二章将讨论关于有限域上 zeta 函数的 Weil 猜想. 我们将

看到 Weil 是如何从计算一个多项式方程在有限域的扩张上的解的个数来导出他的这一著名猜想的. 同时, 我们将介绍证明这一猜想的思想方法. 第三章研究和讨论局部域与整体域. 在本书中, 我们将用阿代尔语言来描述整体域. 第四和第五章是关于函数域的, 其中, 我们将证明 Riemann-Roch 定理, 并介绍结合伊代尔类特征标的 L-函数和 zeta 函数的解析性质. 借助于类域论的一些结果 (书中我们将给出简单的概述), 并结合第五章和第二章中讨论的 L-函数和有限域上曲线的 Riemann 猜想, 我们在第六章将给出一些特征和的估计, 这些估计将用于第九章中的 Ramanujan 图的构造. 第七章讨论经典模形式, 这是一个内容非常丰富且与数学的许多分支都有深刻联系的理论. 我们将概述该理论的发展, 包括 Hecke 算子、 L-函数、模形式逆定理, 以及新形式理论. 我们还将讨论这一领域中的主猜想及其推论, 其中有些推论在数论中有着极其深远的影响, 例如椭圆曲线理论中的 Taniyama-Shimura 猜想, 最近 Wiles 以及 Taylor 和 Wiles 的工作证明它关于半稳定的椭圆曲线是正确的, 这一结果结合早先 Frey 和 Ribet 的结果即可肯定著名的 Fermat 大定理是正确的. 自守形式和自守表示将在第八章讨论, 在这一章中, 我们先用阿代尔语言重新刻画模形式, 由此自然导出 GL(2) 上的自守形式和自守表示的概念. 接下来论述 Jacquet-Langlands 关于 GL(2) 和四元数群上局部表示和整体表示的理论. 特别地, 我们将描述这些群的局部表示是如何被其结合的 L-因子和 ε-因子决定的, 由此得到这些群的局部表示之间的关系. 最后, 我们将在第九章看到数论与组合学的联系. 一方面我们利用前面的讨论给出 Ramanujan 图的精确构造, 另一方面, 通过研究一些由四元数群产生的图的测度的极限, 我们可以得到有关 Hecke 算子的特征值分布的一些结果.

这本书源于作者于 1992 至 1993 年在台湾大学讲授的为期一年的研究生数论课程. 在此之前, 作者曾用该书的基本素材于 1992 年夏在四川大学由国家教委举办的研究生数学夏令营作了一个月

的讲座. 作者非常感谢这两所大学的支持和协助. 听众的热情也给予作者极大的鼓励. 本书的主要部分是作者在 1992 至 1993 年在台湾大学访问时完成的. 我特别要感谢台湾国家科学委员会和美国 National Security Agency 的财政支持, 以及王绣丽女士出色的打字工作. 本书最后是在 1995 年春在作者访问 Berkeley 数学科学研究所时完成的. 在此我也要向该所所给予的热情接待和支持表示由衷的谢意.

本书的原稿是用英文写成的, 中文稿是由中国科技大学李云峰先生翻译整理的. 第七章之后的附录是他写的, 有些习题也是他加的. 对李先生的热心协助及细心编排、翻译和校对, 作者在此表示由衷的谢意. 要是没有他的积极推动, 本书极可能无法与读者见面. 另外, 我还要感谢丁石孙先生的建议, 将本书译成中文, 由北大出版社出版. 作者衷心地希望国内喜爱数论的人士或能从该书中略窥数论之奥秘与精深.

李文卿

1995 年春于加州 Berkeley 数学科学研究所

目　录

第一章　有　限　域

§1　有限域的结构

顾名思义，**有限域**就是只有有限个元素的域. 最简单的例子是素域 $F_p = \mathbf{Z}/p\mathbf{Z}$, 其中 p 为素数.

设 F 是一个域，映射

$$\varphi : \mathbf{Z} \longrightarrow F$$

$$n \longmapsto n \cdot 1 = 1 + 1 + \cdots + 1(n \text{ 次})$$

的像是整环，从而同构于 $\mathbf{Z}$ 或 $\mathbf{Z}/p\mathbf{Z}$, 其中 p 为素数. 对于前者，称 F 为**特征**

rm 0 域; 对于后者，称 F 为**特征** p **域**. F 的特征记作 $\mathrm{char}(F)$. 如果 $\mathrm{char}(F) = p \neq 0$, 那么 p 也是满足 $n \cdot 1 = 0$ 的最小自然数 n.

习题 1　设 F 是一特征 p 域，则对任意自然数 d 有

$$(x + y)^{p^d} = x^{p^d} + y^{p^d}, \qquad x, y \in F.$$

有限域的特征明显是不为 0 的；但反过来，特征不为 0 的域并不一定是有限域. 请有兴趣的读者构造特征 0 的无限域.

设 k 是一有限域，$\mathrm{char}(k) = p$, 则它包含 $\mathbf{Z}/p\mathbf{Z}$ 作为它的一个子域，进而是 $\mathbf{Z}/p\mathbf{Z}$ 上的一个有限维向量空间，因此它的势 $|k| = q = p^d$ 是 p 的幂，其中指数 d 是向量空间 k 在 $\mathbf{Z}/p\mathbf{Z}$ 上的维数. 这也导出 k 的加法群是 d 个的 p 阶循环群的直和.

下面考虑乘法群 $k^\times = k \setminus \{0\}$, 它的阶是 $q - 1$. 于是 k 中任何非 0 元素均满足

$$x^{q-1} = 1.$$

进而 $k^\times$ 中元素的阶整除 $q-1$. 对 $q-1$ 的每个正因子 r, 设

$$\Omega(r)=\{x\in k^\times : x \text{ 的阶是 } r\}.$$

则随着 r 跑遍 $q-1$ 的所有正因子, $k^\times$ 是这些 $\Omega(r)$ 的非交并. 我们希望证明 $\Omega(q-1)$ 是非空的, 即

定理 1 *$k^\times$ 是 $q-1$ 阶循环群.*

为证此定理, 我们先证一个如下的一般的事实.

引理 1 *域 F 上的一个 n 次多项式在 F 中至多有 n 个不同的根.*

证 设 $f(x)\in F[x]$, α 为 $f(x)$ 在 F 中的一个根, 则 $f(\alpha)=0$. 于是

$$f(x)=f(x)-f(\alpha)=(x-\alpha)g(x),$$

这里 $g(x)$ 为 F 上 $n-1$ 次多项式. 若 β 为 $f(x)$ 在 F 中的一个不同于 α 的根, 则可由

$$0=f(\beta)=(\beta-\alpha)g(\beta)$$

和 $\alpha\neq\beta$ 导出 $g(\beta)=0$. 利用归纳法, $n=1$ 时引理显然成立. 假设 $n-1$ 时引理成立, 则 $g(x)$ 在 F 中至多有 $n-1$ 个不同的根. 于是 $f(x)$ 在 F 中至多有 n 个不同的根. 由此引理得证.

由引理 1 可知, 若 $\Omega(r)$ 是非空的, 设它包含有元素 y, 则 y 生成一个 r 阶循环子群 $\langle y\rangle$, 它由所有 $x^r=1$ 在 k 中的解组成. $\Omega(r)$ 为循环群 $\langle y\rangle$ 的生成元集, 即

$$\Omega(r)=\{y^i : 1\le i\le r, \gcd(i,r)=1\}.$$

这就证明了 $\Omega(r)$ 的势或者为 0 或者为 $\phi(r)$. 这里 $\phi(n)$ 是 Euler ϕ 函数, 它表示在 1 到 n 之间与 n 互素的整数的个数. 从而

$$|k^\times|=q-1=\sum_{r|q-1}|\Omega(r)|\le\sum_{r|q-1}\phi(r).$$

在初等数论中有如下一个结论.

引理 2 对自然数 m, $\sum_{r|m} \phi(r) = m$.

我们立刻由此引理及其上面的不等式得出：对任意的 $r|q-1$ 均有 $|\Omega(r)| = \phi(r)$. 特别地, $|\Omega(q-1)| = \phi(q-1) \geq 1$. 由此, 定理 1 得证.

为证引理 2, 我们将 $\{1, 2, \cdots, m\}$ 分拆成下面类型集合的不交并

$$Y(r) = \left\{1 \leq i \leq m : \gcd(i, m) = \frac{m}{r}\right\},$$

这里 r 跑遍 m 的所有正因子. 对 $i \in Y(r)$, 记 $i = j\frac{m}{r}$, 则 $1 \leq j \leq r$ 且 $\gcd(j, r) = 1$. 因此 $|Y(r)| = \phi(r)$, 由此就可导出引理 2.

上述讨论有下面一些推论.

推论 1 在 $\mathbf{Z}/p\mathbf{Z}$ 的一个包含 k 的代数闭包中, 域 k 由方程 $x^q - x = 0$ 的解组成.

推论 2 存在 k 中元素 ξ, 使得 $k = (\mathbf{Z}/p\mathbf{Z})(\xi)$, 即 k 是素域 $\mathbf{Z}/p\mathbf{Z}$ 的一个单扩张.

推论 3 对 $q-1$ 的每个正因子 r, 在 $k^\times$ 中恰好存在 $\phi(r)$ 个元素, 其阶为 r.

推论 4 给出一个正整数 n, 在 $\mathbf{Z}/p\mathbf{Z}$ 的一个代数闭包中, 唯一存在一个 $\mathbf{Z}/p\mathbf{Z}$ 的 n 次域扩张.

证 推论 1 表明：如果存在一个 $\mathbf{Z}/p\mathbf{Z}$ 在其代数闭包中的 n 次扩张, 那么该扩张恰由 $x^{p^n} = x$ 的根所组成. 另一方面, 容易验证：若 α, β 为 $x^{p^n} = x$ 的解, 则 $\alpha - \beta$ 和 $\alpha\beta^{-1}(\beta \neq 0)$ 也是 $x^{p^n} = x$ 的解. 故 $x^{p^n} = x$ 的解构成一个域. 因此推论得证.

推论 5 任给自然数 n, 存在 $\mathbf{Z}/p\mathbf{Z}$ 上的 n 次不可约多项式.

证 设 k 为 $\mathbf{Z}/p\mathbf{Z}$ 上的 n 次扩张. 由推论 2 知, 存在 ξ 使得 $k = (\mathbf{Z}/p\mathbf{Z})(\xi)$. 设 $f(x)$ 为 ξ 在 $\mathbf{Z}/p\mathbf{Z}$ 上的不可约多项式, 则由

$$k = (\mathbf{Z}/p\mathbf{Z})(\xi) = (\mathbf{Z}/p\mathbf{Z})[\xi] \cong (\mathbf{Z}/p\mathbf{Z})[x]/(f(x))$$

可得 $\deg f = [k : \mathbf{Z}/p\mathbf{Z}] = n$.

§2 有限域的扩张

在本节中，设 k 是一个有 q 个元素的有限域，k_n 为 k 的 n 次域扩张. k_n 的任意包含 k 的子域必为 k 的有限扩张；若其扩张次数为 m，则 m 可整除 n. 反过来，由推论 1 可知，对 n 的任意正因子 m，在 k_n 的一个代数闭包中，k 的 m 次扩张均为 k_n 的子域.

习题 2 上述论述中用到了这样一个事实："设 F 为一个有限域，它有一个势为 q 的子域 K，则 F 的势为 q^n，其中 n 是 F 在 K 上的扩张次数 $[F : K]$." 试证明此结论成立.

对域 F 的一个扩张 E，以 $\mathrm{Gal}(E/F)$ 表示 E 的所有使 F 不变的自同构集合，它构成一个群 (请读者自己验证). 注意到 $\mathrm{Gal}(E/F)$ 中元素可视为 E 上的 F 线性变换. 进一步，我们有如下结果.

引理 3 $\mathrm{Gal}(E/F)$ 中的自同构是 E 线性无关的.

证 假设引理不真，则可列出一长度最短的非平凡的线性关系

$$a_1\tau_1 + \cdots + a_r\tau_r = 0$$

$$(a_i \in E^\times, \tau_i \in \mathrm{Gal}(E/F), \quad i = 1, \cdots, r). \tag{2.1}$$

必然有 $r \geq 2$，且 τ_i 都是互不相同的. 因为 $\tau_1 \neq \tau_2$，所以存在元素 $y \in E$，使得 $\tau_1(y) \neq \tau_2(y)$. 由 (2.1) 式得出另一关系：对任意的 $x \in E$，有

$$0 = \sum_{i=1}^{r} a_i\tau_i(yx) = \sum_{i=1}^{r} a_i\tau_i(y)\tau_i(x),$$

从而 $\sum\limits_{i=1}^{r} a_i\tau_i(y)\tau_i = 0$. 这就导出第三个非平凡的线性关系：

$$0 = \sum_{i=1}^{r} a_i\tau_i(y)\tau_i - \tau_1(y)\sum_{i=1}^{r} a_i\tau_i = \sum_{i=2}^{r}(\tau_i(y) - \tau_1(y))\tau_i,$$

其长度比前述关系 (2.1) 要短，这与 (2.1) 式的选取相矛盾.

引理 4 设 E 为域 F 的 n 次扩张，则在 $\mathrm{Gal}(E/F)$ 中至多有 n 个不同的自同构.

证 假设引理不真，则 $\mathrm{Gal}(E/F)$ 中存在 m 个不同的自同构 $\tau_1,\cdots,\tau_m$，且 $m>n$. 又令 $\{v_1,\cdots,v_n\}$ 为 E 在 F 上的一组基. 由于 $m>n$，故线性方程组

$$\begin{pmatrix} \tau_1(v_1) & \tau_2(v_1) & \cdots & \tau_m(v_1) \\ \vdots & \vdots & & \vdots \\ \tau_1(v_n) & \tau_2(v_n) & \cdots & \tau_m(v_n) \end{pmatrix} \begin{pmatrix} x_1 \\ \vdots \\ x_m \end{pmatrix} = \begin{pmatrix} 0 \\ \vdots \\ 0 \end{pmatrix}$$

在 E 中有非平凡解. 设 $(a_1,a_2,\cdots,a_m)$ 为它的一组非平凡解，于是对任意的 $j=1,2,\cdots,n$，有

$$\sum_{i=1}^{m} a_i\tau_i(v_j)=0.$$

因此，对所有的 $x\in E$，均有

$$\sum_{i=1}^{m} a_i\tau_i(x)=0.$$

从而

$$\sum_{i=1}^{m} a_i\tau_i=0$$

换句话说，$\tau_1,\tau_2,\cdots,\tau_m$ 在 E 上线性相关，这与引理 3 矛盾.

下面我们回到有限域 k 和 k_n 上来. 考虑 k_n 上将 x 映为 x^q 的映射 σ. 注意到，对任意的 $x,y\in k_n$，有

$$\sigma(x+y)=(x+y)^q=x^q+y^q=\sigma(x)+\sigma(y),$$

$$\sigma(xy)=(xy)^q=x^qy^q=\sigma(x)\sigma(y),$$

故 σ 为 k_n 的自同态. 进一步，对 k_n 中元 x，若满足 $\sigma(x)=x^q=1$，则 $x\neq 0$. 再结合 $x^{q^n-1}=1$ 就导出 $x=1$. 于是 σ 是单射. 又由于 k_n 是有限域，我们就证明了 σ 为 k_n 上的自同构. 注意到，对 k 中任意元 x，

$$\sigma(x)=x^q=x,$$

这表明 $\sigma \in \mathrm{Gal}(k_n/k)$. 我们称 σ 为 **Frobenius 自同构**. 设 r 为 σ 的阶，则

$$x = \sigma^r(x) = x^{q^r}, \qquad x \in k_n.$$

又因 $k_n^\times$ 是 $q^n - 1$ 阶循环群，故 $r = n$. 因此 $\mathrm{Gal}(k_n/k)$ 包含了 n 阶循环群 $\langle\sigma\rangle$. 再结合引理 4 即知，$\mathrm{Gal}(k_n/k) = \langle\sigma\rangle$. 此时

$$|\mathrm{Gal}(k_n/k)| = |\langle\sigma\rangle| = n = [k_n : k].$$

即 $\mathrm{Gal}(k_n/k)$ 的阶已达到极大. 在此情况下，称 k_n 为 k 上的 **Galois 扩张**.

总结上面的讨论我们得：

定理 2 *域 k_n 是 k 上的 Galois 扩张，其 Galois 群 $\mathrm{Gal}(k_n/k)$ 是由 Frobenius 自同构 σ 生成的 n 阶循环群.*

我们注意到：k_n 中的元素 x 位于 k 中的充要条件是它满足 $x^q = x$. 换句话说，它在 Frobenius 自同构作用下不变，亦即它在 Galois 群 $\mathrm{Gal}(k_n/k)$ 作用下不变. 利用 Galois 群 $\mathrm{Gal}(k_n/k)$，我们可定义两个重要的映射，分别称为关于扩张 k_n/k 的**迹**和**范**，记作 $\mathrm{Tr}_{k_n/k}$ 和 $\mathrm{N}_{k_n/k}$. 其定义如下：

$$\mathrm{Tr}_{k_n/k} : k_n \longrightarrow k,$$

$$x \longmapsto \sum_{\tau \in \mathrm{Gal}(k_n/k)} \tau(x) = \sum_{i=1}^{n} \sigma^i(x)$$

和

$$\mathrm{N}_{k_n/k} : k_n \longrightarrow k,$$

$$x \longmapsto \prod_{\tau \in \mathrm{Gal}(k_n/k)} \tau(x) = \prod_{i=1}^{n} \sigma^i(x).$$

容易验证，迹和范映射的像均在 k 中，而且可以很明显地看出，$\mathrm{Tr}_{k_n/k}$ 是加法群 k_n 到加法群 k 的同态，$\mathrm{N}_{k_n/k}$ 是乘法群 $k_n^\times$ 到乘法群 $k^\times$ 的同态. 下面我们来研究它们的像.

定理 3 (Hilbert 定理 90) 由乘法群 $k_n^\times$ 到乘法群 $k^\times$ 的范映射 $\mathrm{N}_{k_n/k}$ 是一个满射，且它的核是 $\{x/\sigma(x) : x \in k_n^\times\}$.

证 由于对任意的 $x \in k_n$,

$$\mathrm{N}_{k_n/k}(\sigma(x)) = \sum_{i=1}^{n} \sigma^{i+1}(x) = \sum_{i=1}^{n} \sigma^i(x) = \mathrm{N}_{k_n/k}(x).$$

于是对所有的 $x \in k_n^\times$, $\dfrac{x}{\sigma(x)}$ 位于范映射 $\mathrm{N}_{k_n/k}$ 的核中. 进一步，等式

$$\frac{x}{\sigma(x)} = \frac{y}{\sigma(y)}$$

当且仅当 $xy^{-1} \in k^\times$ 时成立，因此 $\{x/\sigma(x) : x \in k_n^\times\}$ 构成了 $k_n^\times$ 的一个 $\dfrac{q^n-1}{q-1}$ 阶子群，故它等于整个范映射的核的充要条件是，范映射 $\mathrm{N}_{k_n/k}$ 是满射. 为证明这一点，注意到对任意的 $x \in k_n^\times$.

$$\begin{aligned}\mathrm{N}_{k_n/k}(x) &= \prod_{i=1}^{n} \sigma^i(x) = x \cdot x^q \cdot \cdots \cdot x^{q^{n-1}} \\ &= x^{1+q+\cdots+q^{n-1}} = x^{(q^n-1)/(q-1)}.\end{aligned}$$

于是 $k_n^\times$ 的任意生成元 x 的范 $\mathrm{N}_{k_n/k}(x)$ 的阶是 $q-1$，即为 $k^\times$ 的生成元，从而范映射 $\mathrm{N}_{k_n/k}$ 是满射.

定理 4(Hilbert 定理 90) 由加法群 k_n 到加法群 k 的迹映射 $\mathrm{Tr}_{k_n/k}$ 是一个满射，且其核为 $\{x - \sigma(x) : x \in k\}$.

证 由于 $\mathrm{Gal}(k_n/k)$ 中元素是 k 线性映射，故迹映射 $\mathrm{Tr}_{k_n/k}$ 的像 $\mathrm{Tr}_{k_n/k}(k_n)$ 是 k 上的向量空间，因此 $\mathrm{Tr}_{k_n/k}(k_n)$ 或者为 k 或者为 0. 若 $\mathrm{Tr}_{k_n/k}(k_n) = 0$, 则 $\sum\limits_{i=1}^{n} \sigma^i = 0$, 这是 $\mathrm{Gal}(k_n/k)$ 中元素的一个非平凡线性关系，由引理 3 知这是不可能的. 于是 $\mathrm{Tr}_{k_n/k}$ 是满射，故其核的势为 q^{n-1}. 明显地

$$\mathrm{Tr}_{k_n/k}(\sigma(x)) = \mathrm{Tr}_{k_n/k}(x),$$

因而核包含有 $\{x - \sigma(x) : x \in k_n\}$. 此外， $y - \sigma(y) = x - \sigma(x)$ 成

立的充要条件为 $x-y\in k$, 于是集合 $\{x-\sigma(x):x\in k_n\}$ 的势是 $q^n/q=q^{n-1}$, 故它等于核.

注 关于范和迹映射的 Hilbert 定理 90 通常是用 Galois 群的一阶上同调来证明的 (参见参考文献 [11]). 在基域有限时, 我们可采用上述方法直接算出.

习题 3 设 k 是一个有限域, k_{mn} 和 k_n 分别为 k 的 mn 次和 m 次有限扩张, 证明

$$\mathrm{Tr}_{k_{mn}/k}=\mathrm{Tr}_{k_m/k}\circ\mathrm{Tr}_{k_{mn}/k_m},$$

$$\mathrm{N}_{k_{mn}/k}=\mathrm{N}_{k_m/k}\circ\mathrm{N}_{k_{mn}/k_m}.$$

给定 k_n 中一元素 z, 它定义了 k_n 上的一个 k 线性变换

$$L_z:x\longmapsto zx,$$

则 L_z 的迹 $\mathrm{Tr}\,L_z$ 和行列式 $\det L_z$ 分别定义为表示线性变换 L_z 的 $n\times n$ 矩阵的迹和行列式. 事实上, 它们由 z 的迹 $\mathrm{Tr}_{k_n/k}(z)$ 和范 $\mathrm{N}_{k_n/k}(z)$ 给出. 精确地讲, 我们有

定理 5 设 $z\in k_n$, 则

(1) $\mathrm{Tr}\,L_z=\mathrm{Tr}_{k_n/k}(z)$, $\det L_z=\mathrm{N}_{k_n/k}(z)$.

(2) 假设 $k(z)=k_n$, 又设 $f(x)=x^n+a_1x^{n-1}+\cdots+a_n$ 为 z 在 k 上的不可约多项式, 那么

$$a_1=-\mathrm{Tr}_{k_n/k}(z)\quad\text{和}\quad a_n=(-1)^n\mathrm{N}_{k_n/k}(z).$$

证 我们将在 $k(z)=k_n$ 的假设下来证定理, 而对 $k(z)$ 为 k_n 的一个真子域时, (1) 的证明留给读者作为练习.

任给 $\tau\in\mathrm{Gal}(k_n/k)$, 由 $0=\tau(f(z))=f(\tau(z))$ 知 $\tau(z)$ 亦为 $f(x)$ 的根. 此外, 若 τ 和 τ' 是 $\mathrm{Gal}(k_n/k)$ 中不同的元素, 则 $\tau(z)$ 与 $\tau'(z)$ 不同 (否则 $k_n=k(z)$ 就不成立了), 这表明 z 在 Galois 群 $\mathrm{Gal}(k_n/k)$ 下有 n 个不同的像, 且均为 $f(x)$ 的根, 从而

$$-a_1=f(x)\text{ 的根之和}=\mathrm{Tr}_{k_n/k}(z),$$