arXiv:2301.03569v1 [math.NT] 9 Jan 2023

编码与模曲线

by

Alain Couvreur

摘要. — 这些讲义为2022年暑期学校的代数编码理论 (ACT)课程编写。该暑期学校在苏黎世大学举行。本课程旨在深入讲解编码理论中一项最引人注目的成果——齐斯曼-弗拉杜茨-津克定理的证明。该定理断言，对于某个素数幂 q，存在定义在 $\mathbb{F}_q$ 上的码序列，其渐近参数优于随机码。

目录

引言.1 1. 线性码.2 2. 代数曲线.4 3. 代数几何码.12 4. 椭圆曲线.15 5. 模曲线.24 6. 主要定理的证明.31 参考文献.32

引言

代数几何（AG）码是一个格外令人振奋的研究主题，处于数论、代数几何与编码理论的交汇处。这一研究领域始于 20 世纪 80 年代初，当时 Goppa [**Gop81**] 引入了一类新码：通过在给定曲线上对某些微分形式的留数进行求值而得到。此后不久，Tsfasman、Vlăduţ、Zink [**TVZ82**] 以及独立工作的 Ihara [**Iha81**] 证明，存在模曲线和志村曲线序列，其渐近的点数$v.s.$ 亏格比非常出色。一个直接却极为惊人的推论是，存在超越 Gilbert–Varshamov 界的码序列，简言之，就是优于随机码的码。这一非凡且完全出乎意料的结果，成为一整套理论发展的基石：代数几何码理论。令人惊讶的是，20 世纪 80 年代末，图论领域也出现了一个相当类似的突破。具体而言，1988 年，Lubotsky、Philips 和 Sarnak [**LPS88**] 以及独立工作的 Margulis [**Mar88**] 利用$\mathbf{SL}(\mathbb{Z})$的商空间上的 Cayley图，证明存在一族图，其围长——$i.e.$ 即最短圈的长度——超过了概率方法所能得到的围长。在编码理论和图论这两种情形中，优雅的代数结构都出乎意料地胜过了随机构造。

本讲的目标是以（几乎）自成一体的方式，介绍这个精彩故事的开端：Tsfasman、Vlăduţ和Zink定理的原始证明。值得一提的是，1995年，Garcia和Stichtenoth [**GS95**] 提出了另一种方法，而且在某种程度上更为明确，可用于设计曲线序列（实际上是函数域序列，但这两个对象是等价的），并达到

所谓的德林费尔德–弗拉杜茨 [**VD83**]。介绍这个原始证明或许会显得有些奇怪，因为事实证明它比Garcia和Stichtenoth的方法复杂得多，但这样做也有一些合理的动机：

- Tsfasman、Vlăduţ 和 Zink 的证明体现了代数几何码理论的丰富内涵；证明中运用了代数几何和数论中的深刻结果。
- 这一原创证明经常被引用，但很少有参考文献对其作完整阐述；而且（依我个人之见），Tsfasman 等人和 Ihara 的论文都没有给出足够详尽的证明。两篇文章中的证明都不到十行，却隐含了大量前置知识。
- 最后，我希望开设这门讲座，因为这个证明优美而精巧；虽然我并非那些为了事物之美(1) 而从事数学研究的数学家之一，但有时花些时间欣赏某个推导的优雅之处，也是一件令人愉快的事。

讲义提纲。— 第 1 节从线性码的基础及其渐近行为讲起。第 2 节介绍代数曲线，并提供代数几何方面所需的知识。第 3 节介绍代数几何码，并陈述主要结果：Tsfasman– Vlăduţ–Zink 定理。讲义其余部分将用于证明这一结论。第 4 节和第 5 节分别补充椭圆曲线和模曲线方面的知识。第 6 节完成证明。

致谢。—— 首先，我想感谢 Gianira Alfarano、Karan Khaturia、Alessandro Neri、Violetta Weger，以及代数编码理论暑期学校(2) 2022的组织者，他们给了我将过去的手写笔记录入电脑的动力。如果他们没有提出这个请求，我可能永远也抽不出时间来做这件事。几位同事花时间仔细阅读了这些笔记。特别要衷心感谢 Elena Berardini、Maxime Bombar、Grégoire Lecerf、Jade Nardi、Christophe Ritzenthaler、Joachim Rosenthal 和 Gilles Zémor，他们对笔记的初稿提出了中肯的意见。

作者获得法国法国国家研究署 资助，用于参与合作项目 ANR-21-CE39-0009-BARRACUDA。

1. 线性码

1.1. 背景。—— 下文我们关注线性 q元码，它们是 $\mathbb{F}_q^n$的线性子空间。研究这类对象之所以困难，但也因此格外有趣，是因为我们考虑的不仅是有限维向量空间这类基本对象，还考虑赋有**度量**的空间：汉明度量。两个向量 $\boldsymbol{x}$、 $\boldsymbol{y} \in \mathbb{F}_q^n$ 之间的汉明距离记作

$$\mathrm{d_H}(\boldsymbol{x}, \boldsymbol{y}) \overset{\mathbf{def}}{=} \sharp\{i \in \{1, \dots, n\} \mid x_i \neq y_i\}.$$

向量的汉明重量 是它与零向量之间的汉明距离。

$$\forall \boldsymbol{x} \in \mathbb{F}_q^n, \qquad \mathrm{w_H}(\boldsymbol{x}) \overset{\mathbf{def}}{=} \mathrm{d_H}(\boldsymbol{x}, \boldsymbol{0}).$$

1.2. 线性码。— 除非另有说明，码 均表示一个线性子空间 $\mathcal{C} \subseteq \mathbb{F}_q^n$。 $\mathcal{C}$ 中的向量通常称为码字。将 $\mathcal{C}$ 视为 $\mathbb{F}_q$–向量空间时，其维数 总记为 k ，其最小距离记为 d ，定义如下：

$$d \overset{\mathbf{def}}{=} \min_{\substack{\boldsymbol{x}, \boldsymbol{y} \in \mathcal{C} \\ \boldsymbol{x} \neq \boldsymbol{y}}} \{\mathrm{d_H}(\boldsymbol{x}, \boldsymbol{y})\} = \min_{\boldsymbol{c} \in \mathcal{C} \setminus \{0\}} \{\mathrm{w_H}(\boldsymbol{c})\},$$

其中，最后一个等号是线性性的推论。码 $\mathcal{C} \subseteq \mathbb{F}_q^n$ 的参数 指三元组 n, k, d，通常记作 $[n, k, d]_q$，其中基域的基数 q 在下标中给出

(1)字面意思："为了事物之美"

(2)https://math.uzh.ch/act/

。最后，人们也会关注码的**码率** 和**相对距离**，其定义和记号如下：

$$R \overset{\text{def}}{=} \frac{k}{n} \qquad \text{and} \qquad \delta \overset{\text{def}}{=} \frac{d}{n}.$$

编码理论中的一个长期问题是：哪些参数三元组 $[n,k,d]$ 可以实现？如果 k 和 d 都尽可能接近 n，则称一个码是“好的”。然而，存在许多上界，其中最基本的是***Singleton* 界**，它指出，对于参数为 $[n,k,d]_q$ 的任意码，都有

$$k + d \leqslant n + 1. \tag{1}$$

提出这个问题的理由在于，k 和 d 都量化了线性码的某种特征。假设给定一个传输信道，例如有线信道，或无线通信中的信道，比如计算机与 WiFi 天线等电子设备之间的通信。码率无非是信息量与实际通过信道发送的数据量之比。因此，码率 $R = k/n$ 量化了编码的效率。

另一方面，最小距离量化了码字彼此之间的距离，因此也量化了从受损码字(3)中恢复原始消息的理论能力。

最后，假设我们的目标是纠正给定信道中的错误。以参数为 $p \in [0, 1 - \frac{1}{q}]$ 的q元对称信道为例，该信道以向量 为输入，并输出向量，其中 $(, \ldots\ldots, e_n)$，而 e_i 是取值于 $\mathbb{F}_q$ 上的独立随机变量，取值为 0 的概率为 $1-p$，取值为 $\mathbb{F}_q \setminus \{0\}$ 中任意其他值的概率为 $\frac{p}{q-1}$。我们的错误向量的平均重量满足

$$\mathbb{E}(\mathrm{w_H}(\boldsymbol{e})) = pn.$$

然而，当 n 较小时，可能会出现偏差，输入向量 $\boldsymbol{c}$ 可能受到远多于 $\lfloor pn \rfloor$ 个错误的破坏。因此，考虑 n 的较大取值是有意义的；此时大数定律可以说明，错误的重量将接近期望值。

最后这番讨论促使我们寻找具有参数 $[n_s, k_s, d_s]$ 的码序列 $(\mathcal{C}_s)_{s\in\mathbb{N}}$，其中

$$\lim_{s\to+\infty} n_s = +\infty$$

and

$$\lim_{s\to+\infty} \frac{k_s}{n_s} = R \qquad \lim_{s\to+\infty} \frac{d_s}{n_s} = \delta.$$

注记 ***1***。——通常在文献中，并不认为序列 $(k_s/n_s)_s$ 和 $(d_s/n_s)_s$ 会收敛，而是使用上极限来代替实际的极限。

在这一设定下，可达参数对 $(\delta,\ R) \in [0,1]\times[0,1]$ 仍是一个悬而未决的问题。目前已知一些界：

- Singleton 界立即推出 $R + \delta \leqslant 1$;
- 一个称为 **普洛特金界** 的更精确界推出 $R + \delta \leqslant 1 - \frac{1}{q}$。例如参见 [**Cou16**，第 4] 章。

- “总能从好码构造出坏码”这一原理可以证明：给定一个可达参数对 $(\delta,\ R)$，任何满足 $\delta' \leqslant \delta$ 且 $R' \leqslant R$ 的参数对 $(\delta',\ R')$ 也是可达的。

练习 ***2***。——证明这一最后的断言。

- 更准确地说，Manin 已证明 [**VM84**]，：在 $[0,1]\times[0,1]$ 中，可达参数对（$\delta,\ R$）与不可达参数对之间的边界是一个连续函数 $R = \alpha_q(\delta)$ 的图像。然而，虽然证明该函数 α_q 的存在性和连续性并不困难，但要明确描述这个函数仍是一个悬而未决的问题。α_q 的一个上界，是所有已知的关于可达参数对（$\delta,\ R$）的上界中的最小值。

(3)在这里，我们不讨论用于纠正错误的实用算法。

- 另一方面，关于随机码平均行为的一项著名结果，即吉尔伯特–瓦尔沙莫夫界，断言：对于码率固定为 R 的随机码(4) $\mathcal{C} \subseteq \mathbb{F}_q^n$，对任意$\varepsilon > 0$， $\mathcal{C}$ 的相对距离 δ 满足以下条件的概率

$$R \in [1 - H_q(\delta) - \varepsilon, 1 - H_q(\delta) + \varepsilon],$$

趋于 当 n 趋于无穷大时趋于 1。函数 $H_q(\cdot)$ 是 q 元熵函数，定义如下

$$H_q : \left\{ \begin{array}{ccc} [0,1] & \longrightarrow & \mathbb{R} \\ x & \longmapsto & \left\{ \begin{array}{ll} -\log_q(q-1) - x\log_q(x) - (1-x)\log_q(1-x) & \text{if} \quad x \neq 0, 1 \\ 0 & \text{otherwise.} \end{array} \right. \end{array} \right.$$

简言之，对于一个随机序列，参数对 (δ, R) 满足 $R = 1 - H_q(\delta)$。

总之，未知函数 $\delta \mapsto \alpha_q(\delta)$ 的图像是可达参数对区域 (δ, R) 的边界。已知该函数连续，其下界为 Gilbert–Varshamov 界$\delta \mapsto 1 - H_q(\delta)$，上界为所有已知上界中的最小值。长期以来，人们一直认为 Gilbert–Varshamov 界是最优的，而且无论如何，都不存在任何码族能够渐近地胜过随机码。Tsfasman、Vlăduţ 和 Zink [**TVZ82**]取得了突破，他们证明渐近 Gilbert–Varshamov 界并非总是最优的。更确切地说，他们证明了以下结论。

定理 *3.* — 设 $q = p^2$，其中 p 是素数。那么对于任意 $R \in [0,1]$，都存在一个码序列，其长度趋于无穷，且其渐近参数 (δ, R) 满足

$$R + \delta \geqslant 1 - \frac{1}{p-1}.$$

注 ***4.*** — 实际上，对于任意满足 p 为素数且 $m \geqslant 1$的 $q = p^{2m}$，该结果均成立。

注 ***5.*** — 实际上，关于码的结果是关于存在具有特定性质的代数曲线序列的一条结论的推论（详见定理 41）。这条关于曲线的结论由 Tsfasman、Vlăduţ 和 Zink 在 [**TVZ82**] 中证明，Ihara 也独立地在 [**Iha81**]中证明。然而，Ihara 并未将这一结果与编码理论联系起来，而 Tsfasman等人 则做到了。

事实证明，正如图 1 和图 2 所示，对于 $q \geqslant 49$，这类码优于 Gilbert–Varshamov 界。这些码实际上远非随机码，而是利用数论和代数几何学中的优雅技巧构造而成。这些讲义旨在概述这一惊人结果的证明；它或许是编码理论最重大的突破之一。

2. 代数曲线

本节的目的**并非**深入讲授代数几何，而只是提供理解本讲义后续内容所需的最低限度的代数几何预备知识。具体而言，这里将省略大部分证明。我建议任何对代数几何感到得心应手，且认为阅读 Harsthorne 的书 [**Har77**] 并不比阅读《哈利·波特》更难的读者**跳过**本节，理由有二：

- 他/她不会从中学到任何东西；
- 对于一位熟悉概形语言的读者来说，本节内容可能显得不够严谨。

如果你想进一步了解代数几何，我可以根据你对这一主题的了解程度，推荐以下读物：

- Walker 的著作 [**Wal00**] 对于完全不了解代数几何和代数几何码的读者来说，是一部极佳的入门读物。

(4)这可以形式化如下：考虑由所有长度为 n 且维数为 Rn 的码在 $\mathbb{F}_q^n$中组成的集合。这个集合是有限的，令 $\mathcal{C}$ 为在该集合上均匀分布的随机变量。

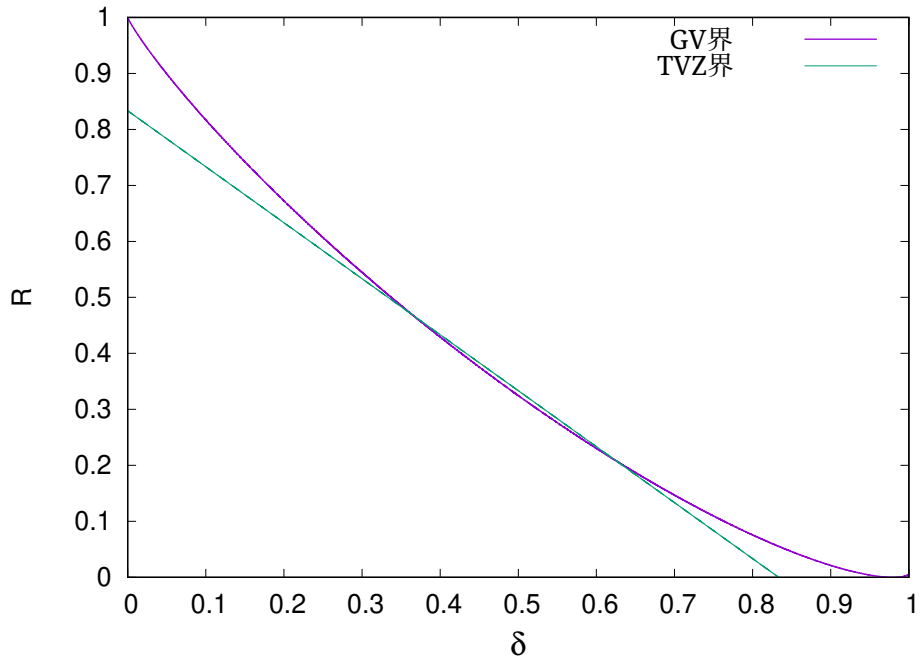


图1。 $q = 49$的TVZ界

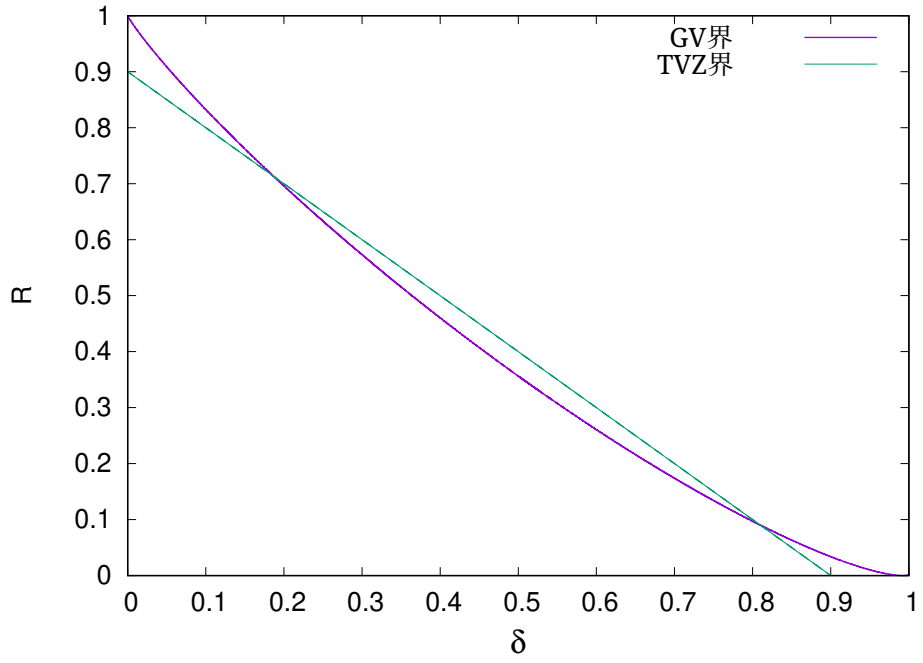


图 2。 $q = 121$ 的 TVZ界

• 如果你不 喜欢几何学，Stichtenoth 的著作 [Sti09] 则从纯粹的算术角度，对代数几何码作了极佳的介绍。书中特别给出了 Tsfasman–Vlăduţ–Zink 定理的另一种证明，该证明基于所谓的函数域递归塔，不涉及任何几何考量。

- 关于代数几何码的更深入介绍，可见 Tsfasman Vlăduţ 和 Nogin 的著作 [**TVN07**]以及 Stepanov 的著作 [**Ste99**]。
- 最后，对于有兴趣在代数编码理论之外了解代数几何的读者，建议（例如）参阅以下著作： [**Ful89, Sha94**]。Lorenzini 的著作 [**Lor96**]也很值得一读，尤其适合希望更深入了解算术方面的读者。

2.1. 平面曲线与函数。 —— 设 $\mathbb{K}$ 为一个完美域[5]， $\mathbb{K}$ 为其代数闭包。分别用 $\mathbb{A}^2(\mathbb{K})$ 和 $\mathbb{P}^2(\mathbb{K})$ 表示 $\mathbb{K}$ 上的仿射平面和射影平面。 $\mathbb{K}$ 上的一条仿射平面曲线 $\mathscr{X}$ 是 $\mathbb{A}^2(\mathbb{K})$ 中非零二元多项式 $f(x,y) \in \mathbb{K}[x,y]$ 的消失轨迹。类似地，一条射影平面曲线是 $\mathbb{P}^2(\mathbb{K})$ 中非零齐次多项式 $F(X,Y,Z) \in \mathbb{K}[X,Y,Z]$ 的消失轨迹。回忆一下，射影平面 $\mathbb{P}^2(\mathbb{K})$ 是 $\mathbb{K}^3$ 的向量直线集合，或者等价地说，是商集

$$\mathbb{P}^2(\overline{\mathbb{K}}) \stackrel{\text{def}}{=} (\overline{\mathbb{K}}^3 \setminus \{0\})/\overline{\mathbb{K}}^\times,$$

其元素表示为三元组 $(u : v : w)$，并满足等价关系：若存在 $\lambda \in \mathbb{K}^\times$，使得 $u = \lambda a$、 $v = \lambda b$ 和 $w = \lambda c$，则 $(u : v : w) \sim (a : b : c)$。

若仿射（分别为射影）曲线的 f（分别为 F）是 $\mathbb{K}[x,y]$（分别为 $\mathbb{K}[X,Y,Z]$）中的不可约多项式，则称该曲线为不可约；若将 f（分别为 F）视为 $\mathbb{K}[x,y]$（分别为 $\mathbb{K}[X,Y,Z]$）中的元素时仍不可约，则称其为绝对不可约。

例 ***6***。—设 $\mathbb{K} = \mathbb{Q}$，并考虑方程为 $x^2 - 2y^2 = 0$ 的仿射曲线 $\mathscr{X}$。这条曲线不可约，但**并非**绝对不可约。事实上，在 $\mathbb{Q}$ 上，曲线的方程可因式分解为 $(x - \sqrt{2}y)\ (x + \sqrt{2}y) = 0$，且此因式分解并非定义在 $\mathbb{Q}$ 上：多项式 $x^2 - 2y^2$ 在 $\mathbb{Q}$ 上不可约，但在 $\mathbb{Q}$ 上可约。从几何角度来看， $\mathscr{X}$ 是由两条直线组成的，它们的方程分别为 $x - \sqrt{2}y = 0$ 和 $x + \sqrt{2}y = 0$。这些直线并非定义在 $\mathbb{Q}$ 上，但它们的并集是。

给定仿射不可约平面曲线 $\mathscr{X}$，商环 $\mathbb{K}[x,y]/(f)$ 是整环，其分式域 $\mathrm{Frac}(K[x,y]/(f))$ 定义良好，称为 $\mathscr{X}$ 的函数域。在射影情形下，函数域也可以定义为分式域 $\frac{A(X,Y,Z)}{B(X,Y,Z)}$，其中，$B$ 是次数**相同**的齐次多项式，且 B 不能被 F 整除，并满足如下关系：

$$\frac{A(X,Y,Z)}{B(X,Y,Z)} = \frac{C(X,Y,Z)}{D(X,Y,Z)} \quad \text{if} \quad F \text{ divides } (AD - BC).$$

对于仿射曲线 $\mathscr{X}$， $\mathbb{K}[x,y]/(f)$ 的元素可以理解为多项式函数在曲线 $\mathscr{X}$ 上的限制。事实上，考虑两个多项式 $a(x,y)$ $b(x,y) \in \mathbb{K}[x,y]$ 视为函数 $\mathbb{A}^2(\mathbb{K}) \to \mathbb{K}$，可以考虑它们在 $\mathscr{X}$ 上的限制。一个通常称为希尔伯特零点定理的著名结果（例如参见 [**Ful89**，§ 1.7]）指出，当且仅当 f 整除 $a - b$ 时，它们在 $\mathscr{X}$ 上的限制相同，因此当且仅当它们模由 f 张成的理想同余。

在射影情形中，齐次多项式不能被解释为函数 $\mathbb{P}^2(\mathbb{K}) \to \mathbb{K}$，因为复数域 $\mathbb{P}^2(\mathbb{K})$ 中的一个元素既可由三元组 $(u : v : w)$ 表示，也可由任意其他三元组 $(\lambda u : \lambda v : \lambda w)$ 表示，其中 $\lambda \in \mathbb{K}^\times$ 可取任意值。因此，给定一个次数为 $d > 0$ 的非恒定齐次多项式 $P \in \mathbb{K}[X,Y,Z]$，其求值并无意义，因为 $P(\lambda u,\ \lambda v,\ \lambda w) = \lambda^d P(u,\ v,\ w)$。不过请注意，对于这样的多项式，在一点处消失是一个定义良好的概念。此外，两个次数相同的齐次多项式之比 P/Q 的求值是有意义的，因为

$$\frac{P(\lambda u, \lambda v, \lambda w)}{Q(\lambda u, \lambda v, \lambda w)} = \frac{\lambda^d P(u,v,w)}{\lambda^d Q(u,v,w)} = \frac{P(u,v,w)}{Q(u,v,w)}.$$

这就是我们引入这些对象、将其作为射影曲线上函数的恰当定义的原因。

注记 ***7***. — 请注意，我们在这里同时涉及 $\mathbb{K}$和 $\mathbb{K}$。这里至关重要的是要注意，曲线被定义为坐标属于 $\mathbb{K}$的点集，而函数应当是系数属于 $\mathbb{K}$的有理函数。另一方面，函数域定义在 $\mathbb{K}$ 上，用来描述这条

(5)下文所关注的域要么是 $\mathbb{C}$，要么是有限域 $\mathbb{F}_q$。

曲线的算术。另一方面，将曲线描述为点集时，如果只考虑坐标属于 $\mathbb{K}$ 的点，就太局限了：例如，设想 $\mathbb{K}$ 是有限域的情形；此时，坐标属于 $\mathbb{K}$ 的点集是有限的，甚至可能为空！于是，截然不同的方程可能给出相同的坐标属于 $\mathbb{K}$ 的点集，而坐标属于$\mathbb{K}$ 的点集则会大不相同。这解释了为何要考虑坐标属于 $\mathbb{K}$ 的点。

注 ***8.*** — 请注意，谈到函数时，这些对象可能并未在曲线上的所有点都有定义，并且可能在某些地方有极点。这些对象可以理解为复分析中亚纯函数的代数几何对应物。

注 ***9.*** — 众所周知，射影平面可以由仿射平面覆盖，这些仿射平面有时称为仿射图。事实上，可以将仿射平面嵌入 $\mathbb{P}^2$ 中，如下所示：

$$\begin{cases} \mathbb{A}^2(\overline{\mathbb{K}}) & \longrightarrow & \mathbb{P}^2(\overline{\mathbb{K}}) \\ (x,y) & \longmapsto & (x:y:1) \end{cases} \text{ or } \begin{cases} \mathbb{A}^2(\overline{\mathbb{K}}) & \longrightarrow & \mathbb{P}^2(\overline{\mathbb{K}}) \\ (x,y) & \longmapsto & (x:1:y) \end{cases} \text{ or } \begin{cases} \mathbb{A}^2(\overline{\mathbb{K}}) & \longrightarrow & \mathbb{P}^2(\overline{\mathbb{K}}) \\ (x,y) & \longmapsto & (1:x:y). \end{cases}$$

这三个嵌入的像覆盖整个射影平面。因此，给定一条射影曲线，可以将该曲线限制在上述某个嵌入的像上，从而得到一条仿射曲线。实际上，从方程为 $F(X,Y,Z)=0$ 的射影曲线出发，例如可以考虑方程为 $F(x,y,1)=0$ 的仿射曲线，也可以考虑方程为 $F(x,1,y)=0$或 $F(1,x,y)=0$的仿射曲线。因此，可以从给定的射影曲线推导出仿射曲线（仿射图）。另一方面，从方程为 $f(x,y)=0$ 的仿射曲线 $\mathscr{X}$出发，次数为 $\deg f$的齐次多项式$F(X,Y,Z)$，满足 $f(x,y)=F(x,y,1)$（这种齐次化是唯一的，细节留给读者），它是有时称为 $\mathscr{X}$的射影闭包的曲线的方程。

一个关键事实是，曲线及其射影闭包共有一个对象：**它们的函数域完全相同**。

2.2. 点。— $\mathscr{X}$ 上的一个点是一个元素 $(a,b)\in\mathbb{A}^2(\mathbb{K})$（分别为 $(u:v:w)\in\mathbb{P}^2(\mathbb{K})$），满足$f(a,b)=0$（分别为 $F(u,v,w)=0$）。如果一个点的所有坐标都属于 $\mathbb{K}$，就称它为有理点或 $\mathbb{K}$点。更一般地，给定一个扩张 $\mathbb{L}/\mathbb{K}$，可以定义 $\mathscr{X}$的 $\mathbb{L}$点。 $\mathscr{X}$ 的 $\mathbb{K}$点或 $\mathbb{L}$点的集合分别记为 $\mathscr{X}(\mathbb{K})$ 和 $\mathscr{X}(\mathbb{L})$。接下来我们感兴趣的主题之一是 $\mathbb{K}=\mathbb{F}_q$这种情形。在这种情况下，很容易看出 $\mathscr{X}(\mathbb{F}_q)$ 是有限的。实际上，它是 $\mathbb{A}^2(\mathbb{F}_q)$ 或 $\mathbb{P}^2(\mathbb{F}_q)$ 的子集，而这两个集合都是有限集。另一方面， $\mathscr{X}$ 被定义为$\mathbb{K}$点的集合，我们有时在下文中称之为几何点，因此，当我们想强调关注的是任意可能的点时，也可以将其记作$\mathscr{X}(\mathbb{K})$。

给定域 $\mathbb{K}$ 上由方程 $f(x,y)=0$（分别为 $F(X,Y,Z)=0$）定义的仿射（分别为射影）曲线 $\mathscr{X}$，若点 $P\in\mathscr{X}(\mathbb{K})$ 的坐标为 (x_P,y_P)（分别为 $(u_P:v_P:w_P)$），则称该点为奇异点，当

$$\frac{\partial f}{\partial x}(x_P,y_P)=\frac{\partial f}{\partial y}(x_P,y_P)=0$$

分别

$$\frac{\partial F}{\partial X}(u_P,v_P,w_P)=\frac{\partial F}{\partial Y}(u_P,v_P,w_P)=\frac{\partial F}{\partial Z}(u_P,v_P,w_P)=0.$$

非奇异点称为正则点。没有奇点的曲线称为正则或光滑曲线。另一方面，至少有一个奇点的曲线称为奇异曲线。可以证明，曲线的奇点集总是有限的。

从现在起，除非另有说明，**任意曲线均为光滑射影且绝对不可约的**。

2.3. 点上的伽罗瓦作用。——回顾一下，为简化起见，我们将定义限定在基域 $\mathbb{K}$ 为完美域的情形。这对后续目的而言并非严格限制，因为 $\mathbb{K}$ 总是有限域或特征零域。

给定一条定义在 $\mathbb{K}$ 上的曲线 $\mathscr{X}$，任意点 $P\in\mathscr{X}(\mathbb{K})$ 的坐标为 (x_P,y_P)（在射影情形下为 $(u_P:v_P:w_P)$）。这些坐标属于 $\mathbb{K}$，而 $\mathscr{X}$ 由系数属于 $\mathbb{K}$ 的多项式方程定义，因此伽罗瓦群 $\mathrm{Gal}(\overline{\mathbb{K}}/\mathbb{K})$ 在 $\mathscr{X}$ 的点上有自然的作用。注意， P 的坐标

在 $\mathbb{K}$ 上是代数的，因此生成 $\mathbb{K}$ 的一个有限扩张，通常记作 $\mathbb{K}(P)$。因此，即使 $\mathrm{Gal}(\mathbb{K}/\mathbb{K})$ 可能是一个复杂的对象（一个序 profinite 群），P 也在 $\mathrm{Gal}(\mathbb{K}/\mathbb{K}(P))$ 的作用下保持不变，因此 P 的轨道是一个有限集合，它恰好是有限群 $\mathrm{Gal}(\mathbb{K}(P)'/\mathbb{K})$ 在 P 上的作用所产生的轨道，其中 $\mathbb{K}(P)'$ 是 $\mathbb{K}(P)$ 在 $\mathbb{K}$ 上的伽罗瓦闭包。

定义**10**。——设 $\mathbb{K}$ 是一个完美域，定义在 $\mathbb{K}$ 上的曲线 $\mathscr{X}$ 的一个闭点是几何点 $\underline{P} \in \mathscr{X}(\overline{\mathbb{K}})$ 在绝对伽罗瓦群 $\mathrm{Gal}(\overline{\mathbb{K}}/\mathbb{K})$ 作用下的轨道。

此类轨道中元素的个数称为闭点的次数。它也等于扩张次数 $[\mathbb{K}(P) : \mathbb{K}]$。有理点总是闭点，因为它在绝对伽罗瓦群的任意元素作用下都保持不变，因此它等于在该群作用下自身的轨道。

注**11**。——如果你更习惯数论的表述，那么闭点不过是函数域 $\mathbb{K}(\mathscr{X})$ 的素位的几何类比。

例**12**。——考虑 $\mathbb{K} = \mathbb{Q}$ 的情形，以及方程为 $x^2 + y^2 - 1 = 0$ 的仿射曲线 $\mathscr{C}$（一个圆）。坐标为 $(1, 0)$ 的点是 $\mathscr{X}$ 的有理点，即 $\mathscr{C}(\mathbb{Q})$ 的一个元素。复点 $(2, \sqrt{3}i)$（其中 $i^2 = -1$）是 $\mathscr{C}$ 的几何点，即 $\mathscr{C}(\mathbb{C})$ 的一个元素。最后，$\{(2, i\sqrt{3}), (2, -i\sqrt{3})\}$ 是 $\mathscr{C}$ 的一个二次闭点。

2.4. 曲线之间的映射。— 与代数中的通常做法一样，一旦引入了结构，例如群、环、模等，就会引入这些对象之间的态射。对于曲线，我们关注两类映射，分别称为态射 和有理映射。两个仿射（分别为射影）曲线 $\mathscr{X}, \mathscr{Y}$（包含于 $\mathbb{A}^2$（分别为 $\mathbb{P}^2$））之间的有理映射 是一个映射：

$$\varphi : \left\{ \begin{array}{ccc} \mathscr{X} & \dashrightarrow & \mathscr{Y} \\ (x,y) & \longmapsto & (\varphi_1(x,y), \varphi_2(x,y)) \end{array} \right.$$

分别

$$\psi : \left\{ \begin{array}{ccc} \mathscr{X} & \dashrightarrow & \mathscr{Y} \\ (u:v:w) & \longmapsto & (\psi_1(u,v,w), \psi_2(u,v,w), \psi_3(u,v,w)). \end{array} \right.$$

其中 ϕ_1, ϕ_2（分别为 ψ_1, ψ_2, ψ_3）是 $\mathbb{K}(\mathscr{X})$ 中的元素（在射影情形下，三个函数 ψ_1, ψ_2, ψ_3 中至少有一个非零）。这里用虚线箭头 $\dashrightarrow$ 强调该映射并非在每一点都有定义，而只在子集[6]上有定义。对于仿射曲线，在 φ_1, φ_2没有极点的任意点处，该映射都有定义，并称为正则。对于射影曲线，在任意一点 P 处，若存在某个 $\eta \in \mathbb{K}(\mathscr{X})^\times$，使得 $\eta\psi_1, \eta\psi_2, \eta\psi_3$ 在 P 处均无极点且不同时消失，则映射 ψ 在该点有良好定义，并称其在 P处正则 。若两个曲线 $\mathscr{X} \dashrightarrow \mathscr{Y}$ 之间的有理映射在 $\mathscr{X}$的每一点处都正则，则称其为正则 。

有理映射 $\varphi : \mathscr{X} \dashrightarrow \mathscr{Y}$ 会反向诱导一个域扩张 $\mathbb{K}(\mathscr{Y}) \hookrightarrow \mathbb{K}(\mathscr{X})$，其定义如下：

$$h \in \mathbb{K}(\mathscr{Y}) \longmapsto h \circ \varphi \in \mathbb{K}(\mathscr{X}).$$

φ 的次数定义为这个域扩张的次数。

例 **13**。——回到例12。映射

$$\left\{ \begin{array}{ccc} \mathscr{C} & \dashrightarrow & \mathbb{P}^1 \\ (x,y) & \longmapsto & (x:1) \end{array} \right. \tag{2}$$

是一个有理映射。也可以构造一个有理映射 $\mathbb{P}^1 \to \mathscr{C}$，如下所示：

$$\left\{ \begin{array}{ccc} \mathbb{P}^1 & \dashrightarrow & \mathscr{C} \\ (u:v) & \longmapsto & \left(\frac{v^2-u^2}{u^2+v^2}, \frac{2uv}{u^2+v^2}\right). \end{array} \right. \tag{3}$$

请注意，这两个映射互不为逆映射。

最后，以下结论是众所周知的，证明从略。

(6)事实证明，对于一种称为扎里斯基拓扑的适当拓扑，这个子集是稠密的

命题 ***14***。— 设 $h : \mathscr{X} \to \mathscr{Y}$ 是两条光滑射影绝对不可约曲线 $\mathscr{X}, \mathscr{Y}$ 之间的有理映射。

(i) 若 $\mathscr{X}$ 是光滑的，则 h 是正则的；*(ii)* 若 h 非常数，则它是满射。

2.5. 赋值。— 回忆一下，局部环是指只有一个极大理想的环。局部一词恰恰源于这样一个事实：许多此类环可以理解为由局部性质刻画的函数环。例如，给定一条仿射曲线 $\mathscr{X}$ 和一个坐标为（x_P， y_P）的有理点 P，环$\mathcal{O}_{\mathscr{X},\,P}$定义为 $\mathbb{K}(\mathscr{X})$的子环，由在 P处正则（即没有极点）的函数组成。也就是说

$$\mathcal{O}_{\mathscr{X},P} \stackrel{\mathbf{def}}{=} \left\{ \frac{a(x,y)}{b(x,y)} \in \mathbb{K}(\mathscr{X}) \;\middle|\; b(x_P, y_P) \neq 0 \right\}.$$

可以证明，这个环是一个局部环，其极大理想为:

$$\mathfrak{m}_{\mathscr{X},P} \stackrel{\mathbf{def}}{=} \left\{ \frac{a(x,y)}{b(x,y)} \in \mathbb{K}(\mathscr{X}) \;\middle|\; b(x_P, y_P) \neq 0 \text{ and } a(x_P, y_P) = 0 \right\}.$$

当点 P 光滑时，已知环$\mathcal{O}_{\mathscr{X},P}$ 是离散赋值环，这意味着极大理想$\mathfrak{m}_{\mathscr{X},P}$ 是主理想；并且给定该极大理想的一个生成元 t，对于任意非零元素$a \in \mathcal{O}_{\mathscr{X},P}$，都存在一个非负整数 n和一个元素$\varphi \in \mathcal{O}^{\times}_{\mathscr{X},P}$，使得 $a = \varphi t^n$。这样的生成元 t （属于）$\mathfrak{m}_{\mathscr{X},P}$称为 P处的局部参数（有时也称为一致化参数）。此外，整数 n 不依赖于生成元 t 的选择，称为 P处 a 的赋值，记作 $v_P(a)$。接下来容易证明， $\mathbb{K}(\mathscr{X})$不过是$\mathcal{O}_{\mathscr{X},P}$的分式域。于是，任意函数 $h \in \mathbb{K}(\mathscr{X})$都可以写成$h = \frac{h_1}{h_2} \in \mathbb{K}(\mathscr{X}) \setminus \{0\}$，其中$h_1, h_2 \in \mathcal{O}_{\mathscr{X},P}$，而 h 在 P处的赋值定义为 —

$$v_P(h) = v_P(h_1) - v_P(h_2).$$

总之，我们引入了一个映射

$$v_P : \mathbb{K}(\mathscr{X}) \setminus \{0\} \to \mathbb{Z}$$

并且已知这个映射满足以下性质:

- $\forall a, b \in \mathbb{K}(\mathscr{X}) \setminus \{0\}$, $v_P(ab) = v_P(a) + v_P(b)$;
- $\forall a,\ b \in \mathbb{K}(\mathscr{X}) \setminus \{0\}$, $v_P(a+b) \geqslant \min\{v_P(a)\ v_P(b)\}$，且当 $v_P(a) \neq v_P(b)$ 时等号成立。

最后需要强调的是，即使我们是在有理点处定义这一概念，实际上也可以将其扩展到任意几何点，只需将 $\mathbb{K}(\mathscr{X})$ 替换为 $\mathbb{K}(\mathscr{X})$，即 $\mathscr{X}$ 上系数取自 $\mathbb{K}$的有理函数域。因此，赋值可以定义在任何可能的点处。

2.6. 除子。—— 研究曲线的几何学和算术时，一个基本对象是除子，它们在某种意义上是曲线/函数域中对应于数域理论中的分式理想的对象。

给定完美域 $\mathbb{K}$ 上的一条**光滑**曲线 $\mathscr{X}$，一个（几何）除子是 $\mathscr{X}$ 的几何点的形式 $\mathbb{Z}$–线性组合。若一个除子在 $\mathrm{Gal}(\mathbb{K}/\mathbb{K})$ 的作用下整体不变，则称其为有理除子。等价地，它是 $\mathscr{X}$ 的闭点的形式和。

因此， $\mathscr{X}$ 上的除子 G 可以表示为

$$G = n_1 P_1 + \cdots + n_r P_r, \tag{4}$$

其中 n_i 是整数， P_i 是 $\mathscr{X}$ 的几何点。集合 $\{P_1, \ldots, P_r\}$ 称为 G 的支撑。如果对于任意 i, $j \in \{1, \ldots, r\}$，只要 P_i P_j 在 $\mathrm{Gal}(\mathbb{K}/\mathbb{K})$ 的作用下属于同一轨道，就有 $n_i = n_j$，则该除子是有理的。

注***15***。——我们强调，有理点之和会给出一个有理除子，但反之不成立。有理除子可能是非有理点之和。参见后面的例16。

例***16***. — 回到例12中定义在 $\mathbb{Q}$ 上的曲线，其方程为 $x^2 + y^2 - 1 = 0$。考虑点 $P = (\frac{1}{2}, \frac{\sqrt{3}}{2})$ $P' = (\frac{1}{2}, -\frac{\sqrt{3}}{2})$ 和 $Q = (1, 0)$。那么，当且仅当 $a = b$时， $aP + bP' + cQ$ 是该曲线上的有理除子。

除子群上定义了一个偏序关系，记为 $\leqslant$，如下所述。给定两个除子

$$G = \sum_{P \in \mathscr{X}(\overline{\mathbb{K}})} n_P P \quad \text{and} \quad G' = \sum_{P \in \mathscr{X}(\overline{\mathbb{K}})} n'_P P,$$

我们称 $G \leqslant G'$ 当

$$\forall P \in \mathscr{X}(\overline{\mathbb{K}}),\ n_P \leqslant n'_P.$$

特别地，若除子 G 满足 $G \geqslant 0$，则称其为 正，其中 0 表示零除子。

给定如 (4) 中的除子 G，其次数定义为

$$\deg G \overset{\text{def}}{=} n_1 + \cdots + n_r.$$

给定函数 $f \in \mathbb{K}(\mathscr{X}) \setminus \{0\}$，可将其除子记作 (f)，并定义为

$$(f) \overset{\text{def}}{=} \sum_{P \in \mathbb{K}(\mathscr{X})} v_P(f) P. \tag{5}$$

这样的除子称为主除子。

注 ***17***。——要使这样的对象成为除子，我们需要证明求和式 (5) 是有限的，也就是说，n_P 中只有有限个不为零。这实际上源于一个众所周知的事实，该事实将在下一个命题中给出，但证明从略。

命题 ***18***。——曲线上的非零有理函数只有有限个零点和极点。

注 ***19***。——值得注意的是，主除子是有理的。事实上，首先可以注意到，由于 $f \in \mathbb{K}(\mathscr{X})$，因此其系数属于 $\mathbb{K}$；于是对于任意几何点 $P \in \mathscr{X}(\mathbb{K})$ 和任意$\sigma \in \mathrm{Gal}(\mathbb{K}/\mathbb{K})$，有 $v_P(f) = v_{\sigma(P)}(f)$。

下面这个非常经典的命题对于后续内容至关重要。

命题 ***20***。——主除子的次数总是0。

我们以一个承认其成立、且将在后文发挥作用的命题结束这段讨论。

命题 ***21***。——与 $f \in \mathbb{K}(\mathscr{X})^\times$ 相关联的主除子(f) 为零，当且仅当 f 是常数。

2.7. 亏格与黎曼–罗赫定理。——最基本的曲线是仿射直线 $\mathbb{A}^1$，其射影闭包是射影直线 $\mathbb{P}^1$。$\mathbb{A}^1$ 上的正则函数无非是一元多项式。将这样的多项式 $h(x) \in \mathbb{K}[x]$ 视为 $\mathbb{P}^1$上的有理函数，它在“无穷远”点处有一个极点，即齐次坐标为 (1 : 0) 的点；并且可以证明，该极点处的赋值无非是 $-\deg h$。

因此，次数小于或等于 n 的多项式空间 $\mathbb{K}[x]_{\leqslant n}$ 可以（十分严谨地说）定义为 $\mathbb{P}^1$ 上的有理函数空间：这些函数在某个仿射图上处处正则，并且在无穷远点处的赋值大于或等于 $-n$。将 P_∞ 记作这个无穷远点，则空间 $\mathbb{K}[x]_{\leqslant n}$ 可以视为有理函数 $h \in \mathbb{K}(\mathbb{P}^1)$ 的空间，其中这些函数要么为 0，要么满足

$$(h) \geqslant -nP_\infty.$$

正如下述定义所示，黎曼–罗赫空间是空间$\mathbb{K}[x]_{\leqslant n}$在曲线上的推广。

定义***22*** **（黎曼–罗赫空间）**。——设 $\mathscr{X}$ 是定义在 $\mathbb{K}$ 上的一条光滑射影绝对不可约曲线，且 G 是 X上的一个有理除子。那么，与 G 相关联的黎曼–罗赫空间定义为

$$L(G) \overset{\text{def}}{=} \{h \in \mathbb{K}(\mathscr{X}) \mid (h) + G \geqslant 0\} \cup \{0\}.$$

这是一个 $\mathbb{K}$上的向量空间。

注***23.*** — 根据前面的讨论，在 $\mathbb{P}^1$ 上，我们有 $L(nP_\infty) \simeq \mathbb{K}[x]_{\leqslant n}$。

以下陈述总结了黎曼–罗赫空间的一些性质。

命题 ***24***。— *(i)* 黎曼–罗赫空间是 $\mathbb{K}$ 上的有限维向量空间；*(ii)* 对任意有理除子 $G<0$，有 $L(G)=\{0\}$；*(iii)* 对任意有理除子 G，有 维数$_{\mathbb{K}} L(G) \leqslant$ 度 $G+1$。

有了上述论述，我们可以引入曲线的一个基本不变量：它的亏格。定义这个对象的方法有几十种，但没有一种是平凡的。这些笔记中给出的定义远不能令人满意，因为它显然不直观。然而，它只需极少的材料就能定义这一对象。

定义 ***25*** **（曲线的亏格）**。— 设 $\mathscr{X}$ 为一条光滑射影绝对不可约曲线。$\mathscr{X}$ 的亏格定义为

$$g=1-\min_{D}\{\dim_{\mathbb{K}} L(D)-\deg D\},$$

其中 D 遍历 $\mathscr{X}$的所有除子。

注记***26***。— 命题 24 (iii) 断言，所涉及的最小值存在，且亏格为非负数。

练习***27.*** — 证明注记26中的陈述。

练习***28.*** — 利用定义 25，证明射影直线 $\mathbb{P}^1$ 的亏格为零。

请注意，亏格的有效计算并非易事。不过，对于次数为 d的光滑平面曲线，存在一个闭合公式（见 [**Ful89**，命题 VIII.5]）：

$$g=\frac{(d-1)(d-2)}{2}.$$

特别地，这使我们能够证明射影直线和光滑圆锥曲线的亏格为 0。

注 ***29.*** — 亏格的概念实际上也可以定义于奇异曲线。在此背景下，可以定义两个不同的不变量，分别称为算术亏格 和几何亏格 。当曲线光滑时，这两个不变量相同。

我们以黎曼–罗赫定理结束本节。这是代数曲线理论中的一个重要命题。此命题作为已知结果，我们请读者参阅 Fulton [**Ful89**] 或 Stichtenoth 的[**Sti09**] 著作以了解证明。该命题的第一部分实际上是我们给出的亏格定义（定义 25）的直接推论。

定理 ***30*** **（黎曼–罗赫定理）**。— 设 $\mathscr{X}$ 是亏格为 g 、定义在 $\mathbb{K}$ 上的光滑绝对不可约曲线，且 G 是 $\mathscr{X}$ 上的有理除子。那么

$$\dim_{\mathbb{K}} L(G)\geqslant \deg G+1-g$$

且当$\deg G>2g-2$时等号成立。

2.8. 黎曼–赫尔维茨公式。— 下文将用到的最后一个结论是黎曼–赫尔维茨公式，它联系了由一个非恒定有理映射 $\varphi\colon \mathscr{X}\dashrightarrow\mathscr{Y}$相连的两条光滑射影绝对不可约曲线$\mathscr{X},\mathscr{Y}$的亏格。回想一下，根据命题 14，这样的映射是正则且满射的。记其次数为 δ （次数的定义见 § 2.4），任取一个几何点 $P\in\mathscr{Y}(\mathbb{K})$。那么可以证明，$\varphi^{-1}(\{P\})$是 $\mathscr{X}(\mathbb{K})$的有限子集，并且对于除有限多个以外的所有 P，$\phi^{-1}(\{P\})$的基数一总是等于 δ。

在有限多个 $\mathscr{Y}(\mathbb{K})$ 的点处，上述性质不再成立，这些点称为分歧点。给定$Q\in\mathscr{X}(\mathbb{K})$、 $P=\varphi(Q)$，以及 t P处的一个局部参数， Q 的分歧指数 定义为

$$e_Q \overset{\text{def}}{=} v_Q(t\circ\varphi),$$

$t\circ\varphi$ 是 $\mathbb{K}(\mathscr{X})$ 的一个元素。可以证明，这个定义与 P 处局部参数 t 的选取无关。根据前面的定义，对于除有限多个点以外的任意点 $Q\in\mathscr{X}(\mathbb{K})$，都有 $e_Q=1$。

现在我们具备了陈述黎曼–赫尔维茨公式所需的材料。

定理 ***31*** **（黎曼–赫尔维茨公式（驯性版本））**。— 设 $\mathscr{X}$、$\mathscr{Y}$ 是定义在 $\mathbb{K}$ 上的两条光滑射影绝对不可约曲线，且 $\varphi\colon \mathscr{X} \dashrightarrow \mathscr{Y}$ 是一个有理映射。假设对任意 $Q \in \mathscr{Y}(\mathbb{K})$，分歧指数 e_Q 与特征 $\mathbb{K}$ 互素。那么，$\mathscr{X}$ 和 $\mathscr{Y}$ 的亏格 $g_{\mathscr{X}}$、$g_{\mathscr{Y}}$ 满足以下公式。

$$(2g_{\mathscr{X}} - 2) = \deg \varphi \cdot (2g_{\mathscr{Y}} - 2) + \sum_{Q \in \mathscr{Y}(\overline{\mathbb{K}})} (e_Q - 1).$$

注 ***32***。— 根据前面的讨论，上述公式中的求和项除有限多项外均为零。

注 ***33***。— 可以放弃“分歧指数与特征互素”这一假设，但须将项 $\sum(e_Q - 1)$ 替换为一个更复杂的项。参见 [Sti09</style}，定理 3.4.13]。

这个公式特别有用，因为许多曲线 $\mathscr{X}$ 都可以用态射 $\mathscr{X} \to \mathbb{P}^1$ 描述。由于已知 $\mathbb{P}^1$ 的亏格为 0，因此根据该映射的次数和分歧指数即可推出 $\mathscr{X}$ 的亏格。

例 ***34.*** — 考虑例 13 中的映射（2），但这里我们将曲线 $\mathscr{C}$ 视为定义在$\mathbb{C}$上的曲线。可以看出，对于任意点 $P = (t : 1) \in \mathbb{P}^1(\mathbb{C})$，当 $t \notin \{-1, 1\}$ 时，该映射有 2 个原像；而当$t \in \{-1, 1\}$时，只有 1 个原像。因此，存在两个分歧点，分歧指数均为 2（可以证明该映射在无穷远处不分歧）。此外，该映射的次数为 2。于是，由黎曼–赫尔维茨公式可得

$$2g_{\mathscr{C}} - 2 = 2(2g_{\mathbb{P}^1} - 2) + 2.$$

由于 $g_{\mathbb{P}^1} = 0$，我们也可推出 $g_{\mathscr{C}} = 0$ 。

2.9. 非平面曲线又如何？ — 最后一个重要事实是，有些曲线不是平面曲线，可能包含在 $\mathbb{P}^N$ 中（其中 $N > 2$）。这一点对后续内容十分重要，因为我们要寻找定义在有限域 $\mathbb{F}_q$ 上的光滑曲线 $\mathscr{X}$，使得 $\sharp\mathscr{X}(\mathbb{F}_q)$任意大。由于 $\sharp\mathbb{P}^2(\mathbb{F}_q)$是有限的（且等于 q^2+q+1），这样的曲线可能无法嵌入 $\mathbb{P}^2$，而需要更高维的环境空间。那么，问题来了.....当考虑 $\mathbb{P}^N$ 中满足 $N > 2$的曲线时，哪些结论仍然成立？实际上，这类对象是如何定义的?

我们将 $\mathbb{P}^N$ 的射影子簇定义为齐次理想 $I \subseteq \mathbb{K}[X_0, \dots, X_N]$中各元素的公共消失轨迹。如果该理想是素理想，则称该代数簇为不可约，在此情形下，代数簇的函数域可以用与平面情形完全相同的方式定义。随后，代数簇的维数可以定义为函数域关于 $\mathbb{K}$的超越次数。曲线是维数为 1 的代数簇。光滑性可以通过要求所有关于 $N + 1$ 变量的偏导数不同时消失来以非常类似的方式定义。所有其他对象——有理映射、赋值、除子、黎曼–罗赫空间——都可以用完全相同的方式定义，只是需要使用更加繁复的记号。最后，前面关于平面曲线的所有论述实际上都适用于任意曲线。

3. 代数几何码

现在，我们已经具备定义代数几何（AG）码所需的材料。在此之前，让我们回顾一下 Reed–Solomon 码的定义，代数几何（AG）码正是对其的推广。

3.1. Reed–Solomon 码。—

定义 ***35***。 — 设 $\alpha_1, \dots, \alpha_n$ 是 $\mathbb{F}_q$ 中互不相同的元素。设 $0 \leqslant k \leqslant n$，码 $\mathbf{RS}_k$ 定义为 as

$$\mathbf{RS}_k(\alpha_1, \dots, \alpha_n) \stackrel{\text{def}}{=} \{(p(\alpha_1), \dots, p(\alpha_n)) \mid p \in \mathbb{F}_q[x]_{\leqslant k-1}\}.$$

众所周知，这些码的参数为 $[n, k, n-k+1]_q$，因此达到 Singleton 界 (1)。然而，它们受到一定限制： α_i 必须互不相同，因此码长最多为 q。所以，即使这些码具有最优参数，也无法用它们在固定域 $\mathbb{F}_q$ 上构造一个码长趋于无穷的无限码族。此时，曲线便派上了用场。首先注意，Reed–Solomon 码还可以用一种更严谨的方式定义如下。考虑射影直线 $\mathbb{P}^1$，并设 $P_1, \dots, P_n$ 是 $\mathbb{P}^1$ 上的有理点，其对应的齐次坐标分别为 $(\alpha_1 : 1), \dots, (\alpha_n : 1)$。那么，$\mathbf{RS}_k(\alpha_1, \dots, \alpha_n)$ 可以定义为

$$\mathbf{RS}_k(\alpha_1, \dots, \alpha_n) = \{(h(P_1), \dots, h(P_n)) \mid h \in L((k-1)P_\infty)\}.$$

这自然引出了向代数曲线的推广。其意义在于，曲线可能比射影直线拥有更多有理点，因此以任意曲线替换 $\mathbb{P}^1$，或许就有机会构造出长度大于 q 的码。

3.2. 代数几何码。—— 我们简要介绍代数几何（AG）码。对更多参考资料感兴趣的读者，不妨查阅综述 [**HvLP98,Duu08, CR21**] 或专著 [**TVN07, Sti09**]。关于代数几何码的译码参考资料，也可参见 [**HP95, BH08**]。

定义 ***36***。—— 设 $\mathscr{X}$ 是定义在 $\mathbb{F}_q$ 上的一条光滑绝对不可约曲线。设 $\mathcal{P} = (P_1, \dots, P_n)$ 是 $\mathscr{X}$ 上一列互不相同的有理点。设 G 是 $\mathscr{X}$ 上的一个有理除子，其支撑避开点 $P_1, \dots, P_n$。那么，代数几何码 $\mathcal{C}_L(\mathscr{X}, \mathcal{P}, G)$ 定义为

$$\mathcal{C}_L(\mathscr{X}, \mathcal{P}, G) \stackrel{\mathbf{def}}{=} \{(f(P_1), \dots, f(P_n)) \mid f \in L(G)\}.$$

定义这些码之后，可以利用前面介绍的代数几何知识来计算它们的参数。

定理 ***37***。—设 $\mathscr{X}$ 是定义在 $\mathbb{F}_q$ 上、亏格为 g 的光滑绝对不可约曲线。设 $\mathcal{P} = (P_1, \dots, P_n)$ 是 $\mathscr{X}$ 上的一组有理点，且 G 是 $\mathscr{X}$ 上的一个有理除子，其支撑不包含 $P_1, \dots, P_n$。假设 度数 $G < n$。那么， $\mathcal{C}_L(\mathscr{X}, \mathcal{P}, G)$ 的参数 $[n, k, d]_q$ 满足

$$k \geqslant \deg G + 1 - g \quad \textit{with equality when } \deg G > 2g - 2; \tag{6}$$

$$d \geqslant n - \deg G. \tag{7}$$

证明。—记除子 $D_{\mathcal{P}} \stackrel{\mathbf{def}}{=} P_1 + \cdots + P_n$. 为 $D_{\mathcal{P}}$。考虑映射

$$ev_{\mathcal{P}} : \begin{cases} L(G) & \longrightarrow & \mathbb{F}_q^n \\ f & \longmapsto & (f(P_1), \dots, f(P_n)). \end{cases}$$

其像显然是 $\mathcal{C}_L(\mathscr{X}, \mathcal{P}, G)$。该映射的核是 $L(G)$ 中在 $P_1, \dots, P_n$处消失的函数 f所构成的子空间。这个子空间就是 $L(G - D_{\mathcal{P}})$。根据假设，$\deg(G - D_{\mathcal{P}}) = -(n - \deg G)$ 为负，因此由命题 24 (ii) 可得 $L(G - D_{\mathcal{P}}) = \ker ev_{\mathcal{P}} = \{0\}$。于是， $ev_{\mathcal{P}}$是单射，并且

$$\dim \mathcal{C}_L(\mathscr{X}, \mathcal{P}, G) = \dim L(G) \geqslant \deg G + 1 - g,$$

当 $\deg G > 2g - 2$ 时取等号。这里，最后一个不等式及其等号成立的情形均由黎曼–罗赫定理（定理 30）得出。

对于最小距离，令 $h \in L(G) \setminus \{0\}$，使得 $ev_{\mathcal{P}}(h)$ 的汉明重量为 d。这意味着在 $P_1, \dots, P_n$ 中，存在互不相同的点 $P_{i_1}, \dots, P_{i_{n-d}}$，使得 h 在这些点处为零。因此，$h \in L(G - P_{i_1} - \cdots - P_{i_{n-d}})$，且由于 $h \neq 0$，空间 $L(G - P_{i_1} - \cdots - P_{i_{n-d}}) \neq \{0\}$；由命题 24 (ii) 同样可知，$\deg(G - P_{i_1} - \cdots - P_{i_{n-d}}) \geqslant 0$，因此

$$d \geqslant n - \deg G.$$

□

我们来讨论一下这个最后的结果。在 § 1.2 中提到，由 Singleton 界 (1) 可知，任意 $[n, k, d]_q$码都满足

$$k + d \leqslant n + 1.$$

另一方面，定理 37 断言，代数几何码 $[n,k,d]_q$AG $\mathcal{C}_L(\mathscr{X},\mathcal{P},G)$ 满足

$$n+1-g\leqslant k+d.$$

总之，在最坏情况下，代数几何码与 Singleton 界的距离为 g。因此，可以期待在亏格 g“不太大”时获得良好的码。另一方面，我们的目标是构造长度超过 q 的码序列，更一般地说，是构造长度趋于无穷的、定义在 $\mathbb{F}_q$ 上的码族。因此，为了使长度足够大，我们要寻找有理点数量尽可能多的曲线。

3.3. 关于构造亏格相较之下有较多点的无限曲线序列的问题。— 我们期望得到定义在 $\mathbb{F}_q$ 上的曲线序列，其亏格增长缓慢，而有理点数量增长迅速。然而，这两个目标在某种程度上相互矛盾：要获得较多的有理点，就需要较大的亏格。Weil 的一个著名结果指出，对于定义在 $\mathbb{F}_q$ 上的光滑绝对不可约曲线 $\mathscr{X}$，

$$\sharp\mathscr{X}(\mathbb{F}_q)\leqslant q+1+2g\sqrt{q}. \tag{8}$$

因此，我们要在亏格与有理点数量之间寻求良好的权衡。现在，我们具备了将构造渐近良好的无限码序列这一编码理论问题，改述为构造具有特定性质的代数曲线序列所需的材料。为此，考虑一个曲线序列 $(\mathscr{X}_s)_{s\in\mathbb{N}}$，其亏格序列为 $(g_s)_{s\in\mathbb{N}}$。我们假设序列 $(\sharp\mathscr{X}_s(\mathbb{F}_q))_{s\in\mathbb{N}}$ 趋于无穷；因此，根据 Weil 界（8），亏格序列也应趋于无穷。令

$$\gamma=\limsup_{s\to+\infty}\frac{\sharp\mathscr{X}_s(\mathbb{F}_q)}{g_s}. \tag{9}$$

对于序列中的任意一条这样的曲线，我们固定一个有理除子 G_s，而有理点序列$\mathcal{P}_s=(P_1,\ldots\ldots,P_{n_s})$将选取为全部有理点的列表，即 $n_s=\sharp\mathscr{X}_s(\mathbb{F}_q)$。

注记 ***38***。— 有人可能会问，是否存在支撑避开 $P_1,\ldots\ldots,P_{n_s}$的任意次数的有理除子 G_s，同时满足 $\{P_1,\ldots,P_{n_s}\}=\mathscr{X}(\mathbb{F}_q)$? 答案是肯定的，这样的除子 G_s确实存在，而且满足支撑避开 $\mathscr{X}(\mathbb{F}_q)$这一约束实际上很容易。关于这个特定问题的详细讨论，参见 [**CR21**，注 15.3。8]

那么，码 $\mathcal{C}_L(\mathscr{X}_s,\ \mathcal{P}_s,\ G_s)$的参数 $[n_s,k_s,d_s]_q$满足

$$\begin{array}{rcl} n_s & = & \sharp\mathscr{X}_s(\mathbb{F}_q)\\ k_s & \geqslant & \deg G_s+1-g_s\\ d_s & \geqslant & n_s-\deg G_s. \end{array}$$

因此，可以消去 $\deg G_s$，得到

$$k_s+d_s\geqslant n_s+1-g_s. \tag{10}$$

Set

$$R=\limsup_{s\to+\infty}\frac{k_s}{n_s}\quad\text{and}\quad\delta=\limsup_{s\to+\infty}\frac{d_s}{n_s}.$$

然后，将 (10) 除以 n_s，并令 s 趋于无穷大，得到

$$R+\delta\geqslant 1-\frac{1}{\gamma},$$

其中 γ 在 (9) 中定义。因此，位于方程为 $R+\delta=1-\frac{1}{\gamma}$ 的直线上的任意一对 $(\delta,\ R)$ 都是可实现的。

注记 ***39***。— 即使 $\deg G_s$ 这一项已被消去，该项仍然有用，因为它可以用来选择你想要达到的方程为 $R+\delta=1-\frac{1}{\gamma}$ 的直线上的点。 –

练习***40.*** — 证明，通过在曲线 $\mathscr{X}_s$ 上选取一个恰当的有理除子序列 (G_s)，可以达到方程为 $R+\delta=1-\frac{1}{\gamma}\cdot$ 的直线上的任意一点 –

3.4. Ihara 常数 $A(q)$**.** — 现在，我们想要估计能够达到的最优渐近参数 (δ, R)。为此，我们引入 *Ihara* 常数：

$$A(q) \stackrel{\text{def}}{=} \limsup_{g\to+\infty} \max_{\substack{\mathscr{X},\ \text{curve}\\ \text{of genus } g}} \frac{\sharp\mathscr{X}(\mathbb{F}_q)}{g}.$$

于是，Tsfasman–Vlăduţ–Zink（TVZ）界断言，存在一些码族，其渐近参数 $(\delta,\ R)$ 满足

$$R+\delta \geqslant 1-\frac{1}{A(q)}.$$

这引出了关于 $A(q)$ 的值的问题。这些讲义的其余部分将概述以下命题的证明。

定理 ***41***。— 对于 $q=p^2$ 和 p 为素数的情形，我们有

$$A(q) \geqslant \sqrt{q}-1.$$

将前面的结果与 TVZ 界结合，可以证明对于 $p\geqslant 7$，因此当 q 是一个大于或等于 49 的素数的平方时，TVZ 界超过 Gilbert–Varshamov 界，从而证明某些由代数曲线构造的码族优于随机码。

最后，我们再谈几点。

- 事实上，对于任意 $m\geqslant 1$，这一结果都推广到 $q=p^{2m}$，但证明会更加复杂，并且涉及其他曲线族。具体而言，下面的证明涉及模曲线，而一般情形则涉及志村曲线。参见 [**Iha81, TVZ82**]。
- 事实上，TVZ界是最优的。确实，在 Tsfasman–Vlăduţ–Zink 的结果发表之后，Drinfeld 和 Vlăduţ 在 [**VD83**] 中证明，对于任意素数幂 q，总有$A(q)\leqslant \sqrt{q}+1$。
- Garcia 和 Stichtenoth 在 [**GS95**]中以一种截然不同的方法给出了定理 41 的另一种证明。

这一精彩结果的证明核心在于使用了称为模曲线 的曲线族，它们参数化了由椭圆曲线组成的代数曲线族。

4. 椭圆曲线

椭圆曲线是数论中另一个引人入胜的主题。它们也是密码学中的基本对象，不过这不是本文的重点。本节首先介绍任意域上的这些对象的基本概念。我们的目标之一是构造这些所谓的模曲线，它们将产生优良的码。这些模曲线是代数曲线，它们参数化了带有一种称为层结构的特定附加结构的椭圆曲线族。

之后，在第5节中，我们将讨论 $\mathbb{C}$上的椭圆曲线和模曲线。在这样的笔记中讨论复曲线，可能会让人感到意外，因为我们显然关注的是有限域上的曲线。然而，预先研究复数情形有若干优点。首先，它能更直观地介绍相关主题，并可借助解析工具。其次，尽管解析证明无法移植到有限域情形，但它们有助于计算代数公式，即 定义模曲线的多项式方程。事实证明，这些方程定义在 $\mathbb{Z}$ 上；接着——这绝非易事——将它们模 p约化，就会得到一条曲线的方程，该曲线参数化了具有某种层结构、定义在 $\mathbb{F}_p$ 或 $\mathbb{F}_p$ 上的椭圆曲线。

注。 本节中，我们假设基域 $\mathbb{K}$ 的特征不为 2 或 3。本节及下一节的大部分内容取自著作 [**Sil09**]和讲义 [**Mil17**]。

4.1 基本定义。— 域 $\mathbb{K}$ 上的椭圆曲线 $\mathscr{E}$ 是一个亏格为 1 且至少含有一个记作 $O_{\mathscr{E}}$ 的有理点的光滑射影曲线。根据命题 21，与零除子相关的黎曼–罗赫空间 $L(0)$ 只包含常数函数，因此其维数为 1。于是，根据黎曼–罗赫定理，空间 $L(2O_{\mathscr{E}})$ 和 $L(3O_{\mathscr{E}})$ 的维数分别为 2 和 3（注意，一旦除子的次数为正，它们就是，因此我们满足黎曼–罗赫定理的等号情形）。

只要除子的次数为正，它们就是 $> 2g-2$，因此我们满足黎曼–罗赫定理的等号情形）。记 x, y 为两个满足下式的函数，

$$L(2O_{\mathscr{E}}) = \mathrm{Span}_{\mathbb{K}}\{1, x\} \quad L(3O_{\mathscr{E}}) = \mathrm{Span}_{\mathbb{K}}\{1, x, y\}.$$

注意， x 和 y 的这些选取并非典范，因此以下任何变量变换都是允许的

$$x' \leftarrow ax + b, \text{ with } a \neq 0 \qquad y' \leftarrow uy + vx + w, \text{ with } u \neq 0. \tag{11}$$

现在，考虑空间 $L(6O_{\mathscr{E}})$。它包含以下函数

$$1, x, y, x^2, xy, x^3, y^2.$$

此外，同样由黎曼–罗赫定理可知， $L(6O_{\mathscr{E}})$的维数为 6，因此这些函数之间存在非平凡的线性关系

$$y^2 + uxy + vy = ax^3 + bx^2 + cx + d.$$

练习 ***42.*** — 证明 y^2 和 x^3 应当出现在这个线性关系中，这解释了为何经过重新归一化后，可以假设 y^2 的系数为 1。由此推出 $a \neq 0$。

现在，我们依次进行允许的变量变换，即也就是形如 (11) 的变量变换。首先进行一次[7]: $y \leftarrow y + \frac{u}{2}x$，得到一个方程: $\quad -$

$$y^2 + v_1 y = a_1 x^3 + b_1 x^2 + c_1 x + d_1, \tag{12}$$

对于某些 $a_1,\ b_1,\ c_1,\ d_1 \in \mathbb{K}$。作变量替换 $y \leftarrow y + \frac{v_1}{2}$后得到

$$y^2 = a_2 x^3 + b_2 x^2 + c_2 x + d_2. \tag{13}$$

fo对于某些 $a_2,\ b_2,\ c_2,\ d_2 \in \mathbb{K}$。接下来，作如下形式的变量替换 $x \longleftarrow x + \frac{b_2}{3a_2}$，得到一个方程 :

$$y^2 = a_3 x^3 + c_3 x + d_3, \tag{14}$$

对于某些 $a_3,\ c_3,\ d_3 \in \mathbb{K}$。最后，应用变量替换 $x \leftarrow a_3 x, \quad y \leftarrow a_3^2 y$ 并将两边除以 a_3^4，得到一个如下形式的方程

$$y^2 = x^3 + Ax + B, \tag{15}$$

对于某些 $A,\ B \in \mathbb{K}$。这样的方程称为该曲线的魏尔斯特拉斯方程 。

练习 ***43***。— 利用练习 42，验证最后一次变量替换是允许的，也就是说，$a_3 \neq 0$。

总之，从定义在 $\mathbb{K}$上的椭圆曲线 $\mathscr{E}$ 出发，也就是说，一条具有有理点 $O_{\mathscr{E}}$的光滑亏格 1 曲线，我们找到了两个函数 $x,\ y \in \mathbb{K}(\mathscr{E})$，它们除在 $O_{\mathscr{E}}$处外处处正则。这两个函数满足关系式 (15)，因此函数 $y^2 - x^3 - Ax - B$ 在 $\mathscr{E}$上处处为零。由此得到以下结论。

定理 ***44***。——设 $\mathscr{E}$ 是一个定义在特征不为 *2* 和 *3* 的域 $\mathbb{K}$ 上的椭圆曲线，即一条亏格为 *1* 且有一个有理点 $O_{\mathscr{E}}$ 的光滑射影曲线，则存在 $x, y \in \mathbb{K}(\mathscr{E})$，使得映射

$$\begin{cases} \mathscr{E} & \dashrightarrow & \mathbb{P}^2 \\ P & \longmapsto & \begin{cases} (x(P) : y(P) : 1) & \text{if} \quad P \neq O_{\mathscr{E}} \\ (0:1:0) & \text{if} \quad P = O_{\mathscr{E}} \end{cases} \end{cases}$$

诱导一个从 $\mathscr{E}$ 到方程为 $Y^2 = X^3 + AXZ^2 + BZ^3$ 的曲线的射影闭包的同构。

---

[7]为了保持记号简洁，我们省略 x', y' 中的撇号，并因此将变量替换的输出记作输入，因此采用记号 $y \leftarrow y + \frac{u}{2}x$。这并非完全严谨的记法；如果读者对此感到困扰,–建议将本页中出现的 x 和 y 替换为合适位置上的 x', x'', x''' 以及 y', y'', y'''。

证明。—— $\mathscr{E}$ 的像包含在这样一条曲线中的事实，是前文讨论的结果。为了证明此映射确实是同构，尤其是目标曲线光滑，我们请读者参阅 [**Sil09**，命题 III.3.1]。

□

注 ***45***。——从几何角度看，这一系列变量变换可以作如下解释。我们从一条椭圆曲线 $\mathscr{E}$以及对函数 x, y在 $\mathbb{K}(\mathscr{E})$中的第一种选取出发，从而得到 $\mathscr{E}$与一条方程为 (12) 的曲线之间的同构。接着，我们对平面依次施加仿射自同构，以得到方程依次为 (13)、(14) 的曲线；这些曲线两两同构，最后得到一条方程为 (15) 的曲线，它也与 $\mathscr{E}$同构。

注 ***46***。——接下来，我们将不再只考虑魏尔斯特拉斯形式。事实上，可以证明，任意一条方程为

$$y^2 = f(x)$$

的曲线，只要其中 f 是一个三次无平方因子多项式，便是一条椭圆曲线，而且存在一种变量替换，可以将它化为魏尔斯特拉斯形式。

4.2. *j***不变量**。——下文中，将需要对椭圆曲线按同构关系进行分类。为此，我们引入一个基本不变量：j不变量。重新考虑魏尔斯特拉斯方程 (15)

$$y^2 = x^3 + Ax + B.$$

这个方程并不唯一，因为得到它之后，仍然可以进行如下形式的变量变换$y \leftarrow u^3 y,\quad x \leftarrow u^2 x$ 并将等式两边除以 u^6。由此可得到另一个魏尔斯特拉斯方程 $y^2 = x^3 + A'x + B'$，其中 $A' = \frac{A}{u^4}$ 且 $B' = \frac{B}{u^6}$。下面引入

$$j \overset{\text{def}}{=} 1728\frac{4A^3}{4A^3 + 27B^2}.$$

这个量定义良好，因为可以证明，分母 $4A^3 + 27B^2$ 为零当且仅当相应的曲线是奇异的（见 [**Sil09**，命题 III.1.4(a)(i)]）。因此，j 对任意椭圆曲线都有定义良好，因为根据定义，这类曲线是光滑的。此外，j 在先前的变量替换下保持不变；并且可以证明，得到魏尔斯特拉斯方程后，保持魏尔斯特拉斯方程结构的变量替换只有前面提到的那些。

我们以以下陈述结束本小节：该 j–不变量以唯一方式刻画$\mathbb{K}$ 上的椭圆曲线。证明从略，可参见 [**Sil09**，命题 III.1.4(b- c)]。

命题 ***47***。— 两条椭圆曲线在 $\mathbb{K}$ 上同构，当且仅当它们具有相同的 $\overline{j}$–不变量。反之，给定 $j_0 \in \mathbb{K}$，存在一条 $\mathscr{E}$ 上的椭圆曲线 $\mathbb{K}$（j_0），其 j–不变量为 j_0。

注记 ***48***。— 注意，定义在 $\mathbb{K}$ 上的两条椭圆曲线可能在 $\mathbb{K}$ 上同构，却不在 $\mathbb{K}$上同构。例如，假设 -1 不是 $\mathbb{K}$中的平方数。那么，以下列方程的曲线之间

$$y^2 = x^3 + Ax + B \quad \text{and} \quad -y^2 = x^3 + Ax + B$$

通过定义在 $\mathbb{K}$ 上的同构 $(x,\ y) \mapsto (x,\ \sqrt{-1}\ y)$ 相互关联，但可能不存在定义在 $\mathbb{K}$上的同构。这样的曲线称为彼此的扭曲。

注记 ***49***。— 从一个 j–不变量 $j_0 \in \mathbb{K}$ 出发，具有该 $\overline{j}$–不变量的椭圆曲线的一个显式方程为

$$y^2 + xy = x^3 - \frac{36}{j_0 - 1728}x - \frac{1}{j_0 - 1728} \quad \text{if} \quad j_0 \neq 0, 1728$$

and

$$y^2 + y = x^3 \ \text{ if } \ j_0 = 0 \qquad \text{and} \qquad y^2 = x^3 + x \ \text{ if } \ j = 1278.$$

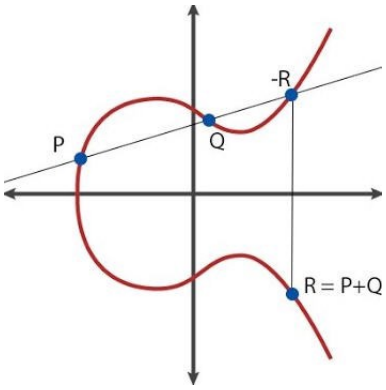


图3. 椭圆曲线上的加法律（来源：Cornelius Schätz 博客）

4.3. 群律。— 这类曲线的一个显著特征是，它们天然具有群结构。具体而言，给定有理数域 $\mathbb{K}$ 上的椭圆曲线 $\mathscr{E}$，集合 $\mathscr{E}(\mathbb{K})$ 具有阿贝尔群结构。更一般地，对于任意代数扩张 $\mathbb{L}$，若其扩张域为 $\mathbb{K}$，则 $\mathscr{E}(\mathbb{L})$ 也具有阿贝尔群结构。这种群结构通常用所谓的弦切法 来表示，如图3所示。其描述如下：

- 给定两个点 $P,\ Q \in \mathscr{E}(\mathbb{L})$，作经过它们的直线 $\mathscr{L} \subseteq \mathbb{A}^2$（或 $\mathbb{P}^2$）。若 $P = Q$ 令 $\mathscr{L}$为 $\mathscr{E}$ 在 P处的切线。
- 由于该曲线是三次曲线，它与 $\mathscr{L}$ 和 $\mathscr{E}$ 的交点按重数计算共有 3 个，因此要么 $\mathscr{L}$ 是竖直的，此时第三个点是 $R_0 = O_{\mathscr{E}}$；要么记 $R_0 = (x_{R_0},\ y_{R_0})$ 为这条直线与 $\mathscr{E}$的第三个(8) 交点。
- 若 $R_0 \neq O_{\mathscr{E}}$，令 R 为坐标为（$x_{R_0},\ -y_{R_0}$）的点；否则令其为点 $O_{\mathscr{E}}$。此点定义为 P 与 Q的和。

习题 ***50.*** — (1) 证明 $\mathscr{E}$ 与一条直线的交点由 $\mathbb{P}^2$ 上的 3 个点构成，重数可以大于 1；

(2) 证明 $R_0 \in \mathscr{E}(\mathbb{L})$;

这种描述简单易懂，但要证明它确实赋予了一个群结构，却并非显而易见。尤其是，利用这种描述，要证明结合律更是远非显而易见。这里我们将说明，这种群结构也可以理解为从除子群的某个商空间继承而来的群律。具体而言，记 $\mathrm{Div}_{\mathbb{K}}(\mathscr{E})$ 为 $\mathscr{E}$ 上的有理除子群，记 $\mathrm{Div}^0_{\mathbb{K}}(\mathscr{E})$ 为次数为 0 的除子子群。最后，记 $\mathrm{Princ}_{\mathbb{K}}(\mathscr{E})$ 为主除子群，即 形如 (f) 的除子，其中 $f \in \mathbb{K}(\mathscr{E}) \setminus \{0\}$。由注 19 和命题 20 可知，$\mathrm{Princ}_{\mathbb{K}}(\mathscr{E})$ 是 $\mathrm{Div}^0_{\mathbb{K}}(\mathscr{E})$ 的子群，其商空间记为

$$\mathrm{Pic}^0_{\mathbb{K}}(\mathscr{E}) \overset{\mathbf{def}}{=} \mathrm{Div}^0_{\mathbb{K}}(\mathscr{E})/\mathrm{Princ}_{\mathbb{K}}(\mathscr{E}).$$

命题***51***。——设 $\mathscr{E}$ 是 $\mathbb{K}$上的一条椭圆曲线。$\mathrm{Pic}^0_{\mathbb{K}}(\mathscr{E})$ 中的任意元素都有一个形如 $P - O_{\mathscr{E}}$ 的代表元，其中 P 是 $\mathscr{E}(\mathbb{K})$中的某个有理点。

证明。——设 $G \in \mathrm{Div}^0_{\mathbb{K}}(\mathscr{E})$。除子 $G + O_{\mathscr{E}}$ 的次数为 1，且根据黎曼–罗赫定理$L(G + O_{\mathscr{E}})$，其维数为 1。因此，存在 $f \in L(G + O_{\mathscr{E}}) \setminus \{0\}$。根据 $L(G + O_{\mathscr{E}})$ 的定义，函数 f 满足

$$(f) + G + O_{\mathscr{E}} \geqslant 0.$$

后一个除子是正的，次数为 1，因此等于某个有理点 P。于是 $(f)+G = P-O_{\mathscr{E}}$，这意味着 G 和 $P - O_{\mathscr{E}}$ 在 $\mathrm{Pic}^0_{\mathbb{K}}(\mathscr{E})$ 中具有相同的类。 □

(8)可能 R_0 等于 P 或 Q。这就是我们提到按重数计算的 3 个点的原因。如果 $\mathscr{L}$ 与 $\mathscr{E}$ 在 P 处（分别在 Q处）的交数为 2，那么我们令 $R_0 \overset{\text{定义}}{=} P$（分别为 Q）。

定理 **52**。—设 $P,Q\in\mathscr{E}(\mathbb{K})$，并令 R 为根据先前引入的加法律得到的 $P+Q$ 之和。则，$R-O_{\mathscr{E}}$ 与 $(P-O_{\mathscr{E}})+(Q-O_{\mathscr{E}})$ 在 $\mathit{Pic}^0_{\mathbb{K}}(\mathbb{E})$ 中具有相同的类。

证明。——根据习题 50（1），存在一点 R_0，它位于连接 P 和 Q 的直线 $\mathscr{L}$ 上。此外，R，R_0 位于竖直直线 $\mathscr{L}'$ 上；从射影的角度来说，竖直性意味着 R_0，R 和 $O_{\mathscr{E}}$ 属于直线 $\mathscr{L}'$ 的射影闭包。设 $H(X,Y,Z)$ 和 $H'(X,Y,Z)$ 分别为次数为 1 的齐次多项式，它们给出了 $\mathscr{L}$ 和 $\mathscr{L}'$ 的射影闭包的方程。有理函数 $h\overset{\text{定义为}}{=}\frac{H}{H'}\in\mathbb{K}(\mathscr{E})$ 的除子为

$$(h)=(P+Q+R_0)-(R_0+R+O_{\mathscr{E}})=(P-O_{\mathscr{E}})+(Q-O_{\mathscr{E}})-(R-O_{\mathscr{E}}),$$

由此证明完毕。 □

综上，我们得到如下双射：

$$\left\{\begin{array}{ccc}\mathscr{E}(\mathbb{K}) & \longrightarrow & \mathrm{Pic}^0_{\mathbb{K}}(\mathscr{E})\\ P & \longmapsto & P-O_{\mathscr{E}}\mod \mathrm{Princ}_{\mathbb{K}}(\mathscr{E})\end{array}\right.\ .$$

通过这个双射，我们可以赋予 $\mathscr{E}(\mathbb{K})$ 一个群结构，其运算恰好就是前面所描述的弦切法则。因此，赋予弦切法则的 $\mathscr{E}(\mathbb{K})$ 具有群结构，并且该群结构与 $\mathrm{Pic}^0_{\mathbb{K}}(\mathscr{E})$ 同构。

注 **53**。——这里还要注意，我们讨论的是有理点集合 $\mathscr{E}(\mathbb{K})$ 的群结构；事实上，对于任意代数扩张 $\mathbb{L}/\mathbb{K}$，集合 $\mathscr{E}(\mathbb{L})$ 也具有群结构，且 $\mathscr{E}(\mathbb{L})$ 是其子群。特别地，整个几何点集合 $\mathscr{E}(\mathbb{K})$ 具有阿贝尔群结构。

4.4. 挠子与同源。——既然我们知道椭圆曲线具有阿贝尔群结构，那么研究这些曲线之间的态射自然是顺理成章的。为此，我们首先需要讨论椭圆曲线上点的一些特殊子群：它们的挠子群。

4.4.1. 挠 p 子群。——给定一条椭圆曲线 $\mathscr{E}$ 和一个整数 ℓ，人们关心群

$$\mathscr{E}[\ell]\overset{\mathbf{def}}{=}\{P\in\mathscr{E}(\overline{\mathbb{K}})\mid \ell P=0\},$$

其中 ℓP 表示“$P+\cdots+P$”（相加 ℓ 次）。有趣的是，这个群自然地具有$\mathbb{Z}/\ell\mathbb{Z}$–模结构；特别地，当 ℓ 为素数时，它是一个 $\mathbb{F}_\ell$–向量空间。下一个定理断言，当 ℓ 与特征互素时，这个空间的维数总是 2。下一个命题的证明从略。

定理 **54.** — 设 $\mathscr{E}$ 是定义在 $\mathbb{K}$上的椭圆曲线。设 ℓ 是一个整数。若 ℓ 与特征数 $\mathbb{K}$互素，则

$$\mathscr{E}[\ell]\simeq\mathbb{Z}/\ell\mathbb{Z}\times\mathbb{Z}/\ell\mathbb{Z}.$$

另外，若 p 表示 $\mathbb{K}$ 和 $p\neq 0$ 的特征，则

$$\mathscr{E}[p]\simeq\left\{\begin{array}{cc}either & \mathbb{Z}/p\mathbb{Z}\\ or & 0.\end{array}\right.$$

前一种 情形下，称该曲线为普通曲线；后一种情形下，称其为超奇异曲线。

4.4.2. 同源。——给定两条椭圆曲线 $\mathscr{E},\mathscr{E}'$，同源 $\phi:\mathscr{E}\to\mathscr{E}'$ 是这两条曲线之间的一个态射，它将单位元 $O_{\mathscr{E}}$ 映到 $O_{\mathscr{E}'}$。这样的映射总是从 $\mathscr{E}(\mathbb{K})$满射到 $\mathscr{E}'(\mathbb{K})$。一个显著性质是，这样的映射必定是群态射（见 [**Sil09**，定理 III.4.8]）。与任何曲线的态射一样，同源 $\phi:\mathscr{E}\to\mathscr{E}'$ 诱导一个域扩张 $\mathbb{K}(\mathscr{E}')/\mathbb{K}(\mathscr{E})$。同源的次数 就是该域扩张的次数；如果域扩张也是可分的，则称该同源为可分同源。次数为 ℓ 的同源通常称为一个 ℓ–同源。

例 **55.** — 摘自 [**Sil09**，例 III.4.5]。设 a，$b\in\mathbb{K}$、$b\neq 0$ 和 $a^2-4b\neq 0$。考虑具有以下方程的曲线：

$$\begin{aligned}\mathscr{E}:y^2&=x^3+ax^2+bx\\ \mathscr{E}':y^2&=x^3-2ax^2+(a^2-4b)x.\end{aligned}$$

下面的映射是一个 2-同源：

$$\left\{\begin{array}{ccc}\mathscr{E} & \longrightarrow & \mathscr{E}' \\ (x,y) & \longmapsto & \left(\frac{y^2}{x^2}, \frac{y(b-x^2)}{x^2}\right).\end{array}\right. \tag{16}$$

练习***56***。——验证映射（16）确实将 $\mathscr{E}$ 映入 $\mathscr{E}'$。 提示：本练习中使用计算机代数软件可能会有所帮助。

例***57***。——有限域 $\mathbb{F}_q$ 特征为p 时椭圆曲线之间同源的另一个例子是弗罗贝尼乌斯映射

$$\left\{\begin{array}{ccc}\mathscr{E} & \longrightarrow & \mathscr{E}^{(p)} \\ (x,y) & \longmapsto & (x^p, y^p).\end{array}\right.$$

此同源是纯不可分的，它将具有魏尔斯特拉斯方程 $y^2 = x^3 + Ax + B$ 的曲线 $\mathscr{E}$ 映到方程为 $y^2 = x^3 + A^p x + B^p$ 的曲线 $\mathscr{E}^{(p)}$。如果 $\mathscr{E}$ 定义在 $\mathbb{F}_q$ 上（即 若 $A, B \in \mathbb{F}_q$），那么弗罗贝尼乌斯映射就是 $\mathscr{E}$ 的自同态。

例***58***。——对于任意与特征互素的 $m > 0$ 素数，以及任意定义在 $\mathbb{K}$ 上的椭圆曲线 $\mathscr{E}$，映射$P \mapsto mP$ 是从 $\mathscr{E}$ 到其自身的同源。其核为 $\mathscr{E}[m]$。

次数为 ℓ 的可分同源，视为群态射 $\mathscr{E}(\mathbb{K}) \to \mathscr{E}(\mathbb{K})$，是满射，且其有限核的基数为 ℓ。其核是 $\mathscr{E}[\ell]$ 的子群。

定理 ***59*** ([**Sil09**，命题 III.4。12]) 。— 对于任意有限子群 $K \subseteq \mathscr{E}(\mathbb{K})$，存在一条定义在 $\mathbb{K}$ 上的椭圆曲线 $\mathscr{E}'$ 以及一个同源 $\phi\colon \mathscr{E} \to \mathscr{E}'$，使得 核$\phi = K$。曲线 $\mathscr{E}'$ 有时记作 $\mathscr{E}/K$。

注***60***。— 在前述陈述中，可以进一步精确说明$\mathscr{E}'$ 和 ϕ 的定义域。群 K 的定义域是满足 K 在伽罗瓦群 $\mathrm{Gal}(\mathbb{K}/\mathbb{L})$ 的作用下整体不变的最小扩张 $\mathbb{L}/\mathbb{K}$。 ϕ 和 $\mathscr{E}'$ 的定义域则是 K 的定义域。

请注意，定义域**并非** K中任意几何点的最小定义域。例如，可能存在非有理的 m 挠点，而 $\mathscr{E}[m]$ 则定义在 $\mathbb{K}$ 上。

最后，尽管同源 $\phi\colon \mathscr{E} \to \mathscr{E}'$ 的次数为 $m > 1$，通常并非同构，因此 ˆ ˆ 没有逆映射，但它有一个所谓的对偶同源 ϕ，它是唯一满足下述条件的同源 $\phi\colon \mathscr{E}' \to \mathscr{E}$：

$$\phi \circ \hat{\phi}\colon \left\{\begin{array}{ccc}\mathscr{E} & \longrightarrow & \mathscr{E} \\ P & \longmapsto & mP\end{array}\right. \quad \text{and} \quad \hat{\phi} \circ \phi\colon \left\{\begin{array}{ccc}\mathscr{E}' & \longrightarrow & \mathscr{E}' \\ Q & \longmapsto & mQ.\end{array}\right.$$

该映射的存在性和唯一性证明见 [**Sil09**，§ III.6]。

例***61.*** — 对于次数为 m 的可分同源 $\phi\colon \mathscr{E} \to \mathscr{E}'$，其核是一个含有$m$ 个元素的群。根据拉格朗日定理，这样的有限群是 m 挠的，因此 $\ker\phi \subseteq \mathscr{E}[m]$。于是 $\phi(\mathscr{E}[m])$ 是一个有限子群；根据定理 59，存在一个同源 $\varphi\colon \mathscr{E}' \to \mathscr{E}'/\phi(\mathscr{E}[m])$，它正是 ϕ 的对偶同源。特别地，$\mathscr{E}'/\phi(\mathscr{E}[m]) \simeq \mathscr{E}/\mathscr{E}[m] \simeq \mathscr{E}$。最后一个同构由映射 $P \mapsto mP$ 诱导。

此前介绍的所有概念：挠、同源和对偶同源，将在下一节关于 $\mathbb{C}$ 上椭圆曲线的内容中重新讨论，并得到更清晰的阐释。在这一背景下，这些概念将更容易理解。

4.5. 复数域上的椭圆曲线。—— 正如前文所述，复椭圆曲线并非本讲的主题。不过，仍有必要对其稍作讨论。为避免在这一主题上花费太多时间，这里省略了许多非平凡结论的证明，改为给出精确的参考文献。显然，以下摘要严格取自 Silverman 著作的第六章[**Sil09**]。

4.5.1. 格与魏尔斯特拉斯 $\wp$ 函数。—— 在复数情形下，椭圆曲线同构于复环面。具体而言， $\mathbb{C}$ 的一个格是一个离散子群 Λ ，其商空间是紧的；众所周知，这样的群具有如下形式

$$\Lambda = \mathbb{Z}\omega_1 \oplus \mathbb{Z}\omega_2$$

其中 ω_1， ω_2 在 $\mathbb{R}$ 上线性无关。环面 $\mathbb{C}/\Lambda$ 与椭圆曲线之间的联系远非显而易见，而连接这两个对象的关键是 Weierstrass $\wp_\Lambda$ 函数，其定义如下

$$\wp_\Lambda(z) \stackrel{\text{def}}{=} \frac{1}{z^2} + \sum_{\omega\in\Lambda\setminus\{0\}} \left(\frac{1}{(z-\omega)^2} - \frac{1}{\omega^2}\right).$$

这是一个亚纯函数，其极点集为 Λ，且以 Λ 为周期，即 对于任意 $z \in \mathbb{C}\setminus\Lambda$ 和 $\omega \in \Lambda$，$\wp(z+\omega) = \wp(z)$。级数收敛性的证明留给读者。

注意，由于 $\wp$ 以 Λ 为周期，它可以下降到商空间，并在环面 $\mathbb{C}/\Lambda$ 上诱导出一个亚纯函数。函数 $\wp$ 具有根本性，因为实际上，任何以 Λ 为周期的亚纯函数都可以表示为关于 $\wp$ 及其导数 $\wp'$ 的有理函数，正如下述命题所说明的那样。

定理 ***62***。— 存在复数 g_2、 g_3，它们依赖于 Λ ，使得

$$\forall z \in \mathbb{C}\setminus\Lambda, \qquad \wp'_\Lambda(z)^2 = 4\wp_\Lambda(z)^3 + g_2\wp_\Lambda(z) + g_3.$$

证明。——级数

$$\wp(z) - \frac{1}{z^2} = \sum_{\omega\in\Lambda\setminus\{0\}} \left(\frac{1}{(z-\omega)^2} - \frac{1}{\omega^2}\right)$$

是偶函数，并且在 0 处为零。因此，在 0 的邻域内，其泰勒级数展开只依赖于z^2。由此可得， $\wp_\Lambda$ 在 0 处具有如下形式的洛朗级数展开

$$\wp_\Lambda(z) = \frac{1}{z^2} + O(z^2),$$

and

$$\wp'_\Lambda(z) = -\frac{2}{z^3} + O(z).$$

因此，在 0 的一个 邻域内， $\wp'_\Lambda(z)^2 - 4\wp_\Lambda(z)^3 = O(\frac{1}{z^2})$，并且存在常数 $g_2 \in \mathbb{C}$ 使得 at

$$\wp'_\Lambda(z)^2 - 4\wp_\Lambda(z)^3 - g_2\wp_\Lambda(z) = O(1). \tag{17}$$

函数 $\wp'_\Lambda(z)^2 - 4\wp_\Lambda(z)^3 - g_2\wp_\Lambda(z)$ 是 Λ–周期的，在 $\mathbb{C}$ 上为亚纯函数，其极点集包含于 Λ 中。由（17）可知，它在 0 处没有极点；根据 Λ–周期性，它处处都没有极点，因此在 $\mathbb{C}$ 上全纯。由于它在 $\mathbb{C}$ 上连续且具有 Λ–周期性，所以它是有界的；根据刘维尔定理，它应为常数。因此，存在 $g_3 \in \mathbb{C}$ 使得 $\wp'_\Lambda(z)^2 = 4\wp_\Lambda(z)^3 + g_2\wp_\Lambda(z) + g_3$。 □

练习 ***63***。— 证明， Λ 周期的全纯函数在 $\mathbb{C}$ 上有界。

对级数作更精细的分析，可以用 Λ 估计 g_2， g_3 ，并证明方程$y^2 = 4x^3 + g_2x + g_3$ 定义的是一条光滑曲线，因此也是一条椭圆曲线。有了这个定理，我们便可推出存在一个从环面 $\mathbb{C}/\Lambda$ 到方程为 $y^2 = 4x^3 + g_2x + g_3$的椭圆曲线 $\mathscr{E}$ 的映射：

$$\Psi_\Lambda : \begin{cases} \mathbb{C}/\Lambda & \longrightarrow & \mathscr{E} \\ z & \longmapsto & (\wp_\Lambda(z) : \wp'_\Lambda(z) : 1). \end{cases} \tag{18}$$

注意，该映射处处有定义，因为在 0 处， $\wp_\Lambda$ 有一个二阶极点， $\wp'_\Lambda$ 有一个三阶极点；此时可以将其重新归一化为 $(z^3\wp_{\Lambda(z)} : z^3\wp'_\Lambda(z) : z^3)$ 并在 0 处求值，得到点$O_{\mathscr{E}} = (0:1:0)$。下面的命题汇集了关于复环面的若干重要且非平凡的结果：它指出椭圆曲线与复环面之间存在一一对应关系，既将它们视为复代数簇，**也将它们视为群**时皆如此。

定理 ***64***. — 式 (18) 中定义的映射 Ψ_Λ 是 $\mathbb{C}/\Lambda$ 与方程为 $y^2 = 4x^3+g_2x+g_3$的椭圆曲线 $\mathscr{E}$ 之间的双全纯同构。此外，它还诱导出一个群同构，将 $\mathbb{C}/\Lambda$

赋予从 $\mathbb{C}$ 继承而来的加法律，映射到 $\mathscr{E}(\mathbb{C})$，后者赋予了*§ 4.3* 中引入的群律。反过来，给定任意定义在 $\mathbb{C}$上的椭圆曲线 $\mathscr{E}_0$，存在一个格 $\Lambda_0 \subset \mathbb{C}$，使得 $\mathscr{E}_0$ 通过映射 Ψ_{Λ_0}与 $\mathbb{C}/\Lambda_0$ 同构。

证明。——群同构的证明见 [**Sil09**，命题 VI.3。6] 关于从椭圆曲线构造格，见 [**Sil09**，§ VI。1]。 □

4.5.2. 挠子与同源。——复数情形的一个优点是，将椭圆曲线视为复环面时，先前关于挠和同源的结果很容易理解。

我们先来看挠。根据定理 54，对于与特征互素的 m 素数，椭圆曲线的 m挠子群同构于 $\mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}$。在复数情形下，考虑环面 $\mathbb{C}/\Lambda$。此时，挠点对应于满足 $mz \in \Lambda$ 的点 $z \in \mathbb{C}$，因此它们对应于格 $\frac{1}{m}\Lambda \supset \Lambda$中的点。于是，$\mathbb{C}/\Lambda$ 的挠子群同构于 $\frac{1}{m}\Lambda/\Lambda$。由于对于某些 $\mathbb{R}$个 ω_1，$\omega_2 \in \mathbb{C}$ 线性无关的元素，Λ 可写成 $\mathbb{Z}\omega_1 \oplus \mathbb{Z}\omega_2$ 的形式，我们得出

$$(\mathbb{C}/\Lambda)[m] \simeq \left(\frac{1}{m}\Lambda\right)/\Lambda = \frac{\mathbb{Z}\frac{\omega_1}{m} \oplus \mathbb{Z}\frac{\omega_2}{m}}{\mathbb{Z}\omega_1 \oplus \mathbb{Z}\omega_2} \simeq \mathbb{Z}/m\mathbb{Z} \oplus \mathbb{Z}/m\mathbb{Z}.$$

现在考虑同源。对于复环面，同源是全纯映射 $\mathbb{C}/\Lambda \to \mathbb{C}/\Lambda'$。事实证明，这类映射可提升到 $\mathbb{C}$，并且具有非常特殊的结构。

定理 ***65***。——设 Λ、$\Lambda' \subset \mathbb{C}$ 是两个格，且 $f\colon\ \mathbb{C}/\Lambda \to \mathbb{C}/\Lambda'$ 是一个将 0 映到 0 的全纯映射。那么 f 可提升为全纯映射 $f_0\colon\ \mathbb{C} \to \mathbb{C}$，使得

$$\forall z \in \mathbb{C}, \quad f_0(z) \mod \Lambda' = f(z \mod \Lambda).$$

此外，f_0 是相似变换，也就是说，存在 $a \in \mathbb{C}$ 使得

$$\forall z \in \mathbb{C},\ f_0(z) = az.$$

证明。——参见 [**Sil09**，定理 VI.4.1]。 □

根据这一结论，我们推得，同源 $\phi\colon\ \mathbb{C}/\Lambda \to \mathbb{C}/\Lambda'$ 是由满足 $a\Lambda \subseteq \Lambda'$ 的映射 $z \mapsto az$ 诱导的。

例 ***66***。——例如，考虑这些格

$$\Lambda = \mathbb{Z} \oplus \mathbb{Z}2i \quad \text{and} \quad \Lambda' = 2\mathbb{Z} \oplus \mathbb{Z}2i$$

于是我们很容易看出，映射 $z \mapsto 2z$ 诱导出一个同源 $\mathbb{C}/\Lambda \to \mathbb{C}/\Lambda'$。

由满足 $a\Lambda \subset \Lambda'$的相似变换 $z \mapsto az$，相应同源的次数为♯$(\Lambda'/a\Lambda)$。在前面的例子中，该同源的次数为 2。

最后，设 ℓ 为一个素数，并假设我们有一个次数为 ℓ 的同源 $\phi_1 : \mathbb{C}/\Lambda \to \mathbb{C}/\Lambda'$。这意味着存在 $a \in \mathbb{C}$，使得 ♯$(\Lambda'/a\Lambda) = \ell$。由主理想环上有限生成模的结构定理，我们推得存在 ω_1，$\omega_2 \in \mathbb{C}$ 使得

$$\Lambda = \mathbb{Z}\frac{\ell\omega_1}{a} \oplus \frac{\omega_2}{a}, \quad \Lambda' = \mathbb{Z}\omega_1 \oplus \mathbb{Z}\omega_2$$

并且 ϕ_1 由相似变换 $z \mapsto az$诱导。

练习 ***67***。 — 证明最后一个断言。

现在考虑映射 $z \mapsto \frac{\ell}{a}z$。它诱导出一个同源 $\phi_2\colon\ \mathbb{C}/\Lambda' \to \mathbb{C}/\Lambda$，其次数为 ℓ。此外，两个同源的复合：

$$\phi_2 \circ \phi_1 : \mathbb{C}/\Lambda \to \mathbb{C}/\Lambda' \to \mathbb{C}/\Lambda''$$

由 $z \bmod \Lambda \mapsto \ell z \bmod \Lambda$ 定义，因此不过是在 $\mathbb{C}/\Lambda$中乘以 ℓ。所以，$\hat{}\phi_2$ 不过是 ϕ_1的对偶同源映射 ϕ_1。

4.6. 自同构。— 现在，我们对复椭圆曲线之间的态射有了很好的描述。此外，椭圆曲线的自同态，或者等价地，复环面 $\mathbb{C}/\Lambda$的自同态，是由相似变换 $z \mapsto az$ 诱导的，且满足 $a\Lambda \subset \Lambda$。

接下来，我们还将关注椭圆曲线的自同构，它们对应于满足 $a\Lambda = \Lambda$ 的相似变换 $z \mapsto az$ 。可以证明，这样的 a 满足 $|a| = 1$。

注 ***68.*** —显然，对于任意整数 N 和任意格 Λ，都有 $N\Lambda \subset \Lambda$，而映射 $z \mapsto Nz$ 诱导出 $\mathbb{C}/\Lambda$ 的一个自同态，该自同态就是乘以 N 的映射。此外，若存在 $a \in \mathbb{C}\backslash\mathbb{Z}$ 使得 $a\Lambda \subset \Lambda$，则相应的椭圆曲线称为具有复乘。

任意复环面的一个初等自同构为 $z \mapsto -z$。回到式 (18) 中的映射 Ψ_Λ ，并利用 $\wp_\Lambda$ 和 $\wp'_\Lambda$ 分别为偶函数和奇函数这一事实，我们推得该映射在椭圆曲线上对应于关于 x 轴的对称:

$$(x, y) \longmapsto (x, -y).$$

此外，一些零星的椭圆曲线具有非平凡的自同构，这些自同构来自 $z \mapsto az$ with$|a| = 1$ 和 $a \notin \{\pm 1\}$。

定理 ***69***。——设 $\mathbb{C}/\Lambda$ 是一个复环面，具有一个自同构 $z \mapsto az$ ，满足 $|a| = 1$ 和 $a \notin \{\pm 1\}$。等价地，格 Λ 满足 $\Lambda = a\Lambda$。那么， Λ 是以下两个格之一经相似变换所得的像:

$$\mathbb{Z} \oplus \mathbb{Z}i \quad or \quad \mathbb{Z} \oplus \mathbb{Z}\rho,$$

其中 $\rho = e^{\frac{i\pi}{3}}$。

证明。——设 Λ 是一个格，满足 $a\Lambda = \Lambda$，并设 $\nu \in \Lambda \setminus \{0\}$ 是模最小的向量。由于我们只考虑相似变换意义下的 Λ，可以假设 $\nu = 1$，且对所有 $\omega \in \Lambda \setminus \{0\}$，都有 $|\omega| \geqslant 1$。假设 $1 \in \Lambda$，那么根据关于 Λ 的假设，我们可推得 a， a^2 也是 Λ 的元素。由于 $a \notin \mathbb{R}$，它在 $\mathbb{R}$ 上的最小多项式为

$$\begin{aligned}(x - a)(x - \bar{a}) &= x^2 + 2\mathrm{Re}(a)x + |a|^2 \\ &= x^2 + 2\mathrm{Re}(a)x + 1,\end{aligned}$$

其中，Re(a)表示 a的实部。因此，

$$a^2 + 1 = -2\mathrm{Re}(a)a.$$

注意， $|a| = 1$ 和 $a \notin \mathbb{R}$ 推出 $-1 <$ Re(a) < 1。若2Re(a) $\notin \mathbb{Z}$，则存在 $\varepsilon \in \{-1, 0, 1\}$ ，使得

$$a^2 + \varepsilon a + 1 = \gamma a$$

对于某个 $0 < \gamma < 1$。由于左端是 Λ中元素的 $\mathbb{Z}$线性组合，因此 $\gamma a \in \Lambda$，这与任何非零 $\omega \in \Lambda$都满足 $|\omega| \geqslant 1$的假设矛盾。因此，Re(a) $\in \{-\frac{1}{2}, 0, \frac{1}{2}\}$。情形Re($a$) $= 0$ 给出了情形 $\Lambda = \mathbb{Z} \oplus \mathbb{Z}i$ ，而另外两种情形给出相同的格，即$\mathbb{Z} \oplus \mathbb{Z}\rho$。

□

可以证明，相应的椭圆曲线分别具有以下方程:

$$\begin{array}{lllll} y^2 = x^3 + x & \text{for} & \Lambda = \mathbb{Z} \oplus \mathbb{Z}i & (j\text{–invariant } 1728) \\ y^2 = x^3 + 1 & \text{for} & \Lambda = \mathbb{Z} \oplus \mathbb{Z}\rho & (j\text{–invariant } 0). \end{array} \tag{19}$$

相应的自同构分别为

$$\begin{aligned}(x, y) &\longmapsto (-x, iy) \\ (x, y) &\longmapsto (\rho x, -y).\end{aligned}$$

注意，这些自同构的阶分别为 4 和 6，恰好是 i 和 ρ 的乘法阶。最后注意，对于任何包含 1 的四次根和六次根的域，方程 (19) 所定义的曲线都具有非平凡自同构群。进一步可以证明，它们是仅有的具有非平凡自同构群的曲线 [**Sil09**，定理 III.10。1] 而且它们的自同构群的基数分别为 4 和 6。

5. 模曲线

5.1. 庞加莱上半平面。— 我们的目标是对 $\mathbb{C}$ 上的椭圆曲线按同构分类。如 § 4.5 中所述，这归结为对格按相似变换分类，其定义已在那里回顾。

定义 **70** （$\mathbb{C}$**的相似变换**）。— A 相似变换 是 $\mathbb{C}$ 的一种映射，其形式为 $z \mapsto az$，其中 $a \in \mathbb{C}^\times$.

除了相似变换群对 $\mathbb{C}$的格集合的作用之外，格还由一个并非唯一的基来描述。因此，需要在可能的基上引入另一个群作用。也就是说，给定一个格

$$\Lambda = \mathbb{Z}\omega_1 \oplus \mathbb{Z}\omega_2,$$

基 (ω_1, ω_2) 并非唯一，任何其他基 (μ_1, μ_2) 都可由 (ω_1, ω_2) 通过以下方式得到

$$\begin{pmatrix}\mu_1\\ \mu_2\end{pmatrix} = M \cdot \begin{pmatrix}\omega_1\\ \omega_2\end{pmatrix}, \quad \text{for some } M \in \mathbf{GL}_2(\mathbb{Z}).$$

交换基的两个元素后，总可以假设我们考虑的基具有相同的定向，即$\mathrm{Im}(\frac{\omega_1}{\omega_2}) > 0$（分别地，$\mathrm{Im}(\frac{\mu_1}{\mu_2}) > 0$），其中 $\mathrm{Im}(\cdot)$ 表示复数的虚部。若基是在这一约束下选取的，那么过渡矩阵 M 总有正行列式，因此属于 $\mathbf{SL}_2(\mathbb{Z})$。因此， $\mathbb{C}$ 的格的集合与满足 $\mathrm{Im}(\frac{\omega_1}{\omega_2}) > 0$ 的有序对 $(\omega_1, \omega_2) \in \mathbb{C}^2$ 在 $\mathbf{SL}_2(\mathbb{Z})$ 的作用下所得的等价类一一对应。接下来，我们需要考虑相似变换的作用。从满足 $\mathrm{Im}(\frac{\omega_1}{\omega_2}) > 0$ 的 $\Lambda = \mathbb{Z}\omega_1 \oplus \mathbb{Z}\omega_2$ 出发，应用相似变换 $z \mapsto \frac{1}{\omega_2} z$，得到一个相似的格：

$$\mathbb{Z} \oplus \mathbb{Z}\tau$$

其中 $\tau = \frac{\omega_1}{\omega_2}$，因此 $\mathrm{Im}(\tau) > 0$。令

$$\mathbb{H} \overset{\mathbf{def}}{=} \{z \in \mathbb{C} \mid \mathrm{Im}(z) > 0\},$$

为庞加莱上半平面。那么，每个格在相似变换意义下都可以与一个元素相关联$\tau \in \mathbb{H}$，而$\mathbf{SL}_2(\mathbb{Z})$ 对格基的作用会在 $\mathbb{H}$ 上诱导出如下作用。从

$$M = \begin{pmatrix}a & b\\ c & d\end{pmatrix} \in \mathbf{SL}_2(\mathbb{Z}),$$

M 对基的作用如下：

$$M \cdot \begin{pmatrix}\omega_1\\ \omega_2\end{pmatrix} = \begin{pmatrix}a\omega_1 + b\omega_2\\ c\omega_1 + d\omega_2\end{pmatrix}.$$

因此，由于 $\tau = \frac{\omega_1}{\omega_2}$，我们自然地将$\mathbf{SL}_2(\mathbb{Z})$ 在 $\mathbb{H}$ 上的作用定义为

$$M \cdot \tau \overset{\mathbf{def}}{=} \frac{a\omega_1 + b\omega_2}{c\omega_1 + d\omega_2} = \frac{a\tau + b}{c\tau + d}. \tag{20}$$

I总之， 根据 § 4.5 的讨论，我们得到如下对应关系 e:

$$\begin{array}{ccccccc}\text{Elliptic curves}\\ \text{up to}\\ \text{isomorphism} & \longleftrightarrow & \text{Complex tori}\\ \text{up to}\\ \text{biholomorphic}\\ \text{isomorphisms} & \longleftrightarrow & \text{Lattices of } \mathbb{C}\\ \text{up to}\\ \text{similitudes} & \longleftrightarrow & \text{Points of } \mathbb{H}\\ \text{modulo}\\ \text{the action (20) of}\\ \mathbf{SL}_2(\mathbb{Z})\end{array}$$

此外，$\mathbf{SL}_2(\mathbb{Z})$ 在 $\mathbb{H}$ 上作用的基本域如图 4 所示。这是一幅著名的图，在许多关于几何学或数论的书中都能见到。

5.2. 曲线 $X_0(1)$。——因此，为了对模同构的椭圆曲线进行参数化，我们可以考虑商空间 $\mathbf{SL}_2(\mathbb{Z})\backslash\mathbb{H}$。 [**Mil17** 命题 2.21]证明，该商空间是一个与 $\mathbb{A}^1$ 同构的复代数簇，即复仿射直线。这并不令人意外；定理 65 表明，模同构的复椭圆曲线与 $\mathbb{C}$ 之间存在一一对应关系，其对应由映射 $\mathscr{E} \mapsto j(\mathscr{E})$ 给出，其中 $j(\mathscr{E})$ 表示 $\mathscr{E}$ 的 j– 不变量。

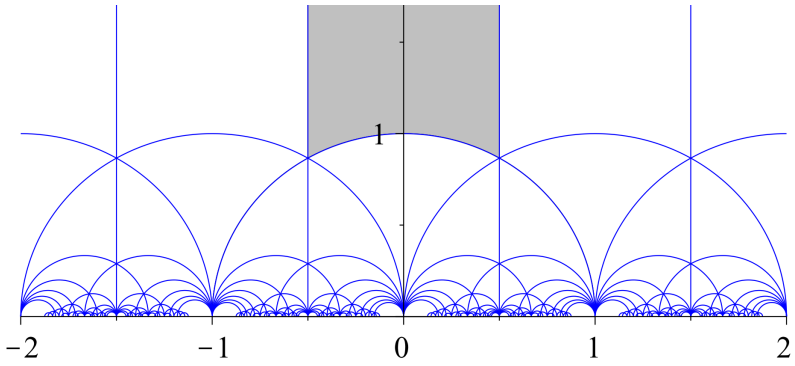


图 4. $\mathbf{SL}_2(\mathbb{Z})$ 在 $\mathbb{H}$ 上的作用的基本区域（来源：维基百科）

接下来，为了方便起见，并为了应用 § 2 中介绍的代数曲线相关结果，我们需要构造这条参数化曲线的某种射影闭包。在复数情形下，这无非是一种紧化，而仿射直线可以通过添加一个点来紧化。不过，出于一个在下文中会显得更加自然的原因，这种紧化将通过一种稍微复杂一些的构造来实现。

其思路是将 $\mathbb{H}$ 边界上的所有 $\mathbb{Q}$ 元素与一个无穷远点一起添加到 $\mathbb{H}$ 中。也就是说，我们定义

$$\mathbb{H}^* \overset{\mathbf{def}}{=} \mathbb{H} \cup \mathbb{P}^1(\mathbb{Q}).$$

接下来我们来看看 $\mathbf{SL}_2(\mathbb{Z})$ 的作用如何扩展到 $\mathbb{P}^1(\mathbb{Q})$。

命题 ***71.*** — 考虑 $\mathbf{SL}_2(\mathbb{Z})$ 在 $\mathbb{P}^1(\mathbb{Q})$ 上的如下作用：

$$\forall M = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathbf{SL}_2(\mathbb{Z}),\ (u:v) \in \mathbb{P}^1(\mathbb{Q}), \quad M \cdot (u:v) = (au+bv : cu+dv).$$

这个作用是传递的，即 对于任意 $(u:\ v)$,$(u':\ v') \in \mathbb{P}^1(\mathbb{Q})$，都存在 $M \in \mathbf{SL}_2(\mathbb{Z})$，使得$M \cdot (u:v) = (u':\ v')$。

Proof. ——首先，我们来证明 $(0:1)$ 的轨道等于整个 $\mathbb{P}^1(\mathbb{Q})$。首先注意到

$$\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \cdot (0:1) = (-1:0) = (1:0).$$

因此，$(1:0)$ 属于 $(0:1)$ 的轨道。接下来，考虑任意其他点 $(s:\ t) \in \mathbb{P}^1(\mathbb{Q}) \setminus \{(1:0)\}$，即满足 $t \neq 0$ 的点。将坐标乘以一个公分母后，可设 $s,\ t \in \mathbb{Z}$再将它们同时除以可能存在的最大公约数后，可设 $s,\ t$ 互素。根据贝祖定理，存在 $u,\ v \in \mathbb{Z}$ 使得 $su+tv=1$，于是

$$\begin{pmatrix} t & u \\ -s & v \end{pmatrix} \cdot (0:1) = (u:v) \quad \text{and} \quad \begin{pmatrix} t & u \\ -s & v \end{pmatrix} \in \mathbf{SL}_2(\mathbb{Z}).$$

因此，$\mathbb{P}^1(\mathbb{Q})$ 中的任意元素都属于 $(0:1)$ 的轨道。最后，给定两个元素 $(u:\ v)$，$(u':v') \in \mathbb{P}^1(\mathbb{Q})$，存在 $M,\ M'$使得 $(u:\ v) = M \cdot (0:1)$，且 $(u':\ v') = M' \cdot (0:1)$，并且 $(u':\ v') = M'M^{-1}(u:\ v)$。 □

因此，商空间$\mathbf{SL}_2(\mathbb{Z})\backslash\mathbb{H}^*$ 不过是通过添加一个点对$\mathbf{SL}_2(\mathbb{Z})\backslash\mathbb{H}$ 进行紧化。这个商空间通常记作 $X_0(1)$，它就是黎曼球面 $\mathbb{P}^1(\mathbb{C})$。

就 $X_0(1)$ 上的函数而言，存在一个全纯函数 $j:\ \mathbb{H} \to \mathbb{C}$，它在 $\mathbf{SL}_2(\mathbb{Z})$ 的作用下保持不变，并且诱导的映射 $\mathbf{SL}_2(\mathbb{Z})\backslash\mathbb{H} \to \mathbb{C}$ 是双射。此映射实现了 $X_0(1)$ 与 $\mathbb{P}^1(\mathbb{C})$ 之间的同构。它可以按如下方式“具体构造”：由 $\tau \in \mathbb{H}$ 构造格 $\Lambda_\tau = \mathbb{Z} \oplus \mathbb{Z}\tau$。然后利用魏尔斯特拉斯 $\wp_{\Lambda_\tau}$ 函数，计算对应于 $\mathbb{C}/\Lambda_\tau$ 的椭圆曲线方程。于是，$j(\tau)$ 不过是这条椭圆曲线的 j 不变量。

5.3. 曲线 $X_0(\ell)$。—虽然我们现在有了一条按同构分类椭圆曲线的参数曲线，但距离目标仍有些远：我们要寻找的是一个曲线族，其亏格序列趋于无穷，而目前得到的 $\mathbb{P}^1$ 亏格为 0。要得到亏格更高的曲线，我们需要丰富其结构。我们的思路不仅是按同构分类椭圆曲线，还要针对固定的整数 ℓ，按同构分类 ℓ–同源 $\mathscr{E} \to \mathscr{E}'$。下文中，我们只关注 ℓ 为素数的情形（不过，后续许多结果也适用于任意次数的同源）。

备注 ***72.*** — 请注意，此处"在同构意义下"是指，若存在两个同构 $\eta\colon \mathscr{E}_1 \to \mathscr{E}_2$ 和 $\nu\colon \mathscr{E}_1' \to \mathscr{E}_2'$，使得下图可交换，则称两个同源 $\phi_1 : \mathscr{E}_1 \to \mathscr{E}_1'$ and$\phi_2\colon \mathscr{E}_2 \to \mathscr{E}_2'$ 是同构 的。

$$\begin{array}{ccc} \mathscr{E}_1 & \xrightarrow{\phi_1} & \mathscr{E}_2 \\ \eta \downarrow & & \downarrow \nu \\ \mathscr{E}_1' & \xrightarrow{\phi_2} & \mathscr{E}_2' \end{array}$$

由定理 59， ℓ–同源 $\mathscr{E} \to \mathscr{E}'$ 对应于一对 $(\mathscr{E}, C)$，其中 $C \subseteq \mathscr{E}[\ell]$ 是基数为 ℓ 的子群。因此，在复数情形下，问题归结为分类满足 $\Lambda \subseteq \Lambda'$ 和 $\sharp(\Lambda'/\Lambda) = \ell$ 的格对 Λ, Λ'。主理想环上有限生成模的结构定理断言，存在 Λ 的一个基 ω_1, ω_2，使得

$$\Lambda = \mathbb{Z}\omega_1 \oplus \mathbb{Z}\omega_2 \quad \text{and} \quad \Lambda' = \mathbb{Z}\frac{\omega_1}{\ell} \oplus \mathbb{Z}\omega_2.$$

由上述描述可轻易看出， $\mathscr{E}[\ell] = (\frac{1}{\ell}\Lambda)/\Lambda \simeq \mathbb{F}_\ell \oplus \mathbb{F}_\ell$和 Λ'/Λ可识别为 $\mathscr{E}[\ell]$的一个维数为 1 的$\mathbb{F}_\ell$子空间，即由 $\frac{\omega_1}{\ell}$的等价类张成的子空间。由于我们希望对具有给定 ℓ挠子群 C的椭圆曲线 $\mathscr{E}$进行分类，因此需要对保持该子群不变的基变换进行分类。注意，$\mathbf{SL}_2(\mathbb{Z})$ 在 Λ 的基上的作用，会在$\mathscr{E}[\ell] = (\frac{1}{\ell}\Lambda)/\Lambda$上诱导出一个自然的 $\mathbf{SL}_2(\mathbb{F}_\ell)$ 作用。固定 $\frac{\omega_1}{\ell}$等价类的 $\mathbf{SL}_2(\mathbb{F}_\ell)$ 元素是上三角矩阵。这促使我们定义同余子群 $\Gamma_0(\ell) \subset \mathbf{SL}_2(\mathbb{Z})$:

$$\Gamma_0(\ell) \overset{\text{def}}{=} \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathbf{SL}_2(\mathbb{Z}) \;\middle|\; c \equiv 0 \mod \ell \right\}.$$

也就是说,这是 $\mathbf{SL}_2(\mathbb{Z})$ 中诱导出 $\mathscr{E}[\ell]$ 自同构且固定 C 的元素所构成的群 .

练习 ***73***。— 证明典范映射

$$\mathbf{SL}_2(\mathbb{Z}) \longrightarrow \mathbf{SL}_2(\mathbb{F}_\ell)$$

由将系数模 ℓ 约化所给出的是满射。证明如下:
(a) 证明 $\mathbf{SL}_2(\mathbb{F}_\ell)$ 的一个元素有一个提升 $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$，其中 a， b， c， $d \in Z$ 使得 a， b 均非零且互素。

(b) 证明对于这样的提升， c， d 可以替换为 c'， d'，使得 $c \equiv c'$ 模 ℓ 且 $d \equiv d'$ 模 ℓ，从而 $\det \begin{pmatrix} a & b \\ c' & d' \end{pmatrix} = 1$.

因此，椭圆曲线之间模同构的 ℓ–同源与复代数簇之间存在一一对应关系

$$\Gamma_0(\ell)\backslash\mathbb{H}.$$

这个代数簇有一个紧化

$$X_0(\ell) \overset{\text{def}}{=} \Gamma_0(\ell)\backslash\mathbb{H}^*.$$

这是一个紧致黎曼曲面，并且可以证明，这种对象实际上是代数的，也就是说与一条光滑复射影曲线双全纯等价。我们将在后文进一步讨论这种代数曲线结构。

下一条陈述给出了一项重要信息，即 $X_0(\ell)$的亏格。

定理 *74.* — 对于素数 $\ell > 3$， $X_0(\ell)$ 的亏格 g_ℓ 等于

$$g_\ell = \begin{cases} \frac{\ell-1}{12} - 1 & if \quad \ell \equiv 1 \mod [12] \\ \frac{\ell-5}{12} & if \quad \ell \equiv 5 \mod [12] \\ \frac{\ell-7}{12} & if \quad \ell \equiv 7 \mod [12] \\ \frac{\ell+1}{12} & if \quad \ell \equiv 11 \mod [12]. \end{cases}$$

我们首先需要两个技术性引理。

引理 *75.* — 设 ℓ 是素数。设 $\Lambda \subseteq \mathbb{C}$ 是一个格， Λ_1和Λ_2 是两个不同的格，它们都包含 Λ 和 $\sharp(\Lambda_1/\Lambda) = \sharp(\Lambda_2/\Lambda) = \ell$。假设对于某个 $a \in \mathbb{C}$，有 $a\Lambda_1 = \Lambda_2$ 。那么 $|a| = 1$ 且$a\Lambda = \Lambda$。等价地，设 $\mathbb{C}$ 上的椭圆曲线为 $\mathscr{E}$，并设 C_1、C_2 是 $\mathscr{E}[\ell]$的两个不同子群，基数均为ℓ 。若曲线 $\mathscr{E}/C_1$ 与 $\mathscr{E}/C_2$ 同构，则存在 $\mathscr{E}$ 的一个自同构，将 C_1映到 C_2。

注 *76*。——注意，如果 $\mathscr{E}$ 具有这样的自同构，那么它必定是定理 69 中提到的两条曲线之一。

引理的证明 *75*。**——步骤 1。适配基**。我们断言，存在 $\omega_1, \omega_2 \in \mathbb{C}$ ，使得

$$\Lambda = \mathbb{Z}\omega_1 \oplus \mathbb{Z}\omega_2 \quad \text{and} \quad \Lambda_1 = \mathbb{Z}\frac{\omega_1}{\ell} \oplus \mathbb{Z}\omega_2 \quad \text{and} \quad \Lambda_2 = \mathbb{Z}\omega_1 \oplus \mathbb{Z}\frac{\omega_2}{\ell}. \tag{21}$$

可按如下方式得到 ω_1, ω_2 的存在性。首先，主理想环上有限生成模的结构定理断言，存在一个基 η_1, η_2 ，使得

$$\Lambda = \mathbb{Z}\eta_1 \oplus \mathbb{Z}\eta_2 \quad \text{and} \quad \Lambda_1 = \mathbb{Z}\frac{\eta_1}{\ell} \oplus \mathbb{Z}\eta_2.$$

接下来，我们断言

$$\Lambda_2 = \mathbb{Z}\eta_1 \oplus \mathbb{Z}\frac{u\eta_1 + \eta_2}{\ell},$$

对于某个 $u \in \{0, \ldots, \ell-1\}$。事实上，考虑与 $\mathbb{F}_\ell \times \mathbb{F}_\ell$同构的 $\left(\frac{1}{\ell}\Lambda\right)/\Lambda$。在这个商空间中，$\Lambda_1/\Lambda$ 和 Λ_2/Λ 被视为直和中的两个维数为 1 的 $\mathbb{F}_\ell$子空间。子空间 Λ_1/Λ由 $\frac{\eta_1}{\ell}$的等价类张成；由于 Λ_1/Λ和 Λ_2/Λ在 $\left(\frac{1}{\ell}\Lambda\right)/\Lambda$中构成直和，因此 Λ_2/Λ 应由某个 $u \in \mathbb{F}_\ell$对应的 $\frac{u\eta_1+\eta_2}{\ell}$的等价类张成。这意味着存在$u \in \{0, \ldots, \ell-1\}$，使得 $\frac{u\eta_1+\eta_2}{\ell} \in \Lambda_2$，因此——

$$\mathbb{Z}\eta_1 \oplus \mathbb{Z}\frac{u\eta_1 + \eta_2}{\ell} \subseteq \Lambda_2.$$

于是，由于 $\sharp(\Lambda_2/\Lambda) = \ell$，我们可以推断上述包含关系实际上是等式。最后，定义ω_1， ω_2 为

$$\begin{pmatrix} \omega_1 \\ \omega_2 \end{pmatrix} \overset{\mathbf{def}}{=} \begin{pmatrix} 1 & u \\ 0 & 1 \end{pmatrix} \cdot \begin{pmatrix} \eta_1 \\ \eta_2 \end{pmatrix}.$$

注意，上述变量替换由一个属于 $\mathbf{SL}_2(\mathbb{Z})$ 的矩阵给出，并为 Λ 提供了一个满足 (21) 的基。

步骤 2. a的模。 格理论中的一个经典概念是格的行列式或体积。它可以定义如下。考虑 $\Lambda = \mathbb{Z}\omega_1 \oplus \mathbb{Z}\omega_2$ ，并将 $\mathbb{C}$ 视为一个以 $(1, i)$ 为典范基的二维$\mathbb{R}$向量空间。由于 Λ 的任意一组基都可以通过对 (ω_1, ω_2) 作用一个属于 $\mathbf{GL}_2(\mathbb{Z})$ 的矩阵得到，即一个行列式为 ± 1 的矩阵，因此，对于 Λ 的任意一组基，量 $|\det(\omega_1, \omega_2)|$ 都相同。故将此量记为 $|\det \Lambda|$。由 (21)，我们有

$$\det \Lambda_1 = \frac{1}{\ell} \det \Lambda = \det \Lambda_2. \tag{22}$$

此外，将乘以 a 的映射 $z \mapsto az$ 视为 $\mathbb{R}$上的线性自同态，其行列式为 $|a|^2$。事实上，写作 $a = a_0 + DA_1$，该映射在基 $(1, i)$ 下由矩阵表示

$$\begin{pmatrix} a_0 & -a_1 \\ a_1 & a_0 \end{pmatrix},$$

其行列式为 $a_0^2+a_1^2=|a|^2$。接下来，假设 $\Lambda_2=a\Lambda_1$ 与 (22) 一起给出

$$\det\Lambda_1=\det\Lambda_2=|a|^2\det\Lambda_1,$$

由此得到 $|a|^2=1$。

步骤 3。我们要证明 $a\Lambda=\Lambda$。假设结论不成立。由于 $\Lambda\subseteq\Lambda_1$, $\Lambda\subseteq\Lambda_2$ 和 $a\Lambda\subseteq a\Lambda_1=\Lambda_2$，因此 $\Lambda+a\Lambda\subseteq\Lambda_2$。回想一下，$\sharp\Lambda_2/\Lambda=\ell$ 且 ℓ 是素数。于是，由于我们假设 $\Lambda\subsetneq\Lambda+a\Lambda$，可得 $\Lambda+a\Lambda=\Lambda_2$。类似地，可以推出 $a^{-1}\Lambda+\Lambda=\Lambda_1$。接下来，由 (21) 可知 $\Lambda_1+\Lambda_2=\frac{1}{\ell}\Lambda$，因此

$$a^{-1}\Lambda+\Lambda+a\Lambda=\frac{1}{\ell}\Lambda.$$

由归纳法，

$$a^{-s}\Lambda+\cdots+a^{-1}\Lambda+\Lambda+a\Lambda+\cdots+a^s\Lambda=\frac{1}{\ell^s}\Lambda.$$

因此，对于任意 $s\geqslant 0$，都存在一个由 Λ 中的元素构成的有限序列 $(\mu_i^s)_{i=-s}^s$，使得

$$\sum_{i=-s}^{s}a^i\mu_i^s=\frac{1}{\ell^s}\omega_1.$$

那么，对于任意 $N\geqslant 0$,

$$\begin{aligned}\sum_{s=0}^{N}\sum_{i=-s}^{s}a^i\mu_i^s &= \sum_{s=0}^{N}\frac{1}{\ell^s}\omega_1,\\ \sum_{i=-N}^{N}a^i\nu_i &= \sum_{s=0}^{N}\frac{1}{\ell^s}\omega_1,\end{aligned}$$

其中 ν_i 属于 Λ。当 N 趋于无穷大时，右边是一个收敛级数。因此左边也如此，所以其通项应趋于 0。由上一步可知，$|a|=1$；又因为 ν_i 属于 Λ，而后者是离散的，所以对于任何充分大的 i，都有 $\nu_i=0$。因此，左边的部分和序列最终保持不变，而右边的部分和序列则不是。矛盾。因此 $a\Lambda=\Lambda$。

□

引理 77。——令 $\mathscr{E}_i\xrightarrow{\text{定义为}}\mathbb{C}/(\mathbb{Z}\oplus\mathbb{Z}i)$，并考虑由 $\mathbb{C}$ 中 $\{\pm1,\pm i\}$ 的乘法诱导的其自同构群 G_i。那么，在 G_i 的作用下具有非平凡稳定子的任意 $P\in\mathscr{E}_i(\mathbb{C})$ 都属于 $\mathscr{E}[2]$。

类似地，令 $\mathscr{E}_\rho\xrightarrow{\text{定义为}}\mathbb{C}/(\mathbb{Z}\oplus\mathbb{Z}\rho)$，其中 $\rho=e^{\frac{i\pi}{3}}$ 的自同构群 G_ρ 由乘以 $\{\pm1,\pm\rho,\pm\rho^2\}$诱导，那么任何在$G_\rho$ 的作用下具有非平凡稳定子的 $P\in\mathscr{E}_\rho(\mathbb{C})$ 都属于 $\mathscr{E}[6]$。

证明。——在 $\mathscr{E}_i$的情形下，记 $\Lambda_i\xrightarrow{\text{定义为}}\mathbb{Z}\oplus\mathbb{Z}i$。由于 G_i 是 4 阶循环群，它的非平凡子群只有 $\{\pm1\}$ 和 G_i 本身。由 $\{\pm1\}$ 稳定的点 $P\in\mathscr{E}_i(\mathbb{C})$ 对应于满足$z\equiv -z$ 模 Λ_i的 $z\in\mathbb{C}$。也就是说 $2z\in\Lambda_i$，因此 $P\in\mathscr{E}_i[2]$。类似地，如果 P被所有 G_i 稳定，那么它更必然被 $\{\pm1\}$ 稳定，因此应属于 $\mathscr{E}_i[2]$。

现在考虑 $\mathscr{E}_\rho$ 的情形。记 $\Lambda_\rho\xrightarrow{\text{定义}}\mathbb{Z}\oplus\mathbb{Z}\rho$。由于 G_ρ 是 6 阶循环群，其可能的非平凡子群只有 $\{\pm1\}$、$\{1,\rho^2,\rho^4\}$ 和 G_ρ 本身。我们来考虑被这些群之一稳定的点。

设 $P\in\mathscr{E}_\rho(\mathbb{C})$ 被 $\{\pm1\}$ 稳定，则与 $\mathscr{E}_i$ 相同的推理可得 $P\in\mathscr{E}_\rho[2]$。

设 $P\in\mathscr{E}_\rho(\mathbb{C})$ 被 $\{1,\rho^2,\rho^4\}$ 稳定。这对应于满足 $\rho^2z\equiv z \mod \Lambda_\rho$ 的 $z\in\mathbb{C}$。令 $z=a+b\rho^2$ 为某个 $a,b\in\mathbb{R}$，并利用关系 $1+\rho^2+\rho^4=0$，可得

$$a+\rho^2b\equiv -b+\rho^2(a-b)\mod\Lambda_\rho.$$

这意味着

$$\begin{cases}-b &= a+\mu\\ a-b &= b+\nu,\end{cases}$$

其中 $\mu, \nu \in \mathbb{Z}$。通过消元，我们推得 $3a \in \mathbb{Z}$ 且 $3b \in \mathbb{Z}$，也就是说 $z \in \frac{1}{3}\Lambda_\rho$，因此$P \in \mathscr{E}_\rho[3]$。

最后，前面的讨论表明，由整个 G_ρ 稳定的点必定属于 $\mathscr{E}_\rho[2] \cap \mathscr{E}_\rho[3]$，因此它只能是 $O_{\mathscr{E}_\rho}$。

□

定理 *74* 的证明. — 思路是考虑投影映射 $\pi : X_0(\ell) \to X_0(1)$，它将同源 $\phi : \mathscr{E} \to \mathscr{E}'$ 的同构类映射到 $\mathscr{E}$ 的同构类。这个映射是代数的（这一点将在 § 5.4 中更自然地呈现）。目标是对 π 应用黎曼－赫尔维茨公式（定理 31），以计算 $X_0(\ell)$ 的亏格。

步骤 1. π 的次数。 π 的次数是 $X_0(1)$ 中一点的原像的一般个数。这样的点对应于一个曲线 $\mathscr{E}$ 的同构类，而它的原像是 ℓ–同源 $\mathscr{E} \to \mathscr{E}'$ 的同构类集合；等价地说，是由一对 $(\mathscr{E}, C)$ 构成的同构类，其中 C 是 $\mathscr{E}[\ell]$ 中基数为 ℓ 的子群。根据引理 75，若 $\mathscr{E}$ 没有非平凡自同构，则两个不同的子群 C_1, C_2 会给出非同构的配对 $(\mathscr{E}, C_1)$,$(\mathscr{E}, C_2)$。因此，在这种情况下，π 下 $\mathscr{E}$ 的原像个数对应于 $\mathscr{E}[\ell]$ 中基数为 ℓ 的子群个数。由于 ℓ 是素数，根据定理 54，$\mathscr{E}[\ell] \simeq \mathbb{F}_\ell \times \mathbb{F}_\ell$，因而是一个在 $\mathbb{F}_\ell$ 上维数为 2 的向量空间。接下来，$\mathscr{E}[\ell]$ 中基数为 ℓ 的子群恰好是一个维数为 1 的子空间，而 $\mathbb{F}_\ell \times \mathbb{F}_\ell$ 中维数为 1 的子空间（即直线）的个数等于 $\sharp\mathbb{P}^1(\mathbb{F}_\ell) = \ell + 1$。因此，

$$\deg \pi = \ell + 1.$$

现在，该映射在对应于具有非平凡自同构的曲线的点处以及可能在无穷远点处分歧。根据定理 69，具有非平凡自同构的曲线对应于环面 $\mathbb{C}/(\mathbb{Z} \oplus \mathbb{Z}i)$ 和 $\mathbb{C}/(\mathbb{Z} \oplus \mathbb{Z}\rho)$，其中 $\rho = e^{\frac{i\pi}{3}}$。对于这些环面，我们需要了解自同构在 ℓ–挠点上的作用。

步骤 2. 在 $\mathbb{C}/(\mathbb{Z} \oplus \mathbb{Z}i)$ 处分歧。该曲线带有一个阶为 4 的非平凡自同构 η，它对应于在 $\mathbb{C}$ 中乘以 i。此自同构作用于 ℓ–挠点；根据 [**Sil09**，定理 III.4.8]，，这样的自同构是群自同构，因此它在被视为 $\mathbb{F}_\ell$–向量空间的 $\mathscr{E}[\ell]$ 上的作用是 $\mathbb{F}_\ell$–线性的。我们将自同构 η 在 $\mathscr{E}[\ell]$ 上的限制记为 η_ℓ。根据引理 77，由于 $\ell > 3$，$\mathscr{E}[\ell] \setminus \{O_{\mathscr{E}}\}$ 中的任意点在 η_ℓ 作用下的轨道基数为 4。因此，η_ℓ 的阶为 4，可能出现两种情况。要么 $\ell \equiv 1$ 模 4，此时 $\mathbb{F}_\ell$ 包含 1 的四次方根，并且作为 $\mathbb{F}_\ell$ 的 $\mathbb{F}_\ell \times \mathbb{F}_\ell$–自同构，$\eta_\ell$ 可对角化为

$$\begin{pmatrix} \iota & 0 \\ 0 & -\iota \end{pmatrix},$$

其中 ι 表示 1 的原始四次方根。在这种情况下，η_ℓ 通过固定对应于 η_ℓ 的特征子空间的两条直线，作用于 $\mathbb{F}_\ell \times \mathbb{F}_\ell$ 的直线上；任何其他直线的轨道基数为 2，事实上 $\eta_\ell^2 = -\mathrm{Id}$，它使任意直线保持不变。$\mathscr{E}[\ell]$ 中同一轨道下的两条直线，在 $X_0(\ell)$ 中对应同一个点。该点是分歧点，分歧指数为 2。因此，若 $\ell \equiv 1 \equiv 1 \bmod 4$，则 $\mathscr{E}$ 的同构类在 π 下的原像中有 2 个非分歧点，以及 $\frac{\ell-1}{2}$ 个分歧指数为 2 的分歧点。

否则，$\ell \equiv 3 \equiv 1 \bmod 4$。在这种情况下，$\eta_\ell$ 在 $\mathscr{E}[\ell]$ 中没有特征子空间，且任意直线的轨道基数均为 2。因此，$\mathscr{E}$ 上方有 $\frac{\ell+1}{2}$ 个点，它们全都是分歧指数为 2 的分歧点。

步骤 3：在 $\mathbb{C}/(\mathbb{Z} \oplus \mathbb{Z}\rho)$。 这里有一个阶为 6 的自同构 η，再次记其在 $\mathscr{E}[\ell]$ 上的限制为 η_ℓ。同样，根据引理 77，我们知道 η_ℓ 的阶也为 6。在这种情况下，如果 $\ell \equiv 1$ 模 3，那么 $\mathbb{F}_\ell$ 包含六次单位根，且 η_ℓ 可对角化。因此，η_ℓ 的两个特征子空间保持不变，而 $\mathscr{E}[\ell]$ 中任何其他 $\mathbb{F}_\ell$ 直线的轨道基数为 3。事实上，同样有 $\rho^3 = -\mathrm{Id}$，因此它使任意直线整体保持不变。在这种情况下，$\mathscr{E}$ 的原像由两个非分歧点组成，它们对应于 $\mathscr{E}[\ell]$ 中 η_ℓ 的两个特征子空间；此外还有 $\frac{\ell-1}{3}$ 个分歧指数为 3 的点。

若 $\ell \equiv 2$ 模 3，则 $\mathscr{E}[\ell]$ 的任一直线在 η_ℓ 的作用下都有一个基数为 3 的轨道，因此，$\mathscr{E}$ 在 π 下的原像由 $\frac{\ell+1}{3}$ 个点组成，且这些点的分歧指数均为 3。

步骤 4. 无穷远处分歧。 $X_0(1)$ 的无穷远点是 $\mathbb{P}^1(\mathbb{Q})$ 在 $\mathbf{SL}_2(\mathbb{Z})$ 作用下的商空间；根据命题 71，它由单个轨道组成。我们希望估计 $\mathbb{P}^1(\mathbb{Q})$ 在 $\Gamma_0(\ell)$ 作用下的轨道数。我们断言其轨道数为 2，即 $(0:1)$ 的轨道和 $(1:0)$ 的轨道。事实上，

$$\Gamma_0(\ell)\cdot(0:1) = \{(b:d) \in \mathbb{P}^1(\mathbb{Q}) \text{ with } \gcd(b,d) = 1 \text{ and } d \text{ prime to } \ell\}$$

and

$$\Gamma_0(\ell)\cdot(1:0) = \{(a:c) \in \mathbb{P}^1(\mathbb{Q}) \text{ with } \gcd(a,c) = 1 \text{ and } \ell \text{ dividing } c\}.$$

容易看出，这两个轨道构成了 $\mathbb{P}(\mathbb{Q})$的一个划分。这意味着，$X_0(1)$的无穷远点的原像由两点组成 P，Q 其分歧指数满足 $e_P + e_Q = \ell + 1$。

最后一步。计算亏格。记 g_ℓ 为 $X_0(\ell)$的亏格，$g_1 = 0$ 为$X_0(1)$的亏格。黎曼–赫尔维茨公式断言

$$2g_\ell - 2 = (2g_1 - 2)(\ell + 1) + \nu_i + \nu_\rho + \nu_\infty,$$

其中 ν_i，ν_ρ 和 ν_∞ 分别是位于 $\mathbb{C}/(\mathbb{Z}\oplus\mathbb{Z}i)$、$\mathbb{C}/(\mathbb{Z}\oplus\mathbb{Z}\rho)$以及无穷远点上方的分歧所作的贡献。我们得到

$$\nu_2 = \begin{cases} \frac{\ell-1}{2} & \text{if } \ell \equiv 1 \mod 4 \\ \frac{\ell+1}{2} & \text{if } \ell \equiv 3 \mod 4 \end{cases}, \quad \nu_3 = \begin{cases} 2\frac{\ell-1}{3} & \text{if } \ell \equiv 1 \mod 3 \\ 2\frac{\ell+1}{3} & \text{if } \ell \equiv 2 \mod 3 \end{cases} \quad \text{and} \quad \nu_\infty = \ell - 1.$$

分别处理四种情形 $\ell \equiv 1$，5，7，11 mod 12，经过简单但繁琐的计算即可得到预期结果。

□

5.4. 模方程。— 作为本节的总结，我们给出一个命题（略去证明），它或许能帮助读者确信 $X_0(\ell)$具有代数曲线的结构。证明见 [**Mil17**，定理 6.1] 。

定理 ***78***。—— 存在一个不可约多项式 $\Phi_\ell \in \mathbb{Z}[x,y]$，使得对于任意一对通过次数为 ℓ 的同源 $\mathscr{E} \to \mathscr{E}'$ 相关联的椭圆曲线 $\mathscr{E}$、$\mathscr{E}'$，都有 $\Phi_\ell(j(\mathscr{E})\ j(\mathscr{E}')) = 0$。

注 ***79***。—— 关于较小 ℓ 值的多项式 Φ_ℓ 数据库可在 Andrew Sutherland 的网页上找到：
https://math.mit.edu/∼drew/ClassicalModPolys.html

我们来对这一陈述作几点说明。首先注意，方程为 $\Phi_\ell(x,\ y) = 0$ 的复曲线的射影闭包是 $X_0(\ell)$ 的一个“奇异模型”。事实上，$X_0(\ell)$ 的任意一点都对应于一个 ℓ 次同源的同构类。这给出了一个有理映射

$$\begin{cases} X_0(\ell) & \longrightarrow & \mathbb{P}^2(\mathbb{C}) \\ (\mathscr{E} \to \mathscr{E}') & \longmapsto & (j(\mathscr{E}) : j(\mathscr{E}') : 1). \end{cases}$$

这个映射的像包含于方程为 $\Phi_\ell(x,\ y) = 0$ 的曲线上。然而，这条曲线布满奇点，因此与 $X_0(\ell)$ 不同构。尽管如此（这远非显而易见），我们仍可由此推得 $X_0(\ell)$ 本身定义在 $\mathbb{Q}$ 上，因此其模 p 约化是有意义的。

一个有趣的事实是，由于 $\Phi_\ell \in \mathbb{Z}[x,y]$，对于任意一对在 $\mathbb{F}_p$ 上 ℓ–同源的曲线 $\mathscr{E} \to \mathscr{E}'$，我们有 $\Phi_\ell(j(\mathscr{E})\ j(\mathscr{E}')) \equiv 0$ 模 p。此外，若 ℓ 和 p 互素，则已知多项式 Φ_ℓ 模 p 不可约（例如参见 [**Mor90**，定理 5.9]）。因此，方程为 $\Phi_\ell(x,\ y) = 0$ 的 $\mathbb{F}_p$ 上的曲线，最终成为一条定义在 $\mathbb{F}_p$ 上的光滑曲线的奇异模型，我们也将这条光滑曲线记作 $X_0(\ell)$，使得 $X_0(\ell)(\mathbb{F}_p)$ 可将 ℓ–同源 $\mathscr{E} \to \mathscr{E}'$ 在 $\mathbb{F}_p$ 上按同构分类。这些定义在 $\mathbb{F}_p$ 上的曲线将是证明本课程主要定理——定理 41——时关注的对象。

最后，对模曲线的约化进行严谨研究的读者无法回避概形语言。关于这方面的论述，读者可参阅 Celgene 和 Rapoport[**DR73**] 的文章，或 Katz 和 Mazur [**KM85**]的著作。

6. 主要定理的证明

现在，我们几乎已经具备证明定理 41 所需的材料。我们有曲线族 $X_0(\ell)$，其中 ℓ 是一个不同于特征 p 的素数。

6.1. 有限域上模曲线的亏格。——我们简要讨论一下曲线的亏格。接下来的讨论并非易事。因此，建议读者先直接接受结论：有限域上模曲线的亏格与其复数域对应曲线的亏格相同。下面简要说明这一结论成立的原因。

众所周知（例如见 [**Mor90**，定理 5.9]），曲线 $X_0(\ell)$ 有一个光滑射影模型，其方程的系数属于 $\mathbb{Z}$，且模 p 约化后仍然光滑。

接下来，正如注 29 中提到的，曲线有两种不同的亏格概念：算术亏格 p_a 和几何亏格 g。定义 25（§ 2.7）引入的是几何亏格。算术亏格可以例如通过代数簇 [**Har77**，第 IV 章], 的希尔伯特函数来定义；它总是大于或等于几何亏格，并且当且仅当曲线光滑时二者相等。

接下来，格劳尔特定理 [**Har77**，推论 III.12.9] 使我们可以断言，前述模型 $X_0(\ell)$模 p 的约化与复曲线本身具有相同的算术亏格。此外，由于该模型及其约化都是光滑的，它们也具有相同的几何亏格。因此，$X_0(\ell)$上曲线的亏格与其复数域对应曲线的亏格相同，故由定理 74 给出。

6.2. 超奇异曲线轨迹。— 接下来还需估计这类曲线上有理点的数量。为此，我们将关注 $\mathbb{F}_{p^2}$-点，因为利用以下两个结论可以给出其数量的下界。

命题 ***80***。— 设 $\mathscr{E}$ 是 $\mathbb{F}_p$上的超奇异椭圆曲线，则 $\mathscr{E}$ 定义在 $\overline{\mathbb{F}}_{p^2}$上 .

证明。— 根据定义，超奇异曲线 $\mathscr{E}$ 满足 $\mathscr{E}[p] = \{0\}$。因此，乘以 p的映射 $[p] : E \to E$ 是纯不可分的。

现在考虑弗罗贝尼乌斯映射

$$\phi : \left\{ \begin{array}{ccc} \mathscr{E} & \longrightarrow & \mathscr{E}^{(p)} \\ (x,y) & \longmapsto & (x^p, y^p). \end{array} \right.$$

ˆ ˆ 它是一个次数为 p 的同源，因此存在一个对偶同源 ϕ，使得 $\phi \circ \phi = [p]$。由于 $[p]$ 是全纯不可分的，ˆϕ 也应当是不可分的，因此弗罗贝尼乌斯映射也应当如此

$$\hat{\phi} : \left\{ \begin{array}{ccc} \mathscr{E}^{(p)} & \longrightarrow & \mathscr{E}^{(p^2)} \\ (x,y) & \longmapsto & (x^p, y^p). \end{array} \right.$$

因此，$\mathscr{E}^{(p^2)} = \mathscr{E}$，从而 $\mathscr{E}$ 定义在 $\mathbb{F}_{p^2}$ 上。 □

定理 ***81***. — 在 $\mathbb{F}_p$ 上的超奇异椭圆曲线的 $\mathbb{F}_p$–同构类数等于

$$\left\lfloor \frac{p}{12} \right\rfloor + \left\{ \begin{array}{lllll} 0 & if & p & \equiv & 1 \mod 12 \\ 1 & if & p & \equiv & 5 \mod 12 \\ 1 & if & p & \equiv & 7 \mod 12 \\ 2 & if & p & \equiv & 11 \mod 12. \end{array} \right.$$

证明. — 参见 [Sil09</style}，定理 V.4.1]。 □

6.3. 主定理的证明。 — 有了最后这两个结论，我们终于可以证明定理 41。我们将证明限制在 $p \geqslant 5$ 的情形。注意，当 $p = 2,3$ 时，Tsfasman–Vlăduţ–Zink 定理仍然成立，但其编码理论意义相当有限。

定理 *41* 的证明。— 考虑曲线序列 $X_0(\ell)$，其中 $\ell \equiv 11$ 模 12。根据定理 74，其亏格为 $g_\ell = \frac{\ell+1}{12}$。根据定理 81，曲线 $X_0(1)$ 至少有 $\frac{p-1}{12}$ $\mathbb{F}_{p^2}$ 个有理点，对应于超奇异椭圆曲线的同构类。没有非平凡自同构的此类椭圆曲线，在 $X_0(\ell)$ 中有 $\ell + 1$ 个原像，这些原像也对应于超奇异椭圆曲线，并且

因此是 $\mathbb{F}_{p^2}$个有理点。根据 p 模 12 的同余类， j不变量为 0 和 1728 的曲线可能是超奇异的。更准确地说，根据 [**Sil09**，习题 V.4.4 和 V.4.5]，

- 当 $p \equiv 1$ 模 12 时，两条曲线都是普通曲线（即 非超奇异曲线），因此任何超奇异曲线都没有非平凡自同构，故在 $X_0(\ell)(\mathbb{F}_{p^2})$ 中有 $\ell+1$ 个原像。因此，根据定理 81，

$$\sharp X_0(\ell)(\mathbb{F}_{p^2}) \geqslant (\ell+1)\frac{p-1}{12}.$$

- 当 $p \equiv 5$ 模 12 时，具有 $j = 0$h的曲线是超奇异的，Ш而具有 $j = 1728$ 的曲线是普通的。因此，共有 $\frac{p-5}{12}+1$ 条超奇异曲线，其中除一条外，其余每条都有 $\ell+1$ 个不同的原像。剩下的曲线是具有 $j=0$ 且自同构群阶为 6 的那条曲线。其处理方式与定理 74 的证明非常相似。考虑阶为 6 的自同构在 ℓ–挠点上的作用。由引理 77，这会诱导出 $\mathscr{E}[\ell] \simeq \mathbb{F}_\ell^2$ 的一个阶为 6 的自同构 η。由于 $\ell \equiv 11$ 模 12，因此 $\ell \equiv 2$ 模 3，故 $\mathbb{F}_\ell$ 不包含六次单位根。因此， η 不可对角化，因而不能固定一条直线。由此可证明，任意直线的轨道都是 3 条不同直线的并（$\eta^3 = -\mathrm{Id}$，它固定这些直线）。因此， j–不变量为 0 的曲线有 $\frac{\ell+1}{3}$ 个原像。于是，利用定理 81：

$$\sharp X_0(\ell)(\mathbb{F}_{p^2}) \geqslant (\ell+1)\frac{p-5}{12} + \frac{\ell+1}{3} = (\ell+1)\frac{p-1}{12}.$$

- 当 $p \equiv 7$ 模 12 时，具有 $j=0$ 的曲线是普通的，而具有 $j=1728$ 的曲线是超奇异的。类似的推理可得

$$\sharp X_0(\ell)(\mathbb{F}_{p^2}) \geqslant (\ell+1)\frac{p-7}{12} + \frac{\ell+1}{2} = (\ell+1)\frac{p-1}{12}.$$

- 当 $p \equiv 11$ 模 12 时，两条曲线都是超奇异的，因此得到：

$$\sharp X_0(\ell)(\mathbb{F}_{p^2}) \geqslant (\ell+1)\frac{p-11}{12} + \frac{\ell+1}{2} + \frac{\ell+1}{3} = (\ell+1)\frac{p-1}{12}.$$

总之 地，我们总能得到有理点数量的下界 $(\ell+1)^{\frac{p-1}{12}}$。 n

$$\frac{\sharp X_0(\ell)(\mathbb{F}_{p^2})}{g_\ell} \geqslant \frac{\frac{p-1}{12}(\ell+1)}{\left(\frac{\ell+1}{12}\right)} = p-1.$$

因此，在 $\mathbb{F}_q$ 上，当 $q=p^2$ 时，我们找到了一个曲线族，其 $\mathbb{F}_q$–有理点的数量趋于无穷，而其比值（ $\mathbb{F}_q$–点的数量除以亏格）趋于 $\sqrt{q}-1$。事实证明，这一结果是最优的。

□

参考文献

[BH08] Peter Beelen 和 Tom Høholdt。代数几何码的译码。载于代数几何码进展，第 5 卷编码理论与密码学丛书，第 49–98 页。世界科学出版社，新泽西州哈肯萨克，2008 年。[Cou16] Alain Couvreur。编码理论导论，2016 年。个人讲义。[CR21] Alain Couvreur 和 Hugues Randriambololona。代数几何码及其若干应用。载于 W. Cary Huffman、Jon-Lark Kim 和 Patrick Solé 编，编码理论简明百科全书。Chapman and Hall/CRC，2021 年。[DR73] P. Deligne 和 M. Rapoport。椭圆曲线模空间。载于单变量模函数，*II*（国际暑期学校论文集，安特卫普大学，安特卫普，*1972* 年），《数学讲义》第 349 卷，第 143–316 页。施普林格，柏林，1973 年。[Duu08] Iwan M. Duursma。代数几何码：一般理论。载于代数几何码进展，《编码理论与密码学丛书》第 5 卷，第 1–48 页。世界科学出版社，新泽西州哈肯萨克，2008 年。[Ful89] William Fulton。代数曲线。高级图书经典系列。艾迪生-韦斯利出版公司高级图书出版计划，加利福尼亚州雷德伍德城，1989 年。代数几何导论；与 Richard Weiss 合作撰写的讲义；1969 年原版重印。[Gop81] Valerii D. Goppa。代数曲线上的码。苏联科学院通报，259(6):1289–1290，1981 年。俄文。

[GS95] Arnaldo Garcia 和 Henning Stichtenoth。达到德林费尔德-弗拉杜特界的函数域阿廷-施赖尔扩张塔。《数学发明》，121:211–222，1995年。[Har77] Robin Hartshorne。代数几何，《数学研究生教材》第 52 卷。施普林格出版社，纽约，1977 年。[HP95] Tom Høholdt 和 Ruud Pellikaan。关于代数几何码的译码。IEEE 信息论汇刊，41(6):1589–1614，1995 年 11 月。[HvLP98] Tom Høholdt、Jacobus Hendricus van Lint 和 Ruud Pellikaan。码的代数几何。载于《编码理论手册》第 I、II 卷，第 871–961 页。北荷兰出版社，阿姆斯特丹，1998 年。[Iha81] Y. Ihara。关于有限域上代数曲线有理点数的一些评述。东京大学理学部纪要 IA 数学，28:721–724，1981 年。[KM85] Nicholas M. Katz 和 Barry Mazur。椭圆曲线的算术模空间，《数学年刊研究》第 108 卷。普林斯顿大学出版社，普林斯顿，新泽西州，1985 年。[Lor96] Dino Lorenzini。算术几何入门，《数学研究生进阶丛书》第 9 卷。美国数学学会，普罗维登斯，罗得岛州，1996 年。[LPS88] A. Lubotzky、R. Phillips 和 P. Sarnak。拉马努金图。《组合数学》，8(3):261–277，1988 年。[Mar88] G. A. Margulis。组合方案的显式群论构造及其在扩展图和集中器构造中的应用。《信息传输问题》，24(1):51–60，1988 年。[Mil17] James S. Milne。模函数与模形式（v1.31），2017 年。网址：www.jmilne.org/math/。[Mor90] Carlos J. Moreno。有限域上的代数曲线。《剑桥数学论丛》。剑桥大学出版社，剑桥，1990 年。[Sha94] Igor R. Shafarevich。基础代数几何，第 1 卷。施普林格出版社，柏林，第 2 版，1994 年。[Sil09] Joseph Silverman。椭圆曲线的算术，第 106 卷。施普林格出版社纽约，第 2 版，2009 年。[Ste99] Serguei A. Stepanov。代数曲线上的码。Kluwer Academic/Plenum Publishers，纽约，1999 年。[Sti09] Henning Stichtenoth。代数函数域与码，《数学研究生教材》第 254 卷。施普林格出版社，柏林，第 2 版，2009 年。[TVN07] Michael A. Tsfasman、Serge Vlăduţ 和 Dmitry Nogin。代数几何码：基本概念，第 139 卷，《数学综述与专著》。美国数学学会，普罗维登斯，罗得岛州，2007 年。[TVZ82] Michael A. Tsfasman、Serge G. Vlăduţ 和 Th. Zink。模曲线、志村曲线与 Goppa 码：优于 Varshamov-Gilbert 界。《数学新消息》，109:21–28，1982 年。[VD83] Sergei G. Vlăduţ 和 Vladimir G. Drinfeld。代数曲线的点数。《函数分析及其应用》，17:53–54，1983 年。[VM84] S. G. Vlăduţ 和 Yu. I. Manin。线性码与模曲线。载于《数学当前问题》第 25 卷，《科学技术成果》第 209–257 页。苏联科学院全苏科学技术信息研究所，莫斯科，1984 年。[Wal00] Judy L. Walker。码与曲线，《学生数学图书馆》第 7 卷。美国数学学会，普罗维登斯，罗得岛州；高等研究院（IAS），普林斯顿，新泽西州，2000 年。IAS/Park City 数学专题丛书。

Alain Couvre ur，Inria，法国 • 电子邮件：alain.couvreur@inr ia.fr