椭圆曲线与模形式——代数数论专题 II

May 26, 2022

0、前言

椭圆曲线最早来自于椭圆积分 $\int \frac{dt}{\sqrt{t(t-a)(t-b)}}$ 的求解，其目标是计算椭圆的弧长. 该积分被积函数的分母形如 $y=\sqrt{t(t-a)(t-b)}$，此即一类椭圆曲线的方程. 而在现代数学中，椭圆曲线是最好的数学研究对象之一，几乎所有的数学分支在这里交汇.

椭圆曲线拥有概型结构、群结构；实椭圆曲线拥有流形结构；复椭圆曲线拥有 Riemann 曲面结构；数域或局部域上的椭圆曲线则是重要的算术对象. 本文第 1 节先以复椭圆曲线为例引入一般域上椭圆曲线的概念并介绍其基本性质，而 2，3，4 节则分别聚焦 $\mathbb{C},\mathbb{Q},\mathbb{Q}_p$ 这些常见域上的椭圆曲线. 在第 2 节中，我们会指出复椭圆曲线作为 Riemann 曲面和模形式、数论之间的联系. 至于第 3，4 节的算术部分，本文虽然只以 $\mathbb{Q}$ 和 $\mathbb{Q}_p$ 为例介绍了其上的椭圆曲线，但这些域上的结论对一般整体域或局部域也对，请读者留意. 第 5 节作为尾声介绍了一些重要的算术不变量，并且以 Dirichlet 类数公式为背景介绍了 B-SD 猜想. 这些内容在椭圆曲线的研究中都是十分重要的！

感谢舒杰 (Tongji)、胡勇 (SUSTech)、周潇翔 (Uni-Bonn)、方江学 (CNU) 等人对笔者的支持；感谢赵俊焱 (UIC) 对首师大 2021 年春季学期《黎曼曲面》课程的支持. 本文的错误必定不少，欢迎勘误！

参考文献

[0] http://www.lmfdb.org/.

[1] J.H. Silverman. The Arithmetic of Elliptic Curves(GTM106). Springer.

[2] O. Forster. Lectures on Riemann Surfaces(GTM81). Springer.

[3] M.E. Kazaryan, S.K. Lando, V.V. Prasolov. Algebraic Curves Towards Moduli Spaces. Springer.

[4] 李文威. 模形式初步. 高等教育出版社. https://www.wwli.asia/index.php/zh/books-item-zh.

[5] R. Bellovin. Notes on Galois Cohomology—Modularity Seminar.

[6] 舒杰. Quadratic Twists of Elliptic Curves. 南科大数论与算术几何周末研讨会.

[7] 周潇翔. Mordell 定理笔记. http://home.ustc.edu.cn/~xx352229/.

[8] K. Kato, N. Kurokawa, T. Saito. Number Theory 1: Fermat's Dream. American Mathematical Society.

[9] 朱子阳. Tate 的论文——代数数论专题 III. https://www.cnblogs.com/zhuziyangcnu.

[10] W. Zhang. The Birch-Swinnerton-Dyer Conjecture and Heegner Points: A Survey. Current Developments in Mathematics, 2013(169-203).

[11] Á. L.-Robledo. Elliptic Curves, Modular Forms and Their L-Functions. American Mathematical Society.

[12] G.K. Francis. A Topological Picturebook. Springer-Verlag.

[13] D. Yott. BSD and the Gross-Zagier Formula. Lecture Notes.

[14] M. Eichler, D. Zagier. On the Zeros of the Weierstrass $\wp$-Function. Mathematische Annalen, 1982(399-407).

[15] W. Duke, Ö. Imamoḡlu. The Zeros of the Weierstrass $\wp$-Function and Hypergeometric Series. Mathematische Annalen, 2008(897-905).

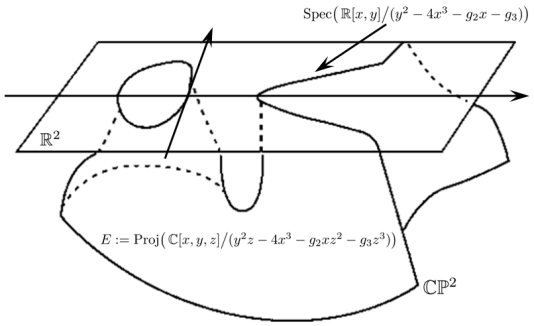
朱子阳[1]，2021 年 5 月于南方科技大学

[1]邮箱 zhuziyang@cnu.edu.cn

1、基本定义：Riemann 曲面 VS 代数曲线

我们先在复几何的背景下考虑例 1.1 中展示的两类基本对象，实际上它们是同一事物的两种不同表现方式. 稍后我们将在一般的域上定义椭圆曲线.

例 1.1(复椭圆曲线) 设 Λ 是 $(\mathbb{C},+)$ 的离散子群，称其为**格点**. 考虑 Riemann 曲面 $E_\Lambda := \mathbb{C}/\Lambda$，根据闭曲面分类定理和单值化定理我们知道这是一个亏格为 1 的紧 Riemann 曲面——**复环面**. 所有的离散子群 Λ 恰对应了环面上所有的复结构，它与命题 2.11(1) 中基本区域内的点一一对应 (从而得到了复环面的分类)，这使得我们可以研究所有复结构上的几何. 基于这种视角我们可以引入**模空间**的概念 (见 [3])，笔者主要关心它蕴含的算术信息.



现考虑另一种针对复环面 E 的分类方式 (旨在导出 E 对应的代数方程). 取 $\mathbb{CP}^2$ 的坐标卡 $U_1 := (1:*:*), U_2 := (*:1:*), U_3 := (*:*:1), U_i \cong \mathbb{C}^2$，指定复环面 E 中的一个点 O(作为加法零元，见定义 1.7). 由 Riemann-Roch 定理，对于除子 $kO \in \mathrm{Div}(E), k \in \mathbb{Z}_{\geq 0}$，若记 $\ell(D) := \dim_{\mathbb{C}}\{f \in \mathcal{M}_E : \forall x \in E, \mathrm{ord}_x(f) \geq -D\}$，则 $\deg(kO) \geq 1$ 蕴含 $\ell(kO) = \deg(kO) = k\Big($设 $g = 1$. 若 $\deg(D) > 0$，则 $\deg(K-D) = 0 - \deg(D) < 0$，这里 K 指典范除子类. 此时 $\ell(K-D) = 0$，故 Riemann-Roch 定理给出 $\ell(D) = \deg(D)\Big)$. 据此我们可以认为存在亚纯函数 $\alpha, \beta \in \mathcal{M}_E$，使得

k	$\ell(kO)$	$\Gamma(E, kO)$的生成元	$\mathrm{ord}_O(\cdot) \geq -k$
0	1	1	常值函数
1	1	1	常值函数
2	2	$1, \alpha$	$\mathrm{ord}_O(\alpha) = -2$
3	3	$1, \alpha, \beta$	$\mathrm{ord}_O(\beta) = -3$
4	4	$1, \alpha, \beta, \alpha^2$	
5	5	$1, \alpha, \beta, \alpha^2, \alpha\beta$	
6	6	$1, \alpha, \beta, \alpha^2, \alpha\beta, \alpha^3, \beta^2$	线性相关

注意到 6 维 $\mathbb{C}$-线性空间 $\Gamma(E, 6O)$ 中我们给出了 7 个生成元，因此它们必然线性相关，这意味着 α, β 满足某个代数方程 $y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$(实际上这就是椭圆曲线的方程)，称之为 **Weierstrass 方程**. 该方程经过非退化换元 $Y := 2y + a_1x + a_3, X := x$ 化简之后得到 $Y^2 = 4X^3 + b_2X^2 + 2b_4X + b_6$，其中 $b_2 = a_1^2 + 4a_2, b_4 = 2a_4 + a_1a_3, b_6 = a_3^2 + 4a_6$. 令 $X := X/Z, Y := Y/Z$，齐次化之后就确定了一条射影代数曲线 $\widetilde{E} \subseteq \mathbb{CP}^2 : Y^2Z - (X - AZ)(X - BZ)(X - CZ) = 0$，这里 A, B, C 两两不同.

现定义**射影嵌入**$\tau : E \hookrightarrow \mathbb{CP}^2, x \mapsto \begin{cases} (\alpha(x):\beta(x):1), & x \neq O \\ (0:1:0), & x = O \end{cases}$，可以验证这是一个良好定义的全纯映射，并且它到 $\mathbb{CP}^2$ 是闭浸入 (即 τ 和切映射 $d\tau_x$ 均是单射)，其像为 $\tau(E) = \widetilde{E}$. 综上，我们有如下一一对应：

$$\text{模空间中的点} \longleftrightarrow \{\text{复环面}\} \underset{\text{单值化定理}}{\overset{\text{Riemann-Roch 定理}}{\rightleftarrows}} \{y^2 = ax^3 + bx^2 + cx + d\text{对应的亏格为 1 的射影代数曲线}\}.$$

所以，我们既称复环面为复椭圆曲线，也称一些形如 $y^2 = ax^3 + bx^2 + cx + d$ 的方程 (的齐次化) 对应的曲

线为复椭圆曲线. 一般地，我们有如下定义：

定义 1.2(椭圆曲线) **椭圆曲线**是一个二元对 (E,O)，其中 E 是亏格为 1 的非奇异曲线 (即不含奇异点. 直观上来讲奇异点指那些没有办法讨论“切线”的点，或那些“不光滑”的点，见例 1.3)，$O\in E$(预定作为加法运算的零元). 此外，设 K 是域，如果 E 作为曲线定义在 K 上 (即 E 对应的方程系数取于 K) 且 $O\in E(K):=\{(x,y,z)\in K^3:x,y,z$满足$E$对应的射影齐次方程$\}$，则称椭圆曲线 (E,O) **定义在 K 上**，记作 E/K. 例 1.1 中给出的复环面就是定义在 $\mathbb{R}$ 的某个子域上的椭圆曲线 $E(\mathbb{C})$.

为了使问题更简单，在 $\mathrm{Char}(K)\neq 2,3$ 的前提下，K 上的代数曲线 $E:y^2=4x^3+b_2x^2+2b_4x+b_6$ 通过换元 $(x,y):=(\frac{x-3b_2}{36},\frac{y}{108})$ 可以杀掉平方项得到 $y^2=x^3-27(b_2^2-24b_4)x-54(-b_2^3+36b_2b_4-216b_6)$，从而 Weierstrass 方程可以进一步化为 $E:y^2=x^3+Ax+B$. 为方便起见，本文更关心这一类曲线.

例 1.3 考虑 $\mathbb{Q}$ 上的代数曲线 $y^2=x^3+Ax+B$，满足 $4A^3+27B^2=0$. 此时方程 $x^3+Ax+B=0$ 有重根 x_0，则 $P=(x_0,0)$ 是方程 $y^2=x^3+Ax+B$ 的重根. 令 $F(x,y)=y^2-x^3-Ax-B$，直接计算得 $\frac{\partial F}{\partial x}|_P=-3x_0^2-A,\frac{\partial F}{\partial y}|_P=0$，故在 P 处 $\frac{dy}{dx}|_P=-(\frac{\partial F}{\partial x}|_P)/(\frac{\partial F}{\partial y}|_P)$ 无定义，从而我们断言 P 是奇异点 (之后我们将从椭圆曲线上的加法运算来重新审视奇异点的病态).

为此我们需要判别式这一概念来判断所谓的重根是否存在，而曲线有无奇异点则和判别式有关.

定义 1.4(Δ，j 与 ω) 定义代数曲线 $E:y^2=4x^3+b_2x^2+2b_4x+b_6$ 的**判别式**为 $\Delta:=-b_2^2(a_1^2a_6+4a_2a_6-a_1a_3a_4+a_2a_3^2-a_4^2)-8b_4^3-27b_6^2+9b_2b_4b_6$(系数 a_i 来自于例 1.1 中的 Weierstrass 方程)，**不变量**为 $j:=\frac{(b_2^2-24b_4)^3}{\Delta}$，**不变微分**为 $\omega:=\frac{dx}{2y+a_1x+a_3}=\frac{dy}{3x^2+2a_2x+a_4-a_1y}$(见命题 1.5). 特别地，可以计算曲线 $y^2=x^3+Ax+B$ 的判别式为 $\Delta=-16(4A^3+27B^2)$，不变量为 $j=-1728\frac{(4A)^3}{\Delta}$.

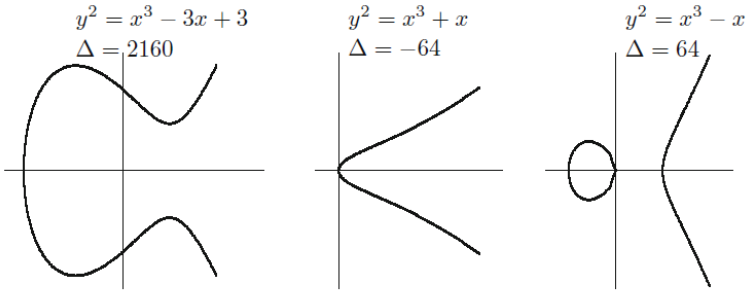
命题 1.5 设 E 是 (定义在任意域上的) 椭圆曲线，则其不变微分 ω 是一个非平凡的全纯微分且无处消没 (注意，我们定义主除子或典范除子时考虑的是非零函数或非零微分！).

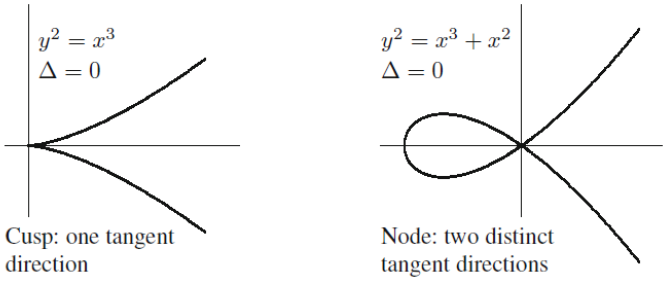
命题 1.6(分类) 对于域 K 上的代数曲线 $E:y^2=4x^3+b_2x^2+2b_4x+b_6$ 而言，

(1)E 非奇异当且仅当 $\Delta\neq 0$. 当 $\Delta=0$ 时，E 只有一个奇异点 (尖点或结点)：该奇异点是尖点 (cusp) 当且仅当 $b_2^2-24b_4=0$；是结点 (node) 当且仅当 $b_2^2-24b_4\neq 0$.

(2) 两条 $\overline{K}$ 上的椭圆曲线同构当且仅当它们的不变量相同.

(3) 任取 $j_0\in\overline{K}$，则必然存在 $K(j_0)$ 上的椭圆曲线使得其不变量就是 j_0.

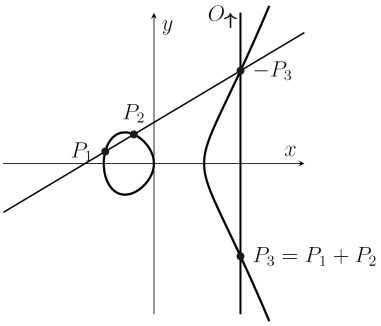




椭圆曲线上还有所谓的“加法运算”.

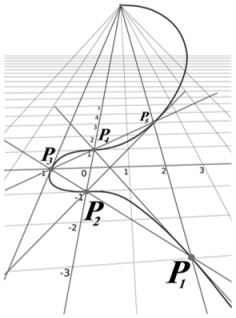
定义 1.7(加法) 设 $E\subseteq\mathbb{P}^2$ 是椭圆曲线，$P_1,P_2\in E$. 设直线 L 穿过 P_1,P_2(若 $P_1=P_2$，则 L 看成 P_1 处

的切线，因此我们需要非奇异的条件) 与 E 相交于 $-P_3$(因为 E 是三次的)，再作穿过 $-P_3$ 与无穷远点 O 的直线 L' 与 E 相交于 P_3. 现定义 $P_1+P_2:=P_3$，称该运算为**加法**，具体的坐标运算可由解析几何给出.



根据代数几何中的 Bézout 定理，利用解析几何的技巧 (Vieta 定理) 我们可以证明：

定理 1.8 椭圆曲线 E 关于该加法作成一个 Abel 群，零元为 O. 若 E 定义在 K 上，则 $E(K)$ 是 E 的子群.



2、复环面及其函数域

本节我们重返复环面的研究. 取定复平面上的格点 $\Lambda:=\mathbb{Z}z_1\oplus\mathbb{Z}z_2(z_1,z_2\in\mathbb{C})$，考虑亚纯函数 $f\in\mathcal{M}_{\mathbb{C}}$. 如果对任意 $\lambda\in\Lambda,z\in\mathbb{C}$，均有 $f(z+\lambda)=f(z)$，则称 f 是以 Λ 为周期的**双周期亚纯函数**或**椭圆函数**，这确定了复环面 $\mathbb{C}/\Lambda$ 上的一个亚纯函数. 而一类最经典的模形式就来自于某个双周期亚纯函数的 Laurent 系数 (见命题 2.2). 由于周期性的存在，我们研究双周期亚纯函数时定义域不必考虑完整的复平面，只需研究某个周期上的行为即可. 我们称由 f 的某个周期作成的区域为**基本区域**，记作 $\mathcal{F}(\mathbb{C}/\Lambda)$.

命题 2.1 设 f 是以 Λ 为周期的双周期亚纯函数，则：

(1) 对紧 Riemann 曲面 $\mathbb{C}/\Lambda$ 用 Liouville 定理可知双周期全纯函数只能是常数；

(2) 由留数定理可知 $\sum_{z\in\mathcal{F}(\mathbb{C}/\Lambda)}\mathrm{Res}_z(f)=0$；

(3) 不难验证 $\frac{f'}{f}$ 也是以 Λ 为周期的双周期亚纯函数，因此由 (2) 知 f 在 $\mathcal{F}(\mathbb{C}/\Lambda)$ 中的零点个数 (计重数) 与极点个数 (计重数) 相等.

最重要的一类双周期亚纯函数为 $\wp$ 函数，它的性质由如下命题给出. 该命题的证明请移步复分析的教材.

命题 2.2(Weierstrass $\wp$ 函数) 设 Λ 是 $\mathbb{C}$ 上的格点，定义级数 $\wp(z):=\frac{1}{z^2}+\sum\limits_{\lambda\in\Lambda\setminus\{0\}}\left(\frac{1}{(z-\lambda)^2}-\frac{1}{\lambda^2}\right)$，则：

(1)$\wp$ 在 $\mathbb{C}$ 的任何紧子集上一致收敛、绝对收敛；

(2)$\wp$ 是以 Λ 为周期的双周期亚纯偶函数 (通常称为 **Weierstrass $\wp$ 函数**)，极点为 Λ 中的点 (阶为 -2)；

(3) 设 $r=\min\{|\lambda|:0\neq\lambda\in\Lambda\}$，则对任意 $0<|z|<r$，有 Laurent 展开

$$\wp(z)=\frac{1}{z^2}+\sum_{n=1}^{\infty}(2n+1)G_{2n+2}(\Lambda)z^{2n},$$

其中 $G_k(\Lambda)=\sum_{\lambda\in\Lambda\setminus\{0\}}\frac{1}{\lambda^k}$，它在 $k\geq 4$ 时绝对收敛；

(4)$\wp$ 满足微分方程 $\big(\wp'(z)\big)^2=4\wp^3(z)-60G_4(\Lambda)\wp(z)-140G_6(\Lambda)$；

(5) 双射 $\mathcal{F}(\mathbb{C}/\Lambda)\setminus\{\wp\text{的极点}\}\xrightarrow{\sim}\big\{(x,y)\in\mathbb{C}^2:y^2=4x^3-60G_4x-140G_6\big\},z\mapsto\big(\wp(z),\wp'(z)\big)$ 使紧 Riemann 曲面 $\mathbb{C}/\Lambda$ 成为 $\mathbb{CP}^2$ 上由方程 $y^2z=4x^3-60G_4xz^2-140G_6z^3$ 确定的复射影代数曲线 (即椭圆曲线)；

(6) 紧 Riemann 曲面 $\mathbb{C}/\Lambda$ 的亚纯函数域 $\mathcal{M}_{\mathbb{C}/\Lambda}=\mathbb{C}(\wp,\wp')$，这是 $\mathbb{C}$ 上超越维数为 1 的超越扩张.

(7) 采用例 1.1 的记号，则 $\alpha=\wp,\beta=\wp'$.

命题 2.2(3) 中出现的级数 $G_k(\Lambda)$ 是一类 Eisenstein 级数，这也是我们将要给出的模形式的具体例子 (见例 2.5).

定义 2.3(模形式) 设 $k\in\mathbb{Z}$，记 $\mathcal{H}:=\{z\in\mathbb{C}:\mathrm{Im}(z)>0\}$ 为上半平面，$f:\mathcal{H}\to\mathbb{C}$ 为全纯函数. 若对任意 $\left(\begin{smallmatrix}a&b\\c&d\end{smallmatrix}\right)\in\Gamma(1):=\mathrm{SL}(2,\mathbb{Z})$，均有 $f\big(\frac{az+b}{cz+d}\big)=(cz+d)^kf(z)$，且 f 在 ∞ 处全纯$\Big(f$ 在 ∞ 处全纯是指透过映射 $q:\mathcal{H}\to\mathcal{D}':=\{z\in\mathbb{C}:0<|z|<1\},z\mapsto e^{2\pi iz}$ 将 $\mathcal{H}$ 覆叠到 $\mathcal{D}'(\infty$ 对应到 0) 之后，函数 $f\circ q^{-1}$(良好定义的前提下) 在 0 处全纯$\Big)$，则称 f 是一个级为 $\Gamma(1)$、权为 k 的**模形式**. 由于本文只讨论级为 $\Gamma(1)$ 的模形式，故我们描述模形式只需要“权”这个指标，以后不再谈及“级”.

特别地，若一个权为 k 的模形式在 ∞ 处消没，则称它是一个权为 k 的**尖点形式**$\Big($在 $\mathcal{D}'$ 中 0 处对应地作函数 $f\circ q^{-1}$ 的 Laurent 展开再通过 q 拉回到 $\mathcal{H}$，我们还可以得到模形式的展开级数 $f(z)=\sum_{n=0}^{\infty}a_ne^{2\pi inz}=\sum_{n=0}^{\infty}a_nq^n$，定义域上均收敛. 此时，判断模形式是否为尖点形式转换为研究展开式中 a_0 是否为 0$\Big)$.

一般地，级为余有限 Fuchs 群的模形式的定义要比定义 2.3 复杂，但本文按下不表. 至于 $\Gamma(1)$ 的情况为何如此简单，问题在于尖点. 之后我们会知道，$\Gamma(1)$ 的尖点只有 ∞ 一个 (见命题 2.10).

注意 2.4 验证模形式的定义时只需遍历 $\Gamma(1)$ 的生成元——$S:=\left(\begin{smallmatrix}0&-1\\1&0\end{smallmatrix}\right)$ 与 $T:=\left(\begin{smallmatrix}1&1\\0&1\end{smallmatrix}\right)$ 即可.

此处我们给出一个具体的偶数权模形式的例子，它的展开式系数含有数论中关心的算术函数 σ_r. 相关论证在解析数论中均是标准的.

例 2.5 选取矩阵 $\left(\begin{smallmatrix}-1&0\\0&-1\end{smallmatrix}\right)$ 代入定义计算可知奇数权模形式只有平凡形式 0，故往后我们只考虑偶数权的模形式. 取定偶数 $k\geq 4$(定理 2.12 告诉我们没有非平凡的权为 2 的模形式)，称级数 $G_k(z):=G_k(\mathbb{Z}z\oplus\mathbb{Z}1)$ 为权为 k 的 **Eisenstein 级数** ($z\in\mathcal{H}$). 此时有展开式 $G_k(z)=2\zeta(k)+2\cdot\frac{(2\pi i)^k}{(k-1)!}\sum_{n=1}^{\infty}\sigma_{k-1}(n)q^n$，其中 $q=e^{2\pi iz}$，$\sigma_r(n):=\sum_{d|n}d^r$. 事实上，根据 Poisson 求和公式 (选取特征标 $\mathbb{R}\to S^1,x\mapsto e^{-2\pi ixn}$) 和留数定理，

$$\sum_{n\in\mathbb{Z}}\frac{1}{(n-z)^k}=\sum_{n\in\mathbb{Z}}\int_{\mathbb{R}}\frac{e^{2\pi ixn}}{(x-z)^k}dx=2\pi i\sum_{n=1}^{\infty}\mathrm{Res}_z\left(\frac{e^{2\pi ixn}}{(x-z)^k}\right)=(2\pi i)^k\sum_{n=1}^{\infty}n^{k-1}\frac{e^{2\pi izn}}{(k-1)!},$$

注意到 $G_k(z)$ 在 $k\geq 4$ 时绝对收敛，据此我们有

$$G_k(z)=\sum_{0\neq n\in\mathbb{Z}}\frac{1}{n^k}+\sum_{(c,d)\in\mathbb{Z}^2\setminus\{0\},c\neq 0}\frac{1}{(cz+d)^k}=2\zeta(k)+\sum_{c=1}^{\infty}\sum_{d=-\infty}^{\infty}\frac{2}{(cz+d)^k}=2\zeta(k)+2\frac{(2\pi i)^k}{(k-1)!}\sum_{c=1}^{\infty}\sum_{n=1}^{\infty}n^{k-1}q^{cn}.$$

直接验证可知 $G_k(z)$ 是权为 k 的模形式，故上述展开式告诉我们 $G_k(z)$ 非尖点形式. 有了 Eisenstein 级数，我们还可以定义**模不变量** (也称**怪兽函数**)

$$j:=1728\frac{\frac{G_4^3}{8\zeta(4)^3}}{\frac{G_4^3}{8\zeta(4)^3}-\frac{G_6^2}{4\zeta(6)^2}}=q^{-1}+744+196884q+21493760q^2+\cdots,$$

这是一个亚纯函数，它确定了所谓的模曲线 (见命题 2.11). 之后我们会知道模形式其实不多，也正是如此在后面讨论维数和基的时候会出现很多有趣的现象.

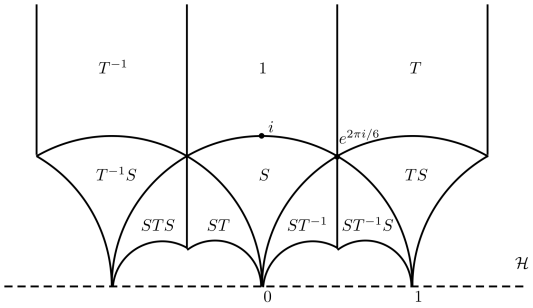
在研究一般的模形式之前，先讨论群 $\Gamma(1)$ 的性质. 首先我们会问：为什么要研究 $\Gamma(1)$？这是因为：

命题 2.6 若记 $\mathcal{H}$ 作为可定向 Riemann 流形的所有保定向等距同构作成的群为 $\mathrm{Iso}^+(\mathcal{H})$；记 $\mathcal{H}$ 作为 Riemann 曲面的全纯自同构群为 $\mathrm{Hol}(\mathcal{H})$，那么 $\mathrm{Iso}^+(\mathcal{H})\cong\mathrm{Hol}(\mathcal{H})\cong\mathrm{PSL}(2,\mathbb{R})$. 模形式正是讨论该群的某个离散子群(例如 $\mathrm{PSL}(2,\mathbb{Z})$)的算术性质.

现考虑群作用 $\mathrm{P}\Gamma(1):=\mathrm{PSL}(2,\mathbb{Z})\rightsquigarrow\mathcal{H},\gamma(z):=\left(\begin{smallmatrix}a&b\\c&d\end{smallmatrix}\right)(z):=\frac{az+b}{cz+d}$(采用射影化是因为不加区分作用效果相同的 $\pm\left(\begin{smallmatrix}1&0\\0&1\end{smallmatrix}\right)$ 之后稳定子群更加简洁)，关于这个作用我们先给出如下概念：

定义 2.7(椭圆点) 对某个点 $z\in\mathcal{H}$，如果 $\mathrm{Stab}_{\mathrm{P}\Gamma(1)}(z)\neq\{\mathrm{id}\}$，则称 z 是 $\Gamma(1)$ 的**椭圆点**. 根据定义立即得到：椭圆点相当于是某个 $\Delta<0$ 的方程 $\gamma(z)=z$ 在 $\mathcal{H}$ 中的根，换言之椭圆点是某个分式线性变换的不动点.

命题 2.8 精确到轨道，由下图 (S 与 T 作用的示意图) 可直接观察出 $\Gamma(1)$ 仅有 2 个椭圆点：i、$e^{2\pi i/6}$. 事实上，$\mathrm{Stab}_{\mathrm{P}\Gamma(1)}(i)=\langle S\rangle\cong\mathbb{Z}/2\,\mathbb{Z}$、$\mathrm{Stab}_{\mathrm{P}\Gamma(1)}(e^{2\pi i/6})=\langle TS\rangle\cong\mathbb{Z}/3\,\mathbb{Z}$.



定义 2.9(尖点) 考虑集合 $\Theta_{\Gamma(1)}:=\left\{t\in\mathbb{R}\sqcup\{\infty\}:\text{存在}\left(\begin{smallmatrix}1&0\\0&1\end{smallmatrix}\right)\neq\gamma\in\mathrm{Stab}_{\mathrm{P}\Gamma(1)}(t)\text{满足}\,\mathrm{Tr}(\gamma)^2=4\det(\gamma)\right\}$，称 $\Theta_{\Gamma(1)}$ 在 $\Gamma(1)$ 按分式线性变换作用下的轨道为 $\Gamma(1)$ 的**尖点**. 直观上来说，精确到轨道，尖点就是某个轨道集在 $\mathbb{R}\sqcup\{\infty\}$ 中的极限点.

命题 2.10 精确到轨道，$\Gamma(1)$ 的尖点只有 ∞ 一个.

证明思路 容易验证 $\Theta_{\Gamma(1)}=\mathbb{Q}\sqcup\{\infty\}$，并且注意到 $\left(\begin{smallmatrix}a&b\\c&d\end{smallmatrix}\right)(\infty)=\frac{a}{c}$ 即可.■

首先应该关心的是群作用 $\mathrm{P}\Gamma(1)\rightsquigarrow\mathcal{H}$ 的几何属性. 我们自然希望该作用与定义 2.3 中的要求兼容，而这导致我们可以讨论基本区域. 此外，从基本区域出发可以构造一个紧 Riemann 曲面——模曲线. 由于在尖点处双曲度量失效，故从复结构着手可以给出一些有价值的信息. 我们以一个命题总结这些事实：

命题 2.11 设 f 是一个权为 k 的模形式，则：

(1) 群作用 $\mathrm{P}\Gamma(1)\rightsquigarrow\mathcal{H}$ 诱导 f 的一个基本区域 $\mathcal{F}(\mathcal{H}/\mathrm{P}\Gamma(1))$，其闭包为 $\overline{\mathcal{F}(\mathcal{H}/\mathrm{P}\Gamma(1))}=\left\{z\in\mathcal{H}:-\frac{1}{2}\leq\mathrm{Re}(z)\leq\frac{1}{2},|z|\geq1\right\}$，详见上图.

(2) 记复平面上所有格点作成的集合为 $\mathcal{L}_{\mathbb{C}}$，定义等价关系 (称为**相似**)：$\mathbb{Z}z_1\oplus\mathbb{Z}z_2\sim\mathbb{Z}w_1\oplus\mathbb{Z}w_2\Leftrightarrow\exists\lambda\in\mathbb{C}^\times$，使得 $\mathbb{Z}z_1\oplus\mathbb{Z}z_2=\mathbb{Z}\lambda w_1\oplus\mathbb{Z}\lambda w_2$. 此时有双射 $(\mathcal{L}_{\mathbb{C}}/\sim)\xleftrightarrow{\sim}\mathcal{F}(\mathcal{H}/\mathrm{P}\Gamma(1))$.

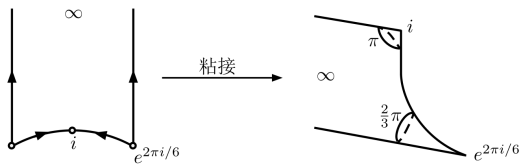
(3) 注意到完备 Riemann 流形 $\mathcal{H}$ 上的测地线直观上皆是与实轴正交的圆弧 (圆的半径可以为无穷大)，且任两点 $z_1,z_2\in\mathcal{H}$ 都可用唯一的测地线段连接，记为 $[z_1,z_2]$，其在双曲度量下的距离为 $d(z_1,z_2)=\cosh^{-1}\left(1+\frac{|z_1-z_2|^2}{2\,\mathrm{Im}(z_1)\,\mathrm{Im}(z_2)}\right)$. 因此，$\overline{\mathcal{F}(\mathcal{H}/\mathrm{P}\Gamma(1))}$ 的边界由测地线围成.

(4) 由 Gauss-Bonnet-Chern 定理可知在双曲度量下，$\mathrm{Vol}\big(\mathcal{F}(\mathcal{H}/\mathrm{P}\Gamma(1))\big)=\frac{\pi}{3}$.

(5) 此处我们由 $\overline{\mathcal{F}(\mathcal{H}/\mathrm{P}\Gamma(1))}$ 构造一个紧 Riemann 曲面. 首先，考虑商拓扑空间

$$\mathbb{S}:=\overline{\mathcal{F}(\mathcal{H}/\mathrm{P}\Gamma(1))}\Big/\big(z_1\sim z_2\Leftrightarrow\exists\gamma\in\mathrm{P}\Gamma(1),\gamma z_1=z_2\big),$$

定义每个点 $z\in\mathbb{S}$ 附近的复结构为 $w\mapsto w^{|\mathrm{Stab}_{\mathrm{P}\Gamma(1)}(z)|}$(请读者留意椭圆点处的行为). 这时我们得到一个非紧的 Riemann 曲面，对其紧化无非是添入尖点 ∞，此时得到紧 Riemann 曲面 $\overline{\mathbb{S}}$. 根据闭曲面分类定理和单值化定理，不难发现这个紧 Riemann 曲面 $\overline{\mathbb{S}}$ 就是 $\mathbb{CP}^1$，同构由模不变量 j 给出. 我们称 $\overline{\mathbb{S}}$ 为 $\Gamma(1)$ 对应的**模曲线**，记作 $X(1)$.



接下来的定理告诉我们模形式可构成线性空间，因而自然还要关心其上的线性代数问题.

定理 2.12 所有权为 k 的模形式模形式作成一个 $\mathbb{C}$-线性空间，记作 $M_k(1)$；而所有权为 k 的尖点形式作成它的一个 $\mathbb{C}$-线性子空间，记作 $S_k(1)$. 此时有：

(1)$\bigoplus_{k=0}^{\infty} M_k(1) \cong \mathbb{C}[G_4, G_6]$ 是一个分次 $\mathbb{C}$-代数.

(2) 若记 $\Delta := (60G_4)^3 - 27\cdot(140G_6)^2$，则 $\Delta \in S_{12}(1)$. 该尖点形式给出 $\mathbb{C}$-线性空间的同构 $M_{k-12}(1) \xrightarrow{\sim} S_k(1), f \mapsto f\cdot\Delta$.

(3)$M_k(1) = \mathrm{span}_{\mathbb{C}}\{G_4^m G_6^n\}, 4m+6n=k, m,n\in\mathbb{Z}_{\geq 0}$；$\dim_{\mathbb{C}} M_k(1) = \begin{cases} 0, & k<0\text{或}k\text{是奇数} \\ [\frac{k}{12}], & k\equiv 2(\mathrm{mod}\ 12), k\geq 0 \\ [\frac{k}{12}]+1, & k\not\equiv 2(\mathrm{mod}\ 12), k\geq 0 \end{cases}$. 因此由 (2) 便可计算 $S_k(1)$ 的维数.

(4) 设 $0\neq f\in M_k(1)$，则 $\underbrace{\sum_{z\in\mathcal{H}/\mathrm{P}\Gamma(1)} \frac{\mathrm{ord}_z(f)}{|\mathrm{Stab}_{\mathrm{P}\Gamma(1)}(z)|}}_{\text{分母在椭圆点处非平凡，见定义 2.7}} + \underbrace{\mathrm{ord}_\infty(f)}_{\text{由尖点贡献，见定义 2.9}} = \frac{k}{12}.$

该定理的证明请参考 [4]Chapter4，主要的工具是 Riemann-Roch 定理. 上述 (4) 中出现的系数 $\frac{1}{12}$ 来源于 $\frac{1}{2}\cdot\frac{\mathrm{Vol}\left(\mathcal{F}(\mathcal{H}/\mathrm{P}\Gamma(1))\right)}{2\pi}$，或来源于一个特殊除子类，见 [4] 定理 4.1.3.

例 2.13 $\frac{G_4}{2\zeta(4)} = 1+240\sum_{n=1}^{\infty}\sigma_3(n)q^n \in M_4(1)$，$(\frac{G_4}{2\zeta(4)})^2 = \frac{G_8}{2\zeta(8)} = 1+480\sum_{n=1}^{\infty}\sigma_7(n)q^n \in M_8(1)$. 对比维数与系数可得 $\frac{\sigma_7(n)-\sigma_3(n)}{120} = \sum_{m=1}^{n-1}\sigma_3(m)\sigma_3(n-m)$.

注意 2.14(自守形式) 设 $\Gamma(1)$ 在 $\mathrm{GL}(2,\widehat{\mathbb{Z}})$ 中的拓扑闭包为 $K(1)$，则会有 Hilbert 空间的酉同构

$$L^2(A)^{K(1)} := L^2\Big(\big(\mathrm{GL}(2,\mathbb{Q})\cdot\big\{\left(\begin{smallmatrix} r & 0 \\ 0 & r \end{smallmatrix}\right) : r\in\mathbb{R}^\times\big\}\big)\Big\backslash \mathrm{GL}(2,\mathbb{A}_{\mathbb{Q}})\Big)^{K(1)} \cong L^2\big(\Gamma(1)\backslash\mathrm{GL}(2,\mathbb{R})^1\big),$$

其中 $\widehat{\mathbb{Z}} = \prod_{p<\infty}\mathbb{Z}_p, \mathrm{GL}(2,\mathbb{R})^1 := \{x\in\mathrm{GL}(2,\mathbb{R}) : |\det(x)| = 1\}, \mathbb{A}_{\mathbb{Q}}$ 是 $\mathbb{Q}$ 的 Adele 环. 事实上如果我们把模形式看成 Hilbert 空间 $L^2(\Gamma(1)\backslash\mathcal{H})$ 中的元素，并且注意到群作用诱导微分同胚 $\mathcal{H}\xrightarrow{\sim}\mathrm{GL}(2,\mathbb{R})^1/\mathrm{O}(2)$，则有嵌入

$$L^2(\Gamma(1)\backslash\mathcal{H}) \xrightarrow{\sim} L^2(\Gamma(1)\backslash\mathrm{GL}(2,\mathbb{R})^1/\mathrm{O}(2)) \xrightarrow{\sim} L^2(\Gamma(1)\backslash\mathrm{GL}(2,\mathbb{R})^1)^{\mathrm{O}(2)} \hookrightarrow L^2(A).$$

一般称右边 Hilbert 空间 $L^2(A)$ 中的元素为**自守形式**，它是模形式的推广. 自守形式以及自守表示是抽象调和分析中重要的研究对象.

3、$\mathbb{Q}$ 上的椭圆曲线

$\mathbb{Q}$ 是最简单的整体域，算术几何关心的最古典的研究对象之一就是其上的椭圆曲线. 本节主要介绍 $\mathbb{Q}$ 上椭圆曲线的有理点及其相关性质，并借此介绍算术几何中最重要也是最基本的 Mordell-Weil 定理——它描述了由有理点构成的 Abel 群的结构 (请读者将该结论与数论中的 Dirichlet 单位定理类比观察)：

定理 3.1(Mordell-Weil) 设 $E/\mathbb{Q}$ 是椭圆曲线，则 $E(\mathbb{Q})$ 是有限生成 Abel 群，即 $E(\mathbb{Q})\cong\mathbb{Z}^r\oplus E(\mathbb{Q})_{\mathrm{tor}}$，其中 $r<\infty$ 称为 **Mordell 秩**，$E(\mathbb{Q})_{\mathrm{tor}}$ 是挠部分作成的有限群.

证明思路 首先我们陈述**弱 Mordell-Weil 定理**：设 $E/\mathbb{Q}$ 是椭圆曲线，则对任何 $m\in\mathbb{Z}_{\geq 2}$，$E(\mathbb{Q})/mE(\mathbb{Q})$ 均是有限群. 在证明了弱 Mordell-Weil 定理之后，用类似无穷递降法的操作即可.

Step1(递降的对象)：设 $P := (x_P, y_P)\in E(\mathbb{Q})$，其中 $x_P = \frac{m}{n}, m,n\in\mathbb{Z}, (m,n)=1$. 定义 P 的**高** (height) 为 $H(P) := \begin{cases} \max\{|m|,|n|\}, & P\neq O \\ 1, & P=O \end{cases}$. 关于高这个概念，直接解析几何可以给出它的如下性质：

(1. 有限性) 对任意 $M>0$，$\{P\in E(\mathbb{Q}) : H(P)<M\}$ 均是有限集.

(2. 加法不等式) 设 $Q\in E(\mathbb{Q})$，则存在依赖于 Q 的正实数 C_1 使得 $H(P+Q)\leq C_1 H(P)^2$ 对任意 $P\in E(\mathbb{Q})$

均成立.

(3. 乘法不等式) 存在正实数 C_2 使得 $H(P)^4 \le C_2 H(2P)$ 对任意 $P \in E(\mathbb{Q})$ 均成立.

Step2(无穷递降法)：若弱 Mordell-Weil 定理成立，则当 $m=2$ 时 $E(\mathbb{Q})/2E(\mathbb{Q})$ 是有限群. 设 $E(\mathbb{Q})/2E(\mathbb{Q})$ 中的代表元为 $S_1,\cdots,S_k$，则任意 $P\in E(\mathbb{Q})$，总存在 $P'\in E(\mathbb{Q}), 1\le j\le k$ 使得 $P-2P'=S_j$. 由 Step1.2 知存在依赖于 i 的常数 $C_1(S_i)$ 使得 $H(P-S_i)<C_1(S_i)H(P)^2$，若取 $N:=\max_{1\le i\le k}\{C_1(S_i)\}$，则由 Step1.3 知存在常数 C_2 使得 $H(P')^4<C_2H(2P')=C_2H(P-S_j)<NC_2H(P)^2$. 记 $C:=NC_2$，则 $H(P')<C^{1/4}\sqrt{H(P)}$，因此当 $H(P)\ge\sqrt{C}$ 时有 $H(P')<H(P)$. 也就是说任给这样的 P，总能找到 P' 使得 $P=2P'+S_j$ 且 $H(P)>H(P')$. 由 Step1.3 可设 $\{T\in E(\mathbb{Q}):H(T)<\sqrt{C}\}=\{T_1,\cdots,T_l\}$，则任给 $P\in E(\mathbb{Q})$，上述操作总能进行有限步 (包括零步) 得到 $P=2^nT_r+\sum_{i=1}^k a_iS_i$. 此时 $E(\mathbb{Q})=\langle S_1,\cdots,S_k,T_1,\cdots,T_l\rangle$，即 $E(\mathbb{Q})$ 是有限生成 Abel 群.

接下来着手处理弱 Mordell-Weil 定理. 大致思路是：先对形如 $y^2=(x-a)(x-b)(x-c)$ 的椭圆曲线证明弱 Mordell-Weil 定理，然后将一般的椭圆曲线 $y^2=ax^3+bx^2+cx+d$ 转化成这种形式. 转化的困难在于方程 $ax^3+bx^2+cx+d=0$ 的根可能跳出 $\mathbb{Q}$. 为了处理这种情况，我们需要 Step4 保证添根的合理性，在更大的域中考虑弱 Mordell-Weil 定理. 首先需要一些预备工作：

Step3(Galois 上同调，拓扑修正版群上同调)：设 $K/\mathbb{Q}$ 是 Galois 扩张 (扩张次数可无限)，其 Galois 群 $\mathbb{G}:=\mathrm{Gal}(K/\mathbb{Q})$ 配备 Profinite 拓扑. 设 M 是一个配备离散拓扑的 Abel 群，约定有一个连续作用 $\mathbb{G}\rightsquigarrow M$ 使 M 成为一个 $\mathbb{G}$-模(一个判定准则是：$\forall m\in M,[\mathbb{G}:\mathrm{Stab}_{\mathbb{G}}(m)]<\infty$). 现定义链复形：

$$C_c^k(\mathbb{G},M):=\begin{cases}0, & k<0\\ M, & k=0\\ \{\varphi:\mathbb{G}^k\to M\text{连续}\}, & k\ge 1\end{cases};$$

$$d^k:C_c^k(\mathbb{G},M)\to C_c^{k+1}(\mathbb{G},M),\varphi\mapsto\left(d^k\varphi:(\sigma_1,\cdots,\sigma_{k+1})\mapsto\begin{bmatrix}\sigma_1\varphi(\sigma_2,\cdots,\sigma_{k+1})\\ +\sum_{i=1}^k(-1)^i\varphi(\sigma_1,\cdots,\sigma_i\sigma_{i+1},\cdots,\sigma_{k+1})\\ +(-1)^{k+1}\varphi(\sigma_1,\cdots,\sigma_k)\end{bmatrix}\right).$$

读者自行验证 $d\circ d=0$. 记该链复形的第 k 个上同调群为 $H_c^k(\mathbb{G},M):=\ker(d^k)/\mathrm{Im}(d^{k-1})$，称其为 **Galois 上同调** (这里用拓扑修正了经典的群上同调，所以在此我们以下标“c”强调. 以后在不引起混淆的前提下可略去下标. 当然，当 $\mathbb{G}$ 有限时 Galois 上同调退化成群上同调). 注意，$H^k(\mathbb{G},\cdot)$ 是 $\mathsf{Mod}(\mathbb{G})\to\mathsf{AbGroups}$ 的函子. 特别地，当指标较低时可直接计算：

$$\begin{aligned}&(d^0m)(\sigma)=\sigma m-m;\quad (d^1\varphi)(\sigma_1,\sigma_2)=\sigma_1\varphi(\sigma_2)-\varphi(\sigma_1\sigma_2)+\varphi(\sigma_1).\\ &H^0(\mathbb{G},M)=\{m\in M:\forall\sigma\in\mathbb{G},\sigma m=m\}:=M^{\mathbb{G}}.\\ &H^1(\mathbb{G},M)=\frac{\{\varphi\in C^1(\mathbb{G},M):\varphi(\sigma_1\sigma_2)=\sigma_1\varphi(\sigma_2)+\varphi(\sigma_1)\}}{\{\varphi\in C^1(\mathbb{G},M):\exists m\in M,\forall\sigma\in\mathbb{G},\varphi(\sigma)=\sigma m-m\}}.\end{aligned}$$

当然我们会有**长正合列定理**：$(\cdot)^{\mathbb{G}}:\mathsf{Mod}(\mathbb{G})\to\mathsf{AbGroups}$ 是左正合共变函子，且对于 $\mathbb{G}$-模正合列 $0\longrightarrow M\longrightarrow N\longrightarrow P\longrightarrow 0$，均有长正合列 $0\longrightarrow M^{\mathbb{G}}\longrightarrow N^{\mathbb{G}}\longrightarrow P^{\mathbb{G}}\longrightarrow H^1(\mathbb{G},M)\longrightarrow H^1(\mathbb{G},N)\longrightarrow H^1(\mathbb{G},P)\longrightarrow\cdots$. 可以证明，当 $\mathbb{G}$ 有限时有范畴等价 $\mathsf{Mod}(\mathbb{G})\leftrightarrow\mathsf{Mod}(\mathbb{Z}[\mathbb{G}])$，故我们可以把函子 $(\cdot)^{\mathbb{G}}$ 等效地看成 $\mathrm{Hom}_{\mathbb{Z}[\mathbb{G}]}(\mathbb{Z},\cdot):\mathsf{Mod}(\mathbb{Z}[\mathbb{G}])\to\mathsf{AbGroups}$，因此用**导出函子**的观点来看会有群同构 $H^k(\mathbb{G},M)\cong\mathrm{Ext}^k_{\mathbb{Z}[\mathbb{G}]}(\mathbb{Z},M)$. 而当 $\mathbb{G}=\varprojlim\mathbb{G}_i$ 无限时，[5] 定理 2.1 断言：如果离散 $\mathbb{G}_i$-模 M_i 作成正向系统，那么 $H_c^k(\varprojlim\mathbb{G}_i,\varinjlim M_i)\cong\varinjlim H^k(\mathbb{G}_i,M_i)$.

现规定 $\mathbb{G}:=\mathrm{Gal}(K/\mathbb{Q})$ 在 $\mathbb{Q}$ 上椭圆曲线的 K-点群 $E(K)$ 上的连续作用为 $\mathbb{G}\ni\sigma:K^2\to K^2,(x,y)\mapsto(\sigma x,\sigma y)$. 我们的目标是套用 Step3.

Step4(添根的合理性)：设 $K/\mathbb{Q}$ 是有限 Galois 扩张，则 $E(K)/mE(K)$ 有限蕴含 $E(\mathbb{Q})/mE(\mathbb{Q})$ 有限. **证：**注意到有正合列 $0\longrightarrow\ker(\theta)\cong\frac{E(\mathbb{Q})\cap mE(K)}{mE(\mathbb{Q})}\longrightarrow E(\mathbb{Q})/mE(\mathbb{Q})\xrightarrow{\theta}E(K)/mE(K)$，故只需证 $\ker(\theta)$ 有限即可. 将左正合函子 $(\cdot)^{\mathbb{G}}$ 作用于正合序列 $0\longrightarrow E(K)[m]\longrightarrow E(K)\xrightarrow{m(\cdot)}mE(K)\longrightarrow 0$ 得长正合列 $0\longrightarrow E(\mathbb{Q})[m]\longrightarrow E(\mathbb{Q})\xrightarrow{m(\cdot)}E(\mathbb{Q})\cap mE(K)\longrightarrow H^1(\mathbb{G},E(K)[m])$，其中记号 $G[m]:=\{x\in G:$

$mx=0\}$(注意，一般我们使用的是 $E[m]$ 而非 $E(K)[m]$！此处我们只是假设 $E[m]\subseteq E(K)$). 此时有单射 $\ker(\theta)\cong\frac{E(\mathbb{Q})\cap mE(K)}{\mathrm{Im}(m(\cdot))}\hookrightarrow H^1(\mathbb{G},E(K)[m])$，而由条件知 $\mathbb{G}$ 和 $E(K)[m]\cong E(K)/mE(K)$ 均是有限群，进而 $H^1(\mathbb{G},E(K)[m])$ 是有限群，故命题得证.

有了 Step4，问题划归为对定义在 $K\supseteq\mathbb{Q}$ 上形如 $y^2=(x-a)(x-b)(x-c)(a,b,c$ 两两不同) 的椭圆曲线证明弱 Mordell-Weil 定理. 我们仍以 $K=\mathbb{Q}$ 为例，椭圆曲线形如 $y^2=(x-a)(x-b)(x-c)$，仅对 $m=2$ 给出该定理的证明 ($m>2$ 时或类群 $\mathrm{Cl}(K)$ 非平凡时处理比较麻烦，本文不再赘述).

Step5(弱 Mordell-Weil 定理，$m=2$)：设 $a,b,c\in\mathbb{Q}$ 两两不同，考虑椭圆曲线 $y^2=(x-a)(x-b)(x-c)$，定义映射 $\partial:E(\mathbb{Q})\to(\mathbb{Q}^\times/(\mathbb{Q}^\times)^2)^3$ 如下：

$$\partial:E(\mathbb{Q})\ni P=(x_P,y_P)\mapsto\begin{cases}(\overline{x_P-a},\overline{x_P-b},\overline{x_P-c}), & P\neq O,(a,0),(b,0),(c,0)\\ \big(\overline{(a-b)(a-c)},\overline{a-b},\overline{a-c}\big), & P=(a,0)\\ \big(\overline{b-a},\overline{(b-a)(b-c)},\overline{b-c}\big), & P=(b,0)\\ \big(\overline{c-a},\overline{c-b},\overline{(c-a)(c-b)}\big), & P=(c,0)\\ (1,1,1), & P=O\end{cases}$$

这里 $\overline{(\cdot)}$ 指 mod $(\mathbb{Q}^\times)^2$. 此时可以验证 ∂ 是群同态且 $\ker(\partial)=2E(\mathbb{Q})$，并且 $\mathrm{Im}(\partial)\subseteq H\times H\times H$，这里 H 为 $a-b,b-c,c-a$ 的分母或分子的素因子以及 -1 生成的 $\mathbb{Q}^\times/(\mathbb{Q}^\times)^2$ 的有限子群 (详细验证见 [8] 命题 1.14，需要用到一些赋值论). 据此可直接导出 $m=2$ 时的弱 Mordell-Weil 定理.■

注意 3.2 Tate 猜测定义在 $\mathbb{Q}$ 上的椭圆曲线的 Mordell 秩是无界的，但是大多数椭圆曲线的 Mordell 秩都很小，直到 2006 年 Elkies 才发现了 Mordell 秩 ≥ 28 的椭圆曲线. 关于此有民间传闻：50% 的椭圆曲线 Mordell 秩为 0；50% 的椭圆曲线 Mordell 秩为 1；0% 的椭圆曲线 Mordell 秩 ≥ 2.

而关于挠部分，则有如下两个结论：

定理 3.3(Mazur) 设 $E/\mathbb{Q}$ 是椭圆曲线，则 $E(\mathbb{Q})_{\mathrm{tor}}$ 必为如下 15 个群之一：

$$\mathbb{Z}/N\mathbb{Z}\ (1\leq N\leq 10\text{或}N=12);\quad \mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/2N\mathbb{Z}\ (1\leq N\leq 4).$$

定理 3.4(Nagell-Lutz) 设 $E/\mathbb{Q}$ 是椭圆曲线，则 $E(\mathbb{Q})$ 中有限阶的点都是整点 (横、纵坐标皆是整数).

4、$\mathbb{Q}_p$ 上的椭圆曲线

在本节中，约定 p 是素数，$\mathbb{Q}_p$ 是 p-进数域，v 是标准离散赋值 (即 $v(p)=1$，这里 p 是单值化子). 现考虑定义在 $\mathbb{Q}_p$ 上的椭圆曲线 $E/\mathbb{Q}_p$.

定义 4.1(极小 Weierstrass 方程) 设 $E/\mathbb{Q}_p$ 是椭圆曲线，设它的一个 Weierstrass 方程为 $y^2+a_1xy+a_3y=x^3+a_2x^2+a_4x+a_6,a_i\in\mathbb{Q}_p$. 通过换元 $(x,y):=(u^{-2}x,u^{-3}y)$(取 $u=p^N$，N 充分大) 可以使该方程的系数落在整数环 $\mathbb{Z}_p$ 中，此时判别式满足 $v(\Delta)\geq 0$. 故对 E 的所有系数取于 $\mathbb{Z}_p$ 的 Weierstrass 方程而言，$v(\Delta)$ 必有极小值. 称 $v(\Delta)$ 取极小值时对应的 Weierstrass 方程为**极小 Weierstrass 方程**.

命题 4.2 (1. 存在性) 任何定义在 $\mathbb{Q}_p$ 上的椭圆曲线 $E/\mathbb{Q}_p$ 均有极小 Weierstrass 方程.

(2. 极小方程的唯一性) 极小 Weierstrass 方程在相差一个坐标变换 $x:=u^2x'+r,y:=u^3y'+u^2sx'+t(u\in\mathbb{Z}_p^\times,r,s,t\in\mathbb{Z}_p)$ 的意义下是唯一的.

(3. 不变微分的唯一性) 极小 Weierstrass 方程对应的不变微分 $\omega:=\frac{dx}{2y+a_1x+a_3}$ 在相差乘以 $\mathbb{Z}_p^\times$ 中某个元素的意义下是唯一的.

(4. 一些判定) 当 Weierstrass 方程的系数取于 $\mathbb{Z}_p$，且满足 $v(\Delta)<12$ 或 $v((a_1^2+4a_4)^2-24(2a_4+a_1a_3))<4$ 或 $v(-(a_1^2+4a_4)^3+36(a_1^2+4a_4)(2a_4+a_1a_3)-216(a_3^2+4a_6))<6$ 三个条件之一，则该 Weierstrass 方程是极小的.

对于 $\mathbb{Q}_p$ 上的椭圆曲线，我们自然希望将其约化到剩余域 $\mathbb{F}_p$ 上考虑. 为此我们给出如下定义：

定义 4.3(约化) 取定椭圆曲线 $E/\mathbb{Q}_p$ 的一个极小 Weierstrass 方程，对其系数 mod p 之后我们得到一条定义在 $\mathbb{F}_p$ 上的曲线 (可能有奇异点)，记作 $\widetilde{E}: y^2+\widetilde{a_1}xy+\widetilde{a_3}y = x^3+\widetilde{a_2}x^2+\widetilde{a_4}x+\widetilde{a_6}, \widetilde{a_i} \in \mathbb{F}_p$. 我们称曲线 $\widetilde{E}/\mathbb{F}_p$ 为 E 模 p 的**约化** (reduction). 定义**约化映射**$p: E(\mathbb{Q}_p) \to \widetilde{E}(\mathbb{F}_p), (x_0 : y_0 : z_0) \mapsto (x_0 \bmod p : y_0 \bmod p : z_0 \bmod p)$，其中 $(x_0 : y_0 : z_0)$ 满足 $x_0, y_0, z_0 \in \mathbb{Z}_p$ 且至少有一个落入 $\mathbb{Z}_p^\times$.

应该强调，约化后的曲线 $\widetilde{E}$ 可能会有奇异点. 但根据代数曲线的常识 (见 [1] 命题 3.2.5)，所有非奇异点 $\widetilde{E}_{\mathrm{ns}}(\mathbb{F}_p) \subseteq \widetilde{E}(\mathbb{F}_p)$ 关于定义 1.7 中的加法作成一个 Abel 群，故我们需要定义 $E(\mathbb{Q}_p)$ 的两个重要子群，即**非奇异约化群**$E_0(\mathbb{Q}_p)$ 和**约化核**$E_1(\mathbb{Q}_p)$：

$$E_0(\mathbb{Q}_p) := \{P \in E(\mathbb{Q}_p) : p(P) \in \widetilde{E}_{\mathrm{ns}}(\mathbb{F}_p)\}; \quad E_1(\mathbb{Q}_p) := \{P \in E(\mathbb{Q}_p) : p(P) = p(O)\}.$$

命题 4.4 有正合列 $0 \longrightarrow E_1(\mathbb{Q}_p) \longrightarrow E_0(\mathbb{Q}_p) \xrightarrow{p} \widetilde{E}_{\mathrm{ns}}(\mathbb{F}_p) \longrightarrow 0$(该命题的证明并不容易). 利用**形式群** (formal group) 的理论可以得到当 $p \geq 3$ 时，$E_1(\mathbb{Q}_p) \cong p\,\mathbb{Z}_p$.

定义 4.5(约化的分类) 考虑约化映射 $p: E(\mathbb{Q}_p) \to \widetilde{E}(\mathbb{F}_p)$，如果：

(1)$\widetilde{E}$ 是一条椭圆曲线 (非奇异)，则称 p 是**好约化**.

(2) 如果 $\widetilde{E}$ 有奇异点，则称 p 是**坏约化**. 更细致一点，如果 $\widetilde{E}$ 有尖点，则称 p 是**加性约化**；如果 $\widetilde{E}$ 有结点，则称 p 是**乘性约化**. 关于乘性约化，如果在该结点处有有理切线，则称 p 是**可裂乘性约化**；否则称 p 为**非可裂乘性约化**.

例 4.6 设素数 $p \geq 5$，则：

$E/\mathbb{Q}_p$	$\widetilde{E}/\mathbb{F}_p$	约化分类
$y^2 = x^3 + px^2 + 1$	$y^2 = x^3 + 1$	好约化
$y^2 = x^3 + x^2 + p$	$y^2 = x^3 + x^2$	(可裂) 乘性约化
$y^2 = x^3 + p$	$y^2 = x^3$	加性约化

命题 4.4 中的正合列某种意义上确定了 $E_0(\mathbb{Q}_p)$. 倘若能得到一些关于商群 $E(\mathbb{Q}_p)/E_0(\mathbb{Q}_p)$ 的信息，便能在某种程度上提炼出 $E(\mathbb{Q}_p)$ 的结构. 为此，我们希望弄清楚 $E(\mathbb{Q}_p)/E_0(\mathbb{Q}_p)$ 的群结构，而这并不容易. 现已有如下结果：

定理 4.7(Kodaira-Néron) 设 $E/\mathbb{Q}_p$ 是椭圆曲线，如果 E 有可裂乘性约化，则 $E(\mathbb{Q}_p)/E_0(\mathbb{Q}_p)$ 是阶为 $v(\Delta)$ 的循环群；在其余的情况下，$|E(\mathbb{Q}_p)/E_0(\mathbb{Q}_p)| \leq 4$. 特别地，如果 E 有好约化，则 $|E(\mathbb{Q}_p)/E_0(\mathbb{Q}_p)| = 1$(这不是充要条件！). 也就是说 $E(\mathbb{Q}_p)/E_0(\mathbb{Q}_p)$ 总是有限群.

5、类数公式与 B-SD 猜想

本节介绍一些算术不变量以及 Birch, Swinnerton-Dyer 猜想 (即 B-SD 猜想)，它猜测由椭圆曲线诱导的 L-函数在某个极点处的留数正由这些算术不变量唯一决定. 之后，我们将类比类数公式解释 B-SD 猜想的合理性.

首先定义椭圆曲线背景下的 L-函数：

定义 5.1(Hasse-Weil L-函数) 设 $E: y^2 = x^3 + Ax + B$ 是定义在 $\mathbb{Q}$ 上的椭圆曲线，$A, B \in \mathbb{Z}$. 对于素数 p，考虑 E mod p 的解的个数 $|\widetilde{E}(\mathbb{F}_p)|$，记

$$t_p := \begin{cases} \begin{cases} 1, & \text{可裂乘性约化} \\ -1, & \text{非可裂乘性约化} \\ 0, & \text{加性约化} \end{cases}, & p|\Delta(\text{坏约化}) \\ p + 1 - |\widetilde{E}(\mathbb{F}_p)|, & p \nmid \Delta(\text{好约化}) \end{cases}$$

定义 **Hasse-Weil L-函数**为

$$L(E,s):=\prod_{p|\Delta}\frac{1}{1-t_pp^{-s}}\cdot\prod_{p\nmid\Delta}\frac{1}{1-t_pp^{-s}+p^{1-2s}},$$

这是个算术函数.

命题 5.2 (1) 若记 $L(E,s)$ 展开得到的 Dirichlet 级数为 $L(E,s)=\sum_{n=1}^{\infty}\frac{a_n}{n^s}$，则 $a_p=t_p$.

(2) 根据有限域上椭圆曲线的 Hasse 定理 (见 [1] 定理 5.1.1)，当 $(p,\Delta)=1$ 时有 $|t_p|\leq 2\sqrt{p}$.

(3)Hasse-Weil L-函数 $L(E,s)$ 在 $\mathrm{Re}(s)>\frac{3}{2}$ 处内闭一致收敛，并且可亚纯延拓至整个复平面.

(4)**谷山志村定理 (Breuil-Conrad-Diamond-Taylor-Wiles)**：对于椭圆曲线 E，存在唯一 (以依赖于 E 导子的同余子群为级的) 尖点形式 $f\in S_2(\Gamma_0(N))$，使得 $L(E,s)=L(f,s)$. 这里尖点形式 f 的 L-函数 $L(f,s):=\sum_{n=1}^{\infty}\frac{f_n}{n^s}$，其中 f_n 为 f 的展开式系数. 特别地，根据模形式中 L-函数的结论可立即得到：(3) 中 $L(E,s)$ 的亚纯延拓其实是定义在整个复平面上的全纯函数 (见 [9] 定理 9.16).

既然谈到 L-函数，就不得不提类数公式，而即将要介绍的 B-SD 猜想则可以与类数公式做一个形式上的类比. 首先回忆类数公式：

定理 5.3(类数公式) 设 K 是数域. 记 K 有 r_1 个实嵌入、r_2 对复嵌入，则 Dedekind-Zeta 函数

$$\zeta_K(s):=\prod_{\mathfrak{p}\in\mathrm{MaxSpec}(\mathcal{O}_K)}\frac{1}{1-|\mathcal{O}_K/\mathfrak{p}|^{-s}}=\sum_{0\neq\mathfrak{a}\lhd\mathcal{O}_K}\frac{1}{|\mathcal{O}_K/\mathfrak{a}|^s},\ \mathrm{Re}(s)>1.$$

可亚纯延拓至整个复平面，其仅有一个 1 阶极点 $s=1$，留数为 $\frac{2^{r_1}(2\pi)^{r_2}R_Kh_K}{w_K\sqrt{|d_K|}}$(这里 R_K,h_K,w_K,d_K 分别指 K 的正规子 (即 $\mathcal{O}_K^\times/(\mathcal{O}_K^\times)_{\mathrm{tor}}$ 作为格点时对应基本区域的体积)、类数、单位根的个数、判别式)；其在一个平凡零点 $s=0$ 处的阶数为 r_1+r_2-1，更准确来说有 $\lim_{s\to0}\frac{\zeta_K(s)}{s^{r_1+r_2-1}}=-\frac{R_Kh_K}{w_K}$(见 [9] 定理 8.29). 特别地，当 $K=\mathbb{Q}$ 时，Dedekind-Zeta 函数退化为 Riemann-Zeta 函数 $\zeta(s):=\sum_{n=1}^{\infty}\frac{1}{n^s}$，此时 $\zeta(0)=-\frac{1}{2},\zeta(1)=\infty$(为 1 阶极点，留数为 1).

类数公式将解析对象 (Dedekind-Zeta 函数) 与算术对象 (类群等) 联系起来，这种联系可以类比到椭圆曲线当中. 之前我们已经定义了解析对象 (Hasse-Weil L-函数)，现在需要引入一些算术对象——m-Selmer 群 $S^{(m)}$ 和 Shafarevich-Tate 群 Ш.

首先，记绝对 Galois 群 $\mathbb{G}_K:=\mathrm{Gal}(\overline{K}/K)$. 对椭圆曲线 $E/\mathbb{Q}$，将函子 $(\cdot)^{\mathbb{G}_{\mathbb{Q}}}$ 作用于正合序列 $0\longrightarrow E(\mathbb{Q})[m]\longrightarrow E(\overline{\mathbb{Q}})\xrightarrow{m(\cdot)}E(\overline{\mathbb{Q}})\longrightarrow 0$ 得长正合列

$$0\longrightarrow E(\mathbb{Q})[m]\longrightarrow E(\mathbb{Q})\xrightarrow{m(\cdot)}E(\mathbb{Q})\longrightarrow H^1(\mathbb{G}_{\mathbb{Q}},E(\mathbb{Q})[m])\longrightarrow H^1(\mathbb{G}_{\mathbb{Q}},E(\overline{\mathbb{Q}})[m])\xrightarrow{m(\cdot)}H^1(\mathbb{G}_{\mathbb{Q}},E(\overline{\mathbb{Q}})[m]),$$

它诱导短正合列 $0\longrightarrow E(\mathbb{Q})/mE(\mathbb{Q})\longrightarrow H^1(\mathbb{G}_{\mathbb{Q}},E(\mathbb{Q})[m])\longrightarrow H^1(\mathbb{G}_{\mathbb{Q}},E(\overline{\mathbb{Q}}))[m]\longrightarrow 0$. 当然我们也有局部域的版本：$0\longrightarrow\prod_pE(\mathbb{Q}_p)/mE(\mathbb{Q}_p)\longrightarrow\prod_pH^1(\mathbb{G}_{\mathbb{Q}_p},E(\mathbb{Q}_p)[m])\longrightarrow\prod_pH^1(\mathbb{G}_{\mathbb{Q}_p},E(\overline{\mathbb{Q}_p}))[m]\longrightarrow 0$. 更明确来说，有如下交换图：

$$\begin{array}{ccccccccc}
0 & \longrightarrow & E(\mathbb{Q})/mE(\mathbb{Q}) & \longrightarrow & H^1(\mathbb{G}_{\mathbb{Q}},E(\mathbb{Q})[m]) & \longrightarrow & H^1(\mathbb{G}_{\mathbb{Q}},E(\overline{\mathbb{Q}}))[m] & \longrightarrow & 0\\
 & & \downarrow & & \downarrow & \overset{\rho}{\searrow} & \downarrow & & \\
0 & \longrightarrow & \prod_pE(\mathbb{Q}_p)/mE(\mathbb{Q}_p) & \longrightarrow & \prod_pH^1(\mathbb{G}_{\mathbb{Q}_p},E(\mathbb{Q}_p)[m]) & \longrightarrow & \prod_pH^1(\mathbb{G}_{\mathbb{Q}_p},E(\overline{\mathbb{Q}_p}))[m] & \longrightarrow & 0
\end{array}$$

以及交换图：

$$\begin{array}{ccccccccc}
0 & \longrightarrow & E(\mathbb{Q})/mE(\mathbb{Q}) & \longrightarrow & H^1(\mathbb{G}_{\mathbb{Q}},E(\mathbb{Q})[m]) & \longrightarrow & H^1(\mathbb{G}_{\mathbb{Q}},E(\overline{\mathbb{Q}}))[m] & \longrightarrow & 0\\
 & & \downarrow & & \downarrow{\scriptstyle\rho} & & \downarrow{\scriptstyle\varepsilon} & & \\
0 & \longrightarrow & 0 & \longrightarrow & \prod_pH^1(\mathbb{G}_{\mathbb{Q}_p},E(\overline{\mathbb{Q}_p}))[m] & \longrightarrow & \prod_pH^1(\mathbb{G}_{\mathbb{Q}_p},E(\overline{\mathbb{Q}_p}))[m] & \longrightarrow & 0
\end{array}$$

定义 5.4(Selmer 群与 Ш 群) 设 $E/\mathbb{Q}$ 是椭圆曲线，定义如下两个群：
(1.m-**Selmer 群**)：$S^{(m)}(E/\mathbb{Q}) := \ker\left[H^1(\mathbb{G}_{\mathbb{Q}}, E(\mathbb{Q})[m]) \to \prod_p H^1(\mathbb{G}_{\mathbb{Q}_p}, E(\overline{\mathbb{Q}_p}))[m]\right]$；
(2.**Shafarevich-Tate 群**)：$Ш(E/\mathbb{Q}) := \ker\left[H^1(\mathbb{G}_{\mathbb{Q}}, E(\overline{\mathbb{Q}})) \to \prod_p H^1(\mathbb{G}_{\mathbb{Q}_p}, E(\overline{\mathbb{Q}_p}))\right]$.

命题 5.5 当 $m \geq 2$ 时，m-Selmer 群是有限群.

注意 5.6 对于上述交换图，蛇引理给出正合列

$$0 \longrightarrow E(\mathbb{Q})/mE(\mathbb{Q}) \longrightarrow \ker(\rho) = S^{(m)}(E/\mathbb{Q}) \longrightarrow \ker(\varepsilon) = Ш(E/\mathbb{Q})[m] \longrightarrow 0,$$

据此结合命题 5.5 立得弱 Mordell-Weil 定理.

现考虑定义在 $\mathbb{Q}$ 上的椭圆曲线 $E: y^2 = x^3 + Ax + B$，设 $p > 3$ 是一个素数. 在忽略掉有限多个素数之后可将 E 的系数 mod p 得到定义在 $\mathbb{F}_p$ 上的椭圆曲线，此时 Hasse 定理给出 $\left||\widetilde{E}(\mathbb{F}_p)| - (p+1)\right| \leq 2\sqrt{p}$. 根据 Birch 和 Swinnerton-Dyer 的工作我们知道 $\prod_{p\leq x} \frac{|\widetilde{E}(\mathbb{F}_p)|}{p} \sim C\ln^r x$，这里 r 是 $E/\mathbb{Q}$ 的 Mordell 秩. 用 L-函数可将该结论重新表述如下：

若记 $L_p(E,s) := \frac{1}{1-t_p p^{-s}+p^{1-2s}}$，则**形式上**有 $L_p(E,1) = \frac{p}{|\widetilde{E}(\mathbb{F}_p)|}$ 且 $L(E,1) = \prod_p L_p(E,1) = \prod_p \frac{p}{|\widetilde{E}(\mathbb{F}_p)|}$. 这意味着当 Mordell 秩 $r > 0$ 时 $E(\mathbb{Q})$ 有相当多的点提供 $\mathbb{F}_p$-点从而迫使 $L(E,1) = 0$. 更一般地，如果 Mordell 秩更大，那么 $|\widetilde{E}(\mathbb{F}_p)|$ 会相当大从而迫使 $L'(E,1) = 0, L''(E,1) = 0\cdots$ 这些估计十分困难，例如 $L'(E,1)$ 的计算方法可由复杂的 Gross-Zagier 公式 (见 [13]) 给出.

猜想 5.7(B-SD) 对于定义在 $\mathbb{Q}$ 上的椭圆曲线 $E: y^2 = x^3 + Ax + B(A, B \in \mathbb{Z})$，定义其**解析秩**为其 Hasse-Weil L- 函数 $L(E,s)$ 在零点 $s = 1$ 处的阶. 则：
(1)E 的 Mordell 秩 = 解析秩.
(2)$Ш(E/\mathbb{Q})$ 是有限群$\Big($类比类群 $\mathrm{Cl}(K) := \ker\left[H^1(\mathbb{G}_K, \mathcal{O}_{\overline{K}}^{\times}) \to \prod_v H^1(\mathbb{G}_{K_v}, \mathcal{O}_{\overline{K_v}}^{\times})\right]$ 有限$\Big)$.
(3) 成立等式

$$\lim_{s\to 1} \frac{L(E,s)}{(s-1)^r} = \frac{R_E \cdot |Ш(E/\mathbb{Q})| \cdot \Omega_E \cdot \prod_p c_p(E)}{|E(\mathbb{Q})_{\mathrm{tor}}|^2},$$

其中 r 指 Mordell 秩或解析秩；R_E 指 E 的**正规子** (即 $E(\mathbb{Q})$ 的自由部分看成某个实内积空间的格点对应基本区域的体积)；$\Omega_E := \int_{E(\mathbb{R})} \frac{dx}{2|y|}$ 指 $E(\mathbb{R})$ 上的 **Néron 周期** (贡献无穷素点)；$c_p(E) := [E(\mathbb{Q}_p) : E_0(\mathbb{Q}_p)]$ 指 **Tamagawa 数** (贡献有限素点).

注意 5.8 以下是 B-SD 猜想的一些进展：Coates 与 Wiles 对带复乘的椭圆曲线证明了 L-函数无零点时的 B-SD 猜想；B. Gross, D. Zagier 与 Kolyvagin 对部分 Mordell 秩为 0 或 1 的椭圆曲线 (带复乘且导子较小) 证明了 B-SD 猜想；张伟与 C. Skinner 等人通过对椭圆曲线的“计数”证明至少有约 2/3 的椭圆曲线满足 B-SD 猜想. 更多相关进展参见 [10] 或其它文献.

附录 A：$\wp$ 的图像

考虑椭圆曲线 $E = \mathbb{C}/(\mathbb{Z}\tau \oplus \mathbb{Z}1): y^2 = 4x^3 + Ax + B$. 本节将用 Riemann-Hurwitz 公式和 Eichler-Zagier 零点定理来研究复椭圆曲线上亚纯函数 $\wp, \wp': E \to \mathbb{CP}^1$ 的几何与拓扑. 注意 $\wp, \wp'$ 均是分歧覆叠映射，命题 2.2 告诉我们覆叠次数分别为 $\deg(\wp) = 2, \deg(\wp') = 3$.

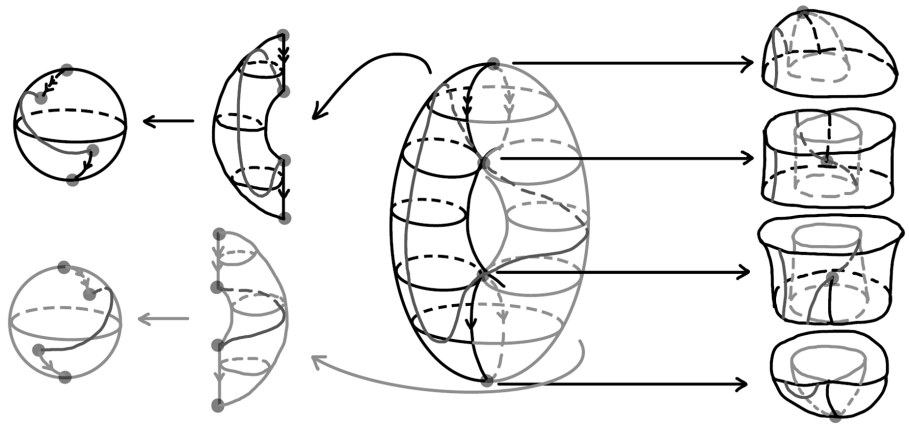
定理 A.1(Riemann-Hurwitz) 设 $f: X \to Y$ 为紧 Riemann 曲面之间的非常值态射. 若记 X, Y 的亏格分别为 g_X, g_Y，则 $2g_X - 2 = \deg(f)(2g_Y - 2) + \sum_{x\in \mathrm{Ram}(f)\subseteq X}(e(x) - 1)$.

例 A.2 (1) 我们知道次数为 1 的态射诱导紧 Riemann 曲面之间的同构，此时没有分歧点.

(2) 考虑 $f: \mathbb{C} \to \mathbb{C}, z \mapsto z^2$，补充无穷远点的定义使 $\mathbb{C}$ 成为一个紧 Riemann 曲面 $\mathbb{CP}^1$，将 f 延拓到 $\mathbb{CP}^1$ 使之成为一个亚纯函数. 此时由 $\deg(f) = 2$ 结合定理 A.1 知映射 f 的分歧点只能有两个，计算 $f'(z) = 0$ 知分歧点即 0 和 ∞.

例 A.3 (1) 考虑 $\wp: E \to \mathbb{CP}^1$. 注意到 $\deg(\wp) = 2$，故由定理 A.1 得 $\sum_{x\in \mathrm{Ram}(\wp)}(e(x)-1) = 4$. 由于 $\wp'$ 是双周期的奇函数，故 $0, \frac{1}{2}, \frac{\tau}{2}, \frac{1+\tau}{2}$ 是方程 $\wp'(z) = 0$ 的四个不同解$\big($除 0 以外它们恰是方程 $4\wp^3(z) + A\wp(z) + B = 0$

的三个不同解)，亦即 $\wp$ 的四个分歧点，分歧指数均只能为 1. 据此可画出覆叠映射 $\wp$ 图像如下：



(2) 考虑 $\wp' : E \to \mathbb{CP}^1$，此时 $\deg(\wp') = 3$. 将微分方程 $y^2 = 4x^3+Ax+B$ 两边求导得 $2\wp'\wp'' = 12\wp^2\wp'+A\wp'$. 分类讨论可知分歧点仅可能在 $0, \frac{1}{2}, \frac{\tau}{2}, \frac{1+\tau}{2}, \wp^{-1}(\pm\sqrt{-A/12})$ 中出现，产生总计 6 个分歧指数 (此处各点分歧指数不一定全为 1！). 具体弄清该分歧覆叠的行为十分困难，此处不再赘述.

至此寻找 $\wp$ 的分歧点有两种方法：找格点的中点或者解以 $\wp$ 为参数的三次方程. 前者是简单的，至于后者则出现了一个新问题：设 C 是复数，如何寻找方程 $\wp(z) = C$ 的解？一般而言这是困难的，虽然可以将其和格点的中点对应起来但还是避免不了计算复杂的级数. 特别地，当 $C = 0$ 时有如下定理 (见 [14] 或 [15])：

定理 A.4(Eichler-Zagier) 设 $\mathbb{Z}\tau \oplus \mathbb{Z}1$ 是 $\mathbb{C}$ 上的格点，若记它对应的 Weierstrass 函数为 $\wp(\tau, z)$，则满足 $\wp(\tau, z) = 0$ 的 z 由下述等式给出：

$$z = m + \frac{1}{2} + n\tau \pm \left(\frac{\ln(5+2\sqrt{6})}{2\pi i} + \frac{\pi i\sqrt{6}}{12} \int_{\tau+i\mathbb{R}_{>0}} (t-\tau) \frac{(G_4(t)/2\zeta(4))^3 - (G_6(t)/2\zeta(6))^2}{(G_6(t)/2\zeta(6))^{3/2}} dt \right), \quad m, n \in \mathbb{Z}.$$

例 A.5 (1) 取 $\tau = e^{2\pi i/3}$，此时格点 $\mathbb{Z}\tau \oplus \mathbb{Z}1$ 对应椭圆曲线 $E : y^2 = 4x^3 - \frac{\Gamma(1/3)^{18}}{(2\pi)^6}$. 显然 $\wp$ 的分歧点为 $0, \frac{1}{2}, \frac{\tau}{2}, \frac{1+\tau}{2}$，它们在 $\mathbb{CP}^1$ 中的像分别为 $\infty, \frac{\Gamma(1/3)^6}{2^{8/3}\pi^2}, \frac{\Gamma(1/3)^6}{2^{8/3}\pi^2}\tau, \frac{\Gamma(1/3)^6}{2^{8/3}\pi^2}\tau^2$，后三者是方程 $4x^3 - \frac{\Gamma(1/3)^{18}}{(2\pi)^6} = 0$ 的解.

(2) 取 $\tau = i$，此时格点 $\mathbb{Z}\tau \oplus \mathbb{Z}1$ 对应椭圆曲线 $E : y^2 = 4x^3 - \frac{\Gamma(1/4)^8}{16\pi^2}x$. 利用微分方程易见 $\wp$ 有且只有一个 2 重零点 (当然也是 $\wp$ 的分歧点)，通过检验所有分歧点可知该零点为 $\frac{1+i}{2}$.