椭圆曲线的历史

宋旭

目录

Chapter 1

椭圆曲线名字的由来

1.1 丢番图方程

丢番图方程是一个整系数或有理系数的多项式方程，解丢番图方程即寻找这个方程的整数解或有理数解。一般来说，一个丢番图方程的变量越多，次数越高，它的难度越大。一个变量的丢番图方程形如

$$a_n x^n + a_{n-1} x^{n-1} + ... + a_1 x + a_0 = 0$$

其中a_i均是整数，a_n不为0。若$x = \frac{p}{q}$是它的一个有理数解，p和q互素，则有$q|a_n, p|a_0$。从而通过有限次的尝试便可以确定该方程的解。由此可见一元的丢番图方程是平凡的。

情况在变量变成两个的时候瞬间改变了。考虑二元的丢番图方程

$$f(x, y) = 0$$

对于一般的二元丢番图方程，至今人们仍没有办法像求一元丢番图方程那样找到某种有效的方法求出它的解，甚至对解的存在性都没法证明。但对于一些次数较小和一些特殊的方程，人们基本掌握了它的解的结构。比如一次方程

$$ax + by = c$$

它有解当且仅当 $gcd(a, b)|c$, 且若x_0, y_0是它的一个解，则它的所有解又以下公式给出

$$\begin{cases} x = x_0 + \dfrac{b}{(a,b)}t \\ y = y_0 - \dfrac{a}{(a,b)}t \end{cases} \tag{1.1}$$

再来考虑二次的方程

$$f(x, y) = ax^2 + bxy + cy^2 + dx + ey + f = 0$$

它的系数均是有理数。事实上，人们基本上掌握了二元二次方程的有理数解的结构。如果在曲线$f(x, y) = 0$上已经找到一个有理点(x_0, y_0)，考虑有理直线(即系数均为有理数的直线$Ax + By + C = 0$)l，它上面的有理点和二次曲线上的有理点基本上是一一对应的：对于曲线上的一个有理点(x_1, y_1)，它与(x_0, y_0)的连线是一个有理直线，与l的交点是一个有理点；对于l上的一个有理点(a, b)，它与(x_0, y_0)的连线是一个有理直线，这个直线与二次曲线交于两个点(也有可能是一个

点，但这种情况有限，可以逐个具体分析)，其中一个点是(x_0, y_0)，由韦达定理，另一个点也是有理点。这建立了直线上有理点与曲线上有理点的一一对应，而直线上的有理点是容易掌握的。

用这种方法可以求出单位圆周$C : x^2 + y^2 = 1$上所有的有理点。首先找到C上的一个有理点$(-1, 0)$，再将他与y轴上的有理点$(0, t)$相连，得到的直线与圆周交于点$(-1, 0), (\frac{1-t^2}{1+t^2}, \frac{2t}{1+t^2})$。从而$C$上的有理点都形如$(\frac{1-t^2}{1+t^2}, \frac{2t}{1+t^2})$,$t$为有理数。注意此时的$(-1, 0)$对应$t = \infty$。

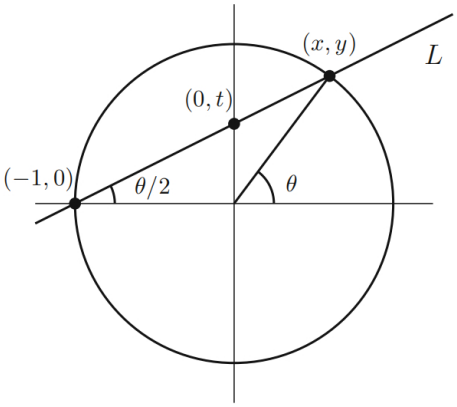


图 1.1: 圆周上的有理点

那如何判断一个二次方程有没有有理数解呢？事实上，任意的二次方程，我们都可以将它齐次化，比如方程$f(x, y) = ax^2+bxy+cy^2+dx+ey+f = 0$的齐次化为$ax^2+bxy+cy^2+dxz+cyz+fz^2 = 0$，同时可以通过乘以公分母使得系数全部化为整数。Hasse有一个定理说，一个齐次的多元的二次方程有整数解当且仅当它在$\mathbb{R}$和$\mathbb{Q}_p$上有解，对任意素数p。从而将判断方程是否整数解的问题化为判断同余方程是否有解的问题，而后者是可以通过尝试得到的。

我们将目光放到二元三次方程$ax^3 + bx^2y + cxy^2 + dy^3 + ex^2 + fxy + gy^2 + hx + iy + j = 0$上面。可以证明，通过一系列变换，可以将方程化为:$y^2 = x^3 + ax^2 + bx + c$，进一步通过将$x$换为$x - a/3$，可以将x的二次项系数变为0，再通过伸缩变换将方程化为Weierstrass标准型

$$y^2 = 4x^3 - g_2x - g_3$$

在之后的章节中我们将证明，当$4x^3 - g_2x - g_3$没有重根时，该方程将定义一条椭圆曲线。

1.2 椭圆积分和椭圆曲线

考虑椭圆 $\frac{x^2}{a^2}+\frac{y^2}{b^2}=1$

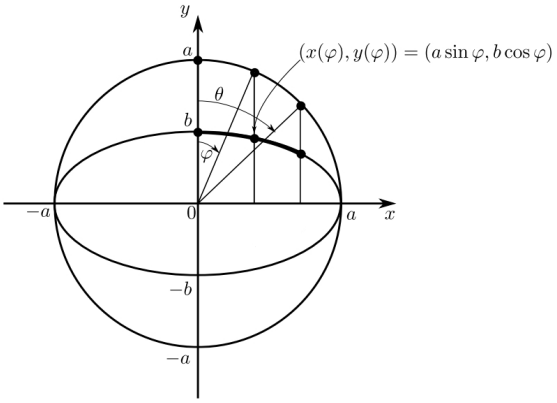


图 1.2: 椭圆

计算图2中加粗的那段弧的长度

$$\begin{aligned} l=&\int_0^\theta \sqrt{(\frac{d}{d\varphi}asin\varphi)^2+(\frac{d}{d\varphi}bcos\varphi)^2}d\varphi \\ =&\int_0^\theta \sqrt{a^2cos^2\varphi+b^2sin^2\varphi}d\varphi \\ =&a\int_0^\theta \sqrt{1-\frac{a^2-b^2}{a^2}sin^2\varphi}d\varphi=a\int_0^\theta \sqrt{1-k^2sin^2\varphi}d\varphi. \end{aligned}$$

这里 $k:=\sqrt{\frac{a^2-b^2}{a^2}}$, 即为椭圆的离心率。定义不完全第二型椭圆积分

$$E(k,\theta):=\int_0^\theta \sqrt{1-k^2sin\varphi}d\varphi$$

当$\theta=\frac{\pi}{2}$ 时，定义

$$E(k):=E(k,\frac{\pi}{2})=\int_0^{\frac{\pi}{2}} \sqrt{1-k^2sin\varphi}d\varphi.$$

令$t=sin\varphi$,得

$$E(k)=\int_0^1 \frac{\sqrt{1-k^2t^2}}{\sqrt{1-t^2}}dt$$

它被称为第二类椭圆积分。人们在计算双扭线的周长时，得到了类似的产物

$$K(k)=\int_0^1 \frac{dz}{\sqrt{(1-z^2)(1-k^2z^2)}}$$

勒让德(Legendre)在他的《研究》中，主要成果是证明了一般椭圆积分

$$\int \frac{P(x)}{\sqrt{R(x)}}dx$$

(其中$P(x)$是X的任一有理函数，而$R(x)$是四次多项式)能化为三种类型：

$$\int \frac{dx}{\sqrt{1-x^2}\sqrt{1-l^2x^2}} \tag{1}$$

$$\int \frac{x^2dx}{\sqrt{1-x^2}\sqrt{1-l^2x^2}} \tag{2}$$

$$\int \frac{dx}{(x-a)\sqrt{1-x^2}\sqrt{1-l^2x^2}} \tag{3}$$

勒让德把上面三类积分分别称为第一、二、三类椭圆积分。他还证明经过进一步的变换这三个积分可化为以下三种形式：

$$F(k,\phi)=\int_0^{\phi}\frac{d\phi}{\sqrt{1-k^2sin^2\phi}},\quad 0<k<1$$

$$E(k,\phi)=\int_0^{\phi}\sqrt{1-k^2sin^2\phi}d\phi,\quad 0<k<1$$

$$\pi(n,k,\phi)=\int_0^{\phi}\frac{d\phi}{(1+nsin^2\phi)\sqrt{1-k^2sin^2\phi}},\quad 0<k<1$$

1826年左右，阿贝尔注意到，如果研究

$$u=\int_0^{x}\frac{dx}{\sqrt{1-x^2}\sqrt{1-k^2x^2}}=\int_0^{\phi}\frac{d\phi}{\sqrt{1-k^2sin^2\phi}} \tag{$*$}$$

其中$x=\sin\phi$，那么会像研究

$$u=\int_o^{x}\frac{dx}{\sqrt{1-x^2}}=\text{arcsinx}$$

时出现相似的困难，因为研究arcsin比研究sin要麻烦许多。因此阿贝尔考虑在椭圆积分中把x作为u的函数来研究。由于$=sin\phi$，所以ϕ也可以作为u的函数。

雅可比(Jacobi)引入了记号

$$\phi=am\ u$$

表示$(*)$定义的u的函数ϕ。他还引进了

$$cos\phi=cos\ am\ u\text{和}\Delta\phi=\Delta\text{am u}=\sqrt{1-\text{k}^2\text{sin}\phi}$$

这个记号被古德曼简化为

$$x=sin\phi=sin\ am\ u=sn\ u,cos\phi=cos\phi=cos\ am\ u=cn\ u$$

$$\Delta\phi=\Delta am\ u=dn\ u$$

我们立即有

$$sn^2u+cn^u=1,dn^2u+k^2sn^2u=1$$

令

$$K=\int_0^{1}\frac{dx}{\sqrt{(1-x^2)(1-k^2x^2)}}=\int_0^{\frac{\pi}{2}}\frac{d\phi}{\sqrt{1-k^2sin^2\phi}}=F(k,\frac{\pi}{2})$$

与K联系着的是超越量K',它作为k'的函数相同与K作为k的函数，其中k'满足$k^2+k'^2=1,0<k<1$。有如下重要性质

$$sn(u+4K)=sn\ u,cn(u+4K)=cn\ u,dn(u\pm 2K)=dn\ u$$

因此sn, cn, dn都是周期函数，我们发现椭圆积分的反函数和三角函数的性质有点像，这是一个振奋人心的结果。然而这还不是故事的全部。到此为止，sn, cn, dn都只对实数有定义，阿贝尔下一步便是引入u的复值。阿贝尔引进了

$$sin\theta = itan\phi,\ cos\theta = \frac{1}{cos\phi},\ \Delta(\theta.k) = \frac{\Delta(\phi, k')}{cos\phi}$$

其中 $\theta = am\ iu$，从而有

$$sn(iu, k) = i\frac{sn(u, k')}{cn(u, k')},\ cn(iu.k) = \frac{1}{cn(u, k')}$$

$$dn(iu, k) = \frac{dn(u, k')}{cn(u, k')}$$

阿贝尔还建立了椭圆函数的加法定理。我们知道，三角函数有和角公式

$$sin(a + b) = sina \cdot cosb + cosa \cdot sinb$$

因此，对于

$$u = A(x) = \int_0^x \frac{1}{\sqrt{1 - x^2}}dx = arcsinx$$

中，有

$$A(x_1) + A(x_2) = A(x_1y_2 + x_2y_1)$$

其中y_1, y_2为对应的余弦值。现在考虑

$$u = E(x) = \int_0^x \frac{dx}{\sqrt{R(x)}}$$

其中$y^2 = R(x)$是一个四次多项式。欧拉曾经得到加法定理

$$E(x_1) + E(x_2) = E(x_3)$$

其中x_3是x_1, x_2, y_1, y_2的一个已知的有理函数，并且$y = \sqrt{R(x)}$。对于反函数$x = \phi(u)$,阿贝尔证明了对于实的u, v有

$$sn(u + v) = \frac{sn\ ucn\ vdn\ v + sn\ vcn\ udn\ u}{1 - k^2sn^2usn^2v}$$

对于$cn(u + v), dn(u + v)$也有类似的公式。这便是椭圆函数的加法定理。对于自变量的实值和虚值定义了椭圆函数以后，阿贝尔借助加法定理将定义推广到复值。具体来说，对于复数$z = u + iv$，由加法定理可以将$snz = sn(u + iv)$用u和iv的sn, cn和dn表示出。对于复数自变量的椭圆函数，有如下性质：

$$sn(iu + 2iK', k) = sn(iu, k)$$

$$cn(iu + 4iK', k) = cn(iu, k)$$

$$dn(iu + 4iK', k) = dn(iu, k)$$

所以$sn\ z$的周期为$4K$和$2iK'$;$cn\ z$的周期是$4K$和$2K + 2iK'$;$dn\ z$的周期为$2K$和$4iK'$。因此椭圆函数是双周期的，这是阿贝尔的伟大发现之一。关于周期，重要的是有两个周期，其比值不是实数。

Abel

Weierstrass

维尔斯特拉斯(Weierstrass)于1860年左右开始研究椭圆函数，它从古德曼那里学习了雅可比的工作，并从阿贝尔的论文里学习了阿贝尔的工作。之前提到，勒让德曾将椭圆积分化简成含有一个四次多项式的平方根的三个标准形式。而维尔斯特拉斯得到含有一个三次多项式的平方根的三个不同形式，即

$$\int \frac{dx}{\sqrt{4x^3 - g_2x - g_3}} \tag{1}$$

$$\int \frac{xdx}{\sqrt{4x^3 - g_2x - g_3}} \tag{2}$$

$$\int \frac{dx}{(x-a)\sqrt{4x^3 - g_2x - g_3}} \tag{3}$$

他把“反演”第一个积分所得的椭圆函数作为基本的椭圆函数，也就是所，如果

$$u = \int_0^x \frac{dx}{\sqrt{4x^3 - g_2x - g_3}}$$

那么u的椭圆函数x为

$$x = \mathfrak{p}(u) = \mathfrak{p}(u|g_2, g_3)$$

其中$\mathfrak{p}$便是著名的Weierstrass $\mathfrak{p}$函数。在教科书中，Weierstrass $\mathfrak{p}$函数定义为

$$\mathfrak{p}(z) = \frac{1}{z^2} + \sum_{\omega \in \Lambda^*} \left[\frac{1}{(z+\omega)^2} - \frac{1}{\omega^2} \right]$$

其中Λ为复平面的一个格点。具体来说，设ω_1, ω_2为两个非零复数，且$\omega_2/\omega_1 \notin \mathbb{R}$。格点即为集合$\Lambda = \mathbb{Z}\omega_1 + \mathbb{Z}\omega_2$。

$\mathfrak{p}$是一个有着二阶极点的双周期亚纯函数。它的导数$\mathfrak{p}'(z)$有着三阶极点。$(\mathfrak{p}, \mathfrak{p}')$满足方程

$$y^2 = 4x^3 - g_2x - g_3$$

这便是椭圆曲线的方程。为了看清这件事，我们将$\mathfrak{p}$展开成幂级数。利用

$$\frac{1}{(1-x)^2} = 1 + \sum_{n=1}^{\infty}(n+1)x^n$$

得

$$\frac{1}{(1-z/\omega)^2} - 1 = \sum_{n=1}^{\infty}(n+1)(\frac{z}{\omega})^n$$

从而

$$\frac{1}{\omega^2}(\frac{1}{(1-z/\omega)}-1)=\sum_{n=1}^{\infty}(n+1)(\frac{z^n}{\omega^{n+1}})$$

带入$\mathfrak{p}$中，得

$$\mathfrak{p}(z)=\frac{1}{z^2}+\sum_{\omega\in\Lambda^*}\left(\sum_{n=1}^{\infty}(n+1)(\frac{z^n}{\omega^{n+2}})\right)$$

交换和号得

$$\mathfrak{p}(z)=\frac{1}{z^2}+\sum_{n=1}^{\infty}(n+1)z^n\left(\sum_{\omega\in\Lambda^*}(\frac{1}{\omega^{n+2}})\right)$$

定义Einsenstein级数为

$$G_n=\sum_{\omega\in\Lambda^*}\frac{1}{\omega^n}$$

其中$n\geq 3$为正整数(只有$n\geq 3$时级数收敛)。注意到$G_{2n+1}=0$,从而

$$\mathfrak{p}(z)=\frac{1}{z^2}+\sum_{n=1}^{\infty}(2n+1)z^{2n}G_{2n+2}$$

计算前面几项，得

$$\mathfrak{p}(z)=z^{-2}+3G_4z^2+5G_6z^4+7G_8z^6+...$$

$$\mathfrak{p}'(z)=-2z^{-3}+6G_4z+20G_6z^3+42G_8z^5+...$$

如此计算$P(z)=\mathfrak{p}'^2-4\mathfrak{p}^3+60G_4\mathfrak{p}+140G_6$，奇迹发生了：所有负次项全部消失了。从而$P(z)$是一个定义在整个复平面的全纯函数，注意到它也是双周期的，所以它是一个有界函数，由Liouville定理知$P(z)$为常函数。容易计算出$P(0)=0$，从而$P(z)\equiv 0$。从而

$$\mathfrak{p}'^2=4\mathfrak{p}^3-60G_4\mathfrak{p}-140G_6$$

回到本章标题提出的问题：椭圆曲线为什么叫这个名字？我想这大概是因为椭圆曲线、椭圆积分、椭圆函数这三个对象彼此有着密切联系。

Chapter 2

代数曲线

2.1 代数簇

2.1.1 仿射代数簇

我们为了介绍椭圆曲线的概念，我们需要先介绍曲线的概念。曲线在不同的数学分支中有着不同的定义。在微分几何中，流形M上的一条(浸入)曲线为光滑浸入$\gamma : (-1, 1) \to M$。在代数几何中，为了定义什么是曲线，需要先了解代数簇(variety)的语言。代数簇的理论基础大部分是在19世纪到20世纪被一些意大利罗马的数学家完成，包括Severi, Castelnuovo和 Enriques等人，他们的团体被称为"The Italian School"。

由于在研究中，我们感兴趣的绝大多数丢番图方程的系数都是数域(有理数域的有限扩张)或者有限域，所以在接下来的章节中，都设K是一个完美域(perfect field),即$K[x]$中的不可约多项式都不可分。设$\bar{K}$ 是K的代数闭包，$G_{\bar{K}/K}$为伽罗瓦群。

定义. *n维仿射空间是集合*

$$\mathbb{A}^n = \mathbb{A}^n(\bar{K}) = \{P = (x_1, x_2, ..., x_n) : x_i \in \bar{K}\}.$$

类似的，定义K有理点集合为

$$\mathbb{A}^n(K) = \{P = (x_1, x_2, ..., x_n) \in \mathbb{A}^n : x_i \in K\}$$

代数几何的理论在域是代数闭域的情况下是较为简单的，因此人们若想研究K上的代数几何，就先研究$\bar{K}$上的代数几何，再通过伽罗瓦理论将两者联系在一起。伽罗瓦群自然地作用在$\mathbb{A}^n$上：对$\sigma \in G_{\bar{K}/K}$以及$P \in \mathbb{A}^n$,有

$$P^\sigma = (x_1^\sigma, x_2^\sigma, ..., x_n^\sigma)$$

从而K有理点集就可以被描述成：

$$\mathbb{A}^n(K) = \{P \in \mathbb{A}^n, P^\sigma = P, \forall \sigma \in G_{\bar{K}/K}\}$$

设$\bar{K}[X] = \bar{K}[X_1, X_2, ..., X_n]$是一个n个变元的多项式环，$I$是一个理想，定义

$$V_I = \{P \in \mathbb{A}^n, f(P) = 0, \forall f \in I\}$$

定义. *称V_I这样的集合为（仿射）代数集。对于一个代数集V,定义它的理想为*

$$I(V) = \{f \in \bar{K}[X] | f(P) = 0, \forall P \in V\}$$

一个代数集被称作是在K上定义的，如果$I(V)$可以被一些K系数的多项式生成，记作V/K。如果V是定义在K上的，则定义V上的K有理点为

$$V(K) = V \cap \mathbb{A}^n(K)$$

且令$I(V/K) = I(V) \cap K[X]$

定义. 一个*(仿射)*代数集V被称为*(仿射)*代数簇，如果$I(V)$是$\bar{K}[X]$中的素理想。如果V/K是定义在K上的，则定义仿射坐标环*(affine coordinate ring)*为

$$K[V] = K[X]/I(V/K)$$

它的分式域记为$K(V/K)$ 将K替换为$\bar{K}$, 同理定义$\bar{K}[V], \bar{K}(V)$.

不难发现，每个$\bar{K}[V]$中的元素定义了V到$\bar{K}$的一个映射。定义局部环

$$K(V)_P = \{f/g | f, g \in \bar{K}[V], g(P) \neq 0\} = \bar{K}[V]_{M_P}$$

其中$M_P = f \in K[V] | f(P) = 0$是一个极大理想。

对于代数簇这个几何对象，许多微分几何中的概念都可以搬过来。

定义. 设一个代数簇V的理想$I(V)$被$f_1, f_2, ..., f_m \in \bar{K}[X]$ 生成。则V在点P处光滑，如果

$$(\partial f_i/\partial X_j(P))_{1 \leq i \leq m, 1 \leq j \leq n}$$

的秩等于$n - r$,其中$r = dim V$.

可以证明，上面的定义等价于局部环$K(V)_P$是一个正则局部环(regular local ring)。

定义 (正则局部环). 设A是一个诺特局部环，m是它的极大理想，$k = A/m$是剩余类域。称A是正则局部环，如果

$$dim_k m/m^2 = dim A$$

2.1.2 射影代数簇

射影代数簇可以粗略地理解为仿射代数簇加上无穷远点，将无穷远点纳入研究的范围是一个大进步。射影几何的最基本的想法要追溯到17世纪的Desargues。当时的几何学家借鉴画家和建筑家的想法，将他们绘图的技巧和思想运用在几何学中，而Desargues试图给其中的一些想法严格化，引入了无穷远点的概念。他还用中心投影的方法从经典欧氏几何中发现新的定理。尽管Desargues的想法启发了Pascal关于圆锥曲线的工作，但可能是Desargues在写作时用的语言相对抽象，抑或是他的著作没有得到广泛传播，他的思想没有引起时代注意。

18世纪的数学家，以Euler和Stirling为代表，暗示了“想象中的点”的存在。这一事实被后来意大利的学者明确指出，他们提出，两个相交的圆的交点的个数是4，除了明确能看到的那两个点外，还有两个点在无穷远。Möbius，Plücker和Cayley等人使用了齐次坐标，使得射影几何的理论更加坚实。

定义. n维射影空间定义为

$$\mathbb{P}^n = \{\mathbb{A}^{n+1} - 0\}/\sim$$

$\sim$ 是一个等价关系：$(x_0, x_1, ..., x_n) \sim (\lambda x_0, \lambda x_1, ..., \lambda x_n), \forall \lambda \in \bar{K}^*$， 记$(x_0, x_1, ..., x_n)$在$\mathbb{P}^n$中的像为$[x_0, x_1, .., x_n]$ 定义K-有理点集为

$$\mathbb{P}^n(K) = \{[x_0, x_1, ..., x_n] \in \mathbb{P}^n, x_0, x_1, ..., x_n \in K\}$$

类似仿射的情形，我们可以定义射影代数集和射影代数簇，不过这回需要用到齐次多项式。

定义. 设$I \subset \bar{K}[X] = \bar{K}[x_0, x_1, ..., x_n]$是一个齐次理想，定义射影代数集为

$$V_I = \{P \in \mathbb{P}^n | f(P) = 0, 对所有I中的齐次多项式f\}$$

对于一个射影代数集V,定义它的理想为$\bar{K}[X]$中满足$f(P) = 0, \forall P \in V$ 的齐次多项式生成的理想，记作$I(V)$。如果$I(V)$是一个素理想，则这个射影代数集为射影代数簇(projective variety)。定义$\bar{K}[V] = \bar{K}[X]/I(V)$

可以类似地定义V的函数域和局部域

$$\bar{K}(V) = \{f/g | f, g \in K[V]为次数相同的齐次多项式, g \neq 0\}$$

$$\begin{aligned}\bar{K}(V)_P =& \{f/g | f, g \in \bar{K}[V], f, g为次数相同的齐次多项式, g(P) \neq 0\} \\ =& \bar{K}[V]_{(m_P)}\end{aligned}$$

其中m_P是由所有齐次的，满足$f(P) = 0$的多项式f生成的理想。

接下来我们来讨论仿射代数簇和射影代数簇的一些简单的联系。
令$U_i = \{(x_0, x_1, ..., x_n) \in \mathbb{P}^n | x_i \neq 0\}$，这是$\mathbb{P}^n$中的一个开集。有自然的同构：

$$\begin{aligned}\phi_i : \mathbb{A}^n &\to U_i \\ (y_1, y_2, ..., y_n) &\mapsto [y_1, y_2, ..., y_i, 1, y_{i+1}, ..., y_n]\end{aligned}$$

它的逆为

$$\begin{aligned}\phi_i^{-1} : U_i &\to \mathbb{A}^n \\ [x_0, x_1, ..., x_n] &\mapsto (\frac{x_0}{x_i}, \frac{x_1}{x_i}, ..., \widehat{\frac{x_i}{x_i}}, ..., \frac{x_n}{x_i})\end{aligned}$$

ϕ_i^{-1}将$V \cap U_i$与$\mathbb{A}^n$中的像等同起来，从而是一个仿射代数簇。反过来，ϕ_i可以将一个$\mathbb{A}^n$中的仿射代数簇V映到U_i中的一个闭集。这个闭集在整个$\mathbb{P}^n$中取闭包，得到的集合称为V的射影闭包(projective closure)，记作$\bar{V}$。　　对于一个多项式$f(Y) \in \bar{K}[Y]$,定义它关于$X_i (0 \leq i \leq n)$的齐次化为

$$f^*(X_0, ..., X_n) = X_i^d f(\frac{X_0}{X_i}, \frac{X_1}{X_i}, ..., \frac{X_{i-1}}{X_i}, \frac{X_{i+1}}{X_i}, ..., \frac{X_n}{X_i})$$

其中d是最小的使得等号右边是多项式的非负整数。不难证明，对于仿射代数簇V，它的射影闭包$\bar{V}$的理想$I(\bar{V})$为所有$f^*, f \in I(V)$ 生成的齐次理想。例如，$\mathbb{A}^2$中的仿射代数簇$y^2 = x^3 + x$ 的射影闭包是$\mathbb{P}^2$中由齐次方程 $y^2 z = x^3 + xz^2$的射影代数簇。

对于射影代数簇，我们仍然可以定义它在某一点处的光滑性。设$V \in \mathbb{P}^n$为一个射影代数簇，P是上面一点。取U_i使得$P \in U_i$，称V在点P处光滑，如果仿射代数簇$V \cap U_i$在点P 处光滑。

可以证明，一个等价的定义是局部环$\bar{K}(V)_P$是一个正则局部环(即一个局部环A满足$dim_k m/m^2 = dim A$)。

2.1.3 代数簇之间的映射

这一小节我们主要讨论射影代数簇之间的映射。

定义. 设$V_1 \subset \mathbb{P}^m, V_2 \subset \mathbb{P}^n$是射影代数簇。他们之间的有理映射形如

$$\phi : V_1 \to V_2$$
$$\phi = [f_0, f_1, ..., f_n]$$

其中$f_0, f_1, ..., f_n \in \bar{K}(V_1)$ 满足：对任意$P \in V_1$使得$f_0, f_1, ..., f_n$在点P均有定义且不全为0，都有

$$\phi(P) = [f_0(P), f_1(P), ..., f_n(P)] \in V_2$$

有时候$f_0(P), ..., f_n(P)$均为0，那么ϕ在点P还可以有定义吗？答案是肯定的。如果能找到一个$g \in \bar{K}(V)$ 使得 $gf_i(P)$都有定义且不全为0，那么就令$\phi(P) = [gf_0(P), gf_1(P), ..., gf_n(P)]$.此时称$\phi$在点P处是正则的(regular)。注意到每一个$\bar{K}(V)$中的元素都可以表示为两个次数相同的齐次多项式的商，从而有理映射可以由以下方式定义：
一个有理映射$\phi : V_1 \to V_2$ 形如

$$\phi = [\phi_0(X), \phi_1(X), ..., \phi_n(X)]$$

其中
(1) $\phi_i(X) \in \bar{K}[X] = \bar{K}[X_0, X_1, ..., X_m]$为次数相同的齐次多项式，且不全在$I(V)$中。
(2) 对任意$f \in I(V_2)$,

$$f(\phi_0(X), ..., \phi_n(X)) \in I(V_1)$$

可以看出，对于$P \in V_!$, 如果$\phi_i(P)$不全为0，那么它的像是良好定义的V_2上的一个点，但如果$\phi_i(X)$全为0，如前面提到的，$\phi(P)$仍有可能是良好定义的。

一个有理函数在点$P \in V_1$处正则(有定义)，如果存在齐次多项式$\psi_0(X), ..., \psi_n(X) \in \bar{K}[X]$，使得
(1) $\psi_0(X), ..., \psi_n(X)$次数相同
(2)$\phi_i\psi_j \equiv \phi_j\psi_i (mod I(V_1))$
(3) $\psi_i(P)$ 不全为0
且令 $\phi(P) = [\psi_0(P), ..., \psi_n(P)]$.

一个有理映射称为正则映射，如果它在每点处都正则。下面我们看一个例子。
设$charK \neq 2, V : x^2 + y^2 = z^2$是一个射影代数簇。考虑有理映射

$$\phi : V \to \mathbb{P}^1$$
$$\phi = [x + z, y].$$

很明显，ϕ在除了点$[1, 0, -1]$之外的所有点处正则。事实上，在$[1, 0, -1]$点也是正则的，这是因为我们有

$$[x + z, y] = [x^2 - z^2, y(x - z)] = [-y^2, y(x - z)] = [-y, x - z]$$

从而有

$$\phi([1, 0. - 1]) = [0, 1]$$

同样，我们可以验证

$$\psi : \mathbb{P}^1 \to V$$
$$\psi = [s^2 - t^2, 2st, s^2 + t^2]$$

在所有点处正则，从而是一个态射(morphism)。它是ϕ的逆。从而我们有$V \cong \mathbb{P}^1$

2.2 代数曲线

2.2.1 维数为1的代数簇

代数几何起源于对曲线和曲面的研究。微分几何中人们研究微分流形的几何，代数几何中人们研究代数簇的几何。代数曲线可以说是最简单的代数簇，因为它的维数只有1，但正因为这种特殊性使得它的性质非常的丰富，理论十分的优美。

定义. 称维数为1的射影代数簇为(代数)曲线.

维数是1带来了很多东西。交换代数告诉我们，若A是一个维数是1的诺特局部环，$m, k = A/m$分别是它的局部环和剩余类域，则以下命题等价:
1) A 是一个离散赋值环(discrete valuation ring,简称DVR).
2) A 是整数闭的.
3) m 是一个主理想.
4) A 是一个正则局部环，即$dim_k(m/m^2) = dimA = 1$

这样，若C是一个曲线，P是一个光滑点，根据定义有$dim_{\bar{K}} M_P/M_P^2 = dimC = 1$。同时由于局部环$\bar{K}[C]_P$是一个1维的诺特局部环，从而是一个DVR。从而存在赋值

$$ord_P : K[C]_P \to \{0, 1, 2, 3, ...\} \cup \infty$$

$$ord_P(f) = max\{d \in \mathbb{Z}_{\geq 0} | f \in M_P^d\}$$

通过$ord_P(f/g) = ord_P(f) - ord_P(g)$将这个赋值延拓到整个函数域$\bar{K}(C)$上，得到

$$ord_P : \bar{K}(C) \to \mathbb{Z} \cup \infty$$

其中约定$ord_P(0) = \infty$
在点P的单值子(uniformizer)为满足$ord_P(t)$的$t \in \bar{K}(C)$.

在复分析中，亚纯函数有零点和极点。这里也有类似的概念。

定义. 设C是一个曲线，$P \in C$是一个光滑点。对于$f \in \bar{K}(C)$,称P是f的零点，如果$ord_P(f) > 0$;称P是f的极点，如果$ord_P(f) < 0$. 如果P是极点，记$f(P) = \infty$.

此外，关于零点和极点，我们有以下性质：

命题. 设C是一个光滑曲线，$f \in \bar{K}(C)^*$，则f只有有限个零点和极点。如果f没有极点，则$f \in \bar{K}$。

在此小节的最后，我们介绍一个在特征p情形下很有用的结果。

命题. 设C/K 是一个定义在K上的曲线，$t \in \bar{K}(C)$是一个在某个光滑点P处的单值子。则$K(C)$是$K(t)$的一个有限可分扩张。

2.2.2 曲线之间的映射

我们之前定义了射影代数簇之间的有理映射，并定义正则映射为在所有点处正则的有理映射。

命题. 设C是一个曲线，$V \subset \mathbb{P}^N$是一个射影代数簇，$P \in C$光滑，$\phi : C \to V$是一个有理映射。则ϕ在点P处正则。特别的，如果C是光滑曲线，则任何有理映射$\phi : C \to V$都是正则映射。

证明. 设$\phi = [f_0, f_1, ..., f_N], f_i \in \bar{K}(C)$，并选取点$P$处的单值子$t \in \bar{K}(C)$。设

$$n = min\{ord_P f_i, 0 \leq i \leq n\}$$

则$\forall i, ord_P t^{-n} f_i \geq 0$.且$\exists j, ord_P t^{-n} f_j$.
这表明ϕ在点P处正则. □

例. 设C/K是一个光滑曲线，$f \in K(C)$是一个函数。则f定义了一个有理映射

$$f : C \to \mathbb{P}^1$$

$$P \mapsto [f(P), 1]$$

由之前的命题这个映射是一个正则映射。它具体由

$$f(P) = \begin{cases} [f(P), 1] & 如果 ord_P f \geq 0 \\ [1, 0] & 如果 ord_P f < 0 \end{cases}$$

给出。反过来，设

$$\phi : C \to \mathbb{P}^1$$

$$\phi = [f, g], f, g \in K(C) 不全为0$$

则

$$\phi = \begin{cases} [1, 0] & 如果 g = 0 \\ [f/g, 1] & 如果 g \neq 0 \end{cases}$$

从而我们有一一对应：

$$K(C) \cup \infty \leftrightarrow \{定义在K上的C \to \mathbb{P}^1的有理映射\}$$

下面的命题是不平凡的。

命题. 设$\phi : C_1 \to C_2$ 是曲线之间的正则映射，则ϕ为常值映射或者是满射。

曲线之间的有理映射可以诱导函数域之间的映射。具体来说，设$C_1/K, C_2/K$是曲线，$\phi : C_1 \to C_2$是非常值的、定义在K上的有理映射。我们有

$$\phi^* : K(C_2) \to K(C_1)$$

$$\phi^* f = f \circ \phi$$

这是一个单射，且限制在K上是恒等映射。关于ϕ^*，我们有以下重要的结果。

定理. 设$C_1/K, C_2/K$是定义在K上的曲线。
*(a)*设$\phi : C_1 \to C_2$是定义在K上的非常值的有理映射，则$K(C_1)/\phi^* K(C_2)$是一个有限扩张。
*(b)*设$\iota : K(C_2) \to K(C_1)$是一个$K-$同态*(必为单射)*,则存在唯一的非常值的定义在$K$上的有理映射$\phi : C_1 \to C_2$使得$\iota = \phi*$
*(c)*设$\mathbb{K} \subset K(C_1)$ 是$K(C_1)$的一个有限指标的、包含K的一个子域。则存在唯一的*(*在$K-$同构意义下的*)*曲线C'/K,以及非常数的有理映射$\phi : C_1 \to C'$,使得$\phi^* K(C') = \mathbb{K}$。

定义. 设$\phi : C_1 \to C_2$是曲线之间定义在K上的一个有理映射。定义次数

$$deg\phi = \begin{cases} 0 & 如果\phi是一个常值映射 \\ [K(C_1) : \phi^* K(C_2)] & 如果\phi不是常值映射 \end{cases}$$

我们可以类似地分别定义可分次数和不可分次数为

$$deg_s\phi = [K(C_1) : \phi^* K(C_2)]_s$$

$$deg_i\phi = [K(C_1) : \phi^* K(C_2)]_i$$

$\phi : C_1 \to C_2$ 不仅能通过函数的复合自然地诱导出$K(C_2) \to K(C_1)$，还可以诱导出$K(C_1) \to K(C_2)$，它的定义为

$$\phi_* : K(C_1) \to K(C_2)$$

$$\phi_* = (\phi^*)^{-1} \circ N_{K(C_1)/\phi^* K(C_2)}$$

如果$deg\phi$是一个整体量，那下面定义的便是一个局部量。

定义. 设$\phi : C_1 \to C_2$是光滑曲线之间的一个非常值的一个映射，设$P \in C_1$。定义ϕ在点P处的分歧指数*(ramification index)*为

$$e_\phi(P) = ord_P(\phi^* t_{\phi(P)})$$

称ϕ在点P非分歧，如果$e_\phi(P) = 1$，否则就在点P处分歧。称ϕ非分歧，如果它在每点处都非分歧。

下面的命题总结了度和分歧指数的一些性质。

命题. 设$\phi : C_1 \to C_2$是光滑曲线之间的一个非常值映射。
(a) $\forall Q \in C_2, \sum_{P \in \phi^{-1}(Q)} e_\phi(P) = deg\phi$
(b) 除有限个点外，对$Q \in C_2$,都有 $\#\phi^{-1}(Q) = deg_s\phi$
*(c)*如果$\psi : C_2 \to C_3$是另一个光滑曲线之间的映射，则$\forall P \in C_1$，有

$$e_{\psi\phi}(P) = e_\phi(P) e_\psi(\phi P)$$

2.2.3 除子

除子(divisor)在代数曲线理论中起到重要的作用，它能很好地反应曲线在局部的信息。

曲线C的除子群(group of divisors)是由所有C上的点生成的自由阿贝尔群，记作$Div(C)$。也就是说，一个除子是$D \in Div(C)$是形式和

$$D = \sum_{P \in C} n_P(P)$$

其中$n_P \in \mathbb{Z}$只有有限个非0。除子D的度定义为 $degD := \sum_{P \in C} n_P$。其中度为0的除子形成$Div(C)$的子群，记作$Div^0(C)$

如果C/K是定义在K上的一个曲线，考虑$G_{\bar{K}/K}$在$Div(C)$上的作用：

$$D^\sigma := \sum_{P \in C} n_P(P^\sigma)$$

除子D被称为是定义在K上的，如果$D^\sigma = D, \forall \sigma \in G_{\bar{K}/K}$。所有定义在$K$上的除子形成一个群，记作 $Div_K(C)$,其中度为0的除子又形成一个群，即 $Div_K(C) \cap Div^0(C)$,记作 $Div_K^0(C)$。

现在假设C是一个光滑曲线。定义映射

$$div : \bar{K}(C)^* \to Div(C)$$

$$div(f) = \sum_{P \in C} ord_P(f)(P)$$

这是一个群同态。容易发现，$Div(f)^\sigma = Div(f^\sigma)$。特别的，若$f \in K(C)^*$,则$Div(f) \in Div_K(C)$

在代数数论中，对于数域L/Q，我们可以定义它的理想类群(ideal class group)为分式理想的自由群商去所有主理想。在这里，我们也可以定义类似的东西。

定义 (Picard群). *称除子D是一个主除子(principal divisor)，如果存在$f \in \bar{K}(C)^*$使得$D = Div(f)$。定义曲线C的Picard群$Pic(C)$ (或除子类群)为$Div(C)$商去所有主除子。由于$G_{\bar{K}/K}$在$Div(C)$上的作用将主除子变为主除子，故它也作用在$Pic(C)$上。记$Pic(C)$被$G_{\bar{K}/K}$固定的元素构成的子群为$Pic_K(C)$。*

以下性质非常重要.

定义. *设C是一个光滑曲线，$f \in \bar{K}(C)^*$.有*
(a) $div(f) \in Div^0(C), i.e. deg(div(f)) = 0$
(b) $divf = 0 \iff f \in \bar{K}^*$

由此，我们可以定义$Pic^0(C)$为$Div^0(C)$商去主除子群。进一步定义$Pic_K^0(C)$ 为$Pic^0(C)$中的被$G_{\bar{K}/K}$固定的群。综合以上的结果，我们有正合列

$$1 \to \bar{K}^* \to \bar{K}(C) \xrightarrow{div} Div^0(C) \to Pic^0(C) \to 1$$

我们之前看到,如果$\phi : C_1 \to C_2$是光滑曲线之间的一个非常值映射，则可以诱导出$\phi^* : \bar{K}(C_2) \to \bar{K}(C_2)$，和$\phi_* : \bar{K}(C_1) \to \bar{K}(C_2)$。其实$\phi$也可以诱导除子群之间的映射。我们定义群同态

$$\phi^* : Div(C_2) \to Div(C_1)$$

$$(Q) \mapsto \sum_{P \in \phi^{-1}(Q)} e_\phi(P)(P)$$

和

$$\phi_* : Div(C_1) \to Div(C_2)$$

$$(P) \mapsto (\phi P)$$

我们不加证明地给出以下性质来结束这一小节。

命题. *设ϕæ$C_1 \to C_2$是光滑曲线之间的非常值的映射。则有以下结果 (a)$deg(\phi^* D) = (deg\phi)(degD) \forall D \in Div(C_2)$.*
(b) $\phi^*(divf) = div(\phi^* f) \forall f \in \bar{K}(C_2)^*$.

(c) $deg(\phi_* D) = degD, \forall D \in Div(C_1)$.
(d) $\phi_*(divf) = div(\phi_* f)$.
(e) $\phi_* \circ \phi^*$作用在$Div(C_2)$上相当于数乘上$deg\phi$.
(f)(函子性) 如果$\psi : C_2 \to C_3$是另一个光滑曲线之间的非常值映射,则有

$$\phi^* \circ \psi^* = (\psi \circ \phi)^*, \psi_* \circ \phi_* = (\psi \circ \phi)_*$$

2.2.4 微分形式

我们熟悉微分流形上的微分形式。微分形式的一般定义最早由嘉当于1899年提出,在微分几何的研究中扮演重要的角色。对代数簇，我们也可以有微分形式和切空间等的概念。$Erich\ Kähler$在20世纪30年代引入了$Kähler$微分的概念，将微分形式推广到一般的交换环和概型(scheme)上。这里我们不使用$scheme$的语言而仅仅使用代数簇的语言。

设A是一个环，B是一个A代数，M是一个B模。一个到M的$A-$derivation是一个映射$d : B \to M$ 使得(1)d是可加的，(2)$d(bb') = bdb' + b'db$, (3) $da = 0, \forall a \in A$。

定义. 我们定义B/A的相关微分形式为一个B模$\Omega_{B/A}$，协同一个$A-derivation\ d : B \to \Omega_{B/A}$,满足泛性质：对任意$B$模$M$,以及任意$A-derivation\ d' : B \to M$, 存在唯一的$B$模同态$f : \Omega_{B/A} \to M$ 使得$d' = f \circ d$。

首先这样的$\Omega_{B/A}$是存在的。先考虑由符号$\{db|b \in B\}$生成的自由B模F，再商去由(1) $d(b+b') - db - db'$,(2) $d(bb') - bdb' - b'db$和 (3) $da, a \in A$ 生成的子模，得到的便是$\Omega_{B/A}$。由以上知识，我们便可以定义曲线上的微分形式。

定义. 设C是一个曲线。C上的微分形式空间Ω_c定义为$\Omega_{\bar{K}(C)/\bar{K}}$。

若B_1, B_2是两个A代数，$f : B_1 \to B_2$是一个A代数同态，则f诱导了

$$\Omega_{B_1/A} \to \Omega_{B_2/A}$$

$$b_1 db_1' \mapsto b_2 db_2'$$

其中$b_1, b_1' \in B_1, b_2 = f(b_1), b_2' = f(b_1')$.

设$\phi : C_1 \to C_2$是曲线之间的非常值映射，则有$\phi^* : \bar{K}(C_2) \to \bar{K}(C_1)$, 进而有

$$\phi^* : \Omega_{C_2} \to \Omega_{C_1}$$

$$\phi^*(\sum f_i dx_i) = \sum (\phi^* f_i) d(\phi^* x_i)$$

以下性质给出了曲线之间映射是否可分的一个判别。

命题. 设C是一个曲线。
(a) Ω_C 是1维的$\bar{K}(C)$-线性空间。

(b) 设$x \in \bar{K}(C)$.则dx是Ω_C 作为$\bar{K}(C)$线性空间的基当且仅当$\bar{K}(C)/\bar{K}(x)$是一个可分扩张。
(c) 设$\phi : C_1 \to C_2$是一个曲线之间的非常值映射，则ϕ是可分的当且仅当$\phi^* : \Omega_{C_2} \to \Omega_{C_1}$非零。

由于我们知道，若t是某个光滑点处的单值子，则$\bar{K}(C)/\bar{K}(t)$是一个有限可分扩张，故由上面的性质，知dt是$\bar{K}(C)$的基，从而对任意非零的微分形式ω,都有唯一的$g \in \bar{K}(C)^*$，使得$\omega = gdt$。记$g = \omega/dt$。此时定义$ord_P(\omega)$为$ord_P(g)$。由下面的性质可知$ord_P(\omega)$不依赖于单值子t的选取。

命题. 设P是C上的光滑点，若$f \in \bar{K}(C)$在点P处正则，则df/dt在点P处正则。

可以证明，若$x \in \bar{K}(C)^*$满足$\bar{K}(C)/\bar{K}(x)$可分，且$ord_P(x) \geq 0$，则$ord_P(dx) = ord_P(x) - 1$. 同样可以证明，只有有限个$P \in C$使得$ord_P(\omega)$非零。因此我们可以有：

定义. 设$\omega \in \Omega_C$。与ω相关联的除子定义为

$$div(\omega) = \sum_{P \in C} ord_P(\omega)(P)$$

在复分析中，我们可以定义全纯函数和亚纯函数，其中全纯函数在定义域上没有极点。在代数曲线的理论中，也有类似的概念。比如C是一个光滑曲线，可以考虑$\bar{K}(C)$中没有极点的函数，我们知道这样的函数只能是常值函数。在微分形式中，也可以考虑类似的事情。

定义. 微分形式ω被称作是全纯*(holomorphic)*的，如果$\forall P \in C, ord_P(\omega) \geq 0$; ω被称为是非消失*(non-vanishing)*的，如果对 $\forall P \in C, ord_P(\omega) \leq 0$

对于非零的两个微分形式$\omega_1.\omega_2$, 由于Ω_C是一维的$\bar{K}(C)$-线性空间，故存在唯一的$f \in \bar{K}(C)$使得 $\omega_1 = f\omega_2$，从而

$$div(\omega_1) = div(f) + div(\omega_2)$$

从而$div(\omega_1), div(\omega_2)$在$Pic(C)$中的同一等价类中。从而我们可以有以下的定义：

定义. $Pic(C)$中的典型除子类为$div(\omega)$所在的类，其中$\omega \in \Omega_C$是任意非零微分形式。

我们接下来看两个简单的例子，虽然简单但却非常重要。

例. 我们来证明$\mathbb{P}^1$没有全纯的微分形式。首先我们知道

$$\begin{aligned} K(\mathbb{P}^1) &= \{f(x,y)/g(x,y) | f, g\text{是次数相同的齐次多项式}, f, g \in K[x,y]\} \\ &= K(\frac{x}{y}) \\ &\cong K(t) \end{aligned}$$

我们来计算$div(dt)$。在$\alpha \in K$处的单值子为$t - \alpha$,且$ord_\alpha(t - \alpha) = 0$，从而$ord_\alpha(dt) = ord_\alpha(d(t - \alpha)) = 0$。在$\infty$处，单值子为$1/t$，有

$$dt = -t^2 d(1/t)$$

从而$ord_\infty(dt) = ord_\infty(-t^2) = -2$。从而$div(dt) = -2(\infty)$，进而对任意非零微分形式$\omega$，都有

$$deg(div\omega) = deg(div(dt)) = -2$$

从而不存在全纯的微分形式.

例. 考虑曲线$C: y^2 = (x-e_1)(x-e_2)(x-e_3)$,其中$e_1, e_2, e_3 \in \bar{K}$为不同的三个数。可以证明，它在$\mathbb{P}^2$中的射影闭包是一个光滑曲线。记$P_1 = [e_1, 0, 1], P_2 = [e_2, 0, 1], P_3 = [e_3, 0, 1]$。可以证明

$$divy = (P_1) + (P_2) + (P_3) - 3(P_\infty)$$

$$div(dx) = (P_1) + (P_2) + (P_3) - 3(P_\infty)$$

从而$div(dx/y) = 0$。这表明C的典型除子类是0。

上面这个例子中的曲线C在接下来的章节会深入讨论，它便是大名鼎鼎的椭圆曲线。

2.2.5 Riemmann-Roch定理

这一小节介绍的Riemman-Roch定理在代数曲线理论中起到极为重要的作用。它最先是在研究紧黎曼面时发现的，利用该定理，可以计算具有指定零点与极点的亚纯函数(meromorphic function)的空间的维数。此定理原先是一个不等式，对黎曼曲面的确定形式由黎曼早逝的学生古斯塔·罗赫于1850年证明，随后推广到代数曲面，高维代数簇等。

设C是一个曲线，我们按下面的方式赋予除子以序关系。

定义. 一个除子$D = \sum_{P \in C} n_P(P)$是正的，如果$n_P \geq 0, \forall P$。定义$D_1 \geq D_2$，如果$D_1 - D_2 \geq 0$

例. 设$f \in \bar{K}(C)$在除点P外的所有点处均正则，且在P的极点的次数不超过n(即$ord_P(f) \geq -n$)。则以上描述等价于

$$div(f) \geq -n(P)$$

类似的，如果f满足$div(f) \geq (Q) - n(P)$,则这表示f在点Q处有一个零点，在P处的极点次数不超过n,在其余点正则。

定义. 设$D \in Div(C)$是一个除子，定义

$$\mathscr{L}(D) = \{f \in \bar{K}(C)^* : div(f) \geq -D\} \cup \{0\}$$

命题. 设$D \in Div(C)$
*(a)*如果$degD < 0$，则$\mathscr{L}(D) = \{0\}$
(b)$\mathscr{L}(D)$是一个有限维K-线性空间，记它的维数为$l(D)$.
(c) 如果除子D'线性等价于D(即他们在$Pic(C)$中处在同一等价类),则

$$\mathscr{L}(D') \cong \mathscr{L}(D), l(D') = l(D)$$

例. 设$K_C \in Div(\omega)$是一个典范除子，也就是说，对某个非零微分形式ω,

$$K_C = div(\omega).$$

从而我们有同构

$$\mathscr{L}(K_C) \to \{C\text{上全纯微分形式}\}$$
$$f \mapsto f\omega$$

我们之前证明了$\mathbb{P}^1$上没有全纯的微分形式，从而$C = \mathbb{P}^1$时，有$\mathscr{L}(K_C) = \{0\}, l(K_C) = 0$
后面可以看到，$l(K_C)$是与曲线C相关的重要的不变量。

有了以上的背景，我们终于可以介绍著名的Riemmann-Roch定理。

定理 (Riemann-Roch)**.** 设C是一个光滑曲线，K_c是一个典范除子。存在整数$g \geq 0$，称作曲线C的亏格, 使得对任意除子D,都有

$$l(D) - l(K_C - D) = degD - g + 1$$

由Riemman-Roch定理，我们不难得到

推论. 设C是一个光滑曲线。
(a) $l(K_C) = g$
(b) $degK_C = 2g - 2$
(c) 如果$degD > 2g - 2$，则

$$l(D) = degD - g + 2$$

我们照例来看$\mathbb{P}^!$和$C : y^2 = (x - e_1)(x - e_2)(x - e_3)$的例子。

例. 设$C = \mathbb{P}^1$。我们有$g = l(K_C) = 0$,即$\mathbb{P}^1$的亏格是*0*。取典范除子$K_C = div(dt) = -2(\infty)$,此时*Riemann-Roch*定理写作

$$l(D) - l(-2(\infty) - D) = degD + 1$$

特别的，当$degD \geq 1$时，有$l(D) = degD + 1$.

例. 设$C : y^2 = (x-e_1)(x-e_2)(x-e_3)$为之前定义的曲线。由$div(dx/y) = 0$知，它的典范除子为*0*.从而$g = l(K_C) = l(0) = 1$,即曲线$C$的亏格为*1*。若$degD \geq 1$,则$l(D) = degD$

在这一小节的最后，我们介绍著名的Hurwitz定理。

定理 (Hurwitz)**.** 设$\phi : C_1 \to C_2$是光滑曲线之间的非常值的可分映射。则有不等式

$$2g_1 - 2 \geq (deg\phi)(2g_2 - 2) + \sum_{P \in C_1} (e_\phi(P) - 1)$$

其中g_i是曲线C_i的亏格。等号成立当且仅当:
(i) $charK = 0$ 或
(ii)$charK = p$ 且p不整除$e_\phi(P), \forall P \in C_1$.

Riemann

Roch

Chapter 3

椭圆曲线的几何

3.1 椭圆曲线的方程

3.1.1 Weiestrass方程

初次接触到椭圆曲线的人可能会说，椭圆曲线就是形如$y^2 = x^3 + ax^2 + bx + c$的方程定义的曲线，但这句话不完全正确。这一章我们将给出椭圆曲线的标准定义，并介绍它的Weiestrass方程及其历史。

定义 (椭圆曲线). *(E, O)是定义在K上的椭圆曲线，如果E是一条光滑的亏格为1的曲线，O为曲线上的一个点.*

读者看到这里可能会困惑：为什么还要选择曲线上的某一个点？这其实是为了强调椭圆曲线的群结构，O便是群的单位元，这在之后的章节会详细说明。我们在之前的章节用著名的Riemann-Roch定理计算出曲线$y^2 = (x - e_1)(x - e_2)(x - e_3)$($e_1, e_2, e_3$两两不同)的亏格为1，因此它就是一条椭圆曲线。更一般的，我们有

定义 (Weierstrass方程). *形如*

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$$

的方程称作定义在K上的Weierstrass方程，其中$a_i \in K$.
它的齐次化

$$Y^2Z + a_1XYZ + a_3YZ^2 = X^3 + a_2X^2Z + a_4XZ^2 + a_6Z^3$$

定义了在$\mathbb{P}^2$中的一条曲线E。该曲线与直线$Z = 0$交于唯一一点$[0, 1, 0]$，称作是无穷远点，记作O。

Weierstrass方程定义的曲线不一定是椭圆曲线，因为它不一定光滑。我们接下来探究非光滑曲线(奇异曲线)的性质。首先，可以证明奇异点一定只有一个,且不是无穷远点。设点$P = (x_0, y_0)$是奇异点，则曲线$f(x, y) = y^2 + a_1xy + a_3 - x^3 - a_2x^2 - a_4x - a_6 = 0$在$(x_0, y_0)$在$P$处的Taylor展开为

$$\begin{aligned} &f(x,y)-f(x_0,y_0) \\ &\quad = [(y - y_0) - \alpha(x - x_0)][(y - y_0) - \beta(x - x_0)] - (x - x_0)^3 \end{aligned}$$

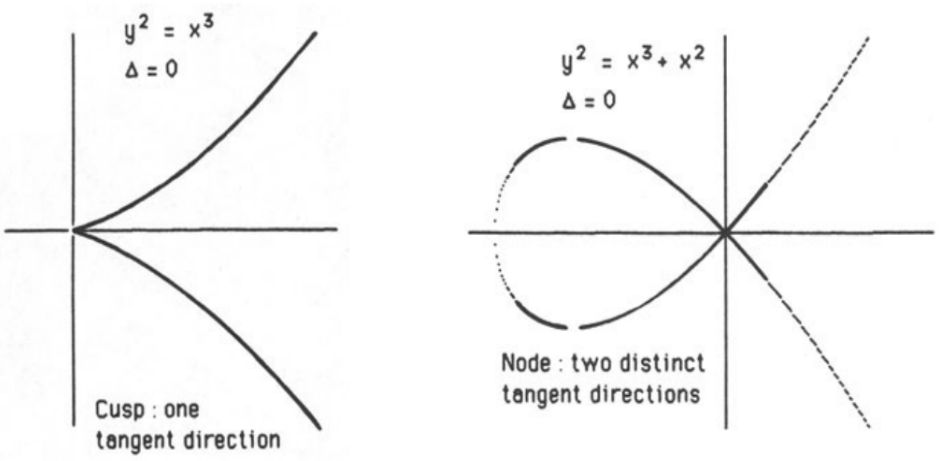
当$\alpha \neq \beta$时，称P是一个节点(node)，此时曲线在P处的切线为

$$y - y_0 = \alpha(x - x_0) \text{ 和 } y - y_0 = \beta(x - x_0)$$

当$\alpha = \beta$时，称P是一个尖点(cusp)，此时曲线在P处的切线为

$$y - y_0 = \alpha(x - x_0)$$

这一事实可以形象地总结为下面两张图：



下面的事实表明，奇异的曲线某种意义上非常简单。

命题. 设E是*Weierstrass*方程定义的一条奇异曲线。则存在度为1的有理映射 $\phi : E \to \mathbb{P}^1$，即$E$ 与 $\mathbb{P}^1$双有理等价*(birational equivalent)*。

证明. 通过线性坐标变换，可以不妨假设奇异点为$(0,0)$。从而方程可以化为

$$y^2 + a_1xy = x^3 + a_2x^2$$

令

$$\phi : E \to \mathbb{P}^1$$

$$(x, y) \mapsto [x, y], \text{ 即 } [x, y, z] \mapsto [\frac{x}{z}, \frac{y}{z}]$$

令$t = \dfrac{y}{x} \in \bar{K}(\mathbb{P}^1)$,则

$$\phi^* : \bar{K}(\mathbb{P}^1) \to \bar{K}(E)$$

$$t \mapsto \frac{y}{x}$$

为了证明 $deg\phi = 1$,只需证明ϕ^*是满射，这等价于$\bar{K}(E) = \bar{K}(y/x)$，而由曲线方程知

$$(\frac{y}{x})^2 + a_1(\frac{y}{x}) = x + a_2$$

因此$x \in \bar{K}(y/x)$，进而$y \in \bar{K}(y/x)$,从而$\bar{K}(y/x) = \bar{K}(E)$. □

与Weierstrass方程相关的另一个非常重要的量便是不变微分(invariant differential).

定义. *与Weierstrass方程$y^2+a_1xy+a_3y=x^3+a_2x^2+a_4x+a_6$相关的不变微分为*

$$\omega=\frac{dx}{F_y}=-\frac{dy}{F_x}$$

其中$F=y^2+a_1xy+a_3y-x^3-a_2x^2-a_4x-a_6$

可以证明如果Weierstrass方程定义的曲线光滑，则有

$$div\omega=0$$

从而$2g-2=deg(div\omega)=0, g=1$。从而$E$是一条椭圆曲线。从而我们得知Weierstrass方程如果非奇异，则定义了一条椭圆曲线；如果奇异，那么定义的曲线和$\mathbb{P}^1$双有理等价。

反过来，是否任何椭圆曲线都可以用一个Weierstrass方程表示呢？答案是肯定的。在历史上，对椭圆积分及其逆的研究促使人们研究复平面上的双周期亚纯函数，而Weierstrass是这方面绝对的专家。他构造了著名的Weierstrass $\wp$函数，这是一个极点次数为2的双周期亚纯函数，它其中一个非常有趣的性质是，$\wp(z)$和它的导数$\wp'(z)$满足方程

$$\wp'(z)^2=4\wp(z)^3-g_2\wp(z)-g_3$$

其中$g_2,g_3\in\mathbb{C}$是常数。因此我们可以构造映射

$$\begin{aligned}\phi:&\mathbb{C}/\Lambda\to\mathbb{CP}^2\\&z\mapsto[\wp(z),\wp'(z),1]\end{aligned}$$

映射的像满足方程$y^2=4x^3-g_2x-g_3$，它的射影闭包$E:y^2z=4x^3-g_2xz^2-g_3z^3$是一个紧黎曼面。可以证明，$\phi:\mathbb{C}/\Lambda\to E$不仅是一个紧黎曼面之间的同构，而且是群的同构，因此是紧李群之间的同构。注意到$\mathbb{C}/\Lambda$是一个亏格为1的紧黎曼面，从而Weierstrass的椭圆函数理论证明了任何亏格为1的紧黎曼面可以用$\mathbb{CP}^2$中的Weierstrass方程$y^2=4x^3-g_2x-g_3$表示。我们在这里考虑一般的代数曲线的情形，虽然这里没有椭圆函数，但相似之处在于都考虑了极点为2和3的函数。下面的证明将Riemann-Roch定理的强大展现得淋漓尽致。

定理. *任何定义在K上的椭圆曲线E/K都$K-$同构于$\mathbb{P}^2$中由某个系数在K中的Weierstrass方程定义的曲线。*

证明. 由Riemann-Roch定理，我们有

$$l(n(O))=dim\mathscr{L}(n(O))=n,\quad 对n\geq 1$$

从而存在$x,y\in\bar{K}(E)$，使得

$$\mathscr{L}(2(O))=span\{1,x\},\mathscr{L}(3(O))=span\{1,x,y\}$$

不难推出$ord_O(x)=-2, ord_O(y)=-3$。考虑$1,x,y,x^2,xy,y^2,x^3$共7个函数，他们在O处的极点次数均不超过6,从而他们均属于$\mathscr{L}(6(O))$,从而他们线性相关，即存在不全为0的$A_i\in K$，使得

$$A_1+A_2x+A_3y+A_4x^2+A_5xy+A_6y^2+A_7x^3=0$$

注意到A_6, A_7均不为0,否则上式的每一项在O处的次数都不相同，他们的和不可能为0。既然A_6, A_7不为0，那么就可以通过线性的坐标变换改变x^3和y^2前的系数使方程化为Weierstrass方程。即$x, y \in K(E)$满足方程

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$$

设这个Weierstrass方程在$\mathbb{P}^2$中定义的曲线为C。接下来我们定义映射

$$\begin{aligned}\phi : E &\to \mathbb{P}^2\\ P &\mapsto [x(P), y(P), 1]\end{aligned}$$

知映射的像落在C上，因此得到

$$\phi : E \to C$$

为了说明这是一个同构，我们只需要说明$deg\phi = 1$且C是光滑曲线。

首先来证明$deg\phi = 1$，即$\phi * K(C) = K(E)$，即$K(x, y) = K(E)$。为此，我们考虑映射

$$\begin{aligned}\psi : E &\to \mathbb{P}^1\\ P &\mapsto [x(P), 1]\end{aligned}$$

我们计算这个映射的度。由公式

$$deg\psi = \sum_{P\in\phi^{-1}(\infty)} e_\phi(P)$$

得 $deg\psi = e_\phi(O) = ord_O(\phi^* t_\infty) = ord_O(\phi^*(\frac{y}{x})) = ord_O(1/x) = 2$
即$[K(E) : K(x)] = 2$。同理可证$[K(E) : K(y)] = 3$ 。从而$[K(E) : K(x, y)] = 1, K(E) = K(x, y)$。

再来说明C是一个光滑曲线。如果C不光滑，那么存在度为1的有理映射$\psi : C \to \mathbb{P}^1$，将其与$\phi$复合得到

$$\psi \circ \phi : E \to \mathbb{P}^1$$

该映射的度为$deg(\psi \circ \phi) = deg\psi \cdot deg\phi = 1$。从而这是一个同构。但$\mathbb{P}^1$的亏格为0,矛盾。

最后，由于$ord_O x = 2, ord_O y = 3$,故ϕ将O映到无穷远点$[0, 1, 0]$。 □

3.1.2 Legendre型

在平时的应用当中，Weierstrass方程可能不太方便，因为它的形式还是相对复杂。我们在这一章介绍一个特殊的Weierstrass方程——Legendre型。

定义 (Legendre型)**.** 一个*Weierstrass*方程是*Legendre*型，如果它形如

$$y^2 = x(x - 1)(x - \lambda)$$

我们希望将Weierstrass方程都化为Legendre方程，幸运的是这件事在大多数情况都能办到。

定理. 设$charK \neq 2$ 则任何椭圆曲线E/K都同构于由*Legendre*型

$$y^2 = x(x - 1)(x - \lambda)$$

定义的椭圆曲线。其中$\lambda \in \bar{K}, \lambda \neq 0, 1.$

证明. 首先E可以由某个Weierstrass方程

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$$

给出。用$((x, 2y + a_1x + a_3)$替换(x, y)，从而方程化为

$$y^2 = 4x^3 + b_2x^2 + 2b_4x + b_6$$

用$(4x, 4y)$替换(x, y)，再将关于x的三次方程因式分解，得到

$$y^2 = (x - e_1)(x - e_2)(x - e_3)$$

最后再令$x = (e_2 - e_1)x' + e_1, y = (e_2 - e_1^{3/2})y'$，得到Legendre型。 □

3.2 椭圆曲线的群结构

椭圆曲线拥有群结构是一个伟大的发现。这件事还得从椭圆曲线上的点之间的操作谈起。一个有理系数的方程

$$y^2 = x^3 + ax + b$$

上的两个有理点P, Q的连线是一条有理直线，它交曲线于第三个点，记作$P * Q$。由根与系数的关系知，$P * Q$也是有理点。记$P * Q$关于x轴反射的点为$P + Q$。

在17世纪，Bachet和Fermat描述了如何将一个点乘以2的代数公式，牛顿展示了曲线上的弦和切线的几何和Bachet、Fermat的公式的联系。在19世纪，Jacobi和Weierstrass将这些工作与椭圆积分和椭圆函数联系起来，直到最后1901年Poincaré统一了以上的工作并将其推广到代数曲线。Poincaré的工作证明了以上定义的加法将赋予椭圆曲线有理点构成的集合一个加法群的结构，并证明其加法单元为无穷远点O。

我们接下来较为严格的讨论椭圆曲线的加法结构。

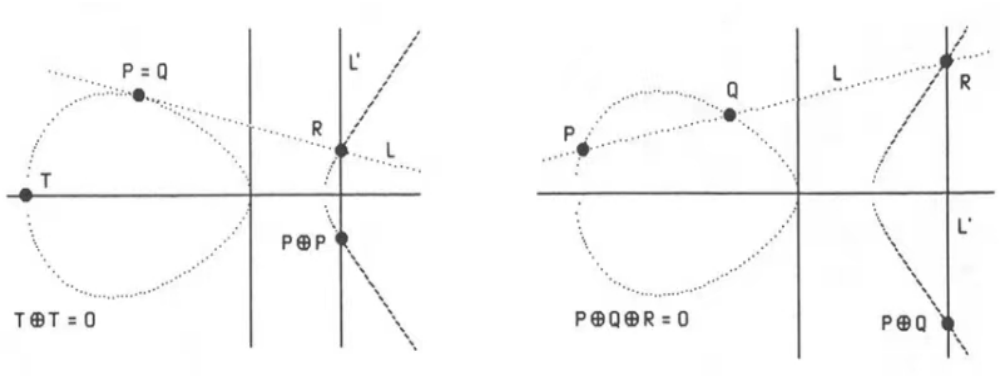
定理 (椭圆曲线的群结构)**.** *对于椭圆曲线(E, O),它有Weierstrass方程*

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$$

记$O = [0, 1.0]$为无穷远点。对于曲线上两点P, Q,经过P, Q的直线(如果P, Q重合，则取P处的切线)交曲线于第三个点$P * Q$，$P * Q$与O连线的交点记为$P + Q$。同时对任意$P \in E$,都存在唯一的$-P \in E$，使得$P + (-P) = O$。此时

$$E \times E \to E$$
$$(P, Q) \mapsto P + Q$$

赋予了E上点的集合一个阿贝尔群结构，O为加法单元。



细心的读者可能注意到，椭圆曲线可能有不同的Weierstrass方程，而上面定义的加法需要用到方程的代数结构，是否这意味着(E,O)上的群结构有很多种？下面我们将说明，对于确定了加法单元的椭圆曲线(E,O)，由以上方式定义的阿贝尔群结构不依赖于曲线方程的选取。为此我们需要一系列的引理和命题。

引理. 设C是一个亏格为1的光滑曲线，则$(P)\sim(Q)$当且仅当$P=Q$。

证明. 设$divf=(P)-(Q)$，对某个$f\in\bar{K}(C)$。从而$f\in\mathscr{L}((Q))$。由Riemann-Roch定理，$dim\mathscr{L}((Q))=l((Q))=1$。又由于$\mathscr{L}((Q))$包含$\bar{K}$,故恰有$\mathscr{L}((Q))=\bar{K}$。从而$f\in\bar{K}$，$P=Q$。 □

命题. 设(E,O)是椭圆曲线。
*(a)*对任意除子$D\in Div^0(E)$,存在唯一的点$P\in E$使得

$$D\sim(P)-(O)$$

这定义了映射

$$\sigma:Div^0(E)\to E$$

(b) σ是满射
(c) 设$D_1,D_2\in Div^0(E)$，则

$$\sigma(D_1)=\sigma(D_2)\iff D_1\sim D_2$$

因此σ诱导了双射

$$\sigma:Pic^0(E)\xrightarrow{\sim}E$$

(d) σ的逆为

$$\kappa:E\xrightarrow{\sim}Pic^0(E)$$
$$P\mapsto(P)-(O)\text{所在的类}$$

证明. (a) 由Riemann-Roch定理，$imL(D+(O))=1$，设它被某个$f\in barK(E)^*$张成。根据定义，有

$$div(f)\geq-D-(O)$$

从而存在$P\in E$使得$div(f)=D+(P)-(O)$，从而

$$D\sim(P)-(O)$$

存在性得证。唯一性由引理即得。
(b) $\sigma((P)-(O))=P$
(c),(d)由定义即得 □

我们现在来证明

定理. 设(E,O)为一个椭圆曲线，它由一个*Weierstrass*方程给出。则之前由直线与曲线相交定义的出的”几何群法则“与上面命题(c)中的双射σ诱导的群法则相同。

证明. 任给$P,Q\in E$。我们只需证明

$$\kappa(P)+\kappa(Q)=\kappa(P+Q)$$

设

$$f(x,y,z)=ax+by+cz=0$$

为 $\mathbb{P}^2$中经过P,Q的直线，并设R为该直线与曲线交的第三点。再设

$$f'(x,y,z)=a'x+b'y+c'z=0$$

为经过O,R的直线。我们有

$$div(f/z)=(P)+(Q)+(R)-3(O)$$

$$div(f'/z)=(O)+(R)+(-R)-3(O)=(P+Q)-2(O)$$

从而

$$(P)+(Q)-(O)-(P+Q)=div(f/f')\sim 0$$

从而有

$$\kappa(P+Q)=\kappa(P)+\kappa(Q)$$

□

3.3 椭圆曲线之间的映射

定义. 设E_1,E_2都是椭圆曲线。一个E_1,E_2之间的同源映射*(isogeny)*是一个态射

$$\phi:E_1\to E_2$$

满足$\phi(O)=O$。E_1,E_2称作是同源的$isogenous$如果它们之间存在一个同源映射ϕ且$\phi(E_1)\neq O$,即这个同源映射不是常值映射。

由于曲线之间的非常值态射总是满射，所以对于一个同源映射$\phi:E_1\to E_2$，有$\phi(E_1)=O$或E_2。对于非常值的曲线之间的映射，$\bar{K}(E_2)/\phi^*\bar{K}(E_1)$是一个有限扩张，将其定义为$\phi$的度。同时我们可以定义$\phi$的可分度，不可分度等。对于常值映射，记作[0],我们约定$deg[0]=0$。

由于椭圆曲线具有群结构，所以$E_1\to E_2$之间同源映射构成的集合$Hom(E_!,E_2)$具有群结构。具体来说，对于$\phi,\psi\in Hom(E_1,E_2)$,定义$\phi+\psi$为

$$(\phi+\psi)(P)=\phi(P)+\psi(P)$$

我们需要验证$\phi+\psi$仍然是一个同源映射。
首先显然$(\phi+\psi)(O)=O$。现在只需说明$\phi+\psi$是一个态射。事实上可以证明对一个椭圆曲线(E,O)，它上面的加法和逆映射

$$\begin{aligned} +: E\times E\to E \qquad & -: E\to E \\ (P_1,P_2)\mapsto P_1+P_2 \qquad & P\mapsto -P \end{aligned}$$

均是代数簇之间的态射。而$\phi+\psi: E_1\to E_2$是

$$\begin{aligned} E_1 &\to E_2\times E_2 \\ P &\mapsto (\phi(P),\psi(P)) \end{aligned}$$

和

$$\begin{aligned} E_2\times E_2 &\to E_2 \\ (P,Q) &\mapsto P+Q \end{aligned}$$

的复合，从而是一个态射。如果$E_1=E_2$，那么令$End(E)=Hom(E,E)$。在它上面可以定义乘法为映射的复合：

$$(\phi\psi)(P):=\phi(\psi(P))$$

可以证明，$End(E)$上定义的加法和乘法将其变为一个环。 $End(E)$中可逆的元素在乘法下构成一个群，记作$Aut(E)$。

当然，研究当中我们更关注定义在一些特殊域上的曲线，因此若E,E_1,E_2是定义在K上的椭圆曲线，可以类似地定义

$$Hom_K(E_1,E_2),\ End_K(E),\ Aut_K(E)$$

例. 设E是一个椭圆曲线，$P\in E$。则可以定义

$$\begin{aligned} \tau_P: E &\to E \\ Q &\mapsto P+Q \end{aligned}$$

知这是E的一个自同构，它的逆为τ_{-P}。

例 (乘m映射)**.** 定义

$$[m]: E\to E$$

$$[m]P=\begin{cases} P+P+...+P(m项) & 如果 m\geq 0 \\ [-m](-P) & 如果 m<0 \end{cases}$$

注意到若E是定义在K上的，则$[m]$是定义在K上的。

下面是关于$[m]$和$End(E)$的一些基本的性质。

命题. *(a)*设E/K是定义在K上的椭圆曲线，$m\in\mathbb{Z}, m\neq 0$。则映射

$$[m]: E\to E$$

不是常值映射。
(b) 设E_1,E_2是椭圆曲线。则同源映射群$Hom(E_1,E_2)$是一个无挠*(torsion-free)*$\mathbb{Z}$模。
(c) 设E是椭圆曲线。则$End(E)$是一个特征 0 的整环*(*不要求交换*)*。

对于一个椭圆曲线E，它的同源自映射环$End(E)$必定包含$[m]$，因此了解$[m]$有助于理解整个$EndE$。

定义. 设E是椭圆曲线，$m \in \mathbb{Z}, m \neq 0$。定义$E$的$m-$挠子群*(m-torsion subgroup)*为

$$E[m] = P \in E : [m]P = O$$

定义挠子群*(torsion subgroup)*为所有有限阶点构成的群:

$$E_{tors} = \cup_{m=1}^{\infty} E[m]$$

如果E/K是定义在K上的，我们关心$K-$有理点，可以相应定义$E_{tors}(K)$。

设$charK = 0$。则

$$[\quad] : \mathbb{Z} \to End(E)$$
$$m \mapsto [m]$$

是一个环同态。由以上的命题(a)知这是一个单射。很多情况下，这是一个同构，也就是说

$$End(E) = \{[m] : m \in \mathbb{Z}\} \cong \mathbb{Z}$$

如果$End(E)$严格比$\mathbb{Z}$大，则称E有复乘(complex multiplication)。复乘理论起源于"Kronecker的青春之梦
(Kronecker's Jugendtraum)。Kronecker的青春之梦致力于通过加入特殊函数的特殊值来构造数域的阿贝尔扩张。由Kronecker-Weber定理，有理数域$\mathbb{Q}$的任何阿贝尔扩张一定包含在某个分圆扩张$\mathbb{Q}(\zeta)$中。因此$\mathbb{Q}$在$\bar{\mathbb{Q}}$中的极大阿贝尔扩张$\mathbb{Q}^{ab}$可以通过添加单位根得到。对于一般的数域K,现在还尚且没有找到其在$\bar{\mathbb{Q}}$中的极大阿贝尔扩张的方法，但可以对虚二次域$\mathbb{Q}(\sqrt{-D})$做到这件事。Kronecker在于1880年3月15日寄给Dedekind的信中写道：

> —- the Abelian equations with square roots of rational numbers are exhausted by the transformation equations of elliptic functions with singular modules, just as the Abelian equations with integral coefficients are exhausted by the cyclotomic equations.

具体来说，构造一个定义在$\mathbb{Q}$上的椭圆曲线$E/\mathbb{Q}$使得$Frac(End(E)) \cong \mathbb{Q}(\sqrt{-D})$，再将这个椭圆曲线的$j-$不变量和挠点的坐标加入。

例. 设$charK \neq 2$,设E/K为椭圆曲线

$$E; y^2 = x^3 - x$$

除了$\mathbb{Z}$，$End(E)$还包含一个元素，我们记为$[i]$:

$$[i] : (x, y) \mapsto (-x, iy)$$

这里$i \in \bar{K}$是一个四次本原单位根。从而E有复乘。同时我们注意到$[i]$是定义在K上的当且仅当$i \in K$。从而即使E是定义在K上的，$End_K(E)$也有可能严格小于$End(E)$。

容易验证$[i] \circ [i] = [-1]$，故我们可以构造环同态

$$\mathbb{Z}[i] \to End(E)$$
$$m + ni \mapsto [m] + [n][i]$$

可以证明，在$charK = 0$时，这是一个同构。从而我们可以得到

$$Aut(E) = \{\pm 1, \pm i\}$$

读者可能在一开始定义同源映射(isogeny)的时候就有疑问：同源映射把加法单元映到加法单元，这么定义很像是群同态的定义。有没有可能，一个同源映射是一个群同态？答案是肯定的。

定理. 设

$$\phi : E_1 \to E_2$$

是一个同源映射。则对任意$P, Q \in E_1$，有

$$\phi(P + Q) = \phi(P) + \phi(Q)$$

证明. 如果ϕ是常值映射，即$\phi(P) = O, \forall P \in E_1$，则命题显然成立。下面设$\phi$不是常值映射。回忆我们曾经定义过的映射

$$\begin{aligned} \phi_* : Div(E_1) &\to Div(E_2) \\ (P) &\mapsto (\phi P) \end{aligned}$$

结合$\phi_*(divf) = div(\phi_* f)$知$\phi_*$诱导了映射

$$\phi_* : Pic^0(E_1) \to Pic^0(E_2)$$

另一方面，我们有双射

$$\begin{aligned} \kappa_i : E_i &\to Pic(E_i), \quad i = 1, 2 \\ P &\mapsto (P) - (O)\text{所在的等价类} \end{aligned}$$

由$\phi(O) = O$知下面的图表交换

$$\begin{array}{ccc} E_1 & \xrightarrow[\kappa_1]{\cong} & Pic^0(E_1) \\ \downarrow{\scriptstyle \phi} & & \downarrow{\scriptstyle \phi_*} \\ E_2 & \xrightarrow[\kappa_2]{\cong} & Pic^0(E_2) \end{array}$$

□

推论. 设$\phi : E_1 \to E_2$是一个非零(非常值)同源映射，则

$$ker\phi = \phi^{-1}(O)$$

是一个E_1的一个有限子群。

回忆代数数论中素理想的分歧。对于数域的扩张L/K,设$\mathfrak{p}$是K的一个非零素理想。则有

$$\mathfrak{p}\mathscr{O}_L = \mathfrak{P}_1^{e_1} ... \mathfrak{P}_l^{e_l}$$

其中$\mathfrak{P}_i$为L中的素理想。当L/K为Galois扩张时，我们有$e_1 = ... = e_l, f_1 = ... = f_l$，其中$f_i = [\mathscr{O}_L/\mathfrak{P}_i : \mathscr{O}_K/\mathfrak{p}]$被称为$\mathfrak{P}_i$的inertia degree. 下面的结果和代数数论中的结果有几分相似。

定理. 设$\phi : E_1 \to E_2$是一个非零的同源映射。
(a) 对任意$Q \in E_2$,

$$\#\phi^{-1}(Q) = deg_s\phi$$

进一步，对任意$P \in E_1$，

$$e_\phi(P) = deg_i\phi$$

(b) 映射

$$ker\phi \to Aut[\bar{K}(E_1)/\phi^*\bar{K}(E_2)]$$
$$T \mapsto \tau_T^*$$

是一个群同构。这里τ_T^*是由$\tau_T^* : \bar{K}(E_1) \to \bar{K}(E_1)$诱导的映射。
*(c)*设ϕ可分。则ϕ非分歧，

$$\#ker\phi = deg\phi$$

且$\bar{K}(E_1)/\phi^*\bar{K}(E_2)$是一个*Galois*扩张。

在证明之前，我们看到(b)和代数拓扑中覆叠空间理论中的deck transformation十分相似，不由感叹数学的奇妙。

证明. (a).我们在之前的章节提到了除了有限个E_2上的点，都有

$$\#\phi^{-1}(Q) = deg_s\phi$$

对于两个点$Q, Q' \in E_2$，我们选取$R \in E_1$，使得$\phi(R) = Q' - Q$。由于ϕ是一个群同态，所以有以下的双射

$$\phi^{-1}(Q) \to \phi^{-1}(Q')$$
$$P \mapsto P + R$$

从而对任意$Q \in E_2$，都有$\phi^{-1}(Q) = deg_s\phi$
现在设$P, P' \in E_1$满足$\phi(P) = \phi(P') = Q$。令$R = P' - P$。则$\phi(R) = O$，从而$\phi \circ \tau_R = \phi$。进而有

$$e_\phi(P) = e_{\phi\circ\tau_R}(P) = e_\phi(\tau_R P) \cdot e_{\tau_R}(P) = e_\phi(P')$$

从而$\phi^{-1}(Q)$中的点有着相同的分歧指数。由

$$\sum_{P\in\phi^{-1}(Q)} e_\phi(P) = deg\phi$$

知$e_\phi)(P) \cdot \#\phi^{-1}(Q) = deg\phi = deg_s\phi \cdot deg_i\phi$，结合之前所证，得$e_\phi(P) = deg_i\phi$。

(b)首先证明确实可以诱导，即我们需要说明$\tau_T^* : \bar{K}(E_1) \to \bar{K}(E_1)$固定$\phi^*\bar{K}(E_2)$。这是因为对任意$g \in \bar{K}(E_2)$，有

$$\tau_T^* \circ \phi^* g = (\phi \circ \tau_T)^* g = g \circ \phi \circ \tau_T = g \circ \phi = \phi^* g$$

容易发现这是一个群同态。由Galois理论，$\#Aut[\bar{K}(E_1)/\phi^*\bar{K}(E_2)] \le deg_s\phi$，结合$\#ker\phi = deg_s\phi$，从而我们只需证明这是一个单射。设$\tau_T^*$固定$\bar{K}(E_1)$,则$\forall f \in \bar{K}(E_1), f(O) = f(T)$。从而$T = O$。

(c)由ϕ可分知$deg_s\phi = deg\phi$，$deg_i\phi = 1$，从而$\forall P \in E_1, e_\phi(P) = deg_i\phi = 1$，即有$\phi$非分歧。且$\#ker\phi = deg_s\phi = deg\phi$。由(b)知

$$\#Aut[\bar{K}(E_1)/\phi^*\bar{K}(E_2)] = \#ker\phi = deg\phi = [\bar{K}(E_1) : \phi^*\bar{K}(E_2)]$$

由此可知$\bar{K}(E_1)/\phi^*\bar{K}(E_2)$是一个Galois扩张。 □

我们有推论:

推论. 设$\phi : E_1 \to E_2$ 和$\psi : E_1 \to E_3$为非零的同源映射。设ϕ可分。如果

$$ker\phi \subset ker\psi$$

则存在唯一的同源映射

$$\lambda : E_2 \to E_3$$

使得$\psi = \lambda \circ \phi$。

证明. 由ϕ是可分的知$\bar{K}(E_1)/\phi^*\bar{K}(E_2)$是Galois扩张。由$ker\phi \subset ker\psi$知

$$Gal(\bar{K}(E_1)/\phi^*\bar{K}(E_2)) \subset Aut[\bar{K}(E_1)/\psi^*\bar{K}(E_3)]$$

这表明

$$\psi^*\bar{K}(E_3) \subset \phi^*\bar{K}(E_2) \subset \bar{K}(E_1)$$

因此我们有唯一的$\lambda : E_2 \to E_3$，使得

$$\psi^*\bar{K}(E_3) = \phi^*(\lambda^*\bar{K}(E_3))$$

从而

$$\psi = \lambda \circ \phi$$

最后，λ是同源映射是因为$\lambda(O) = \lambda(\phi(O)) = \psi(O) = O$。 □

我们在这一小节给出最后一个定理。

定理. 设E是一个椭圆曲线。Φ是E的一个有限子群，则存在唯一的(同构意义下)的椭圆曲线E'和一个可分的同源映射

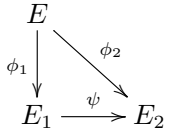
$$\phi : E \to E'$$

使得 $ker\phi = \Phi$。

由这个定理，结合上面的推论，我们便有以下双射：

$$\begin{aligned} \{(E', \phi) | E'\text{为椭圆曲线}, \phi : E \to E'\text{可分的同源映射}\}/\sim \quad &\longleftrightarrow \{E\text{的有限子群}\} \\ (E', \phi) &\longmapsto ker\phi \end{aligned}$$

其中$\sim$表示等价关系：(E_1, ϕ_1)和(E_2, ϕ_2)等价当且仅当存在同源同构 $\psi : E_1 \xrightarrow{\sim} E_2$,使得下图交换



3.4 不变微分

这一章我们继续讨论和椭圆曲线有关的量。之前我们提到，对于椭圆曲线E/K，如果它的Weierstrass方程为

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$$

则不变微分

$$\omega = \frac{dx}{2y + a_1x + a_3}$$

满足$div(\omega) = 0$。现在我们来解释它名字的由来。

命题. *对任意$Q \in E$，有*

$$\tau_Q^*\omega = \omega$$

证明. 由于Ω_E是一个一维的$\bar{K}(E)-$的线性空间，故存在依赖与Q的函数$a_Q \in \bar{K}(E)$，使得

$$\tau_Q^*\omega = a_Q\omega.$$

由于$\tau_Q : E \to E$是一个同构，故τ_Q^*是τ_Q^*的逆，从而$\tau_Q^*\omega \neq 0$，进而$a_Q \neq 0$. 我们有

$$\begin{aligned} div(a_Q) &= div(\tau_Q^*\omega) - div(\omega) \\ &= \tau^* div(\omega) - div(\omega) \\ &= 0 \qquad \text{因为} div(\omega) = 0. \end{aligned}$$

从而$a_Q \in \bar{K}^*$.考虑映射

$$\begin{aligned} f : E &\to \mathbb{P}^1 \\ Q &\mapsto [a_Q, 1] \end{aligned}$$

我们现在来证明这是一个有理映射，也就是说要证明a_Q是关于Q的有理函数。我们利用$\omega = \frac{dx}{2y+a_1x+a_3}$以及$\tau_Q^*\omega = a_Q\omega$得

$$\frac{dx(P+Q)}{2y(P+Q) + a_1x(P+Q) + a_3} = a_Q \cdot \frac{dx(P)}{2y(P) + a_1x(P) + a_3}$$

利用加法公式用关于$x(P), x(Q), y(P), y(Q)$的有理函数表示出$x(P+Q), y(P+Q)$，将$x(Q)$看成常数，计算$dx(P+Q)$。可以看出，a_Q可以表示成关于$x(P), y(P), x(Q), y(Q)$的有理函数，但又因为它跟P无关，从而它是一个关于$x(Q), y(Q)$的有理函数，这便证明了f是有理映射，进而是一个正则映射。我们知道，两个曲线之间的正则映射如果不是常值映射，则一定是满射。但注意到f的像不包括$[0, 1]$(因为$a_Q \neq 0$)和$[1, 0]$(因为$a_Q \neq \infty$)，从而f必为常值映射。而在$Q = O$时，有$a_Q = 1$。从而$\forall Q \in E, a_Q = 1$。从而

$$\tau_Q^*\omega = \omega$$

□

我们还有如下性质:

命题. *设E, E'是椭圆曲线。设$\phi, \psi : E' \to E$是同源映射。ω为E不变微分。有*

$$(\phi + \psi)^*\omega = \phi^*\omega + \psi^*\omega$$

其中第一个加号表示$Hom(E', E)$中的加法，第二个加号表示$\Omega_{E'}$中的加法。

由这个命题，我们可以的得到

推论 (1)**.** 设$m \in \mathbb{Z}$，E是椭圆曲线，ω是其不变微分。则

$$[m]^*\omega = m\omega$$

推论 (2)**.** 设$charK = p > 0$,设E定义在$\mathbb{F}_q$上，设$\phi : E \to E, (x, y) \to (x^q, y^q)$是*Frobenious*自同态。设$m, n \in \mathbb{Z}$。则映射

$$\phi : m + n\phi : E \to E$$

可分当且仅当$p \nmid m$。

证明. 回忆之前提到过的关于曲线之间映射是否可分的一个判别法：设$\phi : C_1 \to C_2$是曲线之间的非常值映射，则ϕ可分当且仅当映射

$$\phi^* : \Omega_{C_2} \to \Omega_{C_1}$$

非零。设ω是E的不变微分。有

$$(m + n\phi)^*\omega = m\omega + n\phi^*\omega$$

因为ϕ不可分，故$\phi^*\omega = 0$。从而

$$(m + n\phi)^*\omega = m\omega$$

则

$$\begin{aligned} m + n\phi\text{可分} &\iff (m + n\phi)^*\omega \neq 0 \\ &\iff m\omega \neq 0 \\ &\iff p \nmid m. \end{aligned}$$

□

这样我们便可以构造出$End(E)$中的可分映射了，比如$1 - \phi$。

3.5 对偶同源

我们之前研究了椭圆曲线的同源映射(isogeny)。事实上，对于两个椭圆曲线之间的一个同源映射$\phi : E_1 \to E_2$，有一个与之对偶的同源映射。

$$\hat{\phi} : E_2 \to E_1$$

它具体是什么样的呢？与ϕ又有什么联系？

我们知道ϕ诱导了映射

$$\phi^* : Pic^0(E_2) \to Pic^0(E_1)$$

同时我们有群同构

$$\begin{aligned} \kappa_i : E_i &\to Pic^0(E_i) \\ P &\mapsto (P) - (O)\text{所在的类} \end{aligned}$$

我们令$\hat{\phi}$为使得以下图表交换的映射。

$$\begin{array}{ccc} E_2 & \xrightarrow{\hat{\phi}} & E_1 \\ \downarrow{\scriptstyle \kappa_2} & & \downarrow{\scriptstyle \kappa_1} \\ Pic^0(E_2) & \xrightarrow{\phi^*} & Pic^0(E_1) \end{array}$$

现在的问题是，$\hat{\phi}$是否是一个同源映射，或者说，是否是一个有理映射？答案是肯定的。我们接下来将介绍包括这个事实在内的一系列关于$\hat{\phi}$的性质。我们称$\hat{\phi}$为ϕ的对偶同源映射(dual isogeny).

我们证明如下定理：

定理. 设$\phi : E_1 \to E_2$是一个度为m的同源映射，$m \neq 0$。
(a) 存在唯一的同源映射

$$\hat{\phi} : E_2 \to E_1$$

使得

$$\hat{\phi} \circ \phi = [m]$$

. *(b)* $\hat{\phi}$由复合

$$\begin{aligned} E_2 \to Div^0(E_2) &\xrightarrow{\phi^*} Div^0(E_1) \xrightarrow{sum} E_1 \\ Q \mapsto (Q) - (O) &\qquad \sum n_P(P) \mapsto \sum [n_P]P \end{aligned}$$

给出。

证明. (a) 先说明唯一性。假设$\hat{\phi}'$也满足$\hat{\phi}' \circ \phi = [m]$。从而有

$$(\hat{\phi} - \hat{\phi}') \circ \phi = [0]$$

由ϕ非零知$\hat{\phi} = \hat{\phi}'$。唯一性得证。
再来说明存在性。注意到，如果$\psi : E_2 \to E_3$另一个非零的同源映射，$deg\psi$，且$\hat{\phi}, \hat{\psi}$均存在。从而

$$\begin{aligned} \hat{\phi} \circ \hat{\psi} \circ \psi \circ \phi &= \hat{\phi} \circ [n] \circ \hat{\phi} \\ &= [n] \circ \hat{\phi} \circ \hat{\phi}' \\ &= [n] \circ [m] \\ &= [mn] = [deg(\psi \circ \phi)] \end{aligned}$$

从而$\psi \hat{\circ} \phi$也存在。而我们知道每个两个光滑曲线之间的映射$f : C_1 \to C_2$总是可以分解成

$$C_1 \to C_1^{(q)} \to C_2$$

第一个映射是Frobenius映射，第二个是可分映射。从而我们只需对于可分映射ϕ和Frobenius映射证明命题。情况1：ϕ是可分映射。我们有

$$\#ker\phi = deg_s\phi = deg\phi = m$$

从而

$$ker\phi \subset ker[m]$$

进而存在唯一同源映射

$$\hat{\phi} : E_2 \to E_1$$

使得 $[m] = \hat{\phi} \circ \phi$。

情况2：ϕ是Frobenius映射，设其为$q = p^e$次Frobenius映射(即映射$(x, y) \mapsto (x^q, y^q)$)。它是$p$次Frobenius映射的$e$次复合。故我们只需对$p$次Frobenius映射证明命题。设$\omega$是不变微分。则$[p]^*\omega = p\omega = 0$。这表明$\phi$不可分，从而它可以的分解中会出现$\phi$:

$$[p] = \psi \circ \phi^l$$

$l \geq 1$。此时令$\hat{\phi} = \psi \circ \phi^{l-1}$即可。
(b)直接计算即可。记复合映射为f。则

$$\begin{aligned} f(Q) &= \sum_{P \in \phi^{-1}(Q)} [e_\phi(P)]P - \sum_{T \in \phi^{-1}(O)} e_\phi(T) \\ &= [deg_i\phi] \cdot (\sum_{P \in \phi^{-1}(Q)} P - \sum_{T \in \phi^{-1}(O)} T) \\ &= [deg_i\phi] \circ [deg_s\phi]P \qquad \forall P \in \phi^{-1}(Q) \\ &= [deg\phi]P \end{aligned}$$

而$\hat{\phi}(Q) = p\hat{h}i(\phi(P)) = [deg\phi]P, \qquad \forall P \in \phi^{-1}(Q)$
这便证明了$f = \hat{\phi}$。 □

接下来我们给出$\hat{\phi}$的若干性质。

命题. 设$\phi : E_1 \to E_2$是一个同源映射。
*(a)*设$deg\phi = m$。则

$$\hat{\phi} \circ \phi = [m]$$

$$\phi \circ \hat{\phi} = [m]$$

*(b)*设$\lambda : E_2 \to E_3$是另外一个同源映射，则

$$\widehat{\lambda \circ \phi} = \hat{\phi} \circ \hat{\lambda}$$

(c) 设$\psi : E_1 \to E_2$是另外一个同源映射，则

$$\widehat{\phi + \psi} = \hat{\phi} + \hat{\psi}$$

*(d)*对任意$m \in \mathbb{Z}$,

$$\hat{[m]} = [m], \qquad 且 deg[m] = m^2$$

(e) $\deg \hat{\phi} = deg\phi$
(f) $\hat{\hat{\phi}} = \phi$

回顾线性代数中学过的二次型，它是从一个$\mathbb{R}-$线性空间到$\mathbb{R}$的一个函数，还满足一些性质。其实我们也可以定义阿贝尔群上的二次型。

定义. 设A是一个阿贝尔群。一个函数

$$d : A \to \mathbb{R}$$

是一个二次型*(quadratic form)*，如果 *(i)* $d(\alpha) = d(-\alpha), \forall \alpha \in A$
(ii) 配对

$$A \times A \to \mathbb{R}$$
$$(\alpha, \beta) \mapsto d(\alpha + \beta) - d(\alpha) - d(\beta)$$

是双线性的。

一个二次型是正定的，如果
(iii) $d(\alpha) \geq 0, \forall \alpha \in A$
(iv) $d(\alpha) = 0 \iff \alpha = 0$

由以上定义，我们有

命题. 设E_1, E_2是椭圆曲线，则

$$deg : Hom(E_1, E_2) \to \mathbb{Z}$$

是一个正定的二次型。

证明. 只需证明

$$\langle \phi, \psi \rangle = deg(\phi + \psi) - deg(\phi) - deg(\psi)$$

是双线性的。但我们有

$$\begin{aligned}[\langle \phi, \psi \rangle] &= [deg(\phi + \psi)] - [deg(\phi)] - [deg(\psi)] \\ &= (\hat{\phi} + \hat{\psi}) \circ (\phi + \psi) - \hat{\phi} \circ \phi - \hat{\psi} \circ \psi \\ &= \hat{\phi} \circ \psi + \hat{\psi} \circ \phi\end{aligned}$$

由上面的(c)知确实是双线性的。 □

由此我有以下非常重要的推论。

推论. 设E为椭圆曲线。
(a) 若$charK = 0$或m与$charK$互素，则

$$E[m] \cong (\mathbb{Z}/m\mathbb{Z}) \times (\mathbb{Z}/m\mathbb{Z})$$

(b) 若$charK = p > 0$。则

$$E[p^e] \cong \{O\}, \qquad \forall e = 1, 2, ...; \text{或者}$$
$$E[p^e] \cong \mathbb{Z}/p^e\mathbb{Z}, \qquad \forall e = 1, 2, ...$$

证明. (a) 设ω是E的不变微分，则

$$[m]^*\omega = m\omega \neq 0$$

表明$[m]$可分，从而

$$\#E[m] = ker[m] = deg_s[m] = deg[m] = m^2$$

同时注意到对任意$d \mid m, d \in \mathbb{Z}_+$，也有$\#E[d] = d^2$，且$E[d] \subset E[m]$，故不难得知只能有

$$E[m] \cong (\mathbb{Z}/m\mathbb{Z}) \times (\mathbb{Z}/m\mathbb{Z})$$

(b) 设ϕ是p次Frobenius映射，则$deg\phi = p$，进而

$$\begin{aligned}\#E[p^e] &= deg_s[p^e] \\ &= (deg_s\hat{\phi} \circ \phi)^e \\ &= (deg_s\hat{\phi})^e\end{aligned}$$

又因为$deg\hat{\phi} = deg\phi = p$，故$deg_s\hat{\phi} = 1$或$p$。从而当$\hat{\phi}$不可分时，$\#E[p^e] = 1$; 当$\hat{\phi}$可分时，$\#E[p^e] = p^e$。由此不难得到

$$\begin{aligned}&E[p^e] \cong \{O\}, \qquad \forall e = 1, 2, ...; \text{或者} \\ &E[p^e] \cong \mathbb{Z}/p^e\mathbb{Z}, \qquad \forall e = 1, 2, ...\end{aligned}$$

□

Chapter 4

有理点的计数

4.1 椭圆曲线上的有理点

在这一章我们约定K是一个特征p的完美域，q是p的幂。

设$K = \mathbb{F}_q$是有限域，E/K是一个椭圆曲线。我们希望知道$E(K)$有多少个点。设E/K的系数在K中的Weierstrass方程为

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$$

选定$x \in K$，y满足一个二次方程，最多有两个解在K中。因此有一个$\#E(K)$有一个粗略的上界$2q+1$。但凭“直觉”，随机选取$x \in K$，大约只有一般的x能使方程在K中有解。这个直觉源自事实：q为奇数时，只有约一半的$a \in K$使得$y^2 = a$在K中有解。所以猜测有理点的个数应该在q左右。当然，这个猜测本质上是没有道理的，如果没有证明那只是凭空想象。下面的定理是E.Artin提出的一个猜想，最终被Hasse于20世纪30年代证明，表明上面的猜测是正确的。

定理. *设E/K是一个定义在$K = \mathbb{F}_q$上的椭圆曲线。则*

$$|\#E(K) - q - 1| = 2\sqrt{q}$$

证明. 取E的一个系数在K中的Weierstrass方程，令

$$\begin{aligned} \phi : E &\to E \\ (x, y) &\mapsto (x^q, y^q) \end{aligned}$$

为$q-$次Frobenius自同态。对于$P \in E(\bar{K})$，

$$P \in E(K) \Longleftrightarrow \phi(P) = P$$

从而$E(K) = ker(1 - \phi)$。而在上一章我们提到$1 - \phi$是一个可分的同源映射，从而

$$\#E(K) = \#ker(1 - \phi) = deg(1 - \phi)$$

下面的引理将给出$deg(1 - \phi)$的估计。 □

引理. 设A是一个阿贝尔群，

$$d : A \to \mathbb{Z}$$

是一个正定的二次型。则对任意$\psi, \phi \in A$，有

$$|d(\psi - \phi) - d(\psi) - d(\phi)| \leq 2\sqrt{d(\psi) \cdot d(\phi)}$$

证明. 对$\psi, \phi \in A$,令

$$L(\psi, \phi) = d(\psi - \phi) - d(\phi) - d(\psi).$$

知L是双线性的。从而对任意$m, n \in \mathbb{Z}$，有

$$0 \leq d(m\psi - n\phi) = m^2 d(\psi) + mnL(\psi, \phi) + n^2 d(\phi)$$

特别的，令

$$m = -L(\psi, \phi), n = 2d(\phi)$$

得

$$0 \leq d(\psi)[4d(\psi)(\phi) - L(\psi.\phi)^2]$$

由此即证。 □

注意到

$$deg : End(E) \to \mathbb{Z}$$

是一个正定的二次型，在引理中令ψ为恒等映射，ϕ为q次Frobenius自同态，即得到

$$|deg(1 - \phi) - 1 - q| \leq 2\sqrt{q}$$

由$\#E(K) = deg(1 - \phi)$得

$$|\#E(K) - q - 1| \leq 2\sqrt{q}.$$

由以上结果，我们有以下得应用。
设K是一个有q个元素的有限域,q为奇数。我们有特征

$$\chi : K^* \to \{\pm 1\}$$

通过定义$\chi(0) = 0$，将χ延拓到K上。$\chi(a) = 1$当且仅当a是平方数。现设$f(x) = ax^3 + bx^2 + cx + d \in K[x]$是一个无重根的三次多项式。从而$E$æ$y^2 = f(x)$是定义在$K$上的椭圆曲线，有

$$|\#E(K) - q - 1| \leq 2\sqrt{q}$$

容易发现

$$\#E(K) = 1 + \sum_{x \in K} (\chi(f(x)) + 1)$$

因此我们得到

$$|\sum_{x \in K} \chi(f(x))| \leq 2\sqrt{q}$$

由于$2\sqrt{q}$相对q可以忽略不计，因此我们可以说，当x遍历K时，$f(x)$基本上一半是平方数，一半不是平方数。

4.2 Weil猜想

4.2.1 Weil猜想的叙述及其历史

1949年，André Weil 作了一系列的关于有限域上代数簇有理点的计数的猜想，包括最著名的Weil猜想。设K是有q个元素的有限域，K_n为K在$\bar{K}$中的n次扩张，即$K_n = \mathbb{F}_{q^n}$。设V/K是定义在K上的射影代数簇, V可以定义为有限个齐次方程的公共零点。记$V(K_n)$为V上坐标在K_n中的点构成的集合, 从而$V(K_n)$是一个有限集。考虑如下$\#V(K_n)$的生成函数:

定义. *V/K的 zeta 函数定义为幂级数*

$$Z(V/K;T) = \exp\left(\sum_{n=1}^{\infty}(\#V(K))\frac{T^n}{n}\right)$$

读者可能会有疑问，为什么不使用更自然的生成函数$\sum \#V(K)T^n$？从下面的例子中我们可以看到原因。

例. *设$V = \mathbb{P}^N$。则V上一点由齐次坐标$[x_0, x_1, ..., x_N]$给出，其中x_i不全为零。不难计算出*

$$\#V(K) = \frac{q^n N + 1 - 1}{q^n - 1} = \sum_{i=0}^{N} q^{ni}$$

从而

$$\begin{aligned}\log(Z(V/K;T)) &= \sum_{n=1}^{\infty}\sum_{i=0}^{N} q^{ni}\frac{T^n}{n} \\ &= \sum_{i=0}^{N}\sum_{n=1}^{\infty} q^{ni}\frac{T^n}{n} \\ &= \sum_{i=0}^{N} -\log(1 - q^i T)\end{aligned}$$

得到

$$Z(\mathbb{P}^N/K;T) = \frac{1}{(1-T)(1-qT)...(1-q^N T)}$$

知 $Z(\mathbb{P}^N/K;T) \in \mathbb{Q}(T)$.

下面我们正式给出Weil猜想。

定理 (Weil猜想)**.** *设K为有q个元素的的有限域，V/K是一个光滑的n维的射影代数簇。*
(a)有理性

$$Z(V/K;T) \in \mathbb{Q}(T)$$

(b)函数方程
存在整数ε(V的欧拉示性数)使得

$$Z(V/K;\frac{1}{q^n T}) = \pm q^{n\varepsilon/2}\, T^{\varepsilon} Z(V/K;T).$$

(c)Riemann假设
存在分解

$$Z(V/K;T) = \frac{P_1(T)...P_{2n-1}(T)}{P_0(T)...P_{2n}(T)}$$

其中$P_i(T) \in \mathbb{Z}[T]$。进一步$P_0(T) = 1 - T, P_{2n}(T) = 1 - q^n T$，且对$1 \leq i \leq 2n-1, P_i(T)$在$\mathbb{C}$上分解为

$$P_i(T) = \prod_j (1 - \alpha_{ij} T),\ |\alpha_{ij}| = q^{i/2}$$

Weil计算了许多特殊的代数簇的例子，将它们的规律总结起来，提出了Weil猜想。Weil证明了猜想对曲线的情形是成立的，其中他利用曲线上的Riemann-Roch定理证明了有理性和函数方程。他利用 Castelnuovo和Severi的一些工作证明了Riemann假设，他的证明后来由Mattuck和 Tate，和Grothendieck简化。Weil还利用阿贝尔簇上Frobenius的l进表示给出了另一个证明，该证明启发了后来的上同调方法。

第一个被引入抽象代数几何的上同调理论是Serre建立的凝聚层上同调。凝聚层上同调有其局限性，因为它的系数只能是代数簇对应的域。经过数学的发展，凝聚层上同调在如今已经被许多更强大的上同调理论替代，但它确确实实是在这之后的出现的上同调理论的基础。Serre还提出一个以Witt向量为系数的上同调理论，但他本人并没能证明这个上同调的一些性质。受到Serre的启发，Grothendieck发现可以通过考虑代数簇及其所有非分歧的覆盖来得到一个好的上同调理论，这便是étale上同调的开端。Grothendieck用étale上同调证明了Weil猜想中zeta函数的有理性。Grothendieck还和Berthelot建立了晶体上同调，晶体上同调同样在Weil猜想的证明中展现出了其强大的威力。

4.2.2 椭圆曲线的Weil猜想

我们在这一章证明椭圆曲线的Weil猜想，在证明之前需要一些前置的知识。

1.Tate 模

设E/K是椭圆曲线，m为正整数。

由于$[m]$是定义在K上的映射，所以$[m]$和$G_{\bar{K}/K}$在E上的作用交换。从而对任意$P \in E[m], \sigma \in G_{\bar{K}/K}$,有

$$[m](P^\sigma) = ([m]P)^\sigma = 0$$

表明$P^\sigma \in E[m]$，从而$G_{\bar{K}/K}$自然地作用在$E[m]$上，因此有表示

$$G_{\bar{K}/K} \to Aut(E[m]) \cong GL_2(\mathbb{Z}/m\mathbb{Z})$$

对每个m我们都可以得到这样的一个表示，但这并不是那么的令人满意，因为表示的系数在$\mathbb{Z}/m\mathbb{Z}$中，而$\mathbb{Z}/m\mathbb{Z}$不是一个整环，处理起来不太方便。于是我们有下面的天才的改进。

定义. 设E/K是椭圆曲线，$l \in \mathbb{Z}$是一个素数。E的*(l-adic) Tate* 模为

$$T_l(E) = \varprojlim_n E[l^n]$$

其中逆向极限由

$$E[l^{n+1}] \xrightarrow{[l]} E[l^n]$$

定义。由于每个$E[l^n]$是一个$\mathbb{Z}/m\mathbb{Z}$模，从而$T_l(E)$有自然的$\varprojlim_n \mathbb{Z}/l^n\mathbb{Z} \cong \mathbb{Z}_l$模结构，其中$\mathbb{Z}_l$是$l$ 进整数。

我们不难得到以下结论：

命题. *Tate*模作为$\mathbb{Z}_l$模，有
(a) $T_l(E) \cong \mathbb{Z}_l \times \mathbb{Z}_l$, 若$l \neq charK$
(b) $T_p(E) \cong \mathbb{Z}_p$，若$charK = p$

由$G_{\bar{K}/K}$作用在每个$E[l^n]$上知，$G_{\bar{K}/K}$作用在Tate模$T_l(E)$上。从而有表示

$$\rho_l : G_{\bar{K}/K} \to Aut(T_l(E))$$

从现在开始，我们约定l是一个不等于$charK$的素数。从而 $T_l(E) \cong \mathbb{Z}_l \times \mathbb{Z}_l$, $Aut(T_l(E)) \cong GL_2(\mathbb{Z}_l)$。由包含$\mathbb{Z}_l \subset \mathbb{Q}_l$，有

$$G_{\bar{K}/K} \to GL_2(\mathbb{Q}_l)$$

从而我们得到 $G_{\bar{K}/K}$的一个二维 $\mathbb{Q}_l$表示。

Tate模是研究同源映射(isogeny)的有力工具。设

$$\phi : E_1 \to E_2$$

是椭圆曲线之间的一个同源映射，则ϕ自然地诱导了

$$\phi : E_1[l^n] \to E_2[l^n]$$

进而诱导了

$$\phi_l : T_l(E_!) \to T_l(E_2)$$

容易证明这是一个$\mathbb{Z}_l$模同态。从而我们得到一个映射

$$Hom(E_1.E_2) \to Hom(T_l(E_1), T_l(E_2))$$
$$\phi \mapsto \phi_l$$

这是阿贝尔群之间的一个同态。
(当$E_1 = E_1 = E$时，有

$$End(E) \to End(T_l(E))$$

事实上，这是一个环同态。)不难证明以上映射是一个单射，但为了真正分析$Hom(E_1, E_2)$，我们不加证明地给出以下结果。

定理. 设E_1, E_2为椭圆曲线，则以下自然的映射

$$Hom(E_1, E_2) \otimes \mathbb{Z}_l \to Hom(T_l(E_1), T_l(E_2))$$
$$\phi \mapsto \phi_l$$

是单射。

由以上定理，我们立马得到非常有用的推论：

推论. 设E_1, E_2为椭圆曲线，则

$$Hom(E_1, E_2)$$

是一个自由$\mathbb{Z}$模，其阶数不超过4。

证明. 我们知道，$Hom(E_1, E_2)$是有限生成的$\mathbb{Z}$模当且仅当$Hom(E_1, E_2)\otimes\mathbb{Z}_l$是一个有限生成的$\mathbb{Z}_l$模，且如果有限生成，则它们均为自由模，此时

$$rank_{\mathbb{Z}}Hom(E_1, E_2) = rank_{\mathbb{Z}_l}Hom(E_1, E_2)\otimes\mathbb{Z}_l$$

由上面的定理知，

$$rank_{\mathbb{Z}_l}Hom(E_1, E_2)\otimes\mathbb{Z}_l \leq rank_{\mathbb{Z}_l}Hom(T_l(E_1), T_l(E_2))$$

而$T_l(E_1) \cong T_L(E_2) \cong \mathbb{Z}_l \times \mathbb{Z}_l$, 故$Hom(T_l(E_1), T_l(E_2)) \cong \mathbb{Z}_l^4$，由此得到结论。 □

2. Weil配对(Weil pairing)

设E/K是椭圆曲线。令$m \geq 2$为整数且在K中非零。我们先前提到过，除子$\sum n_i(P_i)$在$Pic(E)$中为0当且仅当$\sum n_i = 0$且$\sum[n_i]P_i = 0$。设$T \in E[m]$。则存在函数$f \in \bar{K}(E)$使得

$$div(f) = m(T) - m(O).$$

设$T' \in E$满足$[m]T' = T$,则存在函数$g \in \bar{K}(E)$使得

$$div(g) = [m]^*(T) - [m]^*(O) = \sum_{R\in E[m]}(R+T) - (R).$$

简单计算发现，

$$div(f\circ[m]) = div([m]^*f) = [m]^*div(f) = m\cdot([m]^*(T) - [m]^*(O))$$

$$div(g^m) = mdiv(g) = m\cdot([m]^*(T) - [m]^*(O))$$

从而$div(f\circ[m]) = div(g^m)$。将$f$乘以某个$\bar{K}^*$中的数，不妨设

$$f\circ[m] = g^m$$

现在设S也是$E[m]$中的一点。则对任意$X \in E$，

$$g(X+S)^m = f([m]X + [m]S) = f([m]X) = g(X)^m$$

从而我们可以定义配对

$$e_m : E[m]\times E[m] \to \boldsymbol{\mu_m} = m\text{阶单位根构成的群}$$
$$e_m(S,T) = g(X+T)/g(X)$$

其中$X \in E$为任意使得$g(X+T)$和$g(X)$均有定义且非零的点。这个配对被称为Weil e_m-配对。

Weil e_m-配对的性质总结如下：

命题.

*(a)*双线性：

$$e_m(S_1+S_2, T) = e_m(S_1, T)e_m(S_2, T)$$
$$e_m(S, T_1+T_2) = e_m(S, T_1)e_m(S, T_2);$$

*(b)*交错性：

$$e_m(S,T) = e(T,S)^{-1};$$

*(c)*非退化：如果$e_m(S,T) = 1$对任意$T \in E[m]$成立，则$S = O$;
*(d)Galois*不变量: $\forall \sigma \in G_{\bar{K}/K}$, $e_m(S,T)^\sigma = e_m(S^\sigma, T^\sigma)$;
*(e)*相容性：若$S \in E[mm'], T \in E[m]$,则

$$e_{mm'}(S,T) = e_m([m']S, T)$$

由以上性质不难推出：

推论.
(a)

$$e_m : E[m] \times E[m] \to \boldsymbol{\mu_m}$$

是满射。且若$E[m] \subset E(K)$，则$\boldsymbol{\mu_m} \subset K^*$。
*(b)*设$S \in E_1[m], T \in E_2[m]$,$\phi : E_1 \to E_2$是一个同源映射。则$\phi$和$\hat{\phi}$关于*Weil*配对对偶，即

$$e_m(S, \hat{\phi}(T)) = e_m(\phi(S), T)$$

设l是一个与$charK$不同的素数。对每个n，我们有

$$e_{l^n} : E[l^n] \times E[l^n] \to \boldsymbol{\mu_{l^n}}$$

对上式取逆向极限，得到

$$e : T_l(E) \times T_l(E) \to T_l(\boldsymbol{\mu})$$

这是一个双线性的，交错的，非退化的，Galois不变的配对。

设l是一个不同于$charK$的素数。回忆我们有表示

$$End(E) \to End(T_l(E))$$
$$\psi \mapsto \psi_l$$

且$T_l(E)$ 是一个秩为2的自由$\mathbb{Z}_l$模。因此如果我们选取$T_l(E)$的一组基，则我们可以将ψ_l写成一个2的矩阵，因此我们便可以考虑这个矩阵的$det(\psi_l), tr(\psi_l) \in \mathbb{Z}_l$。当然，这两个量不依赖于基的选取。关于这两个量，我们有如下令人震惊的结果。

命题. 设$\psi \in End(E)$，则

$$det(\psi_l) = deg(\psi)$$
$$tr(\psi_l) = 1 + deg(\psi) - deg(1 - \psi)$$

特别的，$\det(\psi_l), tr(\psi_l) \in \mathbb{Z}$且与$l$的选取无关。

证明. 设v_1, v_2是$T_j(E)$的一组$\mathbb{Z})l$基，则ψ_l在这组基下可以表示为矩阵

$$\psi_l = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$$

回忆之前定义的配对

$$e : T_l(E) \times T_l(E) \to T_l(\boldsymbol{\mu})$$

计算

$$\begin{aligned} e(v_1, v_2)^{deg\psi} &= e([deg\psi]v_1, v_2) \\ &= e(\hat{\psi}_l\psi_l v_1, v_2) \\ &= e(\psi_l v_1, \psi_l v_2) \\ &= e(av_1 + cv_2, bv_1 + dv_2) \\ &= e(v_1, v_2)^{ad-bc} \\ &= e(v_1, v_2)^{det\psi_l} \end{aligned}$$

由于e是非退化的，故有$deg\phi = det(\psi_l)$。由因为对任意2×2的矩阵A，都有

$$tr(A) = 1 + detA - det(1 - A)$$

从而 $tr(\psi_l) = 1 + deg(\psi) - deg(1 - \psi)$. □

现在令

$$\phi : E \to E$$

为q次Frobenius自同态。在上一小节，我们得到

$$\#E(K) = deg(1 - \phi)$$

同理，对任意正整数n , ϕ^n为q^n次Frobenius自同构，有

$$\#E(K_n) = deg(1 - \phi^n)$$

由上面证明的命题知ϕ_l的特征多项式的系数在$\mathbb{Z}$中，因此可以在$\mathbb{C}$中分解它，即

$$det(T - \phi_l) = T^2 - tr(\phi_l)T + det(\phi_l) = (T - \alpha)(T - \beta)$$

进一步，由于对任意$\frac{m}{n} \in \mathbb{Q}$，有

$$det((m/n) - \phi_l) = det(m - n\phi)/n^2 = deg(m - n\phi)/n^2 \geq 0$$

从而多项式$det(T - \phi_l)$的根为共轭的复数。因此$|\alpha| = |\beta|$，由$\alpha\beta = det(\phi_l) = deg\phi = q$得

$$|\alpha| = |\beta| = \sqrt{q}$$

最后我们注意到ϕ_l^n的特征多项式为

$$det(T - \phi_l^n) = (T - \alpha^n)(T - \beta^n)$$

从而

$$\begin{aligned} deg(1 - \phi^n) &= deg(1 - \phi^n) \\ &= det(1 - \phi_l^n) \\ &= (1 - \alpha^n)(1 - \beta^n) \end{aligned}$$

现在我们终于可以证明椭圆曲线的Weil猜想了。

定理 (Weil猜想(椭圆曲线)). 设K为有q个元素的有限域，E/K是定义在K上的椭圆曲线。则存在$a \in \mathbb{Z}$，使得

$$Z(E/K;T) = \frac{1 - aT + T^2}{(1-T)(1-qT)}$$

. 进一步,有函数方程

$$Z(E/K;\frac{1}{qT}) = Z(E/K;T)$$

且$1 - aT + T^2 = (1-\alpha T)(1-\beta T), |\alpha| = |\beta| = \sqrt{q}$.

证明.

$$\begin{aligned} logZ(E/K;T) =& \sum_{n=1}^{\infty}(\#E(K_n))T^n/n \\ =& \sum_{n=1}^{\infty}(1-\alpha^n-\beta^n-q^n)T^n/n \\ =& -log(1-T)+log(1-\alpha)+log(1-\beta)-log(1-qT) \end{aligned}$$

从而

$$Z(E/K;T) = \frac{(1-\alpha T)(1-\beta T)}{(1-T)(1-qT)}$$

由于α, β为共轭的模长为$\sqrt{q}$的复数，且

$$a = \alpha + \beta = tr(\phi_l) = 1 + deg(\phi) - deg(1-\phi) \in \mathbb{Z}$$

故$Z(E/K;T)$是一个有理函数，直接验证可知它满足函数方程$Z(E/K;\frac{1}{qT}) = Z(E/K;T)$。 □

Chapter 5

BSD猜想

5.1 Mordell-Weil定理和椭圆曲线的秩

定理 (Mordell-Weil定理). *设A是一个定义在数域K上的阿贝尔簇，则它的K有理点形成的群$A(K)$是有限生成的阿贝尔群，称作*Mordell-Weil群。

早在17世纪，人们已经知道三次曲线的加法定理，也熟知Fermat的无穷递减的方法。Louis Mordell先是证明了$E(\mathbb{Q})/2E(\mathbb{Q})$是一个有限群，这在Mordell-Weil定理证明的历史中是重要的第一步。后来他对有理数域上的椭圆曲线证明了猜想(1922-23)。数年之后，André Weil开始研究这一课题。他在他的博士论文中试图将命题推广，他最终证明了定义在一般数域上的阿贝尔簇的Mordell-Weil定理。

由Mordell-Weil定理，特别的，对于定义在$\mathbb{Q}$上的椭圆曲线$E/\mathbb{Q}$，$E(\mathbb{Q})$是一个有限生成的阿贝尔群，由阿贝尔群的结构性定理知存在唯一整数$r \geq 0$，使得

$$E(\mathbb{Q}) \cong \mathbb{Z}^r \oplus E_{tor}(\mathbb{Q})$$

r称为$E(\mathbb{Q})$的秩。

实践表明，椭圆曲线的torsion部分是相对容易计算和分析的，与之相比，秩r是一个更神秘的量。即使是对一个给定的曲线，想要确定它的秩仍然是非常困难的，更不用提一般的求解方法。关于人类对于椭圆曲线的秩知道的有多么少，或者说确定一个椭圆曲线的秩有多困难，可以由以下的猜想看出——让人不禁感叹：这个竟然还没有被证出来？

猜想: 存在任意大的秩的椭圆曲线$E/\mathbb{Q}$。

这个猜想主要源自Tate和Shafarevich的工作，他们对函数域的情形证明了猜想成立(即把$\mathbb{Q}$换成$\mathbb{F}_p(T)$)。Néron构造了一族$\mathbb{Q}$上的椭圆曲线，这族曲线有无穷个，且它们的秩均不小于11。Mestre给出了拥有更大的秩的椭圆曲线的例子。他说明了

$$y^2 - 246xy + 36599029y = x^3 - 89199x^2 - 19339780x - 36239244$$

的秩不小于12。

在这之后，寻找到的最大的秩的记录被不断刷新。2006年，Noam Elkies找到了一条秩至少为28的椭圆曲线：

$$y^2 + xy + y = x^3 - x^2 + a_1x - b_1$$

其中

$$a_1 = -2006776241557552658503320820933854275093023031217895650 2$$

$$b_1 = 3448161179503055646703298569039072037485594435931918036126600829629193944873224342 9$$

但Elkies并没有给出这条椭圆曲线具体的秩。目前已知精确秩的椭圆曲线的最好记录是Elkies和Zev Klagsbrun创下的，他们证明了椭圆曲线

$$y^2 + xy + y = x^3 - x^2 + a_2x + b_2$$

的秩恰为20。其中

$$a_2 = -2445376733363196014638034871689617692707575738218598537 07$$

$$b_2 = 9617101820531830345462229792588068177432706820289644342389578309898984381511214999 31$$

5.2 BSD猜想的叙述

BSD猜想，即Birch和Swinnerton-Dyer猜想，是千禧年七大猜想之一。它以数学家Bryan John Birch和Peter Swinnerton-Dyer的名字命名(所以B指代一个人，SD指代另一人)。在二十世纪六十年代早期， Peter Swinnerton-Dyer用EDSAC-2计算机对已知秩的椭圆曲线计算模p后有理点的个数N_p。Birch和Swinnerton-Dyer从得到的数据猜测，对于秩为r的椭圆曲线，N_p满足以下渐进关系

$$\prod_{p \leq x} \frac{N_p}{p} \approx C \log(x)^r, \ x \to \infty$$

其中C是一个常数。这个发现促使他们对椭圆曲线的L函数$L(E,s)$在$s=1$处的行为作了一个一般的猜想，即BSD猜想。下面给出BSD猜想的严谨叙述。

设椭圆曲线$E/\mathbb{Q}$有Weierstrass方程

$$y^2 = x^3 + ax + b, a, b \in \mathbb{Z}$$

设Δ是椭圆曲线的判别式，令

$$N_p := \#\{y^2 = x^3 + ax + b(modp)\text{的解}\}$$

$$a_p := p - N_p$$

我们可以定义C的不完备L级数:

$$L(C,s) := \prod_{p \nmid 2\Delta} (1 - a_p p^{-s} + p^{1-2s})^{-1}$$

不难证明这个Euler乘积在$Re > 3/2$的时候收敛。Hasse猜想$L(C,s)$可以解析延拓到整个复平面，此猜想已经被证明。有了上面的概念，我们给出BSD猜想的叙述。

BSD猜想 (Birch, Swinnerton-Dyer) $L(C,s)$在$s=1$处的Taylor展开有以下形式

$$L(C,s) = c(s-1)^r + \text{更高阶项}$$

其中$c \neq 0, r$为$E(Q)$的秩。因此BSD猜想可以简要表述为

算术秩($E(\mathbb{Q})$的秩) = 解析秩($ord_1(L(E,S))$)

这一猜想如此迷人，将算术和解析的两个量联系在一起，向世人展现了数学的深邃。BSD猜想还有一个经过改良的版本，在这个版本，人们定义完备的L函数$L^*(C;s)$，它包括了$p \mid 2\Delta$的项。猜想说，$L^*(C,s) \sim c^*(s-1)^r$，其中

$$c^* = \frac{|\text{Ш}_E| R_\infty w_\infty \prod_{p|2\Delta} w_p}{|E_{tor}(\mathbb{Q})|^2}$$

其中Ш_E是E的Tate-Shafarevich群。这是一个神秘的群，至今人们仍不知道这是否是一个有限群。在证明BSD猜想之前，起码得先说明c^*是一个良好定义的有限的数，因此Tate-Shafarevich群的有限性是必须的。起步尚且如此困难，BSD猜想的攻坚道阻且长。

5.3 BSD猜想的一些进展

尽管BSD猜想非常困难，人们还是取得了一些进展。下面介绍其中的一些结果。

- Coates和Wiles(1977)证明了如果E是定义在数域F上的一条曲线，其中F有复乘结构，其对应一条类数为1的虚二次域，$F = K$或$\mathbb{Q}$且$L(E,1) \neq 0$，则$E(F)$是有限群。

- Gross和Zagier(1986)证明了如果一条模椭圆曲线E在$s=1$有一阶零点，则它有一个有理点的阶数是无穷。

- Kolyvagin(1989)证明了如果一条模椭圆曲线E其$L(E,s)$不是0，那么它的秩为0；如果一条模椭圆曲线E其$L(E,s)$在$s=1$有一阶零点，那么它的秩为1。

- Rubin(1991)证明，对于定义在虚二次域K且拥有复乘K的椭圆曲线E，如果它的L函数在$s=1$处不为0，则它的Tate-Shafarevich群的p部分的阶数与BSD猜想预言的一致，对任意素数$p > 7$。

- Breuil et al.(2001)延续了Wiles(1995)的工作，证明了所有定义在$\mathbb{Q}$上的椭圆曲线都是模曲线，这推出了所有定义在$\mathbb{Q}$上的椭圆曲线的L函数在$s=1$处有定义。

- Bhargava和 Shankar(2015)证明了定义在$\mathbb{Q}$上的椭圆曲线的Mordell-Weil群的平均的秩有上界$7/6$。将其与Nekovář(2009)，Dokchitser&Dokchitser的$p-parity$定理，以及Skinner和Urban(2014)对Iswasa理论的主定理(GL(2)情形)的证明结合，他们推出定义在$\mathbb{Q}$上的椭圆曲线解析秩为0的占比为正，从而根据Kolyvagin(1989)，它们满足BSD猜想。

BSD猜想的进展非常缓慢，到目前为止的研究成果均是秩为0或1的情形，关于秩大于1的情形尚未取得显著进展。不过这也激起了人们的求知欲和好胜心，一代代的数学家将为之持续地奋斗。

参考文献

[1] Joseph H.Silverman, *The Arithmetic of Elliptic Curves*, Springer-Verlag, New York,1986.

[2] Joseph H.Silverman and John T.Tate, *Rational Points on Elliptic Curves*, Springer International Publishing, Switzerland, 2015.

[3] Robin Hartshorne, *Algebraic Geometry*, Springer Science+Business Media, New York, 1977.

[4] M.F.Atiyah and I.G.MacDonald, *Introduction to Commutative Algebra*, Addison-Wesley, Reading, Mass(1969), ix+128pp.

[5] [美]莫里斯·克莱因(Morris Kline), 古今数学思想第二册，石生明，万伟勋，孙树本等译，上海：上海科学技术出版社，2014.