椭圆曲线及其基本定理

龚成
华东师范大学数学系（200241）
E-mail: gongcheng365@126.com

摘　要：椭圆曲线是一类极为重要的代数曲线，而其上的的 Riemann—Roch 定理，则可被称为是椭圆曲线的基本定理。本文通过运用椭圆曲线本身的性质，从代数几何的角度出发，给出了椭圆曲线上 Riemann—Roch 定理的一个简单证明。并在此基础上，本文用简捷的方式逐一证明了椭圆曲线乃至椭圆函数上的一些重要定理，通过整个过程来揭示椭圆曲线与其上有理函数间的深刻关系。

关键词：Riemann—Roch 定理，椭圆曲线，有理函数，椭圆函数，Abel 定理

1. 背景

椭圆曲线（亏格为 1 的代数曲线，有时仅指光滑三次代数曲线）是一类为重要的代数曲线，其在数论，编码乃至特殊函数论中都有重要的作用，而椭圆曲线上的 Riemann—Roch 定理正是椭圆曲线上的一个极为重要的定理，可以毫不过分的称为椭圆曲线的基本定理，该定理对研究椭圆曲线的性质有很大帮助。

但一般的书籍，如[2]，[7]都是在对一般情形的代数曲线，证明了 Riemann—Roch 定理后，将椭圆曲线上的 Riemann—Roch 定理作为推论引入的。在这种情况下，同调类，微分形式，乃至凝聚层等一些概念就不可避免的被引入了。这种作法过多的强调了椭圆曲线对代数拓扑及紧黎曼面理论的依赖性,而削弱了对椭圆曲线内蕴性质的探讨。

但事实上，如果我们合理运用椭圆曲线的内蕴性质，那么就可以给出椭圆曲线上的 Riemann—Roch 定理的一个简单证明。这对我们进一步理解椭圆曲线有很大帮助。

2. 预备定理

以下叙述两个极为重要的预备定理，关于其证明可以在参考文献[6]中找到。（本文中除注明处外，均在复数域上讨论）

预备定理 1（亏格公式）设 $C \subset P^2$ 是d次不可约光滑代数曲线，genus(C)= g.

我们有以下亏格公式：

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

推论：光滑的椭圆曲线的次数为 3。

证明：由于椭圆曲线为亏格为 1 的代数曲线，从而 $g = \frac{(d-1)(d-2)}{2} = 1$，

解得 d=3。

预备定理 2 (Bezout定理) 设两条在 P^2 上的平面代数曲线 C 和 E 无共同的曲线分支,那么用#(C, E)表示 C 和 E 的交点数目,则

#(C, E)= $\deg C * \deg E$

其 $\deg C$，$\deg E$ 分别为平面代数曲线 C 和 E 的次数。

推论：两条光滑椭圆曲线 C 和 E 在 P^2 中相交 9 个点。

证明：由于光滑椭圆曲线为三次代数曲线，

从而#(C, E)= $\deg C * \deg E$ =3*3=9。

3. 椭圆曲线上的 Riemann—Roch 定理

① 光滑代数曲线上的 Riemann 不等式

定义 1：设C是一条平面代数曲线，C上的一个除子是指一个有限和形式：

$$D = m_1 p_1 + m_2 p_2 + ...m_i p_i, \qquad m_j \in \square, \qquad p_j \in C$$

除子次数记为 $\deg D = \sum m_i$

所有C上的除子构成一个Abel群，记为Div(C)。

定义 2：设C是一条平面代数曲线，$D \in$ Div(C),

则 $L(D) = \{ f \in K(C) \mid (f) + D \geq 0 \}$

显然，$L(D)$构成有理函数在复数域上的线性空间。

记 $\dim L(D) = l(D)$。

定理 1（Riemann不等式）设C是一条亏格为g的光滑平面代数曲线，D>0,

则 $l(D) \geq d - g + 1$

证明：设C方程由$F(x, y, z) = 0$给出，且deg F =m.。

设 D>0,deg D =d,

并以S^n表示复系数的三元n 次齐次多项式集合，则S^n是复数域$\square$上的线性空间：

$$\dim S^n = \frac{1}{2}(n+1)(n+2)$$

设$G(x, y, z) \in S^n$,且满足下述两个条件：

a) F不整除G;

b) $G|_c \geq D.$

我们知道，条件$G|_c \geq D$意味着G的系数应满足d 个线性方程。

取一个满足条件a),b)的G,令$E = G|_c - D$，并取

$$S = \{ H \in S^n \mid H|_c \geq G|_c - D \}$$

现计算dim$S$,由Bezout定理，

#(G, C) =deg G *deg F =nm

故条件$H|_c \geq G|_c - D$等价于H的系数应满足（nm-d）个线性方程，

于是

$$\dim S \geq \frac{1}{2}(n+1)(n+2) - nm + d$$

对于每个 $H \in S$ ，定义

$f_H = (\frac{H}{G}|_c)$，

则 $(f_H)+D=(H|_c)-(G|_c)+D\geq(G|_c-D)-(G|_c)+D=0$

于是，$(f_H)\in L(D)$。

注意到 f_H =0 当且仅当 H 在 C 上取值为零,即, $H=F*Q,(Q\in S^{n-m})$

则

$$l(D)\geq \dim S-\dim S^{n-m}$$

$$\geq \frac{1}{2}(n+1)(n+2)-mn+d-\frac{1}{2}(n-m+1)(n-m+2)$$

$$=d-\frac{1}{2}(m^2-3m)=d-\frac{1}{2}(m-1)(m-2)+1$$

运用亏格公式,则有

$$l(D)\geq d-g+1$$

推论:特别当C是椭圆曲线时,g=1,从而 $l(D)\geq d$ 。

② 椭圆曲线上的 Riemann—Roch 定理

引理 1.椭圆函数 $f(z)$ 在它的一个正常基本平行四边形 Λ 内的全部极点的留数和为零,因而在一个正常基本平行四边形 Λ 内至少有两个一级极点或一个不低于二级的极点。

证明：在一个正常基本平行四边形∧内全部极点的留数和等于积分 $\frac{1}{2\pi i}\oint_L f(z)dz$，其中L是Λ的边界。由周期性可知积分为零。这表明个一级极点的留数不为零。从而在一个正常基本平行四边形 Λ 内至少有两个一级极点或一个不低于二级的极点。

根据椭圆函数与椭圆曲线上有理函数一一对应的关系，我们得到如下推论：

椭圆曲线 C 上的非常值有理函数在 C 上至少有两个极点。

引理 2：设 $l(D)>0,0\neq\varphi\in L(D)$,证明 C 上最多只有有限多个点 p 使 $\varphi\in L(D-p)$，所以最多除有限个点 p 外， $l(D-p)=l(D)-1$ 。

证明：令 $E=div(\varphi)+D\geq 0,$

$$E=\sum_{i=1}^{k}n_i p_i,\qquad n_i\geq 0, i=1...k$$

由于 $\varphi\in L(D-p)$ ，于是 $div(\varphi)+D-p\geq 0,$ 可推出 $E-p\geq 0$ ，从而 $\sum_{i=1}^{k}n_i p_i-p\geq 0$ ，这表明p的选取有限。

从而， $p\neq p_i, i=1...k$时, $\varphi\notin L(D-p)$ 。

又因为：

$D-p\le D$,所以$L(D-p)\subset L(D)$,

于是$l(D-p)\le l(D)-1$,

而$D\equiv E$,因此只要验证$l(E-p)\ge l(E)-1$.

$L(E-p)$是$L(E)$中的一个线性条件下的一个子空间，从而$l(E-p)\ge l(E)-1$。

这表明 $l(D-p)=l(E-p)=l(E)-1=l(D)-1$。

引理 3：若$D>0$,那么$l(D+p)\le l(D)+1$.

证明：n_p是D在p点的重数，

作映射

$$\pi:\ L(D+p)\to \quad \square$$

$$\varphi \ \mapsto \quad (t^{n_p+1}\varphi)(p)$$

因为 $div(\varphi)+D+p\ge 0$ ，于是 $v_p(\varphi)+n_p+1\ge 0$ ，则 $v_p(t^{n_p+1}\varphi)=n_p+1+v_p(\varphi)\ge 0$，于是$t^{n_p+1}\varphi(p)\in\square$

$$Ker\pi=\{\varphi\in L(D+P)\,|\,v_p(t^{n_p+1}\varphi)\ge 1\}$$
$$=\{\varphi\in L(D+P)\,|\,v_p(\varphi)+n_p\ge 0\text{且}div(\varphi)+D+p\ge 0\}$$
$$=\{\varphi\in Rat(C)\,|\,div(\varphi)+D\ge 0\}$$

所以 $Ker\pi=L(D)$，$l(D)+\dim \mathrm{Im}\,\pi=l(D+p)$，可推出$l(D+p)\le l(D)+1$。

推论：如果$D\ge 0$,那么$l(D)\le \deg D+1$ 。

证明： 由引理 2，

$d=\deg D\ge 0$,

由于$D\ge 0, D=\sum_{i=1}^{k} n_i p_i, n_i\ge 0, i=1...k, d=n_1+...n_p$

于是$l(D)\le l(0)+d=1+d$.

定理 2：（椭圆曲线上的 Riemann—Roch 定理）

设C是平面椭圆曲线， D>0, 则$l(D)=\deg D$ 。

证明：1）若D= p，则由引理 1 知，椭圆曲线C上的非常值有理函数在C至少有两个极点 ，于是满足$(\varphi)+p\ge 0$的有理函数只有常值函数，于是$l(p)=1$。

2）取D>0 ,由引理 2 知，D上可能有有限个例外点，使$l(D-p)=l(D)$

情形 1，D没有例外点，那么由引理 2 知，$l(D)=l(D-p)+1$，

不断使用引理 2 得，$l(D)=l(p)+d-1$，

由于$l(p)=1$，从而$l(D)=d$ 。

情形 2，若D上有例外点p，那么设p是例外点，那么由引理 2 知，$l(D)=l(D-p)$，

运用引理 3 知，$l(D)\le d-1+1=d$，运用Riemann不等式，有$l(D)\ge d$ 。

由上述 3 个式子，得：$d\ge l(D-p)=l(D)\ge d$，

于是 $l(D-p)=l(D)=d$ 。

若 D 上仍有例外点 q，则用相同方法知，

$d-1\geq l(D-p-q)=l(D-p)=d$ （矛盾）

于是 D 上至多一个例外点。

此时知 D-p 上没有例外点， 从情形 1 知

$l(D-p)=d-1$,于是$l(D)=d-1$, 与Riemann不等式， $l(D)\geq d$ 矛盾。

从而 D 上没有例外点，因此情形 2 不成立。

综上所述，我们完成了定理的证明。

4. 椭圆曲线上的有理函数

① Weiersrass 标准型与椭圆函数

引理 4(Weiersrass 标准型)任给一个光滑的椭圆曲线 C,都双有理等价于无重根的三次多项式:

$$y^2=4x^3+ax+b$$

证明: 作为椭圆曲线上 Riemann—Roch 定理的一个应用,我们来证明这一个定理。

设p为 C 的一点, ,根据Riemann—Roch定理, $l(2P)$ =2。于是有一组基，不妨设为：$1,\xi$；同样对 $l(3P)$ =3，也有一组基，不妨设为：$1,\xi,\eta$；

这样 $\eta^2,\eta\xi,\xi^2,\xi,\eta,\xi,1\in l(6p).$

但 $l(6p)=6$，于是在上述的有理函数间存在一个线性关系。

作线性变换

$$\xi\to c_1\xi+c_2$$

$$\eta\to c_3\xi+c_4\eta+c_5$$

通过比较系数，可将线性关系化简为：

$$\eta^2=\xi^3+A'\xi+B',$$

令 $\eta\to\frac{1}{2}\eta, 4A'=A, 4B'=B$，于是原方程化为：$\eta^2=\xi^3+A\xi+B$

由于原方程未退化，因此 $y^2=4x^3+ax+b$ 也不退化，从而其是没有重根的多项式 。

事实上仅用坐标变换，也可以得到这一结果，具体过程见参考文献[7]。

学过椭圆函数的人都知道，在众多的椭圆函数中，有两个最基本的椭圆函数Weiersrass的椭圆函数 $\mathrm{P}(z)$ 及其导数 $\mathrm{P}'(z)$，且我们知道：

$$P'(z)^2=4P(z)^3-g_2P(z)-g_3 \qquad (\text{这里}g_2=60\sum_{\omega\in\pi,\omega\neq0}\omega^{-4}, g_3=140\sum_{\omega\in\pi,\omega\neq0}\omega^{-6})$$

根据椭圆函数与椭圆曲线上有理函数之间的关系，我们知道：

$P(z)$ 相当于椭圆曲线方程中的x, $P'(z)$ 相当于椭圆曲线方程中的y,

根据这一观点，我们很容易得出一些本来很难得到的结论。

② 椭圆函数的生成定理

定理 3 设 $g(x,y)$ 是定义在光滑椭圆曲线C上的有理函数，那么

$g(x,y)$ 可以写成如下形式：

$g(x,y)=S(x)+yT(x)$，其中 $S(x),T(x)$ 是x的有理函数。

证明：根据引理 4，C 的方程可写为：

$$y^2=4x^3+ax+b \quad (1)$$

由于 $g(x,y)$ 是定义在 C上的有理函数，于是

$$g(x,y)=\frac{g_1(x,y)}{g_2(x,y)},(g_1(x,y),g_2(x,y)\text{均为多项式})$$

根据（1）式，我们得 $g_1(x,y),g_2(x,y)$ 中y高于 1 次项的部分用x的多项式替代，于是

$$g_1(x,y)=g_{11}(x)+yg_{12}(x)$$
$$g_2(x,y)=g_{21}(x)+yg_{22}(x)$$

从而

$$g(x,y)=\frac{g_{11}(x)+yg_{12}(x)}{g_{21}(x)+yg_{22}(x)}=\frac{(g_{11}(x)+yg_{12}(x))(g_{21}(x)-yg_{22}(x))}{{g_{21}}^2(x)-y^2{g_{22}}^2(x)}$$
$$=\frac{(g_{11}(x)g_{21}(x)-y^2g_{12}(x)g_{22}(x))+(g_{12}(x)g_{21}(x)-g_{11}(x)g_{22}(x))}{{g_{21}}^2(x)-y^2{g_{22}}^2(x)}$$

再次运用（1）式，将分母上的 y^2 消去，即可得到：

$g(x,y)=S(x)+yT(x)$。

推论：任何椭圆函数 $F(z)$ 都可写为如下形式：

$g(x,y)=S(x)+yT(x)$，x= $P(z)$,y= $P'(z)$ 。

其中 $S(x),T(x)$ 是x的有理函数。

引理 5 任何两个在 $\Lambda(\omega_1,\omega_2)$ 上的椭圆函数都满足一个非平凡的代数关系.

证明:见参考文献[4]。

定理 4 任何两个在光滑椭圆曲线 C 上的有理函数 $g_1(x),g_2(x)$ 都满足一个非零的多项式 $f(x,y)$ 使得:

$$f(g_1,g_2)=0$$

证明: 对引理 5 运用光滑椭圆曲线上有理函数与椭圆函数的关系,即得证。

5. 椭圆曲线上的 Abel 定理

Abel 定理也是椭圆曲线上的一个基本定理,它在很大程度上告诉了我们有理函数与其除子之间的关系.在证明这一定理之前我们先看一些预备知识。

① 预备知识

⑴椭圆曲线上的群结构

众所周知, 椭圆曲线上一个运算⊕,在这个运算下,C 上的点构成一个加群,并有如下性质:

预备定理 3 :C 为一条椭圆曲线,设 O 为拐点,且 O 是加群的基点,则:

$$P,Q,R\in C\text{共线}\Leftrightarrow P\oplus Q\oplus R=O$$

证明见参考文献[2]。

⑵一些符号:

$Div^0(C):C$上的0次除子群

$\mathrm{Prin(C)}=\{\mathrm{div}(\varphi)\,|\,\varphi$是非零的有理函数$\}$

$$\mathrm{Pic}^0(C)=\frac{Div^0(C)}{\mathrm{Prin(C)}}$$

椭圆曲线上的 Abel 定理

重要引理:用⊕表示 C 上的加法,该运算以 C 上的拐点 O 为加群的基点,

作映射:
$$\begin{aligned}\pi:C&\to Pic^0(C)\\ p&\mapsto p-o+\mathrm{Prin}(C)\end{aligned}$$

则有以下关系:

$$\pi(C,\oplus)\cong \mathrm{Pic}^0(C)$$

该引理在谈胜利教授的《代数几何初步》讲义(参考文献[1])中有详细叙述,并附有许多解释,该讲义对直观理解代数几何有很大帮助。但由于该讲义尚未正式出版,为方便读者理解,在此就该定理的证明,作一简单陈述。

引理说明:①证明π是单的。

若 C 上两点 $P_1\neq P_2$,而 $\pi(P_1)=\pi(P_2)$,于是 $P_1-P_2\in\mathrm{Prin(C)}$,从而 存在有理函数$\varphi$使$P_1-P_2=div(\varphi)$。

这表明 C 上存在单极点的有理函数 ,与引理 1 矛盾。

②证明π是保运算的。即$\pi(P_1\oplus P_2)=\pi(P_1)+\pi(P_2)$

记 $p_1\oplus p_2=R$,于是命题要求证明:

$$\overline{R-O}=\overline{P_1-O}+\overline{P_2-O}+\overline{P_1+P_2-2O}$$

也就是证明: $R-P_1-P_2+O\in\mathrm{Prin}(C)$。

这说明我们要构造有理函数φ使得: $R-P_1-P_2+O=div(\varphi)$。

以下构造φ:

取直线L_1过P_1,P_2,由 Bezuot 定理,L_1与 C 还交一个点P_3,

由于P_1,P_2,P_3共线,于是$P_1\oplus P_2\oplus P_3=O$ …… ①

取直线L_2过R, Q, 则L_2与 C 还交一个点Q_3,

同样,$\mathrm{R}\oplus O\oplus Q_3=O$ …… ②

由于$R=P_1\oplus P_2$,于是由 ① ②得: $Q_3=P_3$

作$\varphi=\frac{L_1}{L_2}|_c$,那么

$$div(\varphi)=R+O+Q_3-P_1-P_2-P_3=R+O-P_1-P_2.$$

③证明 π 是满的。

$$\text{任意}D\in Div^0(C),D=\sum_{i=1}^{d}P_i-\sum_{i=1}^{d}Q_i=\sum_{i=1}^{d}(P_i-Q_i),$$

要证: $D=\pi(P)$,由于 π 包运算,只要证明对任意 i,

$P_i-Q_i=\pi(R_i),R_i\in C$

以下证对任意 P,Q 两点,有 $P-Q=\pi(S),S\in C$.

取 L_1 为过 P 与 Q 的直线,设 R 为 L_1 与 C 交的第三点,

设 L_2 为过 R 与 Q 的直线,S 为 L_2 与 C 交的第三点,

于是作 $\varphi=\frac{L_1}{L_2}|_c$,那么

$$div(\varphi)=R+O+S-P-O-R=Q+S-P-O=(S-O)+Q-P$$

$$P-Q=S-O-div(\varphi)$$

$$\overline{P-Q}=\overline{S-O}=\pi(S)$$

运用该重要引理,就可得到椭圆曲线上的 Abel 定理。

定理 5（椭圆曲线上的 Abel 定理）

$$\text{设}D\in Div^0(C),\text{且}D=\sum_{i=1}^{d}P_i-\sum_{i=1}^{d}Q_i,$$

$$\text{若有}\varphi\neq 0\text{使}D=div(\varphi),\text{等价于}P_1\oplus P_2.\oplus..\oplus P_d=Q_1\oplus Q_2\oplus...\oplus Q_d$$

证明：由于

$$\pi(P_1\oplus P_2.\oplus..\oplus P_d)=\sum_{i=1}^{d}P_i-dO,$$

$$\pi(Q_1\oplus Q_2\oplus...\oplus Q_d)=\sum_{i=1}^{d}Q_i-dO,$$

从而 $\pi(P_1\oplus P_2.\oplus..\oplus P_d)=\pi(Q_1\oplus Q_2\oplus...\oplus Q_d)$

于是由重要引理，即可得到结论。

② **一个重要的定理：**

作为椭圆曲线上的 Abel 定理的应用，我们来证明以下定理：

定理 6 设 $C\subset P^2$ 是光滑平面代数曲线，E，F 是平面三次代数曲线，并且 E 交 C 于 $P_1.....P_9$，若 F 通过九个点中的八个，则必通过剩下的一个点。

证明：由于 C 与 E 交九个点，而 E 是三次曲线，由 Bezout 定理知 C 是三次曲线，从而 C 是椭圆曲线。

不妨设 F 过 $P_1,P_2.....P_8$，另外过点 P',那么，

作 $\varphi=\frac{E}{F}|_c$,那么 $div(\varphi)=P_9-P'$，

由 Able 定理知， $P_9=P'$。

于是 F 过 P_1.....P_9，定理得证。

6. 椭圆曲线的算术性质

以上我们主要从复代数几何的角度来探讨椭圆曲线。事实上如果我们进一步研究椭圆曲线，特别从数论角度来探讨其算术性质后会发现，椭圆曲线还有一些深刻的性质：

以下仅举例式的选取几个：

定理 I （有限基定理）在椭圆曲线上，其有理点构成的群是有限生成的。

定理 II：D 是一条定义在有限域 F_p 上的椭圆曲线，那么它必有一个定义在 F_q 上的点（这里 p 是一个素数，q 是 p 的某个方幂）。

想对椭圆曲线的算术性质有更深了解，可阅读参考文献[3],[5]。

参考文献

[1] 谈胜利，《代数几何初步》，上海:华东师范大学数学系内部讲义 , 2005。
[2] Phillip Griffiths and Joseph Harris, Principles of algebraic geometry, New York : Wiley, 1978
[3] Dale Husemoller ,Elliptic curves, New York:Springer-Verlag ,1987.
[4] Serge.Lang, Elliptic functions, New York: Addison-Wesley, 1973.
[5] Joseph H. Silverman, The arithmetic of elliptic curves, New York: Springer-Verlag ,1986.
[6] Igor R. Shafarevich, Basic algebraic geometry, Berlin : Springer, 1974.
[7] R.Walker, Algebraic curves, New York : Springer-Verlag,1978.

Elliptic curves and their basic theorems

Gong Cheng
Mathematic department ,East china normal university, shanghai（200241）

Abstract

As we know, elliptic curves are important algebraic curves. And Riemann—Roch theorem is the most important theorem on elliptic curves. In this paper,we use the simpler tools to give a proof of the Riemann—Roch theorem on elliptic curves. Then, the paper will tell you some new applications of the Riemann—Roch theorem and some simpler proves of the theorems about elliptic curves and elliptic functions.

Keywords: Riemann—Roch theorem elliptic curves rational functions elliptic functions Abelian theorem