1 The Riemann-Roch Theorem

Let C be a smooth curve defined over a field K with its divisor group $\mathrm{Div}(C)$. For any divisor D in $\mathrm{Div}(C)$ let $L(D)$ be the space of functions associated to D as usual, and $l(D)$ the dimension of $L(D)$. We denote the canonical divisor on C by K_C. The Riemann-Roch theorem then states that

Theorem 1.1. *For any divisor $D \in Div(C)$ there is an integer $g \geq 0$ such that*

$$l(D) - l(K_C - D) = deg\ D - g + 1. \tag{1}$$

We will prove the above theorem for two special cases: the extended complex plane and the elliptic curves over complex numbers.

First, we shall note some facts that will be used in our proofs.

Proposition 1.2. *([Sil], Proposition 5.2)*
(a) If $deg\ \ D < 0$, then $L(D) = \{0\}$ and $l(D) = 0$
(b) If D is linearly equivalent to D', $D \sim D'$, then $L(D) \cong L(D')$ and $l(D) = l(D')$

1.1 Riemann-Roch theorem for $\mathbb{C} \cup \infty$

By Proposition 1.2 (b), we can assume $K_C = -2(\infty)$ (also see Example 4.5, [Sil]). In particular, we will prove that $l(D) - l(-2(\infty) - D) = \deg D + 1$. First note that if $\deg D = -1$ then the equality clearly holds by Proposition 1.2 (a). If $\deg D > -1$ then it suffices to prove $l(D) = \deg D + 1$ as $l(-2(\infty) - D) = 0$. If $\deg D < -1$ then $l(D) = 0$ and the equation reads as $-l(-2(\infty) - D) = \deg D + 1$. Substituting $D' = -2(\infty) - D$ we obtain

$$\begin{aligned} -l(D') &= -2 - \deg D' + 1 \\ &= -\deg D' - 1. \end{aligned}$$

where $\deg D' \geq 0$. Hence, we aim to prove that

$$l(D) = \deg D + 1 \tag{2}$$

for any divisor D with $\deg (D) \geq 0$. If $\deg D =$ k then, by Proposition 1.2 (b), it is enough to consider any divisor D_k of degree $k \geq 0$.

Case 1. $k = 0$: Let $D_0 = \emptyset$. If $f \in L(D_0)$ then f cannot have any pole, and so f must be a constant function. Clearly, any constant function is in $L(D_0)$, whence $l(D_0) = 1 = \deg D_0 + 1$.

Case 2. $k > 0$: Let $D_k = (s_1) + (s_2) + \cdots + (s_k)$ where $s_i \neq s_j$, and $s_i \neq \infty$. The set of functions $1 \cup \{1/(z - s_i)\}_{i=1}^k$ are linearly independent over $\mathbb{C}$ and each of its elements are in $\mathrm{L}(D_k)$, that is, $l(D_k) \geq k + 1$. Now, we show $l(D_k) \leq k + 1$. Let $f \in \mathrm{L}(D_k)$. The only poles of f can be from the set $\{s_i\}_{i=1}^k$ and f can only have a pole of order at most 1. So, we can write

$$f(z) = \frac{g(z)}{(z - s_{i_1})...(z - s_{i_j})}.$$

The polynomial $g(z)$ must also satisfy that deg $g(z) \leq j$ since otherwise f would have a pole at ∞. If deg $g(z) < j$ then using partial fractions technique f can be written as

$$f(z) = \sum_{l=1}^{j} \frac{A_l}{z - s_{i_l}},$$

where each A_l is constant. If deg $g(z) = j$ then similarly as above one can write

$$\begin{aligned} f &= (z - t)\frac{g_1}{(z - s_{i_1})...(z - s_{i_l})} \\ &= (z - t)\sum_{l=1}^{j} \frac{A_l}{z - s_{i_l}} \\ &= \sum_{l=1}^{j}(A_l + \frac{A_l(s_{i_l} - t)}{z - s_{i_l}}). \end{aligned}$$

Hence, we get $f \in \langle 1, 1/(z - s_1), \ldots, 1/(z - s_k)\rangle$ and $l(D_k) \leq k + 1$, as required.

1.2 Elliptic functions

Let w_1, w_2 be two complex numbers linearly independent over $\mathbb{R}$ and define a lattice $\Lambda = \Lambda(w_1, w_2) = \mathbb{Z}w_1 + \mathbb{Z}w_2$ in $\mathbb{C}$. An elliptic function, f, over a lattice Λ is a meromorphic function on $\mathbb{C}$ such that $f(z + l) = f(z)$ for any $l \in \Lambda$. The set of all elliptic functions on Λ defines a field an denoted $\mathbb{C}(\Lambda)$. The two very important examples of elliptic functions are Weirstrass $\wp$-function and its derivative:

$$\begin{aligned} \wp(z) &= \frac{1}{z^2} + \sum_{\substack{w \in \Lambda \\ w \neq 0}} \left(\frac{1}{(z - w)^2} - \frac{1}{w^2} \right), \\ \wp'(z) &= -2\sum_{w \in \Lambda} \left(\frac{1}{(z - w)^3} \right). \end{aligned}$$

It is easy to check that Weirstrass $\wp$-function is an even elliptic function defined everywhere on $\mathbb{C} - \Lambda$, and $\wp'$ is an odd elliptic function defined everywhere on $\mathbb{C} - \Lambda$, ([Sil], Theroem 3.1). In fact, these two functions generate the field of elliptic functions ([Sil], Theroem 3.2):

$$\mathbb{C}(\Lambda) = \mathbb{C}(\wp, \wp'). \tag{3}$$

One can write the Laurent series for $\wp(z)$ as

$$\wp(z) = \frac{1}{z^2} + \sum_{k=1}^{\infty}(2k+1)G_{2k+2}z^{2k}, \tag{4}$$

and obtain the algebraic relation between $\wp(z)$ and $\wp'(z)$

$$\left(\frac{\wp'(z)}{2}\right)^2 = \wp(z)^3 - 15G_4\wp(z) - 35G_6, \tag{5}$$

where $G_{2k} = \sum_{\substack{w\in\Lambda \\ w\neq 0}} w^{-2k}$ is the Eisenstein series which converges absolutely for all $k > 1$ ([Sil], Theorem 3.5).

1.3 Divisors on $\mathbb{C}/\Lambda$

The divisor group $\mathrm{Div}(\mathbb{C}/\Lambda)$ is defined to be the formal sum $\sum_{w\in\mathbb{C}/\lambda} n_w(w)$ where $n_w \in \mathbb{Z}$ and $n_w = 0$ for all but finitely many w. The divisor of an elliptic function $f \in \mathbb{C}(\Lambda)$ is then

$$\mathrm{div}(f) = \sum_{w\in\mathbb{C}/\Lambda} \mathrm{ord}_w(f)(w)$$

The above sum is finite as the zeros and the poles of a meromorphic function are isolated. Before giving some examples of divisors of functions we state the following theorem.

Theorem 1.3. *([Sil], Proposition 2.1, Theorem 2.2)*
(i) An elliptic function with no poles or no zeros is constant.
(ii) $\sum_{w\in\mathbb{C}/\Lambda} Res_w(f) = 0$.
(iii)$\sum_{w\in\mathbb{C}/\Lambda} ord_w(f) = 0$.
(iv) $\sum_{w\in\mathbb{C}/\Lambda} ord_w(f)w \equiv 0 \pmod{\Lambda}$.

Corollary 1.4. *A nonconstant elliptic function has order at least* 2.

Proof. If f has a simple pole then by Theorem 1.3 (ii), f is holomorphic, and by Theorem 1.3 (i), f must be constant. □

Example 1.5. *We will write the divisor of $\wp(z)$. By (4), $\wp(z)$ has only one pole at 0 with multiplicity 2. Since the degree of div($\wp(z)$) is zero by Theorem 1.3, $\wp(z)$ must have 2 zeros counting multiplicities. Moreover, if r is a zero of $\wp(z)$ then $-r$ is a zero of $\wp(z)$ as $\wp(z)$ is an even function. Hence,*

$$div(\wp(z)) = -2(0) + (r) + (-r). \tag{6}$$

From now on, the letter $r \in \mathbb{C}/\Lambda$ is reserved for the zero of $\wp(z)$.

Example 1.6. *We will write the divisor of $\wp'(z)$. By (4), $\wp'(z)$ has only one pole at 0 with multiplicity 3. Since the degree of div($\wp'(z)$) is zero by Theorem 1.3, $\wp'(z)$ must have 3 zeros counting multiplicities. Note that $\wp'(z)$ is an odd function and $2w_1 = 0$ in $\mathbb{C}/\Lambda$. That is, $\wp'(w_1/2) = -\wp'(-w_1/2) = -\wp'(w_1/2)$ and $\wp'(w_1/2) = 0$. Similarly, $\wp'(w_2/2) = \wp'((w_1 + 2)/2) = 0$. Hence,*

$$div(\wp'(z)) = -3(0) + \left(\frac{w_1}{2}\right) + \left(\frac{w_2}{2}\right) + \left(\frac{w_1 + w_2}{2}\right). \tag{7}$$

Now, let $x = \wp(z)$ and $y = \wp'(z)$. Then, x is transcendental over $\mathbb{C}$ since x has a pole at 0. Moreover y is algebraic over $\mathbb{C}(x)$ with degree at most 2 by (5). In fact, the algebraic degree of y is 2 because y is an odd function, that is, $y \notin \mathbb{C}(x)$. Combining this observation with (3) and (5) proves the following proposition

Proposition 1.7. $\mathbb{C}(\Lambda) \cong \mathbb{C}[X, Y]/(Y^2 - X^3 - 15G_4X - 35G_6)$.

The above proposition indicates a close relation between $\mathbb{C}/\Lambda$ and the elliptic curves arising from the corresponding lattice, Λ. In fact, more is true and for each elliptic curve defined over $\mathbb{C}$ there corresponds a unique lattice Λ in $\mathbb{C}$. The precise statement is as follows

Theorem 1.8 ([Sil2], Corollary 4.3)**.** *Let $A, B \in \mathbb{C}$ satisfy $4A^3 + 27B^2 \neq 0$, and let*

$$E = \{(x, y) \in \mathbb{C}^2 : \ y^2 = x^3 + Ax + B\} \cup \{\infty\}$$

be an elliptic curve. Then there is a unique lattice $\Lambda \in \mathbb{C}$ such that the map

$$\begin{aligned} \phi : \mathbb{C}/\Lambda &\rightarrow E \subset \mathbb{C}^2 \cup \{\infty\} \\ z &\mapsto (\wp(z), \frac{\wp'(z)}{2}) \end{aligned}$$

is a complex analytic isomorphism.

1.4 Riemann-Roch theorem for $E/\mathbb{C}$

By Proposition 1.2 (b), we can assume $K_C = \emptyset$ (also see Example 4.6, [Sil]). In particular, we will prove that

$$l(D) - l(-D) = \deg D. \tag{8}$$

If $\deg D > 0$ then we have to prove, by Proposition 1.2 (a), that $l(D) = \deg D$. If $\deg D < 0$ then replacing D by $D' = -D$ in (8), gives $l(D') = \deg D'$ where $\deg D' > 0$. Hence, we left with two cases to prove:

$$l(D) = \deg D, \quad \deg D > 0, \tag{9}$$

$$l(D) - l(-D) = \deg D, \quad \deg D = 0. \tag{10}$$

Moreover, by Theorem 1.8, proving the Riemann-Roch theorem for elliptic curves over $\mathbb{C}$ is the same as proving it for $\mathbb{C}/\Lambda$. Hence, we will prove (9) and (10) for $\mathbb{C}/\Lambda$. Before proceeding we give two important lemmas.

Lemma 1.9. *Let $s_1, s_2 \in \mathbb{C}/\Lambda$, and $D = (s_1) + (s_2)$. Then there exists a nonconstant function $f \in \mathbb{C}(\Lambda)$ such that $f \in L(D)$.*

Proof. We will consider several cases for the values of s_1 and s_2. If $s_1 = s_2 = 0$ then $\wp(z) \in L(D)$, and if $s_1 = s_2 \neq 0$ then $\wp(z - s_1) \in L(D)$ by (6). Similarly, if $s_1 = -s_2$ and $s_1 = r$ then $1/\wp(z) \in L(D)$, and if $s_1 = -s_2$ and $s_1 \neq r$ then $1/(\wp(z) - \wp(s_1)) \in L(D)$. If $s_2 = 0$ and $s_1 \neq s_2$ then setting $f(z) = \wp(z) - \wp(s_1)$ we get

$$\begin{aligned} \operatorname{div}\left(\frac{\wp'(z)}{f(z)}\right) &= -(s_1) - (-s_1) - (0) + \text{positive terms}, \\ \operatorname{div}\left(\frac{1}{f(z)}\right) &= -(s_1) - (-s_1) + \text{positive terms}. \end{aligned}$$

Now, letting $g(z) = \left(\operatorname{Res}_{-s_1}\left(\frac{1}{f(z)}\right)\right) \cdot \left(\frac{\wp'(z)}{f(z)}\right) - \left(\operatorname{Res}_{-s_1}\left(\frac{\wp'(z)}{f(z)}\right)\right) \cdot \left(\frac{1}{f(z)}\right)$, it follows that

$$\operatorname{div}(g(z)) = -(s_1) - (0) + \text{positive terms},$$

that is $g(z) \in L(D)$. Finally, if $s_1 \neq s_2$ then, by applying the previous case, one can construct a nonconstant function, say $g(z) \in L(D')$ where $D' = (s_1 - s_2) + (0)$. Translating $g(z)$ by s_2 completes the proof. $\square$

Lemma 1.10. *Let $s_1, s_2, s_3, s_4 \in \mathbb{C}/\Lambda$. Then $(s_1) + (s_2) \sim (s_3) + (s_4)$ if and only if $s_1 + s_2 = s_3 + s_4$.*

Proof. First suppose that $(s_1) + (s_2) \sim (s_3) + (s_4)$. Then $s_1 + s_2 = s_3 + s_4$ by Theorem 1.3 (iv).

Now, assume $s_1 + s_2 = s_3 + s_4$. We may also assume that that $s_1 \neq s_3, s_4$ and $s_2 \neq s_3, s_4$. because otherwise we get $(s_1) + (s_2) - (s_3) - (s_4) = \emptyset$. By Lemma 1.9, there exist a nonconstant elliptic function $g(z)$ such that $\mathrm{div}(g) = -(s_3) - (s_4) + \text{positive terms}$. Consider the elliptic function $h(z) = g(z) - g(s_1)$ which has a pole at s_3 and s_4, and has a zero at s_1. By Theorem 1.3 (iii), $\mathrm{div}(h)$ has degree 0, and so

$$\mathrm{div}(h) = -(s_3) - (s_4) + (s_1) + (s),$$

for some $s \in \mathbb{C}/\Lambda$. In fact, $s + s_1 = s_3 + s_4$ by Theorem 1.3 (iv), and recalling that $s_1 + s_2 = s_3 + s_4$ gives $s = s_2$, as required. □

1.4.1 Proof of Riemann-Roch

Let D_0 be a degree zero divisor. If $D_0 = \emptyset$ then (10) clearly holds. If $D_0 = (s_1) - (s_2)$ with $s_1 \neq s_2$ then $L(D_0)$ does not contain constant elliptic functions. But if $f(z) \in \mathbb{C}(\Lambda)$ is nonconstant then f has at least two poles by Corollary 1.4, and so $f \notin L(D_0)$. That is, $l(D_0) = l(-D_0) = 0$ and (10) holds. Now, let $D_0 = \sum_{i=1}^{n}(r_i) - \sum_{j=1}^{n}(s_j)$ and $n \geq 2$. Then by Lemma 1.10, $D_0 \sim \sum_{i=1}^{n-2}(r_i) + (r_{n-1} + r_n - s_n) - \sum_{j=1}^{n-1}(s_j)$. So, by induction on n, (10) holds for any degree 0 divisor.

Now, let $D_1 = \sum_{i=1}^{n+1}(r_i) - \sum_{j=1}^{n}(s_j)$ be a degree 1 divisor. If $n = 0$ then $D_1 = (r_1)$ and clearly $\mathrm{L}(D_1)$ contains constant functions. In fact, $l(D_1) = 1$ as any nonconstant function must have a pole of degree at least 2 by by Corollary 1.4. If $D_1 = \sum_{i=1}^{n+1}(r_i) - \sum_{j=1}^{n}(s_j)$ and $n \geq 1$ then by Lemma 1.10, $D_1 \sim \sum_{i=1}^{n-1}(r_i) + (r_n + r_{n+1} - s_n) - \sum_{j=1}^{n-1}(r_j)$, and by induction on n, (9) holds for any degree 1 divisor.

In general, if $k \geq 2$ and $D_k = \sum_{i=1}^{n+k}(r_i) - \sum_{j=1}^{n}(s_j)$ is a degree k divisor then applying Lemma 1.10 repeatedly we may suppose $D_k = \sum_{i=1}^{k}(r_i)$. Moreover, applying the equivalence $(r_{k-1}) + (r_k) \sim (0) + (r_{k-1} + r_k)$ similarly, we can further assume that $D_k = (k-1)(0) + (\rho)$ where $\rho = r_1 + r_2 + \cdots + r_k$.
Case 1. $\rho = 0$: Then $D_k = k(0)$ and let $x = \wp(z), y = \wp'(z)/2$. Recalling Example 6, we get that the functions

$$1, x, x^2, x^3, \ldots$$

have only poles at 0 and the order of the poles are $0, 2, 4, 6, \ldots$, respectively. Similarly, by Example 7, the functions

$$y, xy, x^2y, x^3y, \ldots$$

have only poles at 0 and the order of the poles are $3, 5, 7, 9, \ldots$, respectively. If a function from the above list has a pole at 0 with order i, we denote it by f_i. Note that f_i are linearly independent as x is transcendental over $\mathbb{C}$ and y has algebraic degree 2 over $\mathbb{C}(x)$, as explained in the previous section. Therefore, in order to prove $l(D_k) = k$ it suffices to show $\mathrm{L}(D_k) = \langle f_0, f_2, \ldots, f_k \rangle$ since $f_0, f_2, \ldots, f_k$ are in $\mathrm{L}(D_k)$. Now, let g be any function in $\mathrm{L}(D_k)$. We proceed by induction on $i = \mathrm{ord}_0(g)$. If $i = 0$ then g is constant and $g = c \cdot f_0$. The case $i = -1$ is impossible by Corollary 1.4. So, we can assume g has a pole of order i where $2 \leq i \leq k$. Then the function $h(z) = g(z) - \mathrm{Res}_0(g) f_i$ is either constant or has a pole at 0 with order $2 \leq j < i$. By induction, $h(z) \in \mathrm{L}(D_k)$ and in particular, $\mathrm{L}(D_k) = \langle f_0, f_2, \ldots, f_k \rangle$.
Case 2. $\rho \neq 0$: Then $D_k = (k-1)(0) + (\rho)$ and let $D' = (k-1)0$. First observe that $l(D_k) \geq k - 1$ since any function in $\mathrm{L}(D')$ is also in $\mathrm{L}(D_k)$, and from the previous case we have $l(D') = k - 1$. Now, let $f \in \mathbb{C}(\Lambda)$ be a nonconstant function with divisor (recall Lemma 1.9)

$$\mathrm{div}(f) = -(0) - (\rho) + \text{positive terms}.$$

Since f has a pole at 0, $f \notin \mathrm{L}(D')$ and $l(D_k) \geq k$. Now, we show $l(D_k) \leq k$. Let g be any function in $\mathrm{L}(D_k)$ and consider the function

$$h(z) = (\mathrm{Res}_\rho(f))\, g(z) - (\mathrm{Res}_\rho(g))\, f(z).$$

Note that h can only have a pole at 0, and the multiplicity can be at most $k - 1$. So, $h \in \mathrm{L}(D')$, or $h \in \langle f_0, f_2, \ldots, f_{k-1} \rangle$. In other words, $g \in \langle f, f_0, f_2, \ldots, f_{k-1} \rangle$, as required.

2 Acknowledgments

The proofs of Lemma 1.9, Lemma 1.10, and the section 1.4.1 are based on the lecture notes by David [Jao].

References

[Jao] D. Jao, Topics in Cryptography - Lecture Notes, University of Waterloo, (2007).

[Sil] J. H. Silverman, The Arithmetic of Elliptic Curves, Springer-Verlag, (1986).

[Sil2] J. H. Silverman, Advanced Topics in the Arithmetic of Elliptic Curves, Springer- Verlag, (1994).