Contents

1 Order of Vanishing and Intersection Multiplicity

Order of vanishing simply means the intersection multiplicity of a point that when evaluated on E is zero or a pole.

2 Lemma 11.3

Let $P \neq Q$ and $\operatorname{div}(h) = [P] - [Q] \implies h(Q) = \infty \implies (h - c)(Q) = \infty$. So there must also be one zero of $h - c$.

Let $f \in V(I) : f(Q) \neq 0, \infty$ then

$$\operatorname{div}(g) = \sum \operatorname{ord}_R(f)[h(x, y) - h(R)]$$

remember that $\operatorname{ord}_Q(f) = 0$

Let P be a zero of f, then the factor in $\operatorname{div}(g)$ will be $n[h(x, y) - h(P)]$ so when $x, y = P$, then $h(x, y) - h(P) = 0$. Therefore $\operatorname{div}(g) = \operatorname{div}(f)$. Therefore they are constant multiples of each other. We can simply adjust f (or g) by multiplying by a constant so that $f = g$.

Since $h(Q) = \infty$, then if Q is a zero or pole of f then that factor is undefined. To illustrate this, assume $\operatorname{ord}_Q(f) = 1$, then

$$f(P) = (h(P) - \infty) \cdots$$

Since $\infty - \infty$ is undefined, so $f(Q)$ is undefined.

Now lets look at $\operatorname{ord}_Q(f) = n$. When $n > 0$, then

$$\operatorname{div}(f) = n[Q] + \cdots$$

$$\operatorname{div}(h^n) = -n[Q] + n[P]$$
$$\operatorname{div}(fh^n) = (n - n)[Q] + \cdots$$

which shows that Q is not a zero or pole of fh^n.

When $n < 0$ then f has a pole at Q and

$$\operatorname{div}(f) = n[Q] + \cdots$$
$$\operatorname{div}(f) = -[Q] + [P]$$
$$\operatorname{div}(h^n) = -n[Q] + n[P]$$
$$\operatorname{div}(fh^n) = (n - n)[Q] + \cdots$$

3 Divisors

$$f(x) = (x-a)^3(x-b)^5$$
$$\text{div}(f) = 3[a] + 5[b] - 8[\infty]$$

4 Weil Pairing

$$n \mid \text{char}(K)$$

There exists f such that
$$\text{div}(f) = n[T] - n[\infty]$$
because by theorem 11.2, $\deg(D) = 0, \text{sum}(D) = \infty \implies \exists f : \text{div}(f) = D$.

Likewise for
$$\begin{aligned}\text{div}(g) &= \sum_{R \in E[n]} ([T' + R] - [R]) \\ &= \sum_{R \in E[n]} [T' + R] - \sum_{nR=\infty} [R]\end{aligned}$$

Now we want to show that given an $T' \in E[n^2]$ such that $nT' = T$ then
$$\{T'' : nT'' = T\} = \{T' + R : R \in E[n]\}$$
This is equivalent to the statement that given any $T'' \in E[n^2]$ then
$$T'' = T' + R : R \in E[n]$$
$$\alpha : E[n^2] \to E[n]$$
$$\alpha(T'') = nT''$$
$$[E[n^2] : E[n]] = n^2$$
$$\ker \alpha = E[n]$$
$$T''_1, T''_2 \in E[n^2] : nT''_1 = nT''_2 = T \implies T''_1 \in T''_2 + E[n]$$
which proves the statement from before. Therefore
$$\sum_{R \in E[n]} [T' + R] = \sum_{nT''=T} [T'']$$

Now given
$$\text{div}(f) = n[T] - n[\infty]$$
We want to show that
$$\text{div}(f \circ n) = n \left(\sum_{R \in E[n]} [T' + R] \right) - n \sum_{R \in E[n]} [R]$$

4.1 Function Composition with Multiplication by n Map

$$P \to nP \to f(nP)$$

$T' + R$ generates the group of all $T'' : nT'' = T$.

$f(T) = 0 \implies f \circ n(T'') = 0$.

See here and Silverman's Proposition II.2.6(c).

Also import from Knapp's book page 316:
$$\text{ord}_x(f) = \text{ord}_{\psi(x)}(f \circ \psi^{-1})$$
Using this we see that
$$\text{ord}_{T'}(f \circ n) = \text{ord}_{nT'}(f \circ n \circ n^{-1})$$

5 Tate Pairing

ϕ is the qth power Frobenius. Since $\phi(D) = D$, the points are pemuted without changing the divisor. Since the points satisfy $f(P)$, so $f \in \mathbb{F}_q[x, y]$, and hence $\phi(f) = f$.

6 Computation of Pairings

6.1 Calculating Divisors

$3D = 3[(0, 3)] - 3[\infty]$ is easy. We just use the horizontal line that cuts through $(0, 3)$. So $3D = \text{div}(y - 3)$.

Sage code to see points of intersection with the curve:

```
sage: R.<x, y> = PolynomialRing(GF(7))
sage: I = Ideal(y^2 - x^3 - 2, y - 3)
sage: I.variety()
[{y: 3, x: 0}]
```

As expected. We can also observe that the gradient of the line is 0, which is tangent to the curve at this point.

For the divisor

$$3D_{(5,1)} = 3[(3, 6)] - 3[(6, 1)]$$

Observe that the tangent to the curve is calculated by

$$y' = \frac{3x^2}{2y}$$

So we see that $y'_{(3,6)} = 4$ and that $y = 4x + 1$ is tangent to $(3, 6)$. Likewise $y'_{(6,1)} = 5$ and $y = 5x - 1$ is tangent to $(6, 1)$

$$\implies \text{div}\left(\frac{4x - y + 1}{5x - y - 1}\right) = 3[(3, 6)] - 3[(6, 1)]$$

6.2 Miller Loop Divisors

$$\begin{aligned}
D_j &= j[P + R] - j[R] - [jP] - [\infty] \\
\text{div}(ax + by + c) &= [jP] + [kP] + [-(j + k)P] - 3[\infty] \\
\text{div}(x + d) &= [(j + k)P] + [-(j + k)P] - 2[\infty] \\
\text{div}\left(\frac{ax + by + c}{x + d}\right) &= [jP] + [kP] - [(j + k)P] - [\infty] \\
D_{j+k} &= (j + k)[P + R] - (j + k)[R] - [(j + k)P] + [\infty]
\end{aligned}$$

$$\begin{aligned}
D_j + D_k &= j[P + R] + k[P + R] - j[R] - k[R] - [jP] - [kP] + 2[\infty] \\
&= (j + k)[P + R] - (j + k)[R] - [jP] - [kP] + 2[\infty]
\end{aligned}$$

6.2.1 Example 11.6

This is the double and add algo. j is the final accumulated value, k is the doubled value.

We count up with j until we reach n. i keeps track of how much is left.

6.2.2 Example 11.7

We are calculating f_P, so $R = \infty$.

7 Alternative Weil Pairing

$$D_P \sim [P] - [\infty]$$
$$D_Q \sim [Q] - [\infty]$$
$$\mathrm{supp}(D_P) \cap \mathrm{supp}(D_Q) = \varnothing$$
$$e_n(P,Q) = \frac{f_{D_P}(D_Q)}{f_{D_Q}(D_P)}$$
$$D_P = [P+S] - [S]$$
$$D_Q = [Q] - [\infty]$$

You can also have

$$D_Q = [Q+R] - [R]$$

But the support must be disjoint, and $P, Q \in E[n]$.

$$\begin{aligned} e_n(P,Q) &= \frac{f_{D_P}(D_Q)}{f_{D_Q}(D_P)} \\ &= \frac{f_{D_P}(P+S)}{f_{D_P}(S)} / \frac{f_{D_Q}(Q+T)}{f_{D_Q}(T)} \end{aligned}$$

where $P, Q \in E[n]$ and $S, T \in E(K)$.

7.1 Independence of Choice for D_Q.

Let $D'_Q \sim D_Q$, then $D'_Q - D_Q \in \mathrm{Prin}(E)$. We assume div(h) and D_P have disjoint support. Since $D'_Q \sim D_Q$, then

$$D'_Q = D_Q + \mathrm{div}\,(h)$$
$$\mathrm{div}\,(f'_Q) = nD'_Q, \mathrm{div}\,(f_Q) = nD_Q \implies f'_Q = f_Q h^n$$

$$\begin{aligned} e_n(P,Q) &= \frac{f_{D_P}(D'_Q)}{f_{D'_Q}(D_P)} \\ &= \frac{f_{D_P}(D_Q) f_{D_P}(\mathrm{div}(h)}{f_{D_Q}(D_P) h(D_P)^n} \end{aligned}$$

But note that $h(D_P)^n = h(D_P) \cdots h(D_P) = h(nD_P)$ due to how evaluation on a divisor is defined. Since $\mathrm{div}(f_{D_P}) = nD_P \implies h(D_P)^n = h(\mathrm{div}(f_{D_P}))$.

$$e_n(P,Q) = \frac{f_{D_P}(D_Q) f_{D_P}(\mathrm{div}(h)}{f_{D_Q}(D_P) h(\mathrm{div}\,(f_{D_P}))}$$

Now use the Weil reciprocity to get the relation

$$e_n(P,Q) = \frac{f_{D_P}(D_Q)}{f_{D_Q}(D_P)}$$

8 Linear Equivalence of Riemann Roch Spaces

Let $D' = D + \mathrm{div}\, g$. Then

$$\phi : \mathcal{L}(D') \to \mathcal{L}(D)$$
$$\phi(f) = fg$$

is an isomorphism.

Proof: Let $f \in \mathcal{L}(D)$ then

$$\mathrm{div}\, f \geq -D' \iff \mathrm{div}\, fg = \mathrm{div}\, f + \mathrm{div}\, g \geq -D' + \mathrm{div}\, g$$

But $-D' + \mathrm{div}\, g = -D$ so

$$\mathrm{div}\, fg \geq -D \implies \mathrm{div}\, fg \in \mathcal{L}(D)$$