Contents

Weil Reciprocity

$$f(\mathrm{div}(g)) = g(\mathrm{div}(f))$$

```
sage: E = EllipticCurve([0, 17])
sage: E(2, 5) + E(4, 9) + E(-2, -3)
(0 : 1 : 0)
sage: E(-1, 4) + E(8, 23) + E(-206/81, 541/729)
(0 : 1 : 0)
sage: var("x y z")
(x, y, z)
sage: f = y - 2*x - z
sage: g = 9*y - 19*x - 55*z
sage: f(x=2, y=5, z=1), f(x=4, y=9, z=1), f(x=-2, y=-3, z=1)
(0, 0, 0)
sage: g(x=-1, y=4, z=1), g(x=8, y=23, z=1), g(x=-206/81, y=541/729, z=1)
(0, 0, 0)
sage: f(x=0, y=1, z=0), g(x=0, y=1, z=0)
(1, 9)
sage: f(x=2, y=5, z=1) * f(x=4, y=9, z=1) * f(x=-2, y=-3, z=1) / 1
0
sage: g(x=-1, y=4, z=1) * g(x=8, y=23, z=1) * g(x=-206/81, y=541/729, z=1) / 9^3
0
sage: g(x=2, y=5, z=1) * g(x=4, y=9, z=1) * g(x=-2, y=-3, z=1) / g(x=0, y=1, z=0)^3
-35200/243
sage: f(x=-1, y=4, z=1) * f(x=8, y=23, z=1) * f(x=-206/81, y=541/729, z=1) / f(x=0, y=1
....: , z=0)^3
35200/243
```

Proof

Let $z \in \mathbb{P}^1$ and $f_*\langle g\rangle(z) = g(T_1)\cdots g(T_n)$ where $\{T_1, ..., T_n\} = f^{-1}(z)$ is the fiber for z.

We claim that $f_*\langle g\rangle(\operatorname{div} z) = g(\operatorname{div} f)$.

$$f^{-1}(z) = \{T_1, ..., T_n\}$$

$$f_*\langle g\rangle(z) = g(T_1)\cdots g(T_n)$$

But $\operatorname{div} z = [0] - [\infty]$

$$f_*\langle g\rangle(0) = g(T_1)\cdots g(T_n)$$

where $T_i \in f^{-1}(0)$, which are the zeros of $f \Rightarrow f_*\langle g\rangle([0] - [\infty]) = g(\operatorname{div} f)$.

Likewise $z(\operatorname{div} f_*\langle g\rangle) = f(\operatorname{div} g)$ which using the argument above is easy to see.

$$f_*\langle g\rangle([0] - [\infty]) = f_*\langle g\rangle(0)/f_*\langle g\rangle(\infty) = z(\operatorname{div} f_*\langle g\rangle)$$

By the fact $P/Q(\operatorname{div} z) = (p_0/q_0)/(p_m/q_m) \Rightarrow z(\operatorname{div} P/Q) = ($ product of roots of $P/($ product of roots of $Q)$.

Divisor Construction

We can either use the Miller loop, or Mumford polynomial representation. Both are trivial.

We end up with a polynomial f that represents our divisor.

Proving Interpolation

Let $f \in K(C)^\times$, with roots $P_1, ..., P_n$. Then the norm

$$f(P)f(-P) = (x(P) - x(P_1)) \cdots (x(P) - x(P_n))$$

Canonical form is $f(x, y) = v(x) + yw(x)$. The conjugate of f is $\bar{f} = v(x) - yw(x)$ and the norm is

$$N_f = f \cdot \bar{f} = v(x)^2 - (x^3 + Ax + B)w(x)^2$$

For $r = \frac{f}{g} \in K(C)$

$$\frac{f}{g} = \frac{fg}{gg} = \frac{fg}{N_g}$$

But this norm also counts $-P$ which we want to disallow. We instead use the resultant.