Exercise 3.16. *Alternate Definition of Weil Pairing.* Let (E, O) be an elliptic curve group. We define a pairing

$$\tilde{e}_m : E[m] \times E[m] \longrightarrow \boldsymbol{\mu}_m$$

as follows: Let $P, Q \in E[m]$ and choose divisors D_P and D_Q in $\mathrm{Div}^0(E)$ such that $D_P \sim P - O$ and $D_Q \sim Q - O$. Assume further that D_P and D_Q are chosen with disjoing supports. Since P and Q have order m, there are functions $f_P, f_Q \in \overline{K}(E)$ satisfying

$$\mathsf{div}(f_P) = mD_P \qquad \text{and} \qquad \mathsf{div}(f_Q) = mD_Q.$$

We define

$$\tilde{e}_m = \frac{f_P(D_Q)}{f_Q(D_P)},$$

where $f(D) = \prod_{P \in C} f(P)^{D(P)}$.

(a) Prove that $\tilde{e}_m(P, Q)$ is well-defined.

(b) Prove that $\tilde{e}_m(P, Q) \in \boldsymbol{\mu}_m$.

Solution.

(a) First let $D'_P \sim D_P$. So there is a $g \in \overline{K}(E)$ such that $D'_P = D_P + \mathsf{div}(g)$. There is also a function $f'_P \in \overline{K}(E)$ such that $\mathsf{div}(f'_P) = mD'_P$, since D'_P must be of order m. We wish to show that

$$\frac{f'_P(D_Q)}{f_Q(D'_P)} = \frac{f_P(D_Q)}{f_Q(D_P)}.$$

We know that $mD'_P = mD_P + \mathsf{div}(g^m)$, and so $f'_P = f_P g^m$. Thus $f'_P(D_Q) = (f_P g^m)(D_Q)$ and

$$f_Q(D'_P) = f_Q(D_P + \mathsf{div}(g)) = f_Q(D_P) f_Q(\mathsf{div}(g)) \overset{(*)}{=} f_Q(D_P) g(mD_Q) = f_Q(D_P) g^m(D_Q),$$

where the equality $(*)$ comes from Weil reciprocity.

Thus

$$\frac{f'_P(D_Q)}{f_Q(D'_P)} = \frac{f_P(D_Q) g^m(D_Q)}{f_Q(D_P) g^m(D_Q)} = \frac{f_P(D_Q)}{f_Q(D_P)}.$$

(b) Now note that

$$f_P(D_Q)^m = f_P(mD_Q) = f_P(\mathsf{div}(f_Q)) \overset{(*)}{=} f_Q(\mathsf{div}(f_P)) = f_Q(D_P)^m,$$

where the equality $(*)$ comes from Weil reciprocity. Thus $\dfrac{f_P(D_Q)^m}{f_Q(D_P)^m} = \left(\dfrac{f_P(D_Q)}{f_Q(D_P)}\right)^m = 1$, and so $\tilde{e}_m(P, Q) \in \boldsymbol{\mu}_m$.

□