equality). On the other hand, using the definition of G, the fact that $(a+b)^p = a^p + b^p$ in $\mathbf{F}_{p^f}$, and the obvious observation that $(\frac{j}{q})^p = (\frac{j}{q})$, we compute:

$$G^p = \sum_{j=0}^{q-1} \left(\frac{j}{q}\right) \xi^{pj} = \sum_{j=0}^{q-1} \left(\frac{p}{q}\right)\left(\frac{pj}{q}\right) \xi^{pj},$$

by parts (b) and (c) of Proposition II.2.3. Pulling $(\frac{p}{q})$ outside the summation and making the change of variables $j' = pj$ in the summation, we finally obtain: $G^p = (\frac{p}{q})G$. Equating our two expressions for G^p and dividing by G (which is possible, since $G^2 = \pm q$ and so is not zero in $\mathbf{F}_{p^f}$), we obtain the quadratic reciprocity law. Thus, it remains to prove the following lemma.

Lemma. $G^2 = (-1)^{(q-1)/2}q$.

Proof. Using the definition of G, where in one copy of G we replace the variable of summation j by $-k$ (and note that the summation can start at 1 rather than 0, since $(\frac{0}{q}) = 0$), we have:

$$\begin{aligned} G^2 &= \sum_{j,k=1}^{q-1} \left(\frac{j}{q}\right)\xi^j \left(\frac{-k}{q}\right)\xi^{-k} = \left(\frac{-1}{q}\right) \sum_{j=1}^{q-1}\sum_{k=1}^{q-1} \left(\frac{jk}{q}\right)\xi^{j-k} \\ &= (-1)^{(q-1)/2} \sum_{j=1}^{q-1}\sum_{k=1}^{q-1} \left(\frac{j^2k}{q}\right)\xi^{j(1-k)}, \end{aligned}$$

where we have used Part (d) of Proposition II.2.3 to replace $(\frac{-1}{q})$ by $(-1)^{(q-1)/2}$, and for each value of j we have made a change of variable in the inner summation $k \longleftrightarrow kj$ (i.e., for each fixed j, kj runs through the residues modulo q as k does, and the summands depend only on the residue modulo q). We next use part (c) of Proposition II.2.3, interchange the order of summation, and pull the $(\frac{k}{q})$ outside the inner sum over j. The double sum then becomes $\sum_k (\frac{k}{q}) \sum_j \xi^{j(1-k)}$. Here both sums go from 1 to $q-1$, but if we want we can insert the terms with $j = 0$, since that simply adds to the double sum $\sum_k (\frac{k}{q})$, which is zero (because there are equally many residues and nonresidues modulo q). Thus, the double sum can be written $\sum_{k=1}^{q-1} (\frac{k}{q}) \sum_{j=0}^{q-1} \xi^{j(1-k)}$. But for each k other than 1, the inner sum vanishes. This is because the sum of the distinct powers of a nontrivial ($\neq 1$) root of unity ξ' is zero (the simplest way to see this is to note that multiplying the sum by ξ' just rearranges it, and so the sum multiplied by $\xi' - 1$ is zero). So we are left with the contribution when $k = 1$, and we finally obtain:

$$G^2 = (-1)^{(q-1)/2}\left(\frac{1}{q}\right)\sum_{j=0}^{q-1} \xi^0 = (-1)^{(q-1)/2}q.$$

This completes the proof of the lemma, and hence also the proof of the Law of Quadratic Reciprocity.