Problem 3 from Problem Set 8. Let $Y = \mathbf{G}_m^{\mathrm{an}}/q^{\mathbf{Z}}$ be a Tate curve. Prove that every endomorphism of Y lifts to an endomorphism $\mathbf{G}_m^{\mathrm{an}}$. Conclude that $\mathrm{End}(Y) \simeq \mathbf{Z}$.

Solution (following Tate). Denote the curve Y by Y_q to indicate the dependence on q. We will describe all homomorphisms $Y_q \to Y_r$ for all q and r with absolute value < 1, showing in particular that they can always be lifted to maps $\mathbf{G}_m^{\mathrm{an}} \to \mathbf{G}_m^{\mathrm{an}}$.

First, we take care of isomorphisms. We already know that the j-invariant $j(Y_q)$ satisfies $|j(Y_q)| > 1$ and that $j(Y_q) \neq j(Y_r)$ for $q \neq r$. Moreover, the only elliptic curves with automorphism groups of order > 2 have j-invariant equal to zero or 1728 [Hartshorne IV 4.7] and $|j| \leq 1$ for $j \in \mathbf{Z}$. We conclude that the only isomorphisms between the curves Y_q and Y_r are the identity and the map induced by $w \mapsto w^{-1}$ for $q = r$.

This in particular implies that every isogeny (i.e. nonzero homomorphism) $\alpha \colon Y_q \to Y_r$ is determined uniquely by its kernel: there is a unique isomorphism $Y_r \simeq Y_q/\ker\alpha$. Therefore it suffices to analyze finite subgroup schemes of Y_q.

Suppose that $q^n = r^m$ for some nonzero integers m and n. In this case, the n-th power map $\mathbf{G}_m^{\mathrm{an}} \to \mathbf{G}_m^{\mathrm{an}}$ sends q to r^m and therefore induces an isogeny $\alpha_{m,n} \colon Y_q \to Y_r$. We are going to show the following claim:

$$\textit{Every isogeny } Y_q \to Y_r \textit{ is of the form } \alpha_{m,n} \textit{ for some } m \textit{ and } n \textit{ for which } q^n = r^m. \qquad (*)$$

Specializing $(*)$ to $q = r$, we see that every isogeny $Y_q \to Y_q$ is of the form $\alpha_{n,n}$ for some nonzero n. Note that $\alpha_{n,n}$ is simply the multiplication by n map on Y_q. We conclude that $\mathrm{End}\, Y_q \simeq \mathbf{Z}$ as desired.

To prove $(*)$, note first that after passing to a finite extension of the base field, every isogeny between elliptic curves is a composition of isogenies of prime degree. Indeed, it suffices to show that over an algebraically closed field k, every nontrivial finite subgroup scheme H of an elliptic curve Y contains a subgroup scheme of order p for some prime p. The group $H(k)$ is finite and if it is nontrivial, it contains an element of prime order. The group $H(k)$ can be trivial only if the map $Y \to Y/H$ is purely inseparable, in which case H contains the kernel of Frobenius $F \colon Y \to Y'$ which has order (length) p.

The above combined with the observation that $\alpha_{m',n'} \circ \alpha_{m,n} = \alpha_{mm',nn'}$ implies that it is enough to prove $(*)$ for isogenies of prime degree.

Now, there are two obvious ways of constructing a subgroup scheme of Y_q of a prime order p: the image of $\mu_p \subseteq \mathbf{G}_m^{\mathrm{an}}$, and the image of a subgroup of $\mathbf{G}_m^{\mathrm{an}}$ generated by a p-th root r of q. Note that the former corresponds to the map $\alpha_{p,1} \colon Y_q \to Y_{q^p}$, and the latter to $\alpha_{1,p} \colon Y_q \to Y_r$ where $r^p = q$.

It remains to show that every subgroup scheme of Y_q of order p is of the above form. If p is invertible in K, this is very easy. After extending the ground field, the subgroup scheme is generated by an element $s \in Y_q(K)$ of order p. If $\tilde{s} \in K^\times = \mathbf{G}_m^{\mathrm{an}}(K)$ is an element above s, then $\tilde{s}^p = q^m$ for some integer m, while $\tilde{s} \notin q^{\mathbf{Z}}$. If m is prime to p, write $am + bp = 1$ for integers a and b. Then $r = \tilde{s}^a q^b$ generates the same subgroup and satisfies $r^p = q$. If p divides m, say $m = bp$, then $r = \tilde{s} q^{-b}$ generates the same group and is a primitive p-th root of unity.

Finally, suppose that p is equal to the characteristic of K. If the subgroup scheme in question is infinitesimal, it must be equal to the kernel of Frobenius $F \colon Y_q \to Y_{q^p}$, which is the image of μ_p. Otherwise, after extending the ground field it has a point of order p, and we argue as above. $\square$