(1) Let $E$ be an elliptic curve defined over a field $K$. Let $\alpha$ be a nonzero endomorphism of $E$. Show that $\alpha : E(K) \to E(K)$ is surjective.

(Hint: Let $\alpha(x, y) = (r_1(x), r_2(x)y)$, and write $r_1(x) = p(x)/q(x)$ for polynomials $p, q$. To show that a given point $(a, b)$ is in the image of $\alpha$ consider the following two cases: (i) $p(x) - aq(x)$ is not the zero polynomial, so it has a root $x_0 \in \overline{K}$.

(ii) When $p(x) - aq(x)$ is constant, show that either $p(x)$ or $q(x)$ is not constant. Use this to prove surjectivity.)

(2) Let $E$ be an elliptic curve defined over a field $K$. Weil reciprocity says that two functions $f, g$ on $E$, $f, g : E(\overline{K}) \to \mathbb{K} \cup \infty$ whose divisors have disjoint support satisfy

$$f(\text{div}(g)) = g(\text{div}(f)).$$

(For a divisor $D = \sum n_P P$, $f(D)$ is defined to be $f(D) = \prod f(P)^{n_P}$, so both of the above evaluations take values in $\overline{K} \cup \infty$.)

Use Weil reciprocity to show that the two definitions of the Weil pairing given in class are equivalent. (You do not have to prove that Weil reciprocity holds.)

(3) Let $E$ be an elliptic curve over a field $K$, and let $n$ be a positive integer that is coprime to the characteristic of $K$.

(a) Deduce from the properties of the Weil pairing $e_n$ proved in class that $e_n(S, T) = e_n(T, S)^{-1}$ for all $S, T \in E[n]$, and also that $e_n$ is non-degenerate in the first variable.

(b) Let $\sigma$ be an automorphism of $\overline{K}$ that fixes the coefficients of $E$. Show that

$$\sigma(e_n(S, T)) = e_n(\sigma(S), \sigma(T)).$$

(4) Let $E$ be an elliptic curve over a field $K$. Let $f(x, y)$ be a function on $E$ to $\overline{K} \cup \infty$, and let $n \geq 1$ be an integer not divisible by the characteristic of $K$. Suppose that $f(P + T) = f(P)$ for all $P \in E(\overline{K})$ and all $T \in E[n]$. Show that there is a function $h$ on $E$ such that $f(P) = h(nP)$ for all $P$.

To prove the above statement proceed as follows: Let $f$ be any function as above. The above property means that $f$ is invariant under translations by elements of $E[n]$. Let $F$ be the field of functions with this property. We want to show that

$$F = \overline{K}(g_n(x), yh_n(x)),$$

where the multiplication-by-$n$ map $n(x, y)$ is given by $n(x, y) = (g_n(x), yh_n(x))$. The right-hand-side of the displayed formula are the functions on $E$ that are of the form $h(n(x, y))$.  

1
You may want to prove this in the following steps:

(i) Let \( \overline{K}(x,y) \) be the set of all function on \( E \). Show that we can regard \( \overline{K}(x,y) \) as a degree 2 extension of \( \overline{K}(x) \).

(ii) Let \( T \in E[n] \). There are functions \( R(x,y), S(x,y) \) such that \((x,y) + T = (R(x,y), S(x,y))\). Let \( \sigma_T : \overline{K}(x,y) \to \overline{K}(x,y) \) be the following map:

\[
\sigma_T : f(x,y) \mapsto f(R,S).
\]

Show that \( \sigma_T \) is an automorphism of \( \overline{K}(x,y) \), and show that \( \sigma_T \neq \sigma_{T'} \) for \( T \neq T' \in E[n] \). Show that \( F \) is the fixed field of \( \overline{K}(x,y) \) under the group of automorphisms \( \{ \sigma_T : T \in E[n] \} \), and that \([\overline{K}(x,y) : F] = n^2\).

(iii) Now use the fact that \( g_n(x) = \phi_n/\psi^2_n \) (with \( \phi, \psi \) as on homework 8), whose degrees you computed on homework 8. Use this to deduce that

\[
[\overline{K}(x,y) : \overline{K}(g_n(x), yh_n(x))] = n^2.
\]

(iv) Deduce that \( F = \overline{K}(g_n(x), yh_n(x)) \).