Elliptic Curves

An elliptic curve $E/K$ over a field $K$ is a curve which is defined by an equation of the form

$$(1) \quad E : y^2 + a_1 xy + a_3 y = x^3 + a_2 x^2 + a_4 x + a_6,$$

where $a_i \in K$ and $\Delta_E := b_4^3 - 27 b_6^2 + b_8(36 b_4 - b_2^2) \neq 0$. Here

$$b_2 = a_1^2 + 4 a_2, \quad b_4 = a_1 a_3 + 2 a_4, \quad b_6 = a_3^2 + 4 a_6,$$
$$b_8 = -a_1 a_3 a_4 - a_4^2 + a_1^2 a_6 + a_2 a_3^2 + 4 a_2 a_6.$$

The set of $K$-rational points of $E/K$ is the set $E(K)$ of points $(x, y) \in K^2$ which satisfy equation (1), together with the point $O = P_{\infty}$ at infinity.

If $r, s, t, u \in K$ and $u \neq 0$, then the transformation $T : x = u^2 x' + r, \quad y = u^3 y' + su^2 x' + t,$

takes the elliptic curve $E/K$ to another one, say $E'/K$ (in the variables $x', y'$); we then say that $E'/K$ is isomorphic to $E/K$. Note that $T$ induces a bijection

$$T^* : E'(K) \simarrow E(K)$$

between the sets of $K$-rational points.
If \( \text{char}(K) \neq 2, 3 \), then there is a transformation such that \( E/K \) assumes the (short) Weierstrass form

\[
E : y^2 = x^3 + ax + b,
\]

where \( \Delta_E = -2^4(4a^3 + 27b^2) \neq 0 \). In this case the group law

\[
(x_1, y_1) \ast (x_2, y_2) = (x_3, y_3)
\]

in \( E(K) \) is given by the rule

\[
\begin{align*}
x_3 &= \lambda^2 - x_1 - x_2 \\
y_3 &= \lambda(x_1 - x_3) - y_1
\end{align*}
\]

in which

\[
\lambda = \begin{cases} 
\frac{y_2 - y_1}{x_2 - x_1} & \text{if } x_1 \neq x_2 \\
\frac{3x_1^2 + a}{2y_1} & \text{if } x_1 = x_2 \text{ and } y_1 = y_2.
\end{cases}
\]

**Notes:**

1) We usually write the group law additively, i.e. we write \( P + Q \) in place of \( P \ast Q \) and hence \( kP \) in place of \( \underbrace{P \ast P \ast \cdots \ast P}_k \).

2) The extra point \( P_\infty \) serves as the identity of the group law: \( P_\infty + P = P + P_\infty = P \), for all \( P \in E(K) \). Similarly, \(-P = (x, -y) \) is the inverse of \( P = (x, y) \).