\[
    f(x, y) = y^2 - (ax^3 + bx^2 + cx + d) = y^2 - g(x)
    \]

**Elliptic curve**: no (linear) factor, no double point. (in \( \mathbb{P}^2(\mathbb{R}) \))

\( f(x, y) = 0 \) is an elliptic curve \( \iff g(x) \) has no repeated root.

\[
    \begin{align*}
    F(x, y, z) &= y^2 - (ax^3 + bx^2z + cxz^2 + dz^3) \\
    F_x &= -3ax^2 - 2bz^2 - c \\
    F_y &= 2yz \\
    F_z &= y^2 - bx^2 - 2czx^2 - 3dz^2
    \end{align*}
    \]

\( F = 0 \) when? (\( x_0, y_0, z_0 \))

\[
    \begin{align*}
    F_{x_0} &= 0 \\
    F_{y_0} &= 0 \implies y_0 = 0 \lor z_0 = 0 \quad (\text{bad} \implies x_0 = 0 \not= 0 ) \\
    F_{z_0} &= 0 \\
    F_{y_0} &= 0 \\
    y_0 &= 0 \\
    z_0 &= 0 \\
    y_0 &= 0 \\
    F(x_0, y_0, z_0) = f(x_0, 0) = -g(x_0) = 0 \\
    0 = F_x(x_0, y_0) = -2z_0(23a(z_0)^3 + 24b(z_0)^2 + c) \not= 0 \\
    \end{align*}
    \]
Linea factor? \( f(x,y) = (ax+by+c)R(x,y) \)

\[
F(x,y,z) = L(x,y,z)R(x,y,z)
\]

\[
(aX+bY+c)R(x,y,z)
\]

One of \( a, b, c \neq 0 \), wlog \( c \)

\[
F(x,y,z) = (y-aX-bY)S(x,y,z)
\]

Set \( T(x,z) = S(x,ax+by,z) \)

\[
= \text{homogeneous degree 2}
\]

\[
= \frac{x^3}{x^2} + q\left(\frac{y}{z}\right) + r
\]

\[
= \frac{x^2}{(y-v)(z-v)}
\]

\[
= p(x-v_1)(x-v_2) \quad r_1, r_2 \in \mathbb{C}
\]

\[
\Rightarrow \exists x_1, z_1 \text{ s.t. } x_1-v_1, z_1 = 0
\]

\[
\Rightarrow T(x_1, z_1) = 0 \quad y_1 = ax_1+by_1
\]

\[
S(x_1, y_1, z_1) = 0 \quad \Rightarrow \quad L(x_1, y_1, z_1) = 0
\]

\[
\Rightarrow \quad F_x = L_xS + L_yS_x = 0 \text{ at } x_1, y_1, z_1, \text{ etc.}
\]

\[
\Rightarrow \quad F \text{ has a double singular point}
\]
\[ f(x,y) = y^2 - (a x^3 + b x^2 + c x + d) = y^2 - q(x) \]

Elliptic curve \( \Rightarrow \) no singular point, no linear factor

\[ q(x) \text{ has no repeated root.} \]

Suppose not elliptic \( \Rightarrow \) Projectively \( f(x,y,z) = y^2 z - (a x^3 + b x^2 z + c x z^2 + d z^3) \)

Singular point:
\[
\begin{align*}
    f_x &= -(3a x^2 + 2b x z + c z^2) \\
    f_y &= 2 y z \\
    f_z &= y^2 - (3a x^2 + b x^2 + 2 c x z + 3 d z^2)
\end{align*}
\]

\[ \Rightarrow \text{repeated root.} \quad a x^2 + c z^2 \]

Linear factor \( F(x,y,z) = L(x,z) Q(x,y,z) \)

\[ \Rightarrow \text{repeated root!} \quad \text{singular point.} \]

Repeated root \( \Rightarrow \) not elliptic

\[
\begin{align*}
    q(x_0) &= 0 = q'(x_0) \\
    f_x &= -q'(x) \quad \Rightarrow (x_0,0) \text{ is a singular point.} \\
    f_y &= 2 y
\end{align*}
\]
We've seen that defining, for $A, B, C \in \mathcal{C}_f(\mathbb{R})$,

$AB = \text{the third point on the line through } A \text{ and } B$

$(AA = \text{the other point on the tangent line through } A)$

gives a well-defined, but not well-behaved, product on $\mathcal{C}_f(\mathbb{R})$

Eg., it's not associative!

Eg. if $AA = B$, then

$A(AB) = B$ (because $AB = A$) but

$(AA)B = BB$ is almost certainly not $B$!

To fix this, we introduce another binary operation, $+$, as follows.

Pick any point $O \in \mathcal{C}_f(\mathbb{R})$, then define for $A, B, C \in \mathcal{C}_f(\mathbb{R})$,

$A + B = O(AB)$

Picture:
We will see that this defines a rule: \( C^i_k(\mathbb{R}) \) an (abelian) group, in:

\[
\begin{align*}
A + 0 &= A \quad \text{for all } A \\
A + B &= B + A \quad \text{for all } A, B \\
\text{For every } A \text{ there is exactly one } B \text{ with } A + B = 0 \\
A + (B + C) &= (A + B) + C.
\end{align*}
\]

The first few are straightforward:

\[
A + 0 = 0(A) = \text{the third pt on the line through } 0 \text{ and } (\text{the third pt on the line through } 0 \text{ and } A)
\]

\[
AB = BA, \quad \text{so}
\]

\[
A + B = 0 = 0(AB) = 0(BA) = B + A.
\]

\[
A + B = 0 = 0(AB) \text{ means the line through } 0 \text{ and } AB \text{ is tangent at } 0 \text{. There is only one such line, so } AB = 0(0) = 0. \text{ So } B = A(AB) = A(0) = 0.
\]
**Proof:** Since \( L \not\subseteq C_f(\mathbb{R}) \), \( L \cap C_f(\mathbb{R}) \) consists of at most 3 points (if \( f \) is cubic), so \( L \cap C_f(\mathbb{R}) = \{P_1, P_2, P_3\} \).

Pick a point \( Q \in L \), \( Q \neq P_1, P_2, P_3 \). Then \( f(Q) \neq 0 \);

set \( \alpha = \frac{g(Q)}{f(Q)} \) (well-defined) and set \( h(x,y) = \alpha f(x,y) + g(x,y) \).

Note then that \( h(Q) = \frac{g(Q)}{f(Q)} f(Q) + g(Q) = 0 \). Also note that \( h(P_i) = 0 \) for all \( i = 1, \ldots, 9 \), so in fact,

\[
h(P_1) = h(P_2) = h(P_3) = h(Q) = 0,
\]

so \( L \cap C_h(\mathbb{R}) = \{P_1, P_2, P_3, Q\} \).

But \( h \) is cubic, so \( L \subseteq C_h(\mathbb{R}) \), and moreover,

\[
h(x,y) = L(x,y) g(x,y) \quad \text{where} \quad L(x,y) = 0 \quad \text{defines} \quad L.
\]

Since \( L(P_i) \neq 0 \), \( i = 3, 5, \ldots, 9 \), but \( h(P_i) = 0 \), we must have \( g(P_i) = 0 \), \( i = 3, \ldots, 9 \), i.e.

\[
\text{Note: This is special! Six randomly chosen points generally do not all lie in } C_q(\mathbb{R}) \text{ for some quadratic } g(x,y);
\]

\[
g(x,y) = ax^2 + bxy + cy^2 + dx + ey + f = 0
\]

for 6 values of \( (x,y) \) \( \Rightarrow \) 6 linear eqns: \( a, b, \ldots, f \)

Typically, only solution for all 6 will be \( a = \ldots = f = 0 \).
If given $A$, we set $B = A(20)$, then $A + B = O(AB) = O(A(A(20))) = O(20) = 0$.

Picture:

\[ B = -A \]

**Associativity** is the for one:

\[
A + (B + C) = A + (O(BC)) = O(A(O(BC)))
\]

\[
(A + B) + C = (O(AB)) + C = O((O(AB)) C)
\]

How do you manipulate this? Product **is not** associative.

We need to retreat to the behavior of the equation

**Lemma.** Suppose $f(x,y)$, $g(x,y)$ are cubic polynomials, and $P_1, P_2, \ldots, P_q \in C_1(\mathbb{R}) \cap C_2(\mathbb{R})$, with $P_1, P_2, P_3$ on a line $L$ (but the line is not $C_4(\mathbb{R})$). Then there is a quadratic polynomial $q(x,y)$ so that $P_1, P_2, \ldots, P_q \in C_q(\mathbb{R})$. 
I.e., the result says that for \( P_i = (x_i, y_i) \), \( i = 1, \ldots, 9 \), the vectors \( (x_i, x_{i+1}, y_i, x_{i+1}, 1) \) are linearly dependent.

On to associativity!

Given \( A, B, C \in \mathbb{G}_f(R) \), \( f = \) elliptic curve, we want
\[
A + (B + C) = (A + B) + C = \mathcal{O}(A + (B + C)) = \mathcal{O}((A + B) + C)
\]

*Note:* Enlarge to show \( A(2B + C) = (2A + B)C \).

Set \( P_1 = B, P_2 = BC, P_3 = C \) (all lie on a line).

\( P_4 = AB, P_5 = O, P_6 = O(AB) \)
\( P_7 = A, P_8 = O(BC), P_9 = O((AB) + C) \)

Assume these points are all distinct.

We want to show that \( A(2BC) = P_7P_8 = O((AB))C = P_9 \)

i.e., \( P_7, P_8, P_9 \) lie on a line.

To use the lemma, we need to build a cubic eqn \( g \).

Note that \( P_1, P_4, P_7 \) on \( B, AB, A \) so lie on a line \( L_1 \), let \( L_1(x, y) = 0 \) be its eqn.

\( P_2, P_5, P_8 = BC, O, O(BC) \) lie on \( L_2 \); \( L_2(x, y) = 0 \).

\( P_3, P_6, P_9 = C, O(AB), O((AB) + C) \) lie on \( L_3 \); \( L_3(x, y) = 0 \).
Then set
\[ g(x, y) = L_1(x, y), L_2(x, y), L_3(x, y) \]

So \( P_1, \ldots, P_q \in G_{x, y}(IR) \) = the union of the 3 lines!

All the hypotheses of the Lemma are satisfied

\( P_1, P_2, P_3 = B, B, C \) lie on a line \( L \), \( L \notin G_f(IR) \)

w.f. \( f(x, y) = 0 \) is an elliptic curve.

\( \exists \) a quadratic \( g(x, y) \) so that

\[ P_4, \ldots, P_q \in G_{x, y}(IR) \]

\( P_4, P_5, P_6 = AB, D, D(AB) \) lie on a line \( E \), \( L_4 \), and

\( \exists \) \( L_4 \cap G_{x, y} = \{ P_4, P_5, P_6 \} \) \( \Rightarrow \) \( L_4 \notin G_{x, y}(IR) \) is an

\( \exists \) a degree \( 2 \). So

\( g(x, y) = L_4(x, y), L_5(x, y) \) is a product of linear factors.

\( \Rightarrow \) \( G_{x, y}(IR) = \) a union of two lines, \( L_4, L_5 \).

Then \( P_7, P_8, P_9 \in L_5 \), since otherwise

\( \exists \) \( P_4, P_5, P_6 \) and one of \( P_7, P_8, P_9 \) lie \( \Rightarrow \)

\( \Rightarrow \) \( L_4 \cap G_{x, y} \) has at least \( 1 \) pt. \( \Rightarrow \) \( L_4 \notin G_{x, y}(IR) \)

a contradiction, \( \Rightarrow \) \( P_7, P_8, P_9 \) lie on a line!
What about when the points $P_1, \ldots, P_q$ are not all distinct? Appeal to "continuity"!

$Q, A, B, C \sim$ nearby points $Q', A', B', C'$

$\sim O'A'$ is close to $OA$, etc.

Note that if $A$ (say) is held fixed (continuing) and $B$ (say) moves, then $AB$ is determined by $B$, and if $AB = C = AB'$, then $AB = AC = B'$, so the function $B \mapsto AB$ is one-to-one.

Given $A, B, C$, wiggle them a little (along $C_{p q}(RI)$) to $A', B', C'$ all distinct $(P_1, P_2, P_3)$. Then wiggle $Q$

to $Q'$ so that

Given $A, B, C$, wiggle $Q$ a little (along $C_{q p}(RI)$) to make $Q, Q'AB), Q'BC), (Q'(AB)C = P_5, P_6, P_7, P_8$

distinct from the rest.

Then wiggle $A$ to $A'$ so that $A'BC, Q(A'BC), A', (Q(A'BC))C$

= $P_4, P_5, P_6, P_7, P_8$ are distinct from the rest. ($\times$)

Then wiggle $B$ to $B'$ so that $A'B'C, Q'AB'C), A'(Q'AB'C), B', B'C, Q'(B'C)$ distinct from rest. ($\times$)

Then wiggle $C$ to $C'$ -

($\times$) without making pts formerly distinct the same again!
After all this, the $9$ fits are distinct

(each depends on a distinct collection of the $0, A, B, C$, the first letter where the disagree was addressed, (at the point where)

they were separated, and then never reunited...)

Then our former argument applies, so

$$A'(Q'(B'(i))) = (Q'(A'B') C')$$

So $A(0(BC))$ is close to which is close to

$$0(AB) C$$

So $A(0(BC))$ is close to $(0(AB)) C$, where "close" means as small as we want, $\Rightarrow A(0(BC)) = (0(AB)) C$.

The only problem with this argument: verifying the continuity of "AB".

In the end, this amounts to: If you have a cubic

$p(x, L(x))$ and you wiggle the coefficients a little bit, and it always has three roots, then the roots just wiggle a little bit...
How important is the (arbitrarily chosen) point to call \( O \)? In terms of the group structure, not much.

If we chose a different point \( O' \) to work from, we get a different addition:

\[
A + B = O(AB) \\
A \oplus B = O'(AB)
\]

But if we choose \( W = -O' \) (a first addition) we have

\[
O' + W = O \quad \textit{ie} \quad O(O'W) = O \textit{ ie} \\
(O'W) = OQ, \quad \textit{ie} \quad W = O'(QO), \quad \textit{then}
\]

\[
O' + (A \oplus B) = O(O'(A \oplus B)) = O(O'(O'(AB)))
\]

\[
= O(O'O') = O(AB) = A + B
\]

\[
\Rightarrow W + O' + (A \oplus B) = A + B + W
\]

\[
to \quad A \oplus B
\]