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

Elliptic curve: no (linear) factor, no ~~double~~ singular point. (in $\mathbb{P}_2(\mathbb{R})$)

Hard! Show these over $\mathbb{C}$!

$f(x,y)=0$ is an elliptic curve $/\mathbb{C}$ $\Longleftrightarrow$ $g(x)$ has no repeated root.

Pf Work projectively:

$$F(X,Y,Z) = Y^2Z - (aX^3 + bX^2Z + cXZ^2 + dZ^3)$$

$$F_X = -3aX^2 - 2bXZ - cZ^2$$

$$F_Y = 2YZ$$

$$F_Z = Y^2 - bX^2 - 2cXZ - 3dZ^2$$

$\nabla F = 0$ <u>when</u>? (X_0, Y_0, Z_0)

$F_Y = 0 \Rightarrow Y_0 = 0$ or $Z_0 = 0$ (both $\Rightarrow X_0 = 0$ $\times$)

$$\boxed{\begin{array}{l} Z_0 = 0 \Rightarrow F_X = -3aX_0^2 = 0 \quad (a \neq 0) \Rightarrow X_0 = 0 \\ \quad F_Z = 0 \Rightarrow Y_0 = 0 \quad \times \end{array}}$$

$Z_0 \neq 0 \Rightarrow Y_0 = 0$ $\quad f(X_0,Y_0,Z_0) = f\left(\frac{X_0}{Z_0}, 0\right) = -g\left(\frac{X_0}{Z_0}\right) = 0$

$0 = F_X(X_0,Y_0,Z_0) = -Z_0^2\left(3a\left(\frac{X_0}{Z_0}\right)^2 + 2b\left(\frac{X_0}{Z_0}\right) + c\right)$ $\longrightarrow$ repeated root.

$= -Z_0^2\, g'\left(\frac{X_0}{Z_0}\right) \Rightarrow g'\left(\frac{X_0}{Z_0}\right) = 0$

Linear factor? $f(x,y) = (ax+by+c)\,r(x,y)$ Ec(2

$$F(X,Y,Z) = L(X,Y,Z)\,R(X,Y,Z)$$
$$(aX+bY+cZ)\,R(X,Y,Z)$$

one of $a,b,c \neq 0$, wlog b

degree 2

$$F(X,Y,Z) = (Y-\alpha X-\beta Z)\,S(X,Y,Z)$$

Set $T(X,Z) = S(X,\alpha X+\beta Z, Z)$

$= $ homogeneous degree 2

$$= Z^2\left(p\left(\frac{X}{Z}\right)^2 + q\left(\frac{X}{Z}\right) + r\right)$$
$$= pZ^2\left(\frac{X}{Z}-r_1\right)\left(\frac{X}{Z}-r_2\right)$$
$$= p(X-r_1Z)(X-r_2Z) \quad r_1, r_2 \in \underline{\underline{\mathbb{C}}}.$$

$\Rightarrow \exists\ X_1, Z_1 \in \mathbb{C}$ s.t. $X_1 - r_1 Z_1 = 0$

$\Rightarrow T(X_1,Z_1) = 0 \quad Y_1 = \alpha X_1 + \beta Z_1$

$S(X_1,Y_1,Z_1) = 0 \quad \& \quad L(X_1,Y_1,Z_1) = 0$

$\Rightarrow F_X = L_X S + L S_X = 0$ at X_1, Y_1, Z_1 etc..

$\Rightarrow F$ has a ~~double~~ singular part.

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

Elliptic curve (= no singular point, no linear factor)

$\iff$ $g(x)$ has no repeated root.

Suppose not elliptic. Think projectively. $F(X,Y,Z) = Y^2Z - (aX^3+bX^2Z+cXZ^2+dZ^3)$

Singular point

$$F_X = -(3aX^2+2bXZ+cZ^2)$$
$$F_Y = 2YZ$$
$$F_Z = Y^2 - (\cancel{} bX^2 + 2cXZ + 3dZ^2)$$

$\Longrightarrow$ repeated root.

Linear factor $F(X,Y,Z) = \underbrace{L(X,Y,Z)}_{aX+bY+cZ} Q(X,Y,Z)$

$\Longrightarrow$ ~~repeated root!~~ singular point.

repeated root $\Rightarrow$ not elliptic

$$g(x_0) = 0 = g'(x_0)$$

$f_x = -g'(x)$ $\longrightarrow$ $(x_0, 0)$ is a singular point.

$f_y = 2y$

we've seen that defining, for $A, B \in C_f(\mathbb{R})$,

AB = the third point on the line through A & B

(AA = the other point on the tangent line through A)

gives a well-defined, but not well-behaved, product on $C_f(\mathbb{R})$.

E.g., it's not associative!

eg if $AA = B$, then

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

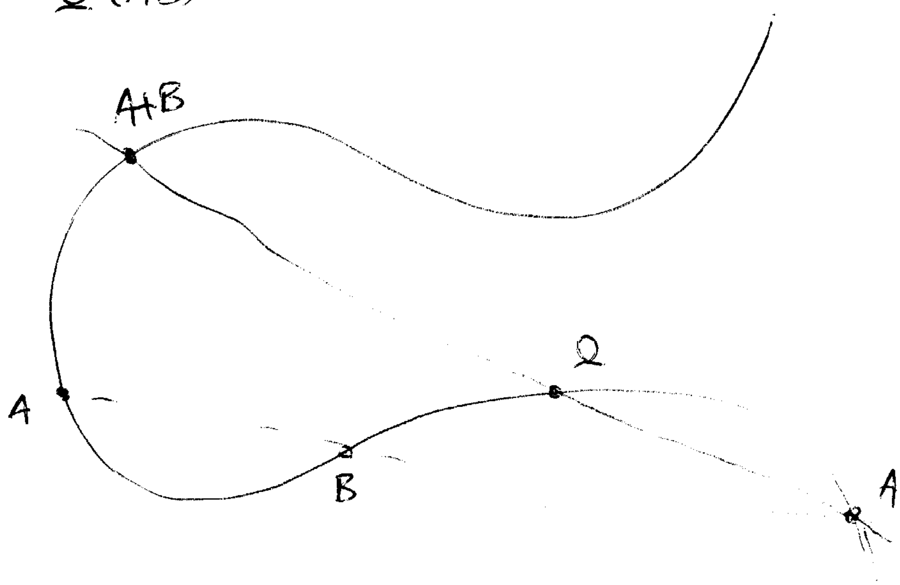
$(AA)B = BB$ is almost certainly not B!

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

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

$$A+B = O(AB)$$

Picture:



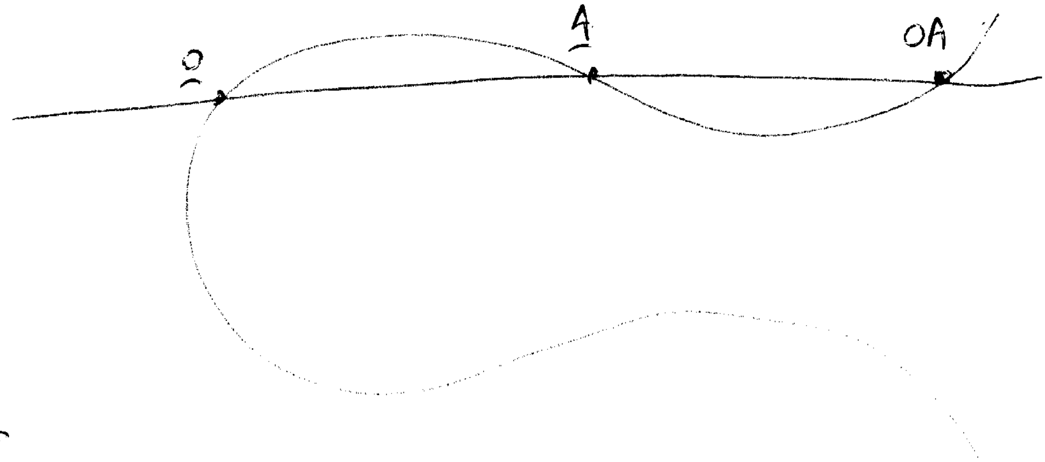
We will see that this ~~defines~~ makes $C_f(\mathbb{R})$ an (abelian) group; i.e.

$$A + \underline{O} = A \quad \text{for all } A$$
$$A + B = B + A \quad \text{for all } A, B$$
for every A there is exactly one B with $A + B = \underline{O}$
$$A + (B + C) = (A + B) + C.$$

The first few are straightforward.

$A + \underline{O} = \underline{O}(A\underline{O})$ = the third pt on the line through $\underline{O}$ and (the third pt on the line through $\underline{O}$ and A)

$= \underline{A}$



$AB = BA$, so

$A + B = \underline{O}(AB) = \underline{O}(BA) = B + A.$

$A + B = \underline{O} = \underline{O}(AB)$ means the line through $\underline{O}$ and AB is tangent at $\underline{O}$. There is only one such line, so $AB = \underline{O}\underline{O}$. So $B = A(AB) = A(\underline{O}\underline{O})$

Proof: Since $L \not\subseteq C_f(\mathbb{R})$, $L \cap C_f(\mathbb{R})$ consists of at most 3 points (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 $\alpha = \dfrac{-g(Q)}{f(Q)}$ (well-defined) and set $h(x,y) = \alpha f(x,y) + g(x,y)$

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

$h(P_1) = h(P_2) = h(P_3) = h(Q) = 0$, so $L \cap C_h(\mathbb{R}) \supseteq \{P_1, P_2, P_3, Q\}$

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

$h(x,y) = L(x,y)\, q(x,y)$ where $L(x,y) = 0$ defines L.

quadratic

Since $L(P_i) \neq 0$, $i = 4, 5, \ldots, 9$ but $h(P_i) = 0$ we must have $q(P_i) = 0$ $i = 4, \ldots, 9$, i.e.

Note: This is special! Six randomly chosen points generally do not all lie on $C_q(\mathbb{R})$ for some quadratic $q(x,y)$:

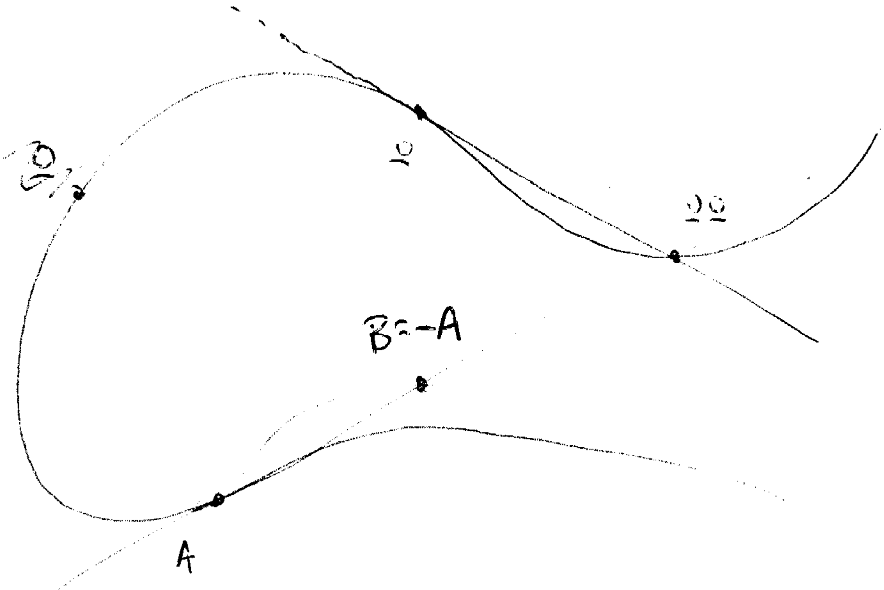
$$q(x,y) = ax^2 + bxy + cy^2 + dx + ey + f = 0$$

for 6 values of (x,y) $\Longrightarrow$ 6 linear eqns in $a, \ldots, f$

Typically, only solution for all 6 will be $a = \cdots = f = 0$.

$\Rightarrow$ unique. OTOH, given A, if we set $B = A(\underline{O}\underline{O})$, then $A + B = \underline{O}(AB) = \underline{O}(A(A(\underline{O}\underline{O}))) = \underline{O}(\underline{O}\underline{O}) = \underline{O}$.

Picture:



Associativity is the fun one:

$$A + (B+C) = A + (\underline{O}(BC)) = \underline{O}(A(\underline{O}(BC)))$$

$$(A+B) + C = (\underline{O}(AB)) + C = \underline{O}((\underline{O}(AB))C)$$

How do you manipulate this?! Product isn't associative!

We need to retreat to the behavior of the equation.

Lemma: Suppose $f(x,y)$, $g(x,y)$ are cubic polynomials, and $P_1, P_2, \ldots, P_9 \in C_f(\mathbb{R}) \cap C_g(\mathbb{R})$, with P_1, P_2, P_3 on a line L (but the line is not $\subseteq C_f(\mathbb{R})$). Then there is a quadratic polynomial $q(x,y)$ so that $P_4, P_5, \ldots, P_9 \in C_q(\mathbb{R})$.

Ie., the result says that for $P_i = (x_i, y_i)$ $i = 4, .., 9$, the vectors $(x_i^2, x_i y_i, y_i^2, x_i, y_i, 1)$ are linearly dependent.

On to associativity!

Given $A, B, C \in G_f(\mathbb{R})$ f = elliptic curve, we want $A + (B + C) = (A + B) + C$ $\quad \underline{O}(A(\underline{O}(BC))) = \underline{O}((\underline{O}(AB))C)$

$\boxed{\text{Note: Enough to show } A(\underline{O}(BC)) = (\underline{O}(AB))C \ \&.}$

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

$P_4 = AB$, $P_5 = \underline{O}$, $P_6 = \underline{O}(AB)$

$P_7 = A$, $P_8 = \underline{O}(BC)$, $P_9 = (\underline{O}(AB))C$

Assume these points are all distinct.

We want to show that $A(\underline{O}(BC)) = P_7 P_8 = (\underline{O}(AB))C = P_9$

ie., 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 are B, AB, A & lie on a line L_1, let $L_1(x, y) = 0$ be its eqn.

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

$P_3, P_6, P_9 = C, \underline{O}(AB), (\underline{O}(AB))C$ 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 $P_1,\dots,P_9 \in C_g(\mathbb{R})$ = the union of the 3 lines!

All the hypotheses of the lemma are satisfied

$P_1, P_2, P_3 = B, BC, C$ lie on a line L, $L \not\subseteq C_f(\mathbb{R})$

b/c $f(x,y)=0$ is an elliptic curve.

So $\exists$ quadratic $q(x,y)$ so that

$P_4,\dots,P_9 \in C_q(\mathbb{R})$

$P_4, P_5, P_6 = AB, Q, Q(AB)$ lie on a line L_4, and

so $L_4 \cap C_q(\mathbb{R}) \supseteq \{P_4, P_5, P_6\} \longrightarrow L_4 \subseteq C_q(\mathbb{R})$ b/c

q has degree 2. So

$q(x,y) = L_4(x,y)L_5(x,y)$ is a product of linear factors

$\Longrightarrow C_q(\mathbb{R})$ = a union of two lines, L_4, L_5.

Then $P_7, P_8, P_9 \in L_5$, since otherwise

L_4 P_4, P_5, P_6 and one of P_7, P_8, P_9 lie on L_4,

$\Longrightarrow L_4 \cap C_f(\mathbb{R})$ has at least 4 pts $\Longrightarrow L_4 \subset C_f(\mathbb{R})$

a contradiction, So P_7, P_8, P_9 lie on a line! ///

What about when the points $P_1, \ldots, P_9$ are not all distinct? Appeal to "continuity"!

$\underline{O}, \underline{A}, \underline{B}, C \rightsquigarrow$ nearby points $\underline{O}', A', B', C'$

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

Note that if $\underline{A}$ (say) is held fixed (= unmoving) and B (say) moves, then AB is determined by B, and if $AB = C = AB'$, then ~~A~~ $B = AC = B'$, so the function $B \longmapsto AB$ is one to one.

Given A, B, C, wiggle them a little ~~the~~ (along $C_f'(\mathbb{R})$) to A', B', C' all distinct (P_1, P_3, P_7). Then wiggle $\underline{O}$ to $\underline{O}'$ so that

Given A, B, C, wiggle $\underline{O}$ a little (along $C_f'(\mathbb{R})$) to make $\underline{O}', \underline{O}'(AB), O'(BC), (\underline{O}'(AB))C = P_5, P_6, P_8, P_9$ distinct from the rest.

Then wiggle A to A' so that $A'B$, $\underline{O}(A'B)$, A', $(\underline{O}(A'B))C = P_4, P_6, P_7, P_9$ are distinct from the rest. (*)

Then wiggle ~~B~~ B to B' so that $A'B'$, $O'(A'B')$, $O(A'B')C$, B', $B'C$, $\underline{O}'(B'C)$ distinct from rest. (*)

Then wiggle C to C' ...

(*) without making pts formerly distinct the same again!

After all this, the 9 pts are distinct

(each depends on a distinct collection of the O, A, B, C,

so 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

$$A'(O'(B'C')) = (O'(A'B')C')$$

So $A(O(BC))$ is close to which is close to $(O(AB))C$

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

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

In the end, this amounts to: If you have a cubic poly $f(x, L(x))$ and you wiggle the coeffs a little bit, and it always has three roots, then the roots just wiggle a little bit...

How important is the (~~seem~~ randomly chosen) point to call $\underline{O}$? In terms of the group structure, not much.

If we chose a different point $\underline{O}'$ to work from, we get a different addition:

$$A + B = \underline{O}(AB)$$
$$A \oplus B = \underline{O}'(AB)$$

But If we choose $W = -\underline{O}'$ (in first addition) ie

$$\underline{O}' + W = \underline{O}, \text{ ie } \underline{O}(\underline{O}'W) = \underline{O} \text{ ie.}$$

$(\underline{O}'W) = \underline{O}\,\underline{O}$, ~~then~~ ie $W = \underline{O}'(\underline{O}\,\underline{O})$, then

$$\underline{O}' + (A \oplus B) = \underline{O}(\underline{O}'(A \oplus B)) = \underline{O}(\underline{O}'(\underline{O}'(AB)))$$
$$= \underline{O}(\underline{O}'C) = \underline{O}(AB) = A + B$$

So $\underbrace{W + \underline{O}'}_{=\underline{O}} + (A \oplus B) = A + B + W$

$$A \oplus B = A + B + W$$