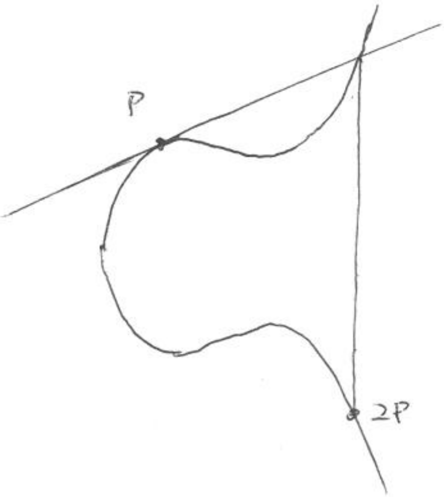
6.1. (Do the example on 5.4 – 5.5).

3-division points.

Can we find P with $3P = O$?

Want $P + 2P = O$

Need $x(P) = x(2P)$.

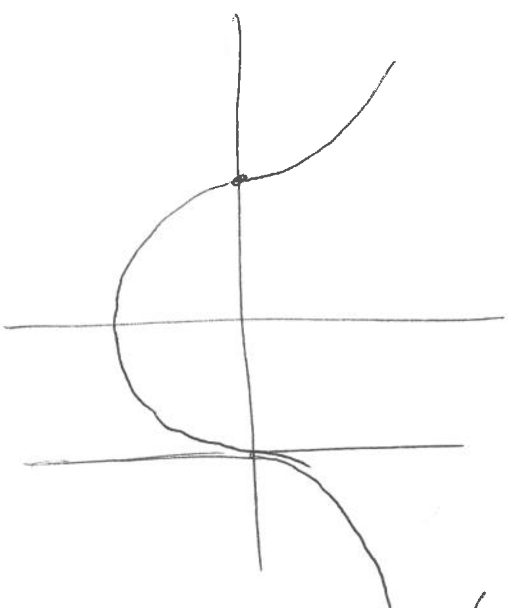


← ?? How can this happen?

If the tangent line is vertical, then $2P = O$.

This can only happen if the tangent line has multiplicity 3.

$y^2 = x^3 + 1$



Given $y^2 = f(x)$,

$$2y \frac{dy}{dx} = f'(x)$$

Tangent line at (x_0, y_0) is

$$y - y_0 = \frac{f'(x)}{2y}(x - x_0)$$

(suitably interpreted if $x_0 = 0$).

Exercise. Given

$$y^2 = x^3 + ax^2 + bx + c,$$

$(x, y) \neq O$ has order 3 if and only if x is a root of

$$\psi_3(x) = 3x^4 + 4ax^3 + 6bx^2 + 12cx + (4ac - b^2).$$

(So eight points total.)

6.2. Proof of the group law.

Need to check:

$P + Q = Q + P$ (tautological)

$P + O = P$ for all P.

(This is easy, no geometry)

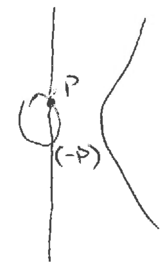
Existence of inverses

(flip across x-axis)

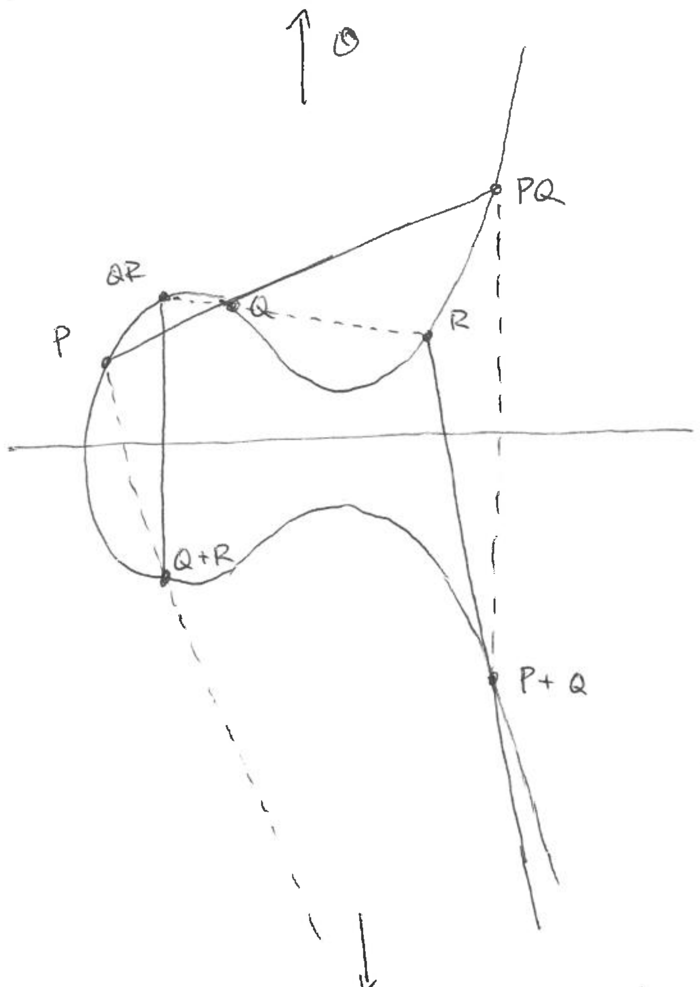
$P + (-P) = O$.

The associative law

$P + (Q + R) = (P + Q) + R$.



6.3. Proof of the associative law



I : intersection pt of
line btn. P and Q + R
line btn. P + Q and R.

Draw the points as shown.

The dashed lines, multiplied together, are cubic curves.

They intersect in nine points: $P, Q, R, PQ, QR, P+Q, Q+R, O$, and I.

The elliptic curve goes through nine of them.

By Cayley – Bacharach <u>it goes through I</u>.

This means
$$P(Q+R) = I$$
$$(P+Q)R = I$$
i.e.
$$P + (Q+R) = -I$$
$$(P+Q)+R = -I$$

i.e. they are equal.

7.1. Elliptic curves. The high brow perspective,

Def. An elliptic curve is a pair (E, O) where E is a curve of genus 1 and $O \in E$.

What do the words mean?

A curve is a projective variety of ~~genus~~ dimension 1.

what is dimension?

If V is a proj. variety (in $\mathbb{P}^n$), its function field is

$$K(V) = \left\{ \begin{array}{l} \text{rat'l functions } \frac{f(X)}{g(X)}, \ f, g \text{ homo polys of same degree} \\ g \notin I(V) \text{ (i.e. } g \text{ does not vanish identically on } V) \\ \frac{f}{g} \sim \frac{f'}{g'} \text{ if } fg' - f'g \in I(V) \end{array} \right\}$$

and $\dim(V)$ is $\operatorname{tr deg} \bar{K}(V) / \bar{K}$.

ex. let $V = V(y^2 z - x^3 - \cancel{xz^2}) \subseteq \mathbb{P}^2(\mathbb{C})$.

Then $K(V)$ = rat'l functions in x, y, z
quotients of homo polys
if it vanishes on V, it's zero.

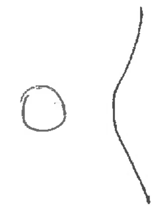
A divisor on a curve C is a formal sum or difference of points, and for a divisor D,

$$L(D) := \{ f \in \bar{K}(C) : \text{"} \operatorname{div}(f) \geq -D \text{"} \}.$$

This means that the function can have poles at worst described by D.

7.2.

Example. Let $C = V(Y^2Z - X^3 - XZ^2) \subseteq \mathbb{P}^2(\mathbb{C})$.



Consider the rational function $\dfrac{X}{Z}$.

What is $\operatorname{div}\left(\dfrac{X}{Z}\right)$?

Zeroes and poles: Zeroes of X $-$ poles of Z.

Zeroes of X: ~~compute~~ Substitute in $X=0$, get Y^2Z.

Double zero at $[0:0:1]$, single at $[0:1:0]$.

Zeroes of Z: get $-X^3$, triple zero at $[0:1:0]$

$$\text{So } \operatorname{div}\left(\frac{X}{Z}\right) = \big(2[0:0:1] + [0:1:0]\big) - 3[0:1:0].$$

$$= 2[0:0:1] - 2[0:1:0].$$

(Affine patch $Z=1$: has a double intersection with $X=0$.)

By Bezout, the divisor of any rat'l fn. has degree zero.

Riemann Roch Theorem. Let C be a smooth curve.

There exist:

an integer $g \geq 0$ (genus of C)

a divisor K_C (the canonical divisor)

such that for every divisor $D \in \operatorname{Div}(C)$ we have

$$\dim L(D) - \dim L(K_C - D) = \deg D - g + 1.$$

Moreover, if $\deg D > 2g-2$ then $L(K_C - D) = \{0\}$ so that term disappears.

7.3.

How to get a Weierstrass equation from an elliptic curve.

Riemann-Roch is just $\dim L(D) = \deg D$.

Look at this for $D = nO$ for $n \geq 1$.

~~n=0 nothing.~~

$n=1$: $\dim L(D) = 1$. (Just scalar constant functions).

$n=2$: $\dim L(D) = 2$.

Have another function, call it "x".

(In our example before was $\frac{X}{Z}$.)

$n=3$: $\dim L(D) = 3$.

Have still another function, call it "y".

$n=4$: $\dim L(D) = 4$.

No new name! x^2 has an ~~double~~ order 4 pole at O.

$n=5$: $\dim L(D) = 5$ $\langle 1, x, y, x^2, xy \rangle$

$n=6$: $\dim L(D) = 6$ $\underbrace{\langle 1, x, y, x^2, xy, x^3, y^2 \rangle}_{??\ 7\ \text{functions}?}$

There must exist a relation, and it gives the Weierstrass equation. Write $C = V(\text{this eqn.})$

So we get a map $\phi : E \longrightarrow \mathbb{P}^2$
$[x : y : 1]$

Here $L(3O)$ is base point free
(the sections are never all zero)

ϕ is automatically a morphism (E is smooth, Sil II.2.1)
surjective (Silk II.2.3)

$\phi(O) = [0:1:0]$ (y has a higher order pole than x, at O)

7.4.

Want to show $\phi : E \to C$ has degree 1.

What does this mean?

If $\phi : C_1 \to C_2$ is a map of curves,

$$\deg \phi = [K(C_1) : \phi^* K(C_2)].$$

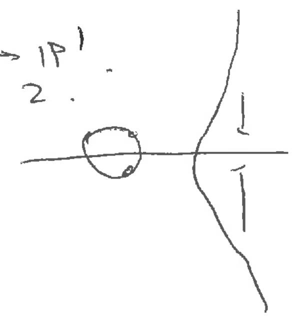
{finite: Silverman says [Har, II.6.8]

An isomorphism if $\deg \phi = 1$.

We basically have $\phi^{-1}(P) = \deg \phi$ points for all P.

What we really have is that

$E \to \mathbb{P}^1$.
degree 2.



$$\sum_{P \in \phi^{-1}(Q)} e_\phi(P) = \deg \phi$$

where the ramification index $e_\phi(P)$ is defined in terms of the local rings.
(Like e-f-g in algebraic number theory.)

Want to show $K(E) = K(x, y)$.

Consider $[x : 1]$ $E \to \mathbb{P}^1$

x has a double pole at O, no other poles so degree 2.

$$\text{So } [K(E) : K(x)] = 2$$

Similarly $[K(E) : K(y)] = 3$.

So $[K(E) : K(x,y)]$ divides 2 and 3 and hence is 1.

Show C is smooth. (omitted)

This is enough to show ϕ is an isomorphism.

7.5. Another example of this.

We could have embedded E in a higher-dimensional projective space.

e.g. ~~$V(Y^2Z = X^3 - X$~~

$$V(WZ^2 - X^3 - XZ^2,\ WZ - Y^2).$$ Same elliptic curve.

Or, consider the map
$$\mathbb{P}^1 \longrightarrow \mathbb{P}^3$$
$$[X:Y] \longrightarrow ?$$

Let $O = [1:0]$.

What is $L(3O)$? It is $\left\langle \frac{Y^3}{X^3}, \frac{Y^2}{X^2}, \frac{Y}{X}, 1 \right\rangle$

And so the linear system associated to the very ample divisor $3O$ is

$$[X:Y] \longrightarrow \left[1 : \frac{Y}{X} : \frac{Y^2}{X^2} : \frac{Y^3}{X^3}\right]$$
$$= [X^3 : X^2Y : XY^2 : Y^3]$$

This is a variety in $\mathbb{P}^3$, can write as
$$\left\{ [X:Y:Z:W] : \begin{array}{l} Y^2 - XZ = 0 \\ Z^2 - YW = 0 \\ XW - YZ = 0 \end{array} \right\}$$

it is called the twisted cubic curve.

8.1. The group law via this theory.

Recall the divisor group $\mathrm{Div}(C)$ is the free abelian group consisting of formal sums of points.

A divisor D is principal if it is $D = \mathrm{div}(f)$ for some $f \in \bar{k}(C)^*$, i.e. (zeroes) − (poles) of the rat'l fn. Write $\mathrm{PDiv}(C)$.

Two divisors D_1 and D_2 are equivalent if their difference is principal.

Define $\mathrm{Pic}(C)$, the divisor class group, as $\frac{\mathrm{Div}(C)}{\mathrm{PDiv}(C)}$.

Also. The degree of a divisor is the sum of the multiplicities.

(e.g. $\deg(2[1:0:0] - 3[0:1:0]) = -1$.)

Since $\mathrm{div}(f)$ has degree 0 for every f, we can also define a degree map $\mathrm{Pic}(C) \longrightarrow \mathbb{Z}$ and $\mathrm{Pic}^0(C)$ is its kernel.

Theorem. If E is an elliptic curve then there are inverse bijections of sets

$$E \longleftrightarrow \mathrm{Pic}^0(E)$$

$$P \longrightarrow (P) - (O) \text{ mod princ. divisors}$$

$$(P) \longleftarrow D$$

where $D \sim (P) - (O)$ for a unique point $P \in E$.

8.2. Moreover, if a line intersects E in P_1, P_2, P_3, then $(P_1) + (P_2) + (P_3) - 3(O) \sim 0$, so that the group law on $\mathrm{Pic}^0(E)$ agrees with the "chord and tangent" law on E.

Proof is a bunch of formalism. Will try to explain what it means.

* an example of a computation.
$\mathbb{P}^1$ is a curve, $K(\mathbb{P}^1)$ = rat'l fns in X and Y
$= \mathbb{C}\left(\frac{X}{Y}\right)$.

What is $\mathrm{Pic}^0(\mathbb{P}^1)$? The trivial group.

Why? A divisor looks like

$$\sum_{i=1}^{n} [\alpha_i : \beta_i] - \sum_{j=1}^{N} [\gamma_j : \delta_j]$$

and this is the divisor of $\dfrac{\prod_i (\beta_i X - \alpha_i Y)}{\prod_j (\delta_j X - \alpha_j Y)}$

For an elliptic curve, why isn't $\mathrm{Pic}^0(E) = 0$?
A direct proof (see link).

Silverman's Lemma 3.3.
Suppose $(P) \sim (O)$ in $\mathrm{Pic}^0(E)$.
Choose $f \in \overline{K}(E)$ with $\mathrm{div}(f) = (P) - (O)$.

8.3.

Look at

$$L((O)) = \{ g \in \bar{K}(C) : \operatorname{div}(g) \geq -(O) \}$$

$$= \left\{ g \in \bar{K}(C) : \begin{array}{l} g \text{ has at most a single pole} \\ \text{at } O, \text{ none anywhere else} \end{array} \right\}$$

But Riemann-Roch, in this case says if $\deg D > 0$,

$$\dim L(D) = \deg D,$$

so $\dim L((O)) = 1$

and it contains the constants.

i.e. $f \in \bar{K}$ and $\underline{\underline{P = O}}$.

So, w.r.t. $E \longleftrightarrow \operatorname{Pic}^0(E)$

this shows that $\begin{array}{l} E \longrightarrow \operatorname{Pic}^0(E) \\ P \longrightarrow (P) - (O) \end{array}$ is <u>injective</u>.

To show it's surjective, take $D \in \operatorname{Pic}^0(E)$.

Must show $D \sim (P) - (O)$ for some $P \in E$.

We have $\dim L(D + (O)) = 1$.

Let $f \in \bar{K}(E)$ be a generator.

Then $\operatorname{div}(f) = -D - (O) + \left\{ \begin{array}{l} \text{something effective} \\ \text{(i.e. all coeffs are positive)} \\ \text{of degree } 1 \end{array} \right\}$

$= -D - (O) + (P)$ for some P.

So $D \sim (P) - (O)$.

8.4.

We must show that if a line L intersects E in P_1, P_2, P_3 then $(P_1) + (P_2) + (P_3) - 3(O) \sim 0$, i.e. there exists a rat'l function whose divisor is $(P_1) + (P_2) + (P_3) - 3(O)$.

Want $f = \frac{g}{h}$ where $\mathrm{div}(g) = (P_1) + (P_2) + (P_3)$
$\mathrm{div}(h) = 3(O)$.

(Here g, h will be linear forms which are not functions on $\mathbb{P}^2$ or on E! But their quotient is.)

This has dropped into our lap:

Take g = equation of L

$h = z$.

Theorem 3.6 (omitted). The group law defines morphisms

$$+ : E \times E \to E \qquad - : E \to E$$
$$(P_1, P_2) \to P_1 + P_2 \qquad P \to -P.$$

//

One last topic.

Let $\mathrm{Spec}(\mathbb{Z}) = \{\text{all prime ideals of } \mathbb{Z}\}$
$= \{(0)\} \cup \{(p) : p \text{ a prime number}\}$.

Then this is an algebraic curve. (Because Scheme Theory.)

Rational functions are just rational numbers.

A rational number $\frac{x}{y}$ (in lowest terms) has a zero at (p) if $p \mid x$ and a pole if $p \mid y$.

(Moreover, multiplicities are $v_p(x)$ and $v_p(y)$.)

(Why a zero? Says $\frac{x}{y}$ belongs to the ideal (p) of the local ring $\mathbb{Z}_{(p)}$.

(In scheme theory, ideals describe functions vanishing there.)

8.5.

We have $\mathrm{Pic}^0(\mathrm{Spec}\,\mathbb{Z}) = 0$.

This is because every divisor is principal.

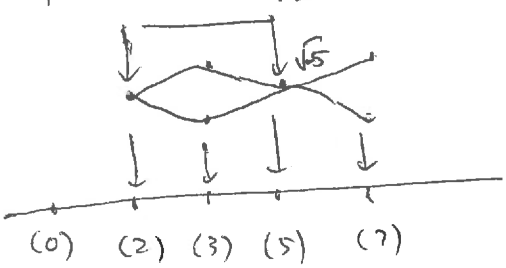
A divisor just looks like $\sum_{p \text{ prime}} n_p (p)$
integer
almost all are 0

and it is the divisor of $\prod_p p^{n_p}$.

Now ~~lete~~ consider $\mathrm{Spec}(\mathbb{Z}[\sqrt{-5}])$.

This is also a curve with a degree 2 map (the norm) to $\mathrm{Spec}\,\mathbb{Z}$.

ramification points.



Every $(p) \in \mathrm{Spec}\,\mathbb{Z}$ has two preimages if you count appropriately. (the "efg theorem")

There are nonprincipal prime ideals of norm 2, 3, ...

i.e. $2\mathbb{Z}[\sqrt{-5}] = \mathfrak{p}_2^2$

$3\mathbb{Z}[\sqrt{-5}] = \mathfrak{p}_3\mathfrak{p}_3'$

etc.

which means there is no

So $\mathrm{Pic}^0(\mathrm{Spec}\,\mathbb{Z}[\sqrt{-5}])$ is just $\mathrm{Cl}(\mathbb{Z}[\sqrt{-5}])$.