4.1. Bezout's Theorem and its applications.

A *projective plane curve* is

$$V(f) = \{[x:y:z] \in \mathbb{P}^2 : f(x,y,z) = 0\}$$

for a single homogeneous polynomial f.

Really it's the pair $(f, V(f))$ because we want to distinguish, e.g. $V(x^2+y^2-z^2)$ and $V((x^2+y^2-z^2)^2)$, even though they describe the same subset of $\mathbb{P}^2$.

(Alternatively we could disallow degenerate curves or introduce scheme theory)

Its *degree* is its (combined) degree as a polynomial.
Its *components* are $V(f_i)$ for the irred factors $f_i | f$.

Bezout's theorem. If $V(f_1)$ and $V(f_2)$ are projective plane curves with no common components, then they intersect in $(\deg f_1)(\deg f_2)$ points, counted with multiplicity.

Example. Suppose

$$f_1 = a_1 x + a_2 y + a_3 z$$
$$f_2 = b_1 x + b_2 y + b_3 z$$

are distinct lines.

They intersect in exactly one point.

The intersection is all $[x:y:z]$ with $\begin{bmatrix} x \\ y \\ z \end{bmatrix} \in \ker \begin{bmatrix} a_1 & a_2 & a_3 \\ b_1 & b_2 & b_3 \end{bmatrix}$

If the lines are different the matrix has rank 2, so nullity 1.

As $\mathbb{P}^2 = \{\text{lines through } (0,0,0) \text{ in } \mathbb{A}^3\}$, intersection is 1 pt.

Example.

$f_1 = a_1 x + \cancel{b} a_2 y + a_3 z$

$f_2 = b_1 x^2 + b_2 xy + b_3 y^2 + b_4 xz + b_5 yz + b_6 z^2$.

(Not all ~~conics~~ b's are zero
multiplying through by a scalar describes the same conic $\longrightarrow$ so $\mathbb{P}^5$ is the moduli space of conics!)

At least one of a_1, a_2, a_3 is nonzero
So we can solve for $x, y,$ or z in terms of others
eliminate it from f_2.

We get, say, $\tilde{f}_2 = c_1 x^2 + c_2 xy + c_3 y^2$.
(or maybe in x and z
or maybe y and z)

By the fundamental theorem of algebra (see exercises!)
it factors as $(d_1 x + e_1 y)(d_2 x + e_2 y)$
where $[d_1 : e_1]$ and $[d_2 : e_2]$ are uniquely determined (up to reordering). Actual values aren't.

The roots are $[e_1 : -d_1]$ and $[e_2 : -d_2]$.
If $[e_1 : -d_1] = [e_2 : -d_2]$ (which can happen) then the intersection has multiplicity 2.

Note. The "obvious" generalization of this defines intersection multiplicity of a line and a higher order curve.

Ex. Prove that if $\tilde{f}_2 = 0$ we had $f_1 | f_2$.

4.3.

Example. (Five points determine a conic)

Given five points $P_i \in \mathbb{P}^2(\mathbb{C})$, no three collinear. There is exactly one conic going through them all.

Proof.

Existence. Given five points $[x_1 : y_1 : z_1] \cdots [x_5 : y_5 : z_5]$

Want to describe

$$\{ ax^2 + bxy + cy^2 + dxz + eyz + fz^2 ;\ ax_i^2 + bx_iy_i + \cdots + cz_i^2 = 0 \text{ for all } i.$$

That is exactly the kernel of $\begin{bmatrix} x_1^2 & x_1y_1 & y_1^2 & x_1z_1 & y_1z_1 & z_1^2 \\ & & \vdots & & & \\ x_5^2 & & \cdots & & & z_5^2 \end{bmatrix}$

The rank is at most 5, so nullity ≥ 1.
(If the matrix has rank $= 5$, nullity $= 1$.)
So there is at least one nonzero solution.
(Recall: a conic is described by a line through the origin, so if nullity $= 1$ it's unique.)

Uniqueness. If two different conics go through all the P_i, then they share a common component. (Because otherwise they intersect in only four pts by Bezout)

It must be a line (unless the conics are identical.)
So both conics are products of two lines (one in common, one distinct).
Look at either conic. If two ~~conics~~ lines contain five points, one contains at least 3. Contrary to assumption.

4.4.

Do nine points determine a cubic?

Why might they?

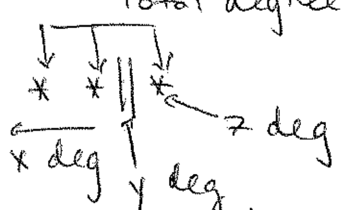
A general cubic looks like

$$a_1 x^3 + a_2 x^2 y + a_3 x y^2 + a_4 y^3 + a_5 x^2 z + a_6 x y z + a_7 y^2 z + a_8 x z^2 + a_9 y z^2 + a_{10} z^3$$

so they form a $\mathbb{P}^9$.

(Shortcut: "stars and bars"

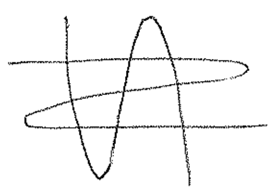
Total degree $= 3$ $\qquad \binom{5}{2} = 10$



Thank you Nikki Haley)

Construct a 9×10 matrix as before.
If the matrix has full rank, is unique.
(if the pts are in "general position")

But:



Cayley - Bacharach Theorem.

Suppose C_1 and C_2 are two cubics which meet in nine fixed points. (As they must, if they don't share a common component.) Then every cubic passing through any eight of the points must pass through the ninth.

4.5.

Sketch proof. (See problem set #2!)

Any eight of the points $P_1, \dots, P_8$ are independent (not obvious), in the sense that
$$\begin{bmatrix} x_1^3 & x_1^2 y & \cdots & z_1^3 \\ \vdots & & & \\ x_8^3 & & \cdots & z_8^3 \end{bmatrix}$$
has rank 8, nullity 2.

So the set of cubics
$$f(x,y,z) = a_1 x^3 + a_2 x^2 y + \cdots + a_{10} y^3 \text{ with } f(P_i)=0 \text{ for}$$
all of them has dimension 2 in $\mathbb{A}^{10}$.
(As a vector space)

This is a $\mathbb{P}^1$ (well def. only up to scalars). For any two distinct cubics f_1 and f_2 ~~so that~~ with $f_j(P_i)=0$ $\forall i$,
$$\{\text{cubics } f : f(P_i)=0 \text{ for all } i\} = \{\lambda f_1 + \mu f_2 : \lambda, \mu \in \mathbb{C}\}.$$

By hypothesis we have two such cubics, C_1 and C_2. So all such cubics are linear combinations of them.

But $C_1(P_9) = C_2(P_9) = 0$, hence $(\lambda C_1 + \mu C_2)(P_9) = 0$ $\forall \lambda, \mu$.

QED.

5.1. Elliptic curves (the lowbrow approach)

Def. A <u>Weierstrass equation</u> is

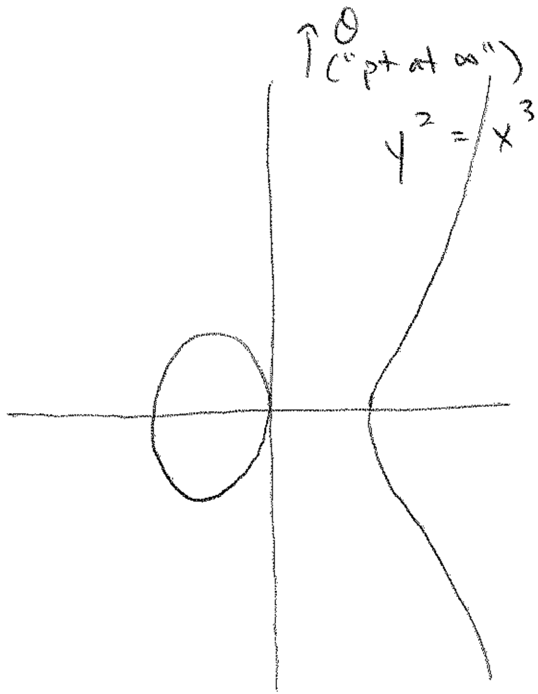
$$E: \ y^2 + a_1 xy + a_3 y = x^3 + a_2 x^2 + a_4 x + a_6$$

or its homogenization

$$Y^2 Z + a_1 XYZ + a_3 YZ^2 = X^3 + a_2 X^2 Z + a_4 XZ^2 + a_6 Z^3.$$

The variety $E = V$(above eqn.), together with the point $\mathcal{O} = [0:1:0]$, is called an <u>elliptic curve</u>, if V is <u>smooth</u>.

Ex.



Note that any curve isomorphic to such is also an elliptic curve.

e.g. linear changes of coordinates

$$\begin{bmatrix} X' \\ Y' \\ Z' \end{bmatrix} = \begin{bmatrix} a_{11} & a_{12} & a_{13} \\ a_{21} & a_{22} & a_{23} \\ a_{31} & a_{32} & a_{33} \end{bmatrix} \begin{bmatrix} X \\ Y \\ Z \end{bmatrix}$$

with the matrix invertible are an isomorphism of $\mathbb{P}^2$.

(Indeed: $\mathrm{Aut}(\mathbb{P}^2) = PGL(2)$.)

5.2. Example. The Fermat cubic $X^3 + Y^3 = Z^3$.

Using the change of variables $Z = Z' + Y$,

$$X^3 + Y^3 = Z'^3 + 3Z'^2 Y + 3Z' Y^2 + Y^3$$

or

$$\frac{1}{3} X^3 = \frac{1}{3} Z'^3 + Z'^2 Y + Z' Y^2$$

which is of the desired form after ~~the~~ rearranging.

If $\mathrm{char}(K) \neq 2, 3$ you can further complete the square and the cube to get

$$Y^2 Z = X^3 + A X Z^2 + B Z^3$$

("reduced Weierstrass form")

$$y^2 = x^3 + A x + B.$$

If our elliptic curve is defined over a field K, so are all these transformations.

We can also put our curve in Legendre normal form

$$y^2 = x(x-1)(x-\lambda)$$

but in this case the isomorphism is defined over $\bar{K}$.

How? Write $y^2 = x^3 + Ax + B = (x-\theta)(x-\theta')(x-\theta'')$ (over $\bar{K}$)

~~we have Let~~ $\cancel{z = \frac{\theta+\theta'+\theta''}{3}}$ ~~which is just~~

We can take $x' = x - \theta$.

Work a little harder to get the 1. (See exercises.)

5.3. If $E : y^2 = x^3 + Ax + B$, define the

discriminant $\quad \Delta := -16(4A^3 + 27B^2)$

j-invariant $\quad j := -1728 \dfrac{(4A)^3}{\Delta}$.

Proposition. E is singular if and only if $\Delta(E) = 0$.

If E is singular we say it has a node if $A \neq 0$

a cusp if $A = 0$.

Exercise. Check the former.

In Legendre normal form we have

$$\hat{E}_\lambda = y^2 - x(x-1)(x-\lambda)$$

$$j(E_\lambda) = 2^8 \frac{(\lambda^2 - \lambda + 1)^3}{\lambda^2(\lambda - 1)^2}.$$

Theorem. (Won't prove here)

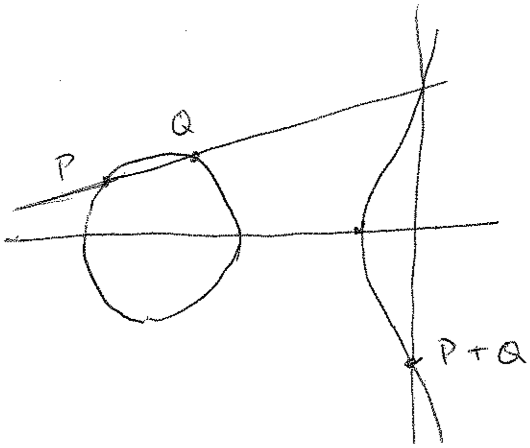
TFAE.

(1) $E_\lambda \cong E_{\lambda'}$

(2) $j(E_\lambda) = j(E_{\lambda'})$

(3) $\lambda' \in \left\{ \lambda, \dfrac{1}{\lambda}, 1 - \lambda, \dfrac{1}{1-\lambda}, \dfrac{\lambda}{\lambda - 1}, \dfrac{\lambda - 1}{\lambda} \right\}$.

5.4. The group law.



Given two points $P, Q \in E$.
Draw the line PQ. By Bezout (or just a computation) it intersects E in a third point.
Reflect across the x-axis, call this $P+Q$.

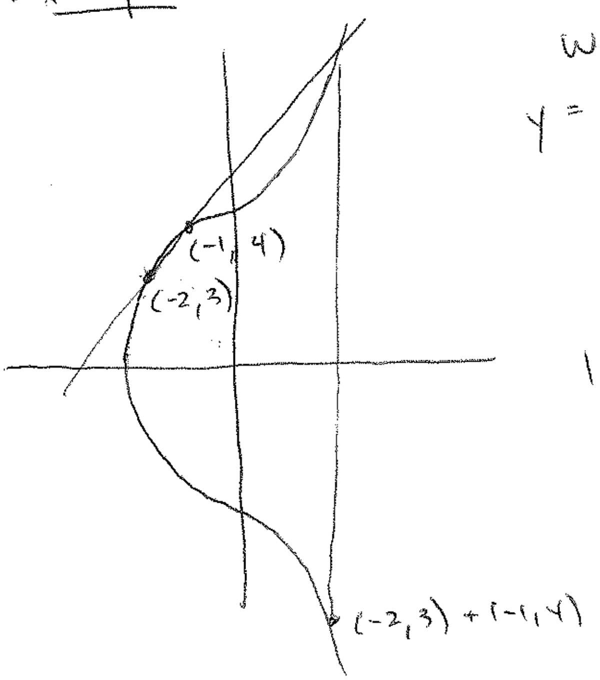
Theorem. This operation defines an abelian group law on $E(K)$, for any field K.

(If we do it for $E(\mathbb{C})$, it is essentially immediate for subfields.)

Proofs.

(1) A bunch of computations.
(2) A cool application of Bezout, Cayley-Bacherach.
(3) Via an isomorphism $E \xrightarrow{\sim} \mathrm{Pic}^0(E)$.
(4) Show that elliptic curves are complex tori.

Example. $E: y^2 = x^3 + 17$



what is $(-2,3) + (-1,4)$?

$y = x+5$, $\quad (x+5)^2 = x^3 + 17$

$x^3 - x^2 - 10x - 8$.

A priori two roots are $-1, -2$.
The sum is 1. So the third is 4.
Intersection is $(4, 9)$

$(-2,3) + (-1,4) = (4,-9)$.

5.5. What is $(-2,3) + (-2,3)$?

Find the tangent line at $(-2,3)$.

$$2y\frac{dy}{dx} = 3x^2, \quad (x,y) = (-2,3)$$

$$\frac{dy}{dx} = \frac{3x^2}{2y} = \frac{3(-2)^2}{2\cdot 3} = 2.$$

So $y-3 = 2(x-(-2))$, $y = 2x+7$

$$(2x+7)^2 = x^3 + 17$$

$$x^3 - 4x^2 - 28x - 32 = 0.$$

Two roots are -2 and -2. Sum is 4.

So: Intersection point has $x = 8$, $y^2 = 17 + 512$

$y = 23$

$$\text{So } 2\cdot(-2,3) = (8,-23).$$

None of this relied on any deep theorem. Just:

(1) A line intersects a cubic in three points (counting multiplicity and the pt at ∞)

(2) If two of them are defined over $\mathbb{Q}$ (or any K), so is the third.

In fact, the group $E(\mathbb{Q})$ is free abelian generated by $(-2,3)$ and $(2,5)$ and in particular has infinitely many distinct rational points.