Lecture 1: Motivation, basic def'ns.

1.1: Rational solutions to polynomial eq'ns.

Let $\{f_1, \dots, f_r\}$ be polynomials in $\mathbb{Z}[x_1, \dots, x_n]$. Given a field k, write

$$V_I(k) = \{(a_1, \dots, a_n) \in k^n \mid \forall i,\ f_i(a_1, \dots, a_n) = 0\} \subseteq k^n.$$

How can you tell whether $V_I(k)$ is ① empty ② finite / ... ?

eg: ① $k = \mathbb{C}$. Then ① & ② can both be decided algorithmically (Grobner basis)

② k finite. Then $V_I(k)$ always finite! $\exists$ algorithm to decide if $V_I(k)$ empty, & also to compute $\#V_I(k)$. Then the game is to do it fast.
Eg: if $n=2$, $r=1$, $\deg f = 3$: fast cryptography, general deg f: coding theory.

③ $k = \mathbb{Q}$ (or a #field, or a global field). Then $V_I(k)$ can be finite, ∞, or empty.
Conj: no algorithm exists to determine this.

eg: $n=3$, $r=1$,

$$f_1 = x_1^m + x_2^m - x_3^m, \quad m \in \mathbb{N}.$$

Thm [Euler, Taylor]: $V_I(\mathbb{Q})$ empty whenever $m > 2$, in $\{(0,0,0), (\pm 1, 0, \pm 1), (0, \pm 1, \pm 1)\}$.

eg $n=2$, $r=1$, degree $(f) > 3$ & f 'smooth'.
Thm [Faltings]: $V_I(\mathbb{Q})$ finite.

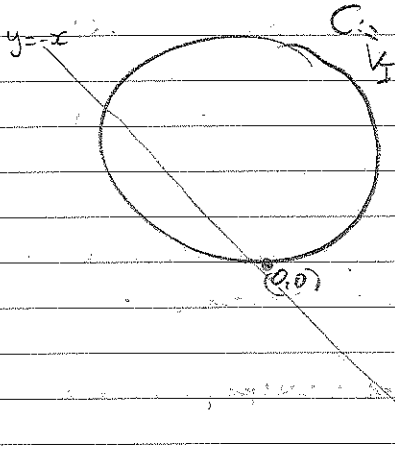
eg $n=2$, $r=1$, $\deg f = 3$, f 'smooth', assume $V_I(\mathbb{Q}) \neq \emptyset$.
Conj [B-S-D]: $\exists$ an algorithm to determine whether $V_I(\mathbb{Q})$ finite.

1.2 Rational points on conics (degree 2 curves)

- Let $n=2$, $r=1$, $f \in \mathbb{Z}[x,y]$ of degree 2.

Thm: If $V_I(\mathbb{Q}) \neq \emptyset$ then $V_I(\mathbb{Q})$ is infinite.

"Pf": Let $(x_0, y_0) \in V_I(\mathbb{Q})$. WLog $x_0 = y_0 = 0$.



Given $\lambda \in \mathbb{R}$, let L_λ be the line in $\mathbb{R}^2$ given by $y = \lambda x$.

Then L_λ meets C at exactly two pts ('in general'); one is $(0,0)$, call the other 'P_λ'.

Moreover, easy to check that if $\lambda \in \mathbb{Q}$ then $P_\lambda \in V_I(\mathbb{Q})$.

(Can make rigorous: definitions to appear). $\square$

- Deciding whether $V_I(\mathbb{Q}) = \emptyset$ is also easy.

Thm (Hasse–Minkowski): $V_I(\mathbb{Q}) \neq \emptyset \iff \left(V_I(\mathbb{R}) \neq \emptyset \;\&\; V_I(\mathbb{Q}_p) \neq \emptyset \;\forall p\right)$

$\mathbb{Q}_p$: p-adic numbers, ...

both easy to test algorithmically.

So curves in the plane cut out by one eq'n of degree 1 or 2 are both 'easy'. What about degree 3?

ex! $\emptyset$

This is more difficult! – will take next 3 weeks to prove
- a few basic facts;
- many open problems & conjectures

Composition law on a smooth cubic curve

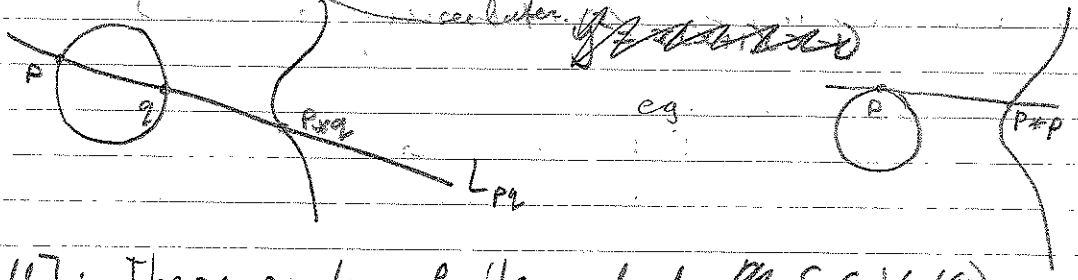
$n=2$, $r=1$, $f \in \mathbb{Z}[x,y]$ of degree 3, 'smooth' (see later, eg. $y^2 = x^3 - 1$, eg not x^3)

[Deciding whether $V_I(\mathbb{Q}) \neq \emptyset$ is hard, beyond scope of course]

Given $p, q \in V_I(\mathbb{Q})$, let L_{pq} = straight line joining p, q.

Then L_{pq} meets $V_I(\mathbb{Q})$ at a third pt, (maybe = one of p, q - count multiplicities) call this $p * q \in V_I(\mathbb{Q})$

eg.



Thm [Mordell]: There exists a finite subset $S \subseteq V_I(\mathbb{Q})$ s.t. every pt in $V_I(\mathbb{Q})$ can be obtained from pts in S by repeatedly applying the above composition law.

One of the main aims of this course will be to prove (a special case of) this thm.

Thm [Mazur]: Let $p \in V_I(\mathbb{Q})$. Let $\langle p \rangle = \{p, p*p, p*(p*p), \dots\}$. Then either (1) $\langle p \rangle$ is infinite; or (2) $\#\langle p \rangle \leq 13$

This is far beyond scope of this course, mentioned just for interest

Warning: '$*$' does not define a gp structure on $V_I(\mathbb{Q})$ - in general, not even associative. Will 'fix' this later.

Before we can begin to prove Mordell's thm, we need a precise statement! We will define affine & projective varieties over fields, the meaning of 'smooth', how to count pts of intersection &c.

We will not assume background in AG, & we will not give very general defs, but will try to do it 'correctly', via functors of pts. Note that it is essential for us to work over non alg. cl. fields, so we have to do things a bit carefully... Extra/alternative work?

End of intro. In h/work etc, please don't assume the results stated thus far.*

Some basic definitions

What is an 'algebraic variety'? Is it a subset of $\mathbb{K}^n$ for some n? Too crude, esp. for families.
Is it a representable sheaf? Takes a while to define...
We will use a 'restricted functor of points' approach.

Def [$\mathbb{A}^n$]: Let k be a field, & $n \geq 0$ an integer. Define affine n-space over k, "$\mathbb{A}^n_k$" to be the (covariant) functor

$$\underline{\mathrm{Fld}}_k \longrightarrow \underline{\mathrm{Set}}$$

$$K \longmapsto K^n$$

$$(L \hookrightarrow K) \longmapsto (L^n \subseteq K^n).$$

Define projective n-space over k, "$\mathbb{P}^n_k$" as the functor

$$\underline{\mathrm{Fld}}/_k \longrightarrow \underline{\mathrm{Set}}$$

$$K \longmapsto K^{n+1}\setminus\{0\}/\sim \quad \text{where } (x_0,\dots,x_n) \sim (y_0,\dots,y_n)$$
$$\iff \exists\, \lambda \in K^\times \text{ s.t. } \forall i,\ \lambda x_i = y_i.$$

$$(L \hookrightarrow K) \longmapsto \left(L^{n+1}\setminus\{0\}/\sim \ \hookrightarrow\ K^{n+1}\setminus\{0\}/\sim\right).$$

Ex: check the functor is well-def'd (do the morphisms make sense?)

Def ['coordinate charts']: For fixed $n \geq 0$, there are $(n+1)$ canonical maps (nat. trans) of functors $\mathbb{A}^n_k \longrightarrow \mathbb{P}^n_k$:

($0 \leq i \leq n$) $\varphi_i : \mathbb{A}^n_k \longrightarrow \mathbb{P}^n_k$, which for each $K \in \mathrm{Fld}_k$, gives the map

$$K^n \longrightarrow K^{n+1}\setminus\{0\}/\sim$$

$$(x_1,\dots,x_n) \longmapsto (x_1,\dots,x_{i-1},1,x_{i+1},\dots,x_n)$$
(1 in the i^{th} place.)

Def [Affine varieties]: Fix k, fix $n \geq 0$. Let $I \subseteq k[x_1,\dots,x_n]$ an ideal. We define a subfunctor $V_I \subseteq \mathbb{A}^n_k$ by

$$V_I : \underline{\mathrm{Fld}}/_k \longrightarrow \underline{\mathrm{Set}}$$

$$K \longmapsto \{(x_1,\dots,x_n) \in K^n \mid f(x_1,\dots,x_n) = 0\ \forall f \in I\}.$$

(Nb. I don't need to give the morphisms, since I have said it is a ~~set~~ subfunctor.)

Def [Homogeneous polynomials, ideals] Let k a field, $n \geq 0$. A polynomial $f \in k[x_0, \dots, x_n]$ is called homogeneous (of degree d) if every monomial in f has the same degree (equal to d). An ideal $I \trianglelefteq k[x_0, \dots, x_n]$ is homogeneous if it can be generated by homogeneous elts.

Def [projective varieties]: Let k a field, $n \geq 0$, Let $I \trianglelefteq k[x_0, \dots, x_n]$ homog. ideal, ~~Let $f_1, \dots, f_r \in k[x_0, \dots, x_n]$ homog.~~ Define $V_I^P \subset \mathbb{P}^n_k$ the subfunctor defined by

$$V_I^P : \underline{Fld}_k \longrightarrow \underline{Set}$$

$$K \longmapsto \left\{ [(x_0, \dots, x_n)] \in \mathbb{K}^{n+1} \setminus \underline{\underline{0}} \;\middle|\; \forall \text{ homog. } f \in I, \text{ we have } f(x_0, \dots, x_n) = 0 \right\}.$$

Remarks: - the condition $f(x_0, \dots, x_n) = 0$ is independant of the choice of representative $(x_0, \dots, x_n)$ exactly because f is homogeneous;

- It can happen that $V_I^{aff} = V_J^{aff}$ even if $I \neq J$, eg if $I = J^2$. See later for more.

- Enough to check $f(-) = 0$ for f in a generating set (can be taken finite!).

~~Weak varieties are isomorphic if the functors are isomorphic!~~

- we often write V_I^P for $V_{(I)}^P$ etc.

- for any $0 \leq i \leq n$, composition with $\varphi_i : \mathbb{A}^n_k \hookrightarrow \mathbb{P}^n_k$ gives a 'restriction map' from projective varieties in $\mathbb{P}^n_k$ to varieties in $\mathbb{A}^n$

Examples: Any k, any $n \geq 0$, $I = (x_1) \trianglelefteq k[x_1, \dots, x_n]$. I claim $V_I^A \simeq \mathbb{A}^{n-1}_k$. Well, define

$$\mathbb{A}^{n-1}_k \longrightarrow V_I^A \quad \text{by, for each } K \geq k, \text{ sending}$$

$(x_1, \dots, x_{n-1})$ to $(0, x_1, \dots, x_{n-1})$.

Ex: check this gives an iso of functors.

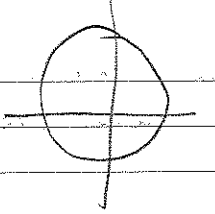
Eg: Any k, any $n \geq 1$, $I = (x_0) \trianglelefteq k[x_0, \dots, x_n]$ I claim $V_I^P \simeq \mathbb{P}^{n-1}_k$. Well, define

$$\mathbb{P}^{n-1}_k \longrightarrow V_I^A$$

$$(x_0 : \dots : x_{n-1}) \longmapsto (0 : x_1 : \dots : x_{n-1}).$$

Ex: Check this gives an iso.

1.6 eg: $k = \mathbb{Q}$, $n = 2$, $I = (x^2+y^2-1) \lhd k[x,y]$. Then have $V_I^{\mathbb{A}} \subseteq \mathbb{A}^2_{\mathbb{Q}}$.

Then $V_I^{\mathbb{A}}(\mathbb{R}) = \{(x,y) \in \mathbb{R}^2 \mid x^2+y^2-1=0\} =$ 

Have $V_I^{\mathbb{A}}(\mathbb{Q}) \subseteq V_I^{\mathbb{A}}(\mathbb{R}) \subseteq V_I^{\mathbb{A}}(\mathbb{C}) \cdots$.

Def: ~~A morphism of varieties/k (affine proj) is a natural trans of functors~~ Equivalent natural transformation.

eg: the maps $\varphi_i : \mathbb{A}^n_k \to \mathbb{P}^n_k$ we saw earlier.

eg: $V_I^{\mathbb{A}}$ as above. Define $\pi : V_I^{\mathbb{A}} \to \mathbb{A}^1_k$, $(x,y) \mapsto x$

So Var_k a full subcat of $\mathrm{Fun}(\mathrm{Fld}_k \to \mathrm{Set})$

eg: Every variety over k has a unique map to $\mathbb{A}^0_k = \mathbb{P}^0_k$.

~~So we have a cat of varieties/k, & it has a terminal object. However it is pretty stupid - eg no products. This is the one we study for simple def. We work w/ schemes w/ morphisms which could do this, but resulting cat is evil - see homework.~~ Def?

~~The cat also has Var$_k$ as has an initial object, the Empty variety~~;

eg/nonexeg. $V_{(1)}^{\mathbb{A}} \subset \mathbb{A}^0_k$; it is the functor $\mathrm{Fld}/_k \to \mathrm{Set}$

$K \mapsto \phi$.

NB It can happen that $V_I^{\mathbb{A}}(k) = \phi$ but $V_I^{\mathbb{A}} \neq \phi$, eg.

$k = \mathbb{Q}$, $I = (x^2+1) \lhd \mathbb{Q}[x]$. However, this cannot happen if $k = \bar{k}$ (see later)

Def [Base-change] Let $k \hookrightarrow l$ an ext. of fields. Then we get a base-change functor

$\mathrm{Var}_k \to \mathrm{Var}_l$

sending a variety $V : \mathrm{Fld}/_k \to \mathrm{Set}$ to the functor

$\mathrm{Fld}/_l \xrightarrow{\text{forget}} \mathrm{Fld}/_k \xrightarrow{V} \mathrm{Set} \in \mathrm{Var}_l$

$L/_l \mapsto L/_k \mapsto V(L)$.

Trivial, but often useful!

Smoothness

Def Let $V \in \mathrm{Var}_k$, so $V \subset \mathbb{A}^n_k$ (or $\mathbb{P}^n_k$) for some n. A *presentation* of V is an ideal $I \subset k[x_1, \dots, x_n]$ (or $I \subset k[x_0, \dots, x_n]$ homog.) such that

$$V = V_I^{\mathbb{A}} \quad (\text{or } V = V_I^{\mathbb{P}})$$

By def'n, every variety admits a presentation.

Def: A variety V is called an affine (projective) hypersurface if it can be written as $V_{(f)}^{\mathbb{A}(\mathbb{P})}$ for some $f \neq 0, \text{unit}$.

Def: An affine hypersurface $V_I^{\mathbb{A}} \subset \mathbb{A}^n_k$ is *smooth* if $\exists f$ s.t. $V_{(f)}^{\mathbb{A}} = V_I^{\mathbb{A}}$ & s.t.

$$V_J^{\mathbb{A}} = \emptyset \text{ (empty var.) where } J = \left(f, \frac{\partial f}{\partial x_1}, \dots, \frac{\partial f}{\partial x_n}\right).$$

This is an awkward def'n, sorry! There is a general def for when a variety is smooth (don't need 'embedded'), & it is then true that smoothness is stable under isomorphisms! (when def'd – not for hypersurfaces)

eg $I = (x^2+y^2-1) \lhd \mathbb{Q}[x,y]$ as before. Let $f = x^2+y^2-1$, then

$$\left(f, \frac{\partial f}{\partial x}, \frac{\partial f}{\partial y}\right) = \left(x^2+y^2-1, x, y\right) = (1), \text{ & } V_I^{\mathbb{A}} = \emptyset \text{ so } V_I^{\mathbb{A}} \text{ is smooth.}$$

It is slightly harder right now to give examples of non-smooth things, because we must prove something for *all* possible f defining V. Later it will become easier.

eg $I = (x^2) \lhd \mathbb{Q}[x,y]$. Then $\left(x^2, \frac{\partial x^2}{\partial x}, \frac{\partial x^2}{\partial y}\right) = (x)$, & $V_{(x)}^{\mathbb{A}} \neq \emptyset$.

However, $V_I^{\mathbb{A}} = V_{(x)}^{\mathbb{A}}$, & $\left(x, \frac{\partial x}{\partial x}, \frac{\partial x}{\partial y}\right) = (1)$, so $V_I^{\mathbb{A}}$ is smooth

Def: A projective hypersurface $V_I^{\mathbb{P}} \subset \mathbb{P}^n_k$ is *smooth* iff each of the $(n+1)$ restrictions to affine opens is smooth.

1.8 Uniqueness of presentations (& they aren't!)

Thm [Hilbert's Nullstellensatz]: Let k a field & $n \geq 0$. Let K an alg. cl. field containing k. Let $I, J \subseteq k[x_1, \dots, x_n]$. Then

$$V_I^A = V_J^A \iff \sqrt{I} = \sqrt{J}$$

(Here $\sqrt{I}$ denotes the radical of I, $= \{f \in k[x_1, \dots, x_n] \mid f^r \in I \text{ for some } r\}$.)

Pf: Omitted; not easy (~ end of a 1st comm. alg. course). (□).

Cor: k a field, $n \geq 0$, $I \subsetneq k[x_1, \dots, x_n]$. TFAE:

1) V_I^A is empty;
2) $I = (1)$;
3) $V_I^A(K)$ is empty for some alg. closed field $K \supseteq k$.

Pf: The implications $2 \Rightarrow 1 \Rightarrow 3$ are clear. Assume 3. Then NSZ implies $\sqrt{I} = (1)$, which implies $I = (1)$. □

Cor: Let $f \in k[x_1, \dots, x_n]$ irreducible. Then $V_{(f)}^A$ is smooth iff $(f, \frac{\partial f}{\partial x_1}, \dots, \frac{\partial f}{\partial x_n}) = (1)$.

Pf: $\Leftarrow$ is clear. Assume $V_{(f)}^A$ smooth. Then $\exists\, g \in k[x_1, \dots, x_n]$ s.t. $V_{(f)}^A = V_g^A$ & s.t. $(g, \frac{\partial g}{\partial x_1}, \dots, \frac{\partial g}{\partial x_n}) = (1)$. But NSZ $\Rightarrow \sqrt{(f)} = \sqrt{(g)}$. $\xrightarrow{\text{fixed, } k[x_1,\dots,x_n] \text{ UFD}}$ $g = f^m \cdot u$ some $u \in k^\times$, $m \geq 1$

Then $(1) = (g, \frac{\partial g}{\partial x_1}, \dots, \frac{\partial g}{\partial x_n}) = (f^m, \frac{\partial f^m}{\partial x_1}, \dots, \frac{\partial f^m}{\partial x_n}) = f^{m-1}(f, \frac{\partial f}{\partial x_1}, \dots, \frac{\partial f}{\partial x_n})$.

Hence either

- $m = 1$ & we're done

or

- $m > 1$ & $f = 1$ (then done).

□