Historical motivation for commutative algebra: Algebraic Curves.

Start with $f(x,y) \in \mathbb{Z}[x,y]$.

Formalities:

$$f(x,y) = \sum_{i,j \geq 0} a_{ij} x^i y^j$$

where $a_{ij} \in \mathbb{Z}$

and $a_{ij} = 0$ for "almost all" i, j.

Monomial: $ax^i y^j$ $(a \neq 0)$.

Degree: $\deg(ax^i y^j) = i + j$.

$$\deg\left(\sum a_{ij} x^i y^j\right) = \max\{i+j : a_{ij} \neq 0\}$$

Since $\mathbb{Z}$ is integral domain (i.e., $a, b \neq 0 \Rightarrow ab \neq 0$), for any monomials $m = ax^i y^j$

$n = bx^k y^l$,

we have

$$\deg(mn) = \deg(ab\, x^{i+k} y^{j+\ell})$$
$$= (i+k)+(j+\ell)$$
$$= (i+j)+(k+\ell)$$
$$= \deg(m) + \deg(n).$$

Hence, for <u>any</u> $F(x,y), g(x,y) \in \mathbb{Z}[x,y]$ we have

$$\deg(fg) = \deg(f) + \deg(g).$$

Proof: Leading term of fg.

= (leading term f)(leading term g). ///

For any ring $(A, +, \times, 0_A, 1_A)$, there exists a <u>unique</u> ring homomorphism

$$\iota : \mathbb{Z} \to A$$

Indeed, one can check that

$$\iota(n) := \begin{cases} 1_A + 1_A + \cdots + 1_A & n > 0, \\ 0_A & n = 0, \\ -(1_A + 1_A + \cdots + 1_A) & n < 0. \end{cases}$$

Then for any $\alpha, \beta \in A$, there exists a unique ring homomorphism

$$\iota_{\alpha,\beta} : \mathbb{Z}[x,y] \to A$$

sending $x \mapsto \alpha$, $y \mapsto \beta$. Indeed,

$$\iota_{\alpha,\beta}\left(\sum a_{ij} x^i y^j \right) = \sum \iota(a_{ij}) \alpha^i \beta^j. \quad ///$$

This homomophism is called "evaluation at the point $(\alpha, \beta) \in A^2$." For short:

$$\mathbb{Z}[x,y] \ni f(x,y) \longmapsto f(\alpha,\beta) \in A.$$

Algebraic Curves:

Given $f(x,y) \in \mathbb{Z}[x,y]$, we have an "abstract curve" C_f.

What kind of thing is it?

For any ring A, the abstract curve defines a set of "A-points":

$$C_f(A) := \{(\alpha,\beta) \in A^2 : f(\alpha,\beta) = 0\}$$

[Jargon: C_f is a "scheme." Formally, it is a functor Rings $\to$ Sets.]

What kind of question about C_f might be interesting?

Diophantine: $\mathbb{Z}$-points, $\mathbb{Q}$-points

Geometry: $\mathbb{R}$-points.

Modern Number Theory: $\mathbb{F}_q$-points

[$\mathbb{F}_q$ = finite field of size $q = p^k$]

Look very different, but there is an underlying structure.

Miracle: For any $f(x,y) \in \mathbb{Z}[x,y]$ there is a special integer $g \geq 0$ called the "genus" of the abstract curve C_f, which influences the behavior of the A-points for any A.

Some Famous Theorems:
[To make statements cleaner I will include "points at infinity." I.O.U.]

- $\mathbb{Z}, \mathbb{Q}$-points:

$g = 0$: $C_f(\mathbb{Q}) \longleftrightarrow \mathbb{Q}$

$C_f(\mathbb{Z})$ harder but completely understood related to continued fractions, & Pell's equation $x^2 - ny^2 = \pm 1$.

$g = 1$: $C_f(\mathbb{Q})$ is finitely generated abelian group (Mordell, 1922)

$g \geq 1$: $\#C_f(\mathbb{Z}) < \infty$ (Siegel, 1929)

$g \geq 2$: $\#C_f(\mathbb{Q}) < \infty$ (Faltings, 1983)

- $\mathbb{R}$-points:

$g = 0$: Conic sections

$g = 1$: Elliptic curves

$\approx$ $y^2 = (x-a_1)(x-a_2)(x-a_3)$

a_1, a_2, a_3 distinct.

Plücker's Formula (1830): If $C_f(\mathbb{R})$ has only double points & cusps, and $\deg(f) = d$, then

$$g = \frac{(d-1)(d-2)}{2} - \#\text{double points} - \#\text{cusps}.$$

Harnack's Theorem (1876):

$$\#\text{connected components of } C_f(\mathbb{R}) \leq g+1.$$

- $\mathbb{F}_q$-points:

$g=0$: $\#C_f(\mathbb{F}_q) = q+1$.

$g=1$: (Hasse, 1933)

$$|\#C_f(\mathbb{F}_q) - (q+1)| \leq 2\sqrt{q}.$$

$g \geq 2$: (Weil, 1949)

$$|\#C_f(\mathbb{F}_q) - (q+1)| \leq 2g\sqrt{q}.$$

Questions:

- How to define g?
- How to compute g?

Key: We should consider the complex points of the curve!

$$C_f(\mathbb{C}) \subseteq \mathbb{CP}^2$$