We have covered a lot of theory in this course so far.
In this lecture and the next, I want to revisit some of these results and provide additional examples and motivation.

§1 Commutative algebra developed from the desire to understand polynomial equations

The general formulation:

·) R a ring, e.g. $\mathbb{Z}$, $\mathbb{Q}$ or $\mathbb{C}$.

·) $n, m \geq 0$ and $f_1, \ldots, f_m \in R[T_1, \ldots, T_n]$.

·) For any R-algebra B, define the solution set

$$X(B) := \{ (x_1, \ldots, x_n) \text{ s.th. } f_1(x_1, \ldots, x_n) = \ldots = f_m(x_1, \ldots, x_n) = 0 \}$$

Most basic questions: Is $X(B) \neq \emptyset$?

If yes, then what are its properties?

Example: Pythagorean Triples

Pythagorean Triple $\underset{def}{=}$ triple $(0,0,0) \neq (a,b,c) \in \mathbb{Z}^3$ s.th. $a^2+b^2=c^2$

(a,b,c) **primitive** $\underset{def}{=}$ $\gcd(a,b,c)=1, \quad c>0.$

Every Pythagorean Triple is a multiple of a primitive triple, so it suffices to determine these.

Lem 1 There is a bijection

$$\{\text{primitive Pyth. triples } (a,b,c)\} \xrightarrow{1:1} \{(x,y) \in \mathbb{Q}^2 \text{ s.th. } x^2+y^2=1\}$$

$$(a,b,c) \longmapsto (a/c, b/c)$$

Proof The converse map is given as follows:

Given x,y with $x^2+y^2=1$, write $x=\frac{a}{c}$, $y=\frac{b}{c}$ with $c>0$ and $\gcd(a,b,c)=1$. Then map (x,y) to (a,b,c). $\square$

Define $X(R) := \{(x,y) \in R \mid x^2+y^2=1\}$

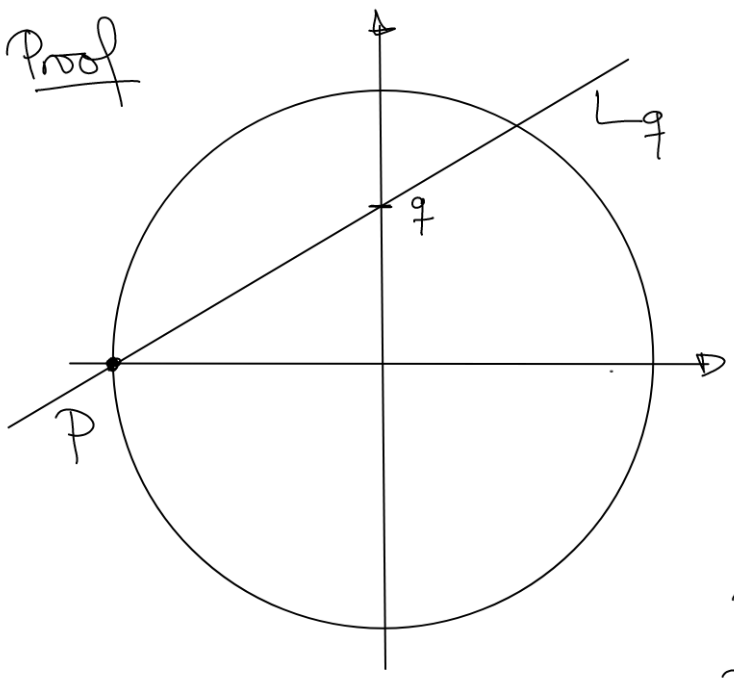
The point $P = (-1, 0)$ lies in $X(\mathbb{Q})$. Our aim is to find all other points of $X(\mathbb{Q})$.

<u>Prop 2</u> There is a bijection

$$\begin{aligned} \mathbb{Q} &\xrightarrow{\sim} X(\mathbb{Q}) \setminus \{P\} \\ q &\longmapsto \left(\frac{1-q^2}{1+q^2}, \frac{2q}{1+q^2} \right) \qquad @ \\ \frac{y}{x+1} &\longmapsfrom (x, y) \end{aligned}$$

Note that $1+q^2 > 0$ $\forall q \in \mathbb{Q}$ and that $x \neq -1$ for all $(x, y) \in X(\mathbb{Q}) \setminus \{P\}$.

<u>Proof</u>



For $q \in \mathbb{Q}$, consider the line L_q of slope q through P.

It intersects the circle in precisely one other point.

We show that this point lies in $\mathbb{Q}^2$ and has the coordinates written in @.

L_q is defined by $y = qx + q$.

Thus we need to solve $\begin{cases} qx + q = y & (\mathrm{I}) \\ x^2 + y^2 = 1. & (\mathrm{II}) \end{cases}$

Substituting (I) in (II) gives

$$1 = x^2 + (qx+q)^2 = (1+q^2)\,x^2 + 2q^2 x + q^2.$$

The beautiful phenomenon here is that we already know that $P \in L_q$, meaning that $x = -1$ is a zero of this quadratic polynomial. Then the other zero has to lie in $\mathbb{Q}$ as well!

Since $(x-\alpha)(x-\beta) = x^2 - (\alpha+\beta)x + \alpha\beta$, we directly see it equals $\frac{1-q^2}{1+q^2}$. (Namely $\alpha = -1$, $\alpha\beta = \frac{q^2-1}{q^2+1}$ in our case.)

We obtain that

$$L_q \cap \left(X(\mathbb{Q}) \setminus \{P\}\right) = \left(\frac{1-q^2}{1+q^2}, \frac{2q}{1+q^2}\right),$$

and in ptic the map is defined.

Converse map: Given $(x,y) \in X(\mathbb{Q}) \setminus P$, the slope of the line through P and (x,y) is $q = \dfrac{y}{x+1}$. $\square$

We can get back to Pythagorean Triples:

Write $q = u/v$ with $\gcd(u,v) = 1$. Then

$$\left(\frac{1-q^2}{1+q^2}, \frac{2q}{1+q^2}\right) \longmapsto (1-q^2, 2q, 1+q^2)$$

$$\underset{\cdot v^2 \text{ or } \cdot v^2/2}{\longmapsto} \begin{cases} (v^2-u^2, 2uv, v^2+u^2) & \text{if one out of } u,v \text{ even.} \\ \left(\frac{v^2-u^2}{2}, uv, \frac{v^2+u^2}{2}\right) & \text{if both } u,v \text{ even.} \end{cases}$$

is the corresponding primitive Pythagorean triple.

More precisely, we have shown:

<u>Thm</u> Every Pyth. Triple is of the form

$$\begin{cases} (v^2-u^2, 2uv, v^2+u^2) & \text{one out of } u,v \text{ even.} \\ \left(\frac{v^2-u^2}{2}, uv, \frac{v^2+u^2}{2}\right) & u,v \text{ both odd} \end{cases}$$

for a unique pair $u \in \mathbb{Z}$, $v \in \mathbb{Z}_{>0}$, $(u,v) = 1$.

Question: This is indeed a pretty result, but how is it related to our course?

Consider the general situation of $f_1, \dots, f_m \in R[T_1, \dots, T_n]$ again for a moment. Let $A = R[T_1, \dots, T_n]/(f_1, \dots, f_m)$.

Then we have seen that

$$\begin{array}{ccc} \mathrm{Hom}_{R\text{-alg}}(A, B) & \xrightarrow{\sim} & X(B) \\ \varphi & \longmapsto & (\varphi(T_1), \dots, \varphi(T_n)) \end{array} \qquad (*)$$

In other words, the R-algebra A fully encodes the system of equations $f_1(x_1, \dots, x_n) = \dots = f_m(x_1, \dots, x_n) = 0$!

Proof of $(*)$ Consider the situation

$$\begin{tikzcd} R[T_1, \dots, T_n] \arrow[r, "T_i \mapsto x_i", "\widetilde{\varphi}_x"'] \arrow[d] & B \\ R[T_1, \dots, T_n]/(f_1, \dots, f_m) \arrow[ur, dotted, "\varphi_x"'] & \end{tikzcd}$$

Given $\widetilde{\varphi}_x$, at most one factorization φ_x exists.

It exists $\Leftrightarrow \widetilde{\varphi}_x(f_j) = f_j(x_1, \dots, x_n) = 0 \quad \forall j = 1, \dots, m$ $\square$

For our Pyth. Triples, we wanted to compute

$$\mathrm{Hom}_{\mathbb{Q}\text{-alg}}\left(\mathbb{Q}[X,Y,\tfrac{1}{X+1}]/(X^2+Y^2-1),\ \mathbb{Q}\right)$$

<u>Prop 3</u> (Improves Prop 2) Let $R = \mathbb{Z}[\frac{1}{2}]$. There is an isomorphism of R-algebras

$$R[X,Y,\tfrac{1}{X+1}]/(X^2+Y^2-1) \cong R[q, \tfrac{1}{1+q^2}]$$

given by $X \mapsto \dfrac{1-q^2}{1+q^2}$, $Y \mapsto \dfrac{2q}{1+q^2}$.

The inverse map is given by $q \mapsto \dfrac{Y}{X+1}$.

<u>Proof</u> The formulas give the following <u>diagonal</u> maps:

$$\begin{tikzcd}
R[X,Y] \arrow[d] \arrow[drr] & & R[q] \arrow[d] \arrow[dll] \\
R[X,Y,\frac{1}{X+1}]/(X^2+Y^2-1) \arrow[rr, dashed, shift left, "\Phi"] & & R[q,\frac{1}{q^2+1}] \arrow[ll, dashed, shift left, "\Psi"]
\end{tikzcd}$$

We need to show they factor over the quotient and/or localization:

$$X^2+Y^2-1 \mapsto \frac{(1-q^2)^2+4q^2}{(1+q^2)^2} - 1 = 0$$

$$X+1 \longmapsto \frac{1-q^2}{1+q^2}+1 = \frac{1-q^2+1+q^2}{1+q^2} = \frac{2}{1+q^2}$$

This element lies in $\mathbb{Z}[\frac{1}{2}, q, \frac{1}{q^2+1}]^\times$ so we have shown that Φ exists.

$$q^2+1 \longmapsto \left(\frac{Y}{X+1}\right)^2+1 = \frac{Y^2+X^2+2X+1}{(X+1)^2}$$

$$= 2\cdot\frac{X+1}{(X+1)^2} = \frac{2}{X+1}.$$

since $X^2+Y^2=1$

This element lies in $\mathbb{Z}[\frac{1}{2}, X, Y, \frac{1}{X+1}]/(X^2+Y^2-1)^\times$, so we have shown that Ψ exists.

One can now check directly that Φ and Ψ are mutual inverses. $\square$

<u>Cor 4</u> Let B be any ring s.th. $2\in B^\times$. Then

$$\{q\in B \mid 1+q^2\in B^\times\} \xrightarrow{\sim} \left\{(x,y)\in B^2 \;\middle|\; \begin{matrix} x^2+y^2=1 \\ x+1\in B^\times \end{matrix}\right\}.$$

$$q \longmapsto \left(\frac{1-q^2}{1+q^2}, \frac{2q}{1+q^2}\right). \qquad \square$$

I want to mention a famous, and famously difficult results in this context.

<u>Thm (Fermat's Last Theorem, Andrew Wiles 1994)</u>

Assume that $n \geq 3$. There is no triple $(x, y, z) \in \mathbb{Q}^3$ with $xyz \neq 0$ s.th. $x^n + y^n = z^n$.

·) The condition $xyz \neq 0$ excludes the obvious solutions
$$x^n + 0^n = x^n, \quad 0^n + y^n = y^n \quad \text{etc.}$$

·) Fermat stated this "result" in 1637 and it has motivated generations of mathematicians since then.

I highly recommend to have a look at its Wikipedia article.

§2 The Spectrum, revisited

Question: OK, this is all interesting. But why did we spend so much time studying the spectrum?

Short Answer: The spectrum parametrizes solutions of the given equations in field extensions.

Recall the setting from before:

- ·) R ring, $f_1, \dots, f_m \in R[T_1, \dots, T_n]$
- ·) $A = R[T_1, \dots, T_n]/(f_1, \dots, f_m)$
- ·) For B an R-algebra

$$X(B) = \{ (x_1, \dots, x_n) \in B^n \mid f_j(x_1, \dots, x_n) = 0 \;\; \forall j = 1, \dots, m \}.$$

Now consider an R-algebra $R \to \Omega$ that is a field.
Given $x = (x_1, \dots, x_n) \in X(\Omega)$, let $\varphi_x : A \to \Omega$ be the corresponding R-alg. homomorphism. Then $\ker(\varphi_x)$ is a prime ideal and φ_x induces a map

$$\overline{\varphi}_x : \mathrm{Quot}(A/\ker(\varphi_x)) \hookrightarrow \Omega$$

Conversely, assume $\mathfrak{p} \subseteq A$ is a prime ideal, and

$$\varphi : \kappa(\mathfrak{p}) = \mathrm{Quot}(A/\mathfrak{p}) \longrightarrow \Omega$$

an embedding of $\kappa(\mathfrak{p})$ into a field Ω. Then the composition $R \to A \to \kappa(\mathfrak{p}) \to \Omega$ makes Ω into an R-algebra and φ defines a solution $\in X(\Omega)$.

§3 A concrete realization

We will soon prove the following theorem:

<u>Thm (Hilbert's Nullstellensatz)</u> Every maximal ideal of $\mathbb{C}[X_1, \ldots, X_n]$ has the form $\mathfrak{m}_x = (X_1 - x_1, \ldots, X_n - x_n)$ for a unique tuple $x = (x_1, \ldots, x_n) \in \mathbb{C}^n$.

Consider now a map of polynomial rings

$$h : \mathbb{C}[Y_1, \ldots, Y_m] \longrightarrow \mathbb{C}[X_1, \ldots, X_n]$$

$$Y_j \longmapsto f_j(X_1, \ldots, X_n) \quad j = 1, \ldots, m$$

Prop 5 The following diagram commutes:

$$\begin{tikzcd}
x \arrow[d, mapsto] & \mathbb{C}^n \arrow[r, "\sim"] \arrow[d] & \operatorname{MaxSpec} \mathbb{C}[X_1, \dots, X_n] \arrow[d, "\operatorname{Spec}(h)"] \\
(f_1(x), \dots, f_m(x)) & \mathbb{C}^m \arrow[r, "\sim"] & \operatorname{MaxSpec} \mathbb{C}[Y_1, \dots, Y_m]
\end{tikzcd}$$

$$x \longmapsfrom \mathfrak{m}_x$$

$$y \longmapsto \mathfrak{m}_y$$

Proof Let $\mathfrak{m}_x = (X_1 - x_1, \dots, X_n - x_n) \subseteq \mathbb{C}[X_1, \dots, X_n]$.

This ideal is the kernel of

$$\varphi_x : \mathbb{C}[X_1, \dots, X_n] \longrightarrow \mathbb{C}$$
$$X_i \longmapsto x_i.$$

It follows that $(\operatorname{Spec} h)(\mathfrak{m}_x) = h^{-1}(\mathfrak{m}_x)$ equals the kernel of the composition

$$\mathbb{C}[Y_1, \dots, Y_m] \xrightarrow{h} \mathbb{C}[X_1, \dots, X_n] \xrightarrow{\varphi_x} \mathbb{C}$$
$$Y_i \longmapsto f_i(X_1, \dots, X_n) \longmapsto f_i(x_1, \dots, x_n),$$

i.e. is equal to $(Y_1 - f_1(x_1, \dots, x_n), \dots, Y_m - f_m(x_1, \dots, x_n))$ as claimed in the proposition. $\square$

The significance of Hilbert's Nullstellensatz and Prop 5 is that it allows to translate all statements about polynomial maps and systems of polynomial equat. into commutative algebra.