Bevezető algebrai geometria

Szikszai Márton

Debreceni Egyetem
Algebra és Számelmélet Tanszék

2016. március 4.

Debrecen

Motiváló példák

Miért érdemes a diofantikus problémákat geometriai szemléletmóddal vizsgálni?

Pitagoraszi számhármasok

Primitív pitagoraszi számhármasok

Parametrizáljuk azokat az a, b, c relatív prím pozitív egészeket, melyek megoldják az

$$a^2 + b^2 = c^2$$

egyenletet!

Az egyenlet egy ekvivalens alakja

$$\left(\frac{a}{c}\right)^2 + \left(\frac{b}{c}\right)^2 = 1.$$

Az $x = a/c$ és $y = b/c$ helyettesítésen keresztül az egyenlet egész megoldásait megfeleltethetjük az

$$x^2 + y^2 = 1$$

egységkör racionális pontjainak.

Pitagoraszi számhármasok

Tétel

Az összes primitív pitagoraszi számhármas

$$a = 2mn,\ b = m^2 - n^2,\ c = m^2 + n^2$$

alakú, ahol m, n relatív prím pozitív egészek és $n < m$.

Megmutatható, hogy a $(0, 1)$ pontból végzett sztereografikus projekció esetén a $(0, 1)$ és P' pontokon átmenő egyenes az egységkört a

$$P = \left(\frac{2mn}{m^2 + n^2}, \frac{m^2 - n^2}{m^2 + n^2}\right)$$

pontban metszi.

Algebrai geometria nyelvén: az affin egyenes és az egységkör által definiált algebrai görbe biracionálisan ekvivalens, ahol a transzformációkat a sztereografikus projekció és inverze adja meg.

Fermat utolsó tétele

Tétel (Fermat-Wiles)

Az

$$x^n + y^n = z^n$$

egyenletnek nincs nem triviális megoldása, ha $n \geq 3$.

Yves Hellegouarch (60-as évek vége): a Fermat egyenlet egy a, b, c megoldásához rendeljük hozzá az

$$E_n : y^2 = x(x - a^n)(x - b^n)$$

elliptikus görbét.

Modularitás-tétel (korábban Taniyama-Shimura-Weil-sejtés): a $\mathbb{Q}$ feletti elliptikus görbék modulárisak.

Fermat utolsó tétele

Frey (1982-85): ha létezne ellenpélda Fermat-tételére, akkor E_n nem moduláris (ekkor még a modularitás-tétel csak sejtés volt).

Serre (1985): a Taniyama-Shimura-Weil-sejtés ún. "szemistabil" esetéből következne Fermat tétele. Csak részben bizonyította, a kimaradó részből lett az úgynevezett epszilon-sejtés.

Ribet (1986): epszilon-sejtés igazolása.

Wiles (1993): a Taniyama-Shimura-Weil-sejtés szemistabil esetének egy nem teljes bizonyítása.

Wiles, Taylor (1995): a kimaradó rész áthidalása.

Breuil, Conrad, Diamond, Taylor (1998): a modularitás-tétel.

A kongruens szám probléma

Az $n \in \mathbb{N}$ kongruens szám, ha létezik $a, b, c \in \mathbb{Q}$, hogy

$$a^2 + b^2 = c^2 \qquad \text{és} \qquad n = \frac{ab}{2}.$$

Klasszikus megfogalmazásban: létezik olyan derékszögű háromszög, hogy oldalai racionálisak és területe n.

Kongruens szám probléma

Adott természetes számról döntsük el, hogy kongruens szám-e.

Vegyük észre, hogy

$$\left(\frac{a+b}{2}\right)^2 = \frac{a^2 + 2ab + b^2}{4} = \frac{c^2 + 4n}{4} = \left(\frac{c}{2}\right)^2 + n,$$

$$\left(\frac{a-b}{2}\right)^2 = \frac{a^2 - 2ab + b^2}{4} = \frac{c^2 - 4n}{4} = \left(\frac{c}{2}\right)^2 - n.$$

Legyen $x = (c/2)^2$. Ekkor

$$x - n = \left(\frac{a-b}{2}\right)^2 \qquad \text{és} \qquad x + n = \left(\frac{a+b}{2}\right)^2.$$

Azaz olyan $x \in \mathbb{Q}$ számot keresünk, hogy $x-n, x, x+n$ egyszerre racionális négyzetek. Következésképpen

$$y^2 = (x-n)x(x+n) = x^3 - n^2 x.$$

Tétel

Az $n \in \mathbb{N}$ pontosan akkor kongruens szám, ha az $E: \; y^2 = x^3 - n^2 x$ elliptikus görbe rangja pozitív.

A kongruens szám tulajdonságra Tunnell adott egyszerűen ellenőrizhető kritériumot Birch és Swinnerton-Dyer sejtését feltételezve.

Algebrai halmazok

Példa egy geometriai objektum algebrai vizsgálatára.

Affin algebrai halmazok

Legyen $\mathbb{K}$ egy test. A $\mathbb{K}$ feletti n dimenziós affin tér

$$\mathbb{A}^n(\mathbb{K}) = \mathbb{K}^n.$$

$\mathbb{A}^n(\mathbb{K})$ elemeit pontoknak nevezzük.

- $n = 1$: affin tengely.
- $n = 2$: affin sík.
- $n = 3$: affin tér.

Ha $F \in \mathbb{K}[X_1, \ldots, X_n]$, akkor egy $P = (a_1, \ldots, a_n) \in \mathbb{A}^n(\mathbb{K})$ pont az F zérója, ha $F(P) = 0$.

Ha F nem konstans, akkor zéróinak halmaza $V(F)$ az F által definiált hiperfelület.

Affin algebrai halmazok

Ha $\deg F = 1$, akkor $\mathbb{A}^n(\mathbb{K})$ egy hipersíkjáról beszélünk.

- $\mathbb{K} = \mathbb{R}$, $n = 2$, $F(x, y) = ax + by + c$ - $V(F)$ egyenes;
- $\mathbb{K} = \mathbb{R}$, $n = 3$, $F(x, y) = ax + by + cz + d$ - $V(F)$ sík.
- és így tovább...

Általánosabban, ha $S \subset \mathbb{K}[X_1, \ldots, X_n]$ polinomok egy halmaza, akkor

$$V(S) = \{P \in \mathbb{A}^n(\mathbb{K}) : F(P) = 0 \text{ bármely } F \in S \text{ esetén}\}.$$

A $V \subset \mathbb{A}^n(\mathbb{K})$ affin algebrai halmaz vagy egyszerűen algebrai halmaz, ha $V = V(S)$ valamely $S \subset \mathbb{K}[X_1, \ldots, X_n]$ esetén.

Algebrai halmazok szerkezete

Emlékeztetésképpen, ha R egy gyűrű, akkor I az R egy ideálja, amennyiben

- I az $(R, +)$ részcsoportja;
- I zárt az R-beli elemekkel való szorzásra.

Ha $S \subset R$, akkor az S által generált ideál a legszűkebb ideál I, hogy $S \subset I$. Ha R kommutatív és egységelemes, akkor az $S = \{s_1, \ldots, s_r\}$ által generált ideál

$$\{a_1 s_1 + \cdots + a_r s_r : a_i \in R\}.$$

Speciálisan, az $S = \{F_1, \ldots, F_r\} \subset \mathbb{K}[X_1, \ldots, X_n]$ által generált ideál

$$\{G_1 F_1 + \cdots + G_r F_r : G_i \in \mathbb{K}[X_1, \ldots, X_n]\}.$$

Algebrai halmazok szerkezete

Állítás

Ha I az S által generált ideál $\mathbb{K}[X_1, \ldots, X_n]$-ben, akkor $V(S) = V(I)$.

Bizonyítás.

Standard. Megmutatható, hogy $V(I) \subset V(S)$ és $V(S) \subset V(I)$. □

Azaz, minden algebrai halmaz előállítható az S-beli polinomok által generált ideál segítségével.

Ennél többet is mondhatunk.

Tétel

Minden algebrai halmaz véges sok hiperfelület metszete.

Az eredeti definícióban S akármennyi polinom halmaza is lehetett.

Algebrai halmazok szerkezete

Újabb algebrai eszközökre lesz szükségünk.

Egy gyűrű Noether, ha benne minden ideál végesen generált.

Tétel (Hilbert bázistétele)

Ha R Noether gyűrű, akkor $R[X_1, \ldots, X_N]$ is Noether gyűrű.

A bázistételt nem igazoljuk, azonban (mivel a testek Noether gyűrűk) az előző állítás most már egyszerű következménnyé változik.

Bizonyítás.

Legyen $V(I)$ az algebrai halmaz. Mivel $\mathbb{K}[X_1, \ldots, X_n]$ Noether, ezért $I = (F_1, \ldots, F_r)$ végesen generált és $V(I) = V(F_1) \cap \cdots \cap V(F_r)$. $\square$

Algebrai halmazok szerkezete

$V \subset \mathbb{A}^n(\mathbb{K})$ algebrai halmaz reducibilis, ha léteznek olyan $V \neq V_1, V_2 \subset \mathbb{A}^n(\mathbb{K})$ algebrai halmazok, hogy $V = V_1 \cup V_2$. Ellenkező esetben V irreducibilis.

Emlékeztetésképpen, egy I ideál prímideál, ha nem az egész gyűrű és a gyűrű bármely olyan a, b elemeire, melyre $ab \in I$, $a \in I$ vagy $b \in I$ teljesül.

Állítás

A V algebrai halmaz pontosan akkor irreducibilis, ha $I(V)$ prímideál $\mathbb{A}^n(\mathbb{K})$-ban.

Tétel

Minden algebrai halmaz egyértelműen felbontható véges sok irreducibilis páronként egymást nem tartalmazó algebrai halmaz uniójára.

Hilbert Nullstellensatz

Algebrailag zárt test felett ideálbeli polinomoknak van közös zérója, amennyiben az ideál nem a teljes polinomgyűrű.

Tétel ("Gyenge" Nullstellensatz)

Tegyük fel, hogy $\mathbb{K}$ algebrailag zárt, I egy $\mathbb{K}[X_1, \ldots, X_n]$, ami nem a teljes polinomgyűrű. Ekkor $V(I) \neq \emptyset$.

Az Nullstellensatz teljes erejű kimondásához bevezetjük az ideál radikáljának fogalmát.

Ha I ideál $\mathbb{K}[X_1, \ldots, X_n]$-ben, akkor radikálja

$$\sqrt{I} = \{F \in \mathbb{K}[X_1, \ldots, X_n] : \exists m \in \mathbb{N}, \text{ hogy } F^m \in I\}.$$

Ha $I = \mathrm{Rad}(I)$, akkor I radikál ideálnak nevezzük.

Hilbert Nullstellensatz

Tétel (Nullstellensatz)

Legyen $\mathbb{K}$ algebrailag zárt, I egy $\mathbb{K}[X_1, \dots, X_n]$-beli ideál. Ekkor $I(V(I)) = \mathrm{Rad}(I)$.

A tétel egy értelmezése: ha $F_1, \dots, F_r, G \in \mathbb{K}[X_1, \dots, X_n]$ és G eltűnik minden esetben, amikor $F_1, \dots, F_r$ eltűnik, akkor

$$G^m = G_1 F_1 + \cdots + G_r F_r \qquad (m \in \mathbb{N},\ G_i \in \mathbb{K}[X_1, \dots, X_n]).$$

Következmény

Ha I radikál ideál, akkor $I(V(I)) = I$. Azaz egyértelmű megfeleltetés van a radikál ideálok és az algebrai halmazok között.

Következmény

Ha I prímideál, akkor $V(I)$ irreducibilis. Azaz egyértelmű megfeleltetés van a prímideálok és az algebrai halmazok között.

Köszönöm a figyelmet!

Folytatás?