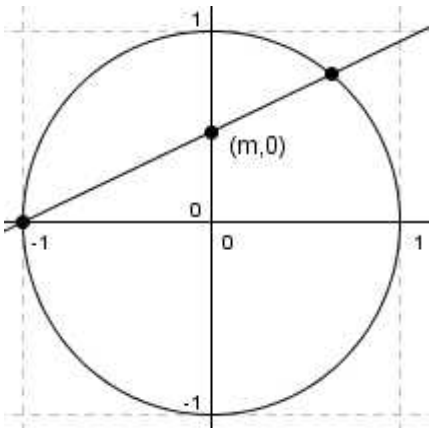
Algebrai síkgörbék

Algebrai síkgörbéknek az olyan görbéket nevezzük, amelyek pontjai egy kétváltozós polinommal jellemezhetők. Ilyenek az egyenesek (ezek az elsőfokú síkgörbék).



1. *ábra*

Másodfokú síkgörbék: pl. $x^2+y^2=1$ egy kör.
Ennek pontjai az $\mathbb{R}_{(x|y)^2}$ síkon vannak, amit azért hívunk így, mert egy-egy valós (x,y) számpárral határozzuk meg a pontjait.
Az ábrán látható egyenes egyenlete $y=mx+m$
Ennek a metszéspontja a körrel azok a pontok, amelyekre

$x^2+y^2=1$ és $y=mx+m$ teljesül. Helyettesítsük be az első egyenletbe a másodikat:

$$x^2+(mx+m)^2=1 \Leftrightarrow (m^2+1)x^2+2m^2x+(m^2-1)=0 \quad .$$

ez egy másodfokú egyenlet az egyenes és a kör metszéspontjainak *x* koordinátáira.

$$\frac{-2m^2\pm\sqrt{4m^4-(m^2+1)(m^2-1)}}{2(m^2+1)}=\frac{-m^2\pm1}{m^2+1} \quad .$$

Ennek gyökei : -1 és $\frac{-m^2+1}{m^2+1}$. Ebből következik, hogy y lehet 0 és $\frac{2m^2}{m^2+1}$.

$$\Lambda:(x,y)=\left(\frac{1-m^2}{1+m^2},\frac{2m^2}{m^2+1}\right) \quad .$$

Ez egy függvény, mely egy *m* meredekséghez hozzárendeli annak a pontnak a koordinátáit ami egy *m* meredekségű ((-1;0)-ból induló) húron van.

Mindkét koordináta az *m*-nek úgynevezett racionális függvénye, azaz *m* két polinomjának a hányadosa. Az ilyen függvény racionális *m*-hez racionális koordinátákat rendel.

Sikerült tehát egy paraméterrel (racionálisan) leírnunk az egységkört, azaz ha ebbe a függvénybe beírjuk az összes valós számot „egyesével” megkapjuk az egységkör pontjait.

A racionális síkot $\mathbb{Q}^2_{(x,y)}$ -nak hívjuk, mert ezen minden pont megfeleltethető egy racionális x, y számpárnak. Nézzük most csak ezen a síkon az előbb leírt kört és egyenest.

Legyen $\frac{M}{N}=m\in\mathbb{Q}$ és $M, N\in\mathbb{N}$

Legyen $x=\frac{X}{Z}\wedge y=\frac{Y}{Z}$ ahol $X, Y, Z\in\mathbb{N}$ (mert x,y mindig racionális) és feltehetjük, hogy *X*, *Y* és *Z* összeségükben relatív prímek (mert *x*, *y* mindig racionális).

$x^2+y^2=1$ -be behelyettesítve $X^2+Y^2=Z^2$ tehát *X*, *Y*, *Z* pitagoraszi számhármas, azaz a racionális egységkör minden pontja (kivéve a (-1;0) pontot) egy-egyértelműen megfeleltethető egy leegyszerűsített (*X*, *Y*, *Z* lnko.-ja egy) pitagoraszi számhármasnak. Bármilyen eredmény, amit kihozunk a racionális kör pontjainak koordinátáira, igaz lesz a pitagoraszi számhármasokra is.

Az előbbi eredmény alapján a $\Lambda:(x,y)$ függvény az *m* meredekséghez az

$$x=\frac{X}{Z}=\frac{1-m^2}{1+m^2}=\frac{1-\frac{M^2}{N^2}}{1+\frac{M^2}{N^2}}=\frac{N^2-M^2}{N^2+M^2}$$

illetve az

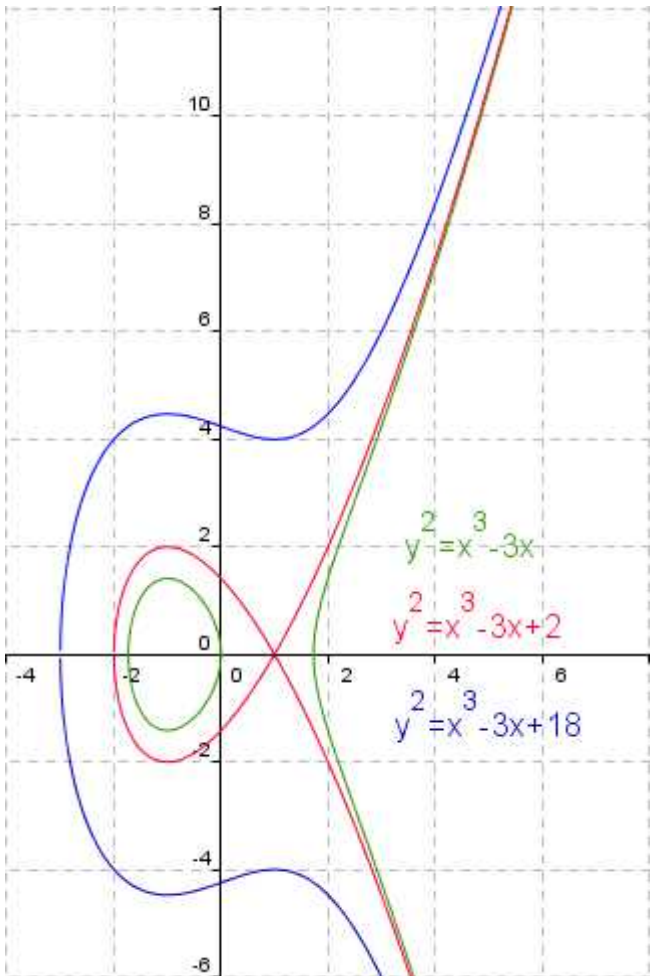
$$y=\frac{Y}{Z}=\frac{2m^2}{1+m^2}=\frac{2\frac{M^2}{N^2}}{1+\frac{M^2}{N^2}}=\frac{2MN}{N^2+M^2}$$

koordinátákat rendeli hozzá, tehát csak azok a jó X, Y, Z számhármasok amikre találunk olyan M, N (egész) számpárt, hogy a fenti két egyenlet igaz legyen.

Az egyenletekből következik (mert (X, Y, Z)=1), hogy:

$$X=N^2-M^2$$
$$Y=2MN$$
$$Z=M^2+N^2$$

Tehát csakkor adható meg M, N egész számpár, ha X, Y, Z leegyszerűsített pitagoraszi számhármas.
Ez egy jó példa arra, hogy milyen meglepő kapcsolata lehet a síkgörbéknek a matematika más területeivel.



2. *ábra*

Harmadfokú síkgörbék.

Weierstrass tétele szerint minden harmadfokú síkgörbe felírható

$$y^2=x^3+ax+b$$

alakban (alkalmas koordinátarendszerben[1]).

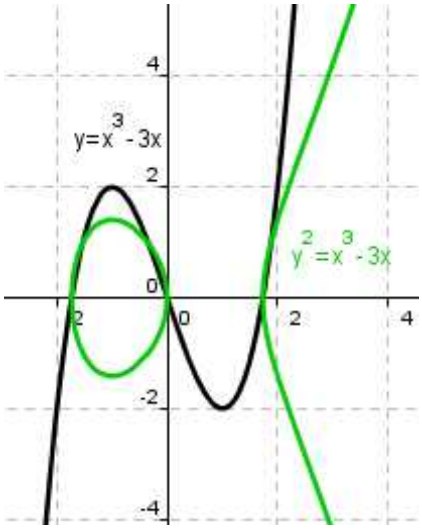
Nézzünk néhány példát harmadfokú síkgörbékre: (2. ábra)
Ez három lehetőség, ezen kívül vannak még más típusok, pl. három egyenes uniója is egy harmadfokú görbe.

Ezek abból látszanak szemléletesen, hogy harmadfokú görbét úgy kaphatunk, hogy egy harmadfokú

1 Alkalmas koordinátarendszerben – vagyis meg kell engedni, hogy projektív transzformációt végezzünk a görbével. Csak így írható fel például az $y=x^3+px+q$ egyenlet kívánt alakban, ti. az $(x,y)\to(\frac{x}{y},\frac{1}{y})$ transzformáció segítségével, mert elvégezve rajta ezt a transzformációt az $\frac{1}{y}=\left(\frac{x}{y}\right)^3+p\frac{x}{y}+q$ azaz $y^2=x^3+pxy^2+q$ alakot kapjuk, amiből már viszonylag könnyen kapunk Weierstrass alakot. A tétel a Weierstrass formáról igazából projektív harmadfokú görbékről szól.

polinomból „gyököt vonunk”, azaz minden x-re az addig felvett *y* érték helyett az *y* érték gyökét veszi fel. Tehát olyan *x*-ekre amelyekre *y* negativ volt, nem vesz fel semmit, a többi helyen pedig y négyzetgyökét és *y* négyzetgyökének -1-szeresét is felveszi, mert mindkettőnek a négyzete *y*.

($y^2=x^3-3x \Leftrightarrow y=\pm\sqrt{x^3-3x}$) (3. ábra)

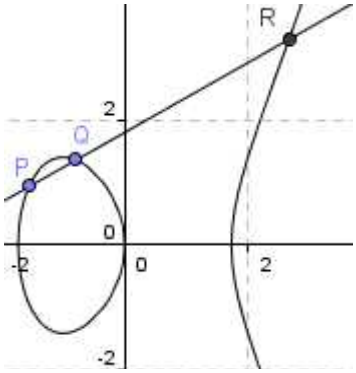


3. *ábra*

Az x-tengely 3-szor, 2-szer vagy 1-szer metszi a harmadfokú polinomot, ennek megfelelően kapjuk a három különböző típusú harmadfokú görbét.

Az előző részben sikerült a kört mint egyetlen változó racionális függvényét leírni:
($\Lambda:(x,y)=\left(\frac{1-m^2}{1+m^2},\frac{2m^2}{m^2+1}\right)$). Harmadfokú görbéknél azonban, ezt már nem tudjuk megcsinálni a következő tétel miatt:

TÉTEL. Nincsenek olyan $x(m)$ és $y(m)$ racionális törtfüggvények, amelyekre igaz, hogy az $(x|y)$ pont pontosan akkor van a harmadfokú síkgörbén, ha van olyan m, amelyre $x = x(m)$ és $y = y(m)$, másképp megfogalmazva: nincsenek olyan $x(m)$, $y(m)$ racionális törtfüggvények, hogy $y(m)^2=x(m)^3+ax(m)+b$ általános (a,b)-re.



4. *ábra*

Emiatt valami hasonlóval próbálkozunk, megprobálunk valami másféle struktúrát találni ahol racionális függvények szerepet játszanak
Nézzük a következő műveletet:

A görbe *P*, *Q* pontjaihoz hozzárendeljük a *PQ* egyenes és a görbe harmadik metszéspontját (a 4. ábrán látható módon. (4 metszéspont nem lehet mert akkor lenne olyan harmadfokú polinom aminek 4 gyöke volna.)
Ha nincs harmadik metszéspont, akkor két eset van. Ha *Q* a *P* pont tükörképe az *x*-tengelyre. Ebben az esetben rendeljük hozzájuk a $\underline{0}$ nullelemet (ez később kelleni fog).
Ha *P* nem tükörképe *Q*-nak, akkor az egyenes egy pontban metszi, egyben érinti a görbénket (a harmadfokú görbe egyenlete és az egyenes egyenlete által alkotott egyenletrendszert átrendezve *x*-re harmadfokú egyenletet kapunk, aminek ha van 2 valós gyöke, akkor három is, az egyik kettős gyök)
Ekkor az érintési pontot rendeljük hozzá a (*P*, *Q*) párhoz.

Legyen $P=(x_1|y_1)$, $Q=(x_2|y_2)$, $R=(x_3|y_3)$, *P*, *Q* ismert, *R* ismeretlen.
A *PQ*-n átmenő egyenesre igaz, hogy

$$\frac{x_3-x_2}{x_2-x_1}=\frac{y_3-y_2}{y_2-y_1} ,$$

a harmadfokú görbére pedig $y_3^2=x_3^3+ax_3+b$.

Először kifejezzük az első egyenletből *y*-t:

$$\frac{(y_2-y_1)}{x_2-x_1}x_3-\frac{(y_2-y_1)x_2}{x_2-x_1}+y_2=y_3$$

ezt behelyettesítve:

$$\left(\frac{(y_2-y_1)}{x_2-x_1}x_3-\frac{(y_2-y_1)x_2}{x_2-x_1}+y_2\right)^2=x_3^3+ax_3+b \quad ,$$

ez egy harmadfokú egyenlet x_3 -ra, szerencsére azonban nem kell kiszámolnunk mást, csak a konstans tagját, mert ismerjük két gyökét és a gyökök és együtthatók közti összefüggés segítségével:

$$x_1x_2x_3=b-\left(\frac{(y_2-y_1)x_2}{x_2-x_1}+y_2\right)^2 \quad \text{, azaz}$$

$$x_3=\frac{b-\left(\frac{(y_2-y_1)x_2}{x_2-x_1}+y_2\right)^2}{x_1x_2} \quad ,$$

$$y_3=\frac{(y_2-y_1)}{x_2-x_1}\underbrace{\frac{b-\left(\frac{(y_2-y_1)x_2}{x_2-x_1}+y_2\right)^2}{x_1x_2}}_{x_3}-\frac{(y_2-y_1)x_2}{x_2-x_1}+y_2 \quad ,$$

tehát az x_1, y_1, x_2, y_2 változók racionális függvényeként megadhatóak a harmadik metszéspont koordinátái.

A körnél lerögzítettünk egy pontot, és így egy változó változtatásával leírtuk az egész kört. Ha itt lerögzítünk egy pontot (x_1, y_1) , akkor egy változópár változtatásával (x_2, y_2) azaz egy pontnak a görbén való végigmozgatásával leírjuk a görbét.

Most definiáljuk a $\times$ műveletet, ami a görbe két tetszőleges pontjához hozzárendeli az általuk meghatározott egyenes és a görbe metszéspontjának x tengelyre való **tükörképét**. Ha a két pont azonos, akkor az e pontbeli érintő másik metszéspontjának (ilyen van) tükörképe a művelet eredménye. Ha pedig a két pont egymás tükörképe, akkor $\underline{0}$ a művelet eredménye.

Ez a $(G_{3-adfokú\ görbe} \cup \underline{0}; \times)$ struktúra csoport lesz (általános a,b-re)[2]!!! mert:

Nem vezet ki az alaphalmazból.
Van egységelem, az $\underline{0}$, ha $P \times \underline{0} = P$ -nek definiáljuk
Van inverz: minden P pont inverze a tükörképe, P': $P \times P' = \underline{0}$ ha egymás P és P' egymás tükörképei az x tengelyre.
Ráadásul kommutativ is ($P \times Q = Q \times P$) bár ez nem szükséges ahhoz, hogy csoport legyen.
Asszociativ is($(P \times (Q \times R) = (P \times Q) \times R)$) de ezt nehezebb bizonyítani. Bizonyítása szerepelt a következő előadásban, amelyet Hraskó tanár úr tartott. Lásd itt.

2 Azaz a görbe $y^2 = x^3 + ax + b$ egyenletében *a*, *b* általános. Ez azzal ekvivalens, hogy a görbe „sima”, és a kimondott tételek általában csak a „sima” harmadfokú görbékre igaz. Akkor sima egy görbe, ha minden pontban deriválható, azaz sehol sem „szúr”. Parciális deriváltakkal kiszámolható, hogy ez pontosan akkor igaz, ha $4a^3 + 27b^2 \neq 0$.

Most nézzük meg, mit tudhatunk a *komplex* harmadfokú görbékről.

Először tisztázzuk, hogy a kétdimenziós $\mathbb{C}^2_{(x|y)}$ komplex számsík ekvivalens a négydimenziós $\mathbb{R}^4_{(a|b|c|d)}$ valós térrel, ha az $x = a + b$i, $y = c + d$i megfeleltetést tekintjük. Vagyis $\mathbb{C}^2_{(a+bi|c+di)} \equiv \mathbb{R}^4_{(a|b|c|d)}$. Hogy mit jelent ez és hogy mit jelent egy „komplex algebrai síkgörbe", azt először pár egyszerűbb példán világítjuk meg.

A legegyszerűbb eset, amikor x=0. Ez a görbe most a $\mathbb{C}^2_{(x|y)}$ (komplex) számsíkon van, azonban a görbe leírható valós egyenletekkel is, mégpedig nagyon egyszerűekkel. Az x=0 egyenlet ugyanis azt jelenti, hogy a+bi=0, azaz a=b=0. Viszont c-re és d-re nincs kikötés, c és d tehát tetszőleges értéket felvehet. Vagyis az x=0 egyenletet az $\mathbb{R}^4_{(a|b|c|d)}$ tér (0|0|c|d) pontjai elégítik ki. Ez egy két (valós) dimenziós síkot jelent, amiről könnyen látható, hogy topológiailag ekvivalens azzal a gömbfelülettel, amelyből elhagytunk egy pontot. Hagyjuk ki ugyanis a gömbből az „Északi Sarkot" (É-t) és vetítsük belőle a gömbfelület minden pontját a „Déli Sarkot" érintő S síkra. (A gömbfelület tetszőleges P pontjának képe az ÉP egyenes és az S sík metszéspontja. Az $x = 0$ egyenletű komplex algebrai görbe tehát topológiailag a „gömbfelület – 1 pont".

Nézzük most, hogy mit jelent egy egyszerű másodfokú görbe, a „kör".

Az egyenlet most is: $x^2 + y^2 = 1$. A különbség csak az, hogy most x, y komplex, azaz $x = a + bi, y = c + di$, ahol a, b, c és d valós számok.

Ez a görbe most is a $\mathbb{C}^2_{(x|y)}$ (komplex) számsíkon van, azonban a görbe leírható egy valós egyenletpárral is, mert

$$x^2 + y^2 = (a+bi)^2 + (c+di)^2 = a^2 + c^2 - b^2 - d^2 + i(2ab + 2cd)$$

azaz

$$a^2 + c^2 - b^2 = 1 \quad \text{és} \quad ab + cd = 0 \ .$$

Az $\mathbb{R}^4_{(a|b|c|d)}$ négydimenziós valós számtérben ez egy két egyenlettel definiált alakzat. Ismét belátható, hogy a kapott alakzat topológiailag ekvivalens a „gömbfelület – 1 pont"-tal.

Ugyanígy egy harmadfokú komplex egyenlet, tehát

$$y^2 = x^2 + Ax + B \, ; \, x, y, A, B \in \mathbb{C}$$

is felbontható két valós egyenletre.

A kérdés ismét az, hogy milyen geometriai alakzatnak felel meg azon pontok halmaza, amelyre igaz ez az egyenlet, vagyis mi a 3-adfokú (komplex) síkgörbe „geometriája".

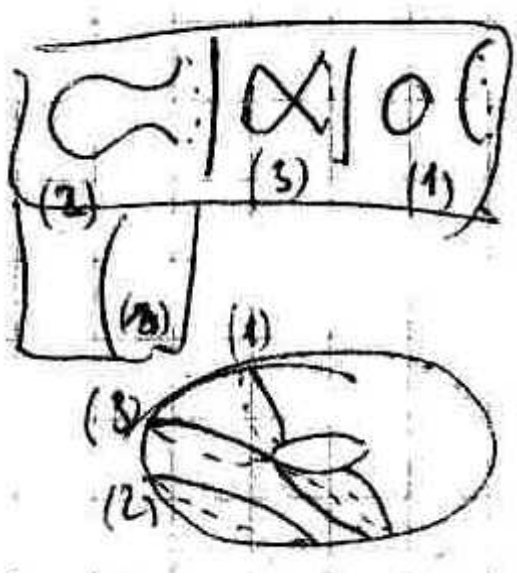
Mivel az előbb említett módon 2 (valós) egyenletünk van 4 ismeretlennel, $\mathbb{R}^4_{(a|b|c|d)}$-ben van 2 szabad paraméterünk. Ebből sejthető, hogy a harmadfokú görbe egy felület lesz, hiszen 2 független irányba „mozoghatunk" rajta, azaz két független ismeretlent változtatunk.

Pontosabban tehát az a kérdés, hogy milyen típusú felület azon pontok halmaza, amelyre igaz az

$$y^2 = x^2 + Ax + B \, ; \, x, y, A, B \in \mathbb{C}$$

egyenlet, vagy a neki megfelelő két (valós) egyenletből álló rendszer.

Ezt a következőképp állapítjuk meg.
Megnézzük a síkmetszeteit: itt van egy korántsem triviális tétel, ami azt mondja, hogy ezek olyanok mint amilyeneket az elején a valós harmadfokú síkgörbéknél tárgyaltunk. Ezek mind topológiailag azonosak a tórusz síkmetszeteivel: ha hozzávesszük a síkhoz a végtelen távoli pontokat, akkor a görbe széttartó szélei találkoznak, ezt mutatja az 5. ábránk, ott a „végtelen távoli pontnak" megfelelő pont van jelölve pontozással.



5. *ábra*

Ebből sejteni lehet, hogy a görbénk valamilyen tóruszféleség lesz. Valójában egy kilyukasztott tórusz, azaz egy tórusz aminek egy pontját elhagytuk *(ez a végtelen távoli pont a síkmetszetekben)*

Általánosan: egy (sima) *d*-edfokú komplex síkgörbe (*d*-edfokú polinomja $(x|y); x, y \in \mathbb{C}$ -nak, azaz minden tagban összesen legfeljebb *d*-edik hatványon van, pl. $x^3 y^2$ 5-fokú[3]) topologikusan (néhány pont elhagyásával) egy *g* lyukú tóruszfelületnek felel meg, ahol $g = \frac{(d-1)(d-2)}{2}$!!!

d = 1,2-re gömbfelület (néhány pontot elhagyva), azaz 0 lyukú tórusz.
d = 3-ra egylyukú tórusz.

Ebből levezethető tételek:
Az algebrai görbek geometriáját alapvetően meghatározza a *g* paraméter.
Beláthato hogy:

- egy algebrai görbe akkor és csak akkor paraméterezhető racionális függvényekkel ha *g* = 0;

- egy algebrai görbén csak akkor van csoportstruktúra ha g=1.
- A három fő eset *g* = 0, *g* = 1, *g* >1. Ez a harmas felosztás pontosan megfelel a három fajta síkgeometriának: gömbi, lapos (euklideszi), hiperbolikus (Bolyai-féle). Azaz a *g* = 0 eset geometriája gömbi, a *g* = 1 eseté lapos, a többié hiperbolikus.

3 Pontosabban: Egy $f(x, y) = 0$ polinomegyenlet fokszámának a legmagasabb fokú (nem-nulla együtthatójú) monom fokszámát nevezzük; egy $x^a y^b$ monom fokszáma $a + b$. Egy *n*-edfokú görbe egy *n*-edfokú *f* polinom nullhelyeinek halmaza az (x,y)($\mathbb{R}^2_{(x,y)}$) síkban.