

# ALGEBRAI GEOMETRIA TEMATIKA (1999. ŐSZ)

PETE GÁBOR <gpete@sol.cc.u-szeged.hu>

Ajánlott irodalom: **Ahlfors – Sario:** Riemann surfaces, **Dubrovin – Fomenko – Novikov:** Modern geometry — methods and applications I-III., **Fulton:** Algebraic curves, **Atiyah – MacDonald:** Introduction to commutative algebra, **Shafarevich:** Basic algebraic geometry, **Madsen – Tornehave:** From calculus to cohomology, **Silverman:** The arithmetic of elliptic curves I-II. Fontos még, hogy ezen a rövid jegyzeten kívül a kurzushoz készült feladatsor is lényeges dolgokat tartalmaz. Bármilyen kérdést vagy megjegyzést örömmel fogadok.

## *Riemann-felületek, Picard-csoport*

Egy  $\mathbb{K}$  test feletti  $\mathbb{P}^n\mathbb{K}$  projektív tér fogalma, projektív transzformációk.

Komplex sokaságok, Riemann-felületek definíciója. Riemann-felületek közötti holomorf függvények, meromorf függvények helyett  $\mathbb{P}^1\mathbb{C}$ -re képző holomorfak.

Komplex függvénytan ismétlés: Liouville-tétel, Cauchy integrálformula, Taylor- és Laurent-sor. Minden holomorf függvény egy nyílt leképezés. Reziduum-tétel.  $\text{ord}_x f = \text{res}(f'/f; x)$  definíció: zéróhelyek és pólusok multiplicitása.

Ha  $f : R \rightarrow S$  holomorf, akkor  $z_0 \in R$  egy környezetében  $f(z) = f(z_0) + g(z)^N$  előállítás, ahol  $g$  konformis,  $N = \deg f(z_0) = \nu_f(z_0)$  fok avagy elágazási szám; kritikus hely, ha  $\nu_f(z_0) > 1$ . (Nyilván köze van az  $\text{ord}_z f$ -hez.) A  $\deg f(w) = \sum_{f(z)=w} \deg f(z)$  érték független  $w$ -től. Ha  $w$  reguláris, akkor pontosan  $\deg f$  db ösképe van. Példa: az algebra alaptétele.

Riemann-felületek közötti holomorf függvények deriváltjai, a meromorf és holomorf differenciálok két definíciója:  $\eta = fdg$  ekvivalenciaosztályok, illetve a differenciáloknak megfelelő összeragasztási tulajdonságokkal rendelkező  $\eta = \{\eta_\alpha : V_\alpha \rightarrow \mathbb{C}\}$  kollekciónak egy adott  $\phi_\alpha : U_\alpha \rightarrow V_\alpha$  atlaszhoz. A második def szerinti tetszőleges két meromorf differenciál hányadosa egy meromorf függvény, és így ha létezik legalább egy nemkonstans meromorf függvény  $X$ -en (márpedig létezik), akkor minden meromorf differenciál  $fdg$  alakú, azaz a két def valóban ekvivalens.

Egy  $X$  kompakt R-felületen a divizorok  $\text{Div}(X)$  csoportja. Minden  $f \in \mathfrak{M}^*(X)$  függvényhez (a nem azonosan nulla meromorf függvények csoportja) tartozik egy  $\text{div} f = \sum_{x \in X} \text{ord}_x f \cdot (x)$  principális divizor, ezek részcsoportha a  $P(X)$ . Természetesen  $\mathfrak{M}^*(X)/\mathbb{C}^* \simeq P(X)$ . Az  $\omega$  differenciálokhöz tartoznak a  $\kappa = \text{div} \omega$  kanonikus divizorok. Definiálható a  $\text{Pic}(X) = \text{Div}(X)/P(X)$  Picard-csoport. Azt mondjuk, hogy két divizor lineárisan ekvivalens,  $D \sim D'$ , ha  $\text{Pic}(X)$ -ben megegyeznek; például egy előző bekezdésbeli megjegyzés miatt bármely két kanonikus differenciál lineárisan ekvivalens. A reziduum-tétel miatt  $P(X) \subseteq \ker(\text{deg} : \text{Div}(X) \rightarrow \mathbb{Z}) = \text{Div}^0(X)$ . Ismét  $\text{Pic}^0(X)$  faktorcsoport, ami (talán a látszat ellenére) többnyire nem-triviális. Látni fogjuk például, hogy egy  $X = \mathbb{C}/\Lambda$  tóruszra  $\text{Pic}^0(X) \simeq (X, +)$ , de ehhez már majd  $\theta$ -függvények is kellenek.

## Algebrai görbék, Bézout-tétel

Polinom homogenizáltja. Polinom által meghatározott affin és projektív görbe. Görbe szinguláris pontjai, érintőegyenesei. A másodrendű görbék (kúpszeletek) klasszifikációja  $\mathbb{R}$  és  $\mathbb{C}$  fölött.

Metszési index. Rezultáns. Bézout-tétel.

Minden nonszinguláris görbe irreducibilis, és egy irreducibilis görbének csak véges sok szingularitása van. Ha a szingularitásokat kihagyjuk, egy Riemann-felületet kapunk. A  $P(z, w(z)) = 0$  felületen lehet értelmezni a  $w(z)$  többértékű holomorf függvényt, mint pld. a  $\sqrt{z}$  vagy  $\log z$ . Minden nonszinguláris kúpszelet konformekvivalens  $\mathbb{P}^1\mathbb{C}$ -vel.

Hesse-mátrix a második deriváltakból; inflexió pont, ha ez elfajul. Pascal misztikus hatszög tétele a kúpszeletekről, Cayley-Bacharach-tétel.

## Sima leképezések foka, fedések, univerzális fedő

Topologikus felületek közötti sima fedő és elágazó fedő leképezések fogalma: lokális illetve környezetenként max egy pont kivételével lokális homeomorfizmusok.

Egy sima  $f : M \rightarrow N$  leképezésnél minden  $y \in N$  reguláris értékre (azaz a Jacobi nem-elfajuló) definiálható  $\deg f(y) = \sum_{f(x)=y} \text{sign det } Df(x)$ . Sard tétele szerint m.m. pont  $N$ -en reguláris. Másik nem bizonyított tétel, hogy ez a  $\deg$  független  $y$ -tól. Harmadik, hogy  $N = S^n$  esetén az  $f$  homotópiaosztálya csak a fokától függ. Az egész ügy spec. esete a holomorf leképezések  $\mathbb{R}$ -felületek között — ott még a kritikus helyeken is tudunk fokot definiálni. Jegyezzük meg, hogy egy holomorf leképezés mindig irányítástartó: a nem kritikus  $x$  pontokban  $\det Df(x) > 0$ .

Ha nincsen kritikus hely, akkor az inverzfüggvény-tétel szerint fedőleképezésről van szó. Az általános holomorf esetben pedig elágazó fedésről.

Ha  $p : \tilde{M} \rightarrow M$  fedőleképezés, akkor minden  $\gamma : x \rightarrow y$   $M$ -beli görbe lokálisan felemelhető tetszőleges  $x$  feletti  $x^*$  pontból indulón, és az egész  $\gamma$ -nak legfeljebb egy innen induló felemeltje van. Ezentúl minden fedés reguláris legyen, azaz létezzen is mindenütt a teljes felemelés, az épeszű példák ilyenek. Monodrómia-tétel:  $x$  és  $y$  közötti homotóp görbék ugyanabba az  $x^*$ -ba való felemeltjeinek végpontjai megegyeznek, és a felemeltek is homotópok.

$D(x^*) = \{\gamma : x \rightarrow x^* \text{ görbék, amelyek felemeltje záródik } x^* \text{-ban}\}$  részcsoportja  $\pi_1(M, x)$ -nek, és különböző  $x^*$  felemeltkekhez ezek konjugált részcsoportok. Ráadásul minden  $D \leq \pi_1(M)$ -hez konstruálható  $(\tilde{M}, p)$  fedés, amely ezt a  $D$ -t adja vissza; sőt,  $\pi_1(\tilde{M}) = D$ . Kisebb részcsoporthoz erősebb fedő tartozik,  $D = \pi_1(M)$  esetén  $\tilde{M} \simeq M$ ,  $D = \{1\}$  esetén  $\tilde{M}$  az univerzális fedő, ami 1-összefüggő.

Minden  $\gamma$   $M$ -beli görbéhez természetes módon tartozik egy  $f_\gamma \in \text{Aut}(\tilde{M}, p) = \{\phi : \tilde{M} \rightarrow \tilde{M} \text{ homeomorfizmus, amire } p(x^*) = p(\phi(x^*)) \forall x^* \in \tilde{M}\}$  fedőautomorfizmus, sőt,  $\text{Aut}(\tilde{M}, p) \simeq N_{\pi_1(M)}(D)/D$ , ahol  $N_G(H)$  a normalizátort jelenti egy  $H \leq G$  részcsoportra. Ez a csoport fixpontmentesen és tranzitíven hat a fedés fibrumain, így  $\tilde{M}/\text{Aut}(\tilde{M}, p) \simeq M$ ; speciálisan az univ. fedőre  $\tilde{M}/\pi_1(M) \simeq M$ , mint pld.  $\mathbb{R}^2/\mathbb{Z}^2 \simeq \mathbb{T}^2$ .

### Riemann-felületek fedései, Riemann-Hurwitz és Riemann-Roch tétel

Ha  $M$  egy Riemann-felület vagy Riemann-sokaság, és  $(\tilde{M}, p)$  fedés, akkor létezik  $\tilde{M}$ -en pontosan egy komplex struktúra vagy Riemann-metrika, hogy a  $p$  holomorf avagy izometria legyen. Ilyenkor  $\text{Aut}(\tilde{M}, p)$  egy tetszőleges diszkrét részcsoport az  $\text{Aut}(\tilde{M})$  holomorf automorfizmusok vagy az  $\text{Isom}(\tilde{M})$  izometriák csoportjában. Itt a diszkrét részcsoport azt jelenti, hogy minden pont pályája uniforman diszkrét, beleértve a fixpontmentességet.

Nagy eredmény Koebe uniformizálási tétele: minden  $\mathbb{R}$ -felületnek az univerzális fedője konformekvivalens a  $\mathbb{C}$ , a  $\mathbb{P}^1\mathbb{C}$ , vagy a  $\mathbb{D}$  (a nyílt egységkör)  $\mathbb{R}$ -felületek egyikével. (Ennek speciális esete a konform leképezések Riemann-tétele.) Mivel túl sok diszkrét részcsoportja  $\text{Aut}(\mathbb{C})$ -nek és  $\text{Aut}\mathbb{P}^1\mathbb{C}$ -nek nincsen, majdnem minden  $\mathbb{R}$ -felületnek a  $\mathbb{D}$  az univ. fedője; az  $\text{Aut}(\mathbb{D})$  diszkrét részcsoportjait hívják Fuchs-csoportoknak. Vegyük észre még, hogy a  $\mathbb{D}$  konform-ekvivalens a felső félsíkkal, és létezik pontosan egy Riemann-metrika  $\mathbb{D}$ -n, amire minden holomorf automorfizmus távolságtartó is: a hiperbolikus metrika. Így  $\text{Aut}(\mathbb{D}) \leq \text{Isom}^+(\mathbb{H}^2) \simeq PSL(2, \mathbb{R})$ .

Alkalmas triangulációk választásával nem nehéz látni a Riemann-Hurwitz formulát: Ha  $f : R \rightarrow S$  kompakt Riemann-felületek közötti holomorf, aminek foka  $d$ , akkor

$$\chi(R) = d\chi(S) - \sum_{p \in R} (\nu_f(p) - 1).$$

Azonnali látványos következmény: ha  $C$  egy  $d$ -edfokú nemszinguláris komplex projektív görbe,  $[0 : 1 : 0] \notin C$  feltehető, akkor a  $\phi : C \rightarrow \mathbb{P}^1\mathbb{C}$ ,  $\phi[x : y : z] = [x : z]$  elágazó fedés mutatja, hogy  $\chi(C) = d(3-d)$ , avagy  $g(C) = \frac{1}{2}(d-1)(d-2)$  foksám-génusz formula.

Ha  $D$  egy kompakt  $X$   $\mathbb{R}$ -felület fölötti divizor, akkor definiáljuk az  $\mathcal{L}(D) = \{f \in \mathfrak{M}^*(X) : \text{div } f + D \geq 0\} \cup \{0\}$  komplex vektorteret. Legyen  $l(D) = \dim_{\mathbb{C}} \mathcal{L}(D)$ . Ennek meghatározása a Riemann-Roch probléma, amivel azt közelítjük meg, hogy mi is az  $\mathfrak{M}^*(X)$  csoport. Pld.  $l(0) = \dim_{\mathbb{C}} \{\text{holomorf függvények } X\text{-en}\} = 1$ , és minden  $\kappa$  kanonikus divizorra  $l(\kappa) = \dim_{\mathbb{C}} \{\text{holomorf differenciálok } X\text{-en}\}$ . Ha  $\deg D < 0$ , akkor  $l(D) = 0$ , és ha  $D \sim D'$ , akkor  $\mathcal{L}(D) \simeq \mathcal{L}(D')$ . Riemann-Roch tétel:

$$l(D) - l(\kappa - D) = \deg(D) + 1 - g(X).$$

Például  $l(\kappa) = g(X)$ . Nagyon fontos következmény, hogy egy nemszinguláris komplex projektív görbén minden meromorf függvény racionális törtfüggvény — a GAGA-elv első általunk látott tétele.

Ennek bizonyítása a RR-tétel bizonyítása szempontjából is tanulságos. Legyen  $X, L \subseteq \mathbb{P}^2\mathbb{C}$  a görbe és egy tetszőleges egyenes,  $\deg P = d$  és  $\deg R = 1$  definiáló homogén polinomokkal. Nézzük  $X$ -en a  $H = \sum_{p \in C} I_p(X, L)p$  divizort,  $\deg H = d$  Bézout tétele szerint. Ha  $m$  elég nagy, akkor  $l(\kappa - mH) = 0$ . Legyen most  $Q$  tetszőleges  $m$ -edfokú homogén polinom, és  $f = Q/R^m$ . Ekkor  $f$  egy értelmes meromorf függvény  $X$ -en, amire  $\text{div } f + mH \geq 0$ , azaz  $f \in \mathcal{L}(mH)$ . Másrészt egy  $Q$  és egy  $Q'$  ugyanazt az  $f$ -et definiálják  $X$ -en, ha  $P|(Q - Q')$ , így  $l(mH) \geq \dim(\mathbb{C}_m[x, y, z]/P(x, y, z)\mathbb{C}_{m-d}[x, y, z]) = 1/2(m+1)(m+2) - 1/2(m-d+1)(m-d+2) = md + 1 - g$  a foksám-génusz formula szerint, ahol  $\mathbb{C}_m[x, y, z]$  az  $m$ -edfokú homogén háromváltozós polinomok tere. Tehát, ha  $m$  elég nagy, akkor  $l(mH) - l(\kappa - mH) \geq \deg(mH) + 1 - g$ , viszont a RR-tétel pont egyenlőséget

mond, azaz  $\mathcal{L}(mH)$  minden függvénye ténylegesen  $Q/R^m$  alakú, azaz racionális. Hasonlóan, ha  $L_1, \dots, L_m$  egyeneseket, és a hozzájuk tartozó  $H_1, \dots, H_m$  divizorokat vesszük, akkor minden  $\mathcal{L}(H_1 + \dots + H_m)$ -beli függvény racionális. Viszont minden  $f \in \mathfrak{M}^*(X)$  függvényhez vannak  $L_1, \dots, L_m$  egyenesek, amikre  $f \in \mathcal{L}(H_1 + \dots + H_m)$ , így  $X$ -en minden meromorf függvény racionális. A Riemann-Roch tétel bizonyítása a következő három lemmán múlik: Lemma 1: Tetszőleges  $D \in \text{Div}(X)$ -re,  $L$  egyenesre, az őáltala definiált  $H$  divizorra, és  $m_0 > 0$  egészre  $\exists m \geq m_0$  és  $p_1, \dots, p_k \in X$  pontok, hogy  $D + (p_1) + \dots + (p_k) \sim mH$ . Lemma 2: Ha  $\omega$  egy meromorf differenciál  $X$ -en pontosan egy pólussal, akkor ez a pólus nem lehet egyszerűes. Lemma 3: Tetszőleges  $D \in \text{Div}(X)$  és  $p \in X$  esetén  $0 \leq l(D+p) - l(D) - l(\kappa - D - (p)) + l(\kappa - D) \leq 1$ . Ezután, hasonlóan az előző alkalmazáshoz, Lemma 1+3-ból azonnal  $l(D) - l(\kappa - D) \geq \deg D - g + 1$  adódik, amit  $D$ -re és  $\kappa - D$ -re is felírva, és használva a kiszámolható  $\deg \kappa = 2g - 2$  eredményt, adódik a RR-tétel.

### Lie-csoportok, lokálisan triviális fibrált nyalábok

Lie csoport definíciója,  $e \in G$  egységelem. Ha  $\psi_g : G \rightarrow G$  a  $g$ -vel való konjugálás, akkor az  $\text{Ad}(g) = (D\psi_g)_e : T_e G \rightarrow T_e G$  leképezéssel definiálhatjuk az  $\text{Ad} : G \rightarrow \text{Aut}(T_e G)$  csoportreprezentációt, és vehetjük ennek  $\text{ad} : T_e G \rightarrow \text{End}(T_e G)$  deriváltját az egységben. Ezzel bevezettük a  $G$  Lie-csoport  $\mathfrak{g} = T_e G$  Lie-algebráját, az  $[X, Y] = (\text{ad}X)(Y)$  Lie-zárójellel. Ebben az egészben az a pláne, hogy minden  $\varphi : G \rightarrow H$  Lie-csoport homomorfizmus egyértelműen meghatározódik a  $D\varphi : \mathfrak{g} \rightarrow \mathfrak{h}$  egységbeli deriváltja által, ami egy Lie-algebra homomorfizmus lesz, és ha  $G$  1-összefüggő, akkor egy  $\mathfrak{g} \rightarrow \mathfrak{h}$  lineáris leképezés pontosan akkor deriváltja egy csoport homomorfizmusnak, ha Lie-algebra homomorfizmus.

Egy  $F \rightarrow E \rightarrow B$  lokálisan triviális fibrált nyaláb definíciója  $B$  alaptérrel,  $E$ -ről szürjektív leképezéssel (az  $E$  a totális tér), és  $F$  fibrummal: minden  $p \in B$  pontnak van  $U$  környezete, hogy  $E|_U \simeq U \times F$ . Példák:

- $\mathbb{R}^n \rightarrow TM \rightarrow M$  érintőnyaláb. Például a  $TS^2$  nem globálisan triviális a sündisznótétel miatt.
- $[0, 1] \rightarrow \text{Möbius-szalag} \rightarrow S^1$ . Persze ez sem triviális globálisan, hisz nem homeomorf a hengerrel.
- $H \rightarrow G \rightarrow G/H$ , ahol  $H \leq G$  Lie-csoportok. Ilyenkor az  $M = G/H$  sokaságon a  $G$  tranzitíven hat  $H$  stabilizátorral —  $M$  egy homogén  $G$ -tér. Például  $SO(n-1) \rightarrow SO(n) \rightarrow S^{n-1}$ .

Egy (valós vagy komplex) vektornyaláb az egy olyan fibrált nyaláb, ahol a fibrum egy (valós vagy komplex) vektortér, és a lokális trivializálásoknál egy tetszőleges  $U_\alpha$  és  $U_\beta$  közötti áttérés egy  $\phi_{\alpha\beta} : F \rightarrow F$  vektortérizomorfizmust indukál. Persze lehet szó komplex sokaság feletti valós vektornyalábról, és valós sokaság feletti komplex vektornyalábról is. Minden komplex nyaláb egyben valós is.

A fundamentális csoport általánosításai a  $\pi_k(M)$  homotópia-csoportok. Ezek kiszámításához nagyon fontos a fibrált nyalábok egzakt homotópia sorozata:

$$\cdots \rightarrow \pi_{k+1}(B) \xrightarrow{\partial} \pi_k(F) \xrightarrow{t_*} \pi_k(E) \xrightarrow{p_*} \pi_k(B) \xrightarrow{\partial} \pi_{k-1}(F) \rightarrow \cdots$$

Nem meglepő, hogy ha  $k < n$ , akkor  $\pi_k(S^n) = 0$ , ugyanis a Sard-tétel miatt nem létezik szürjektív  $S^k \rightarrow S^n$ . A leképezések fokáról tanultak szerint szintúgy nem

meglepő, hogy  $\pi_n(S^n) = \mathbb{Z}$ . Az  $\mathbb{R} \rightarrow S^1$  fedés a monodrómia-tétel felhasználásával adja a harmadik nemmeglepő tételt, miszerint  $\pi_k(S^1) = 0$ , ha  $k > 1$ . Ezek után viszont igencsak meglepő, hogy  $\pi_3(S^2) = \mathbb{Z}$ , sőt,  $\pi_k(S^2) \neq 0$ , ha  $k \geq 2$ , viszont még csak nem is sejtik, hogy pontosan mik ezek a csoportok. A  $\pi_3(S^2) = \mathbb{Z}$  eredmény az  $S^1 \rightarrow S^3 \xrightarrow{\gamma} S^2$  Hopf-fibrációból és az egzakt homotópia sorozatból következik, ahol  $\gamma: S^3 \rightarrow S^2$  a következő:  $S^3 = \{(z, w) \in \mathbb{C}^2 : |z|^2 + |w|^2 = 1\} \simeq SU(2)$ ,  $S^2 \simeq \mathbb{P}^1\mathbb{C}$ ,  $\gamma: (z, w) \mapsto -z/\bar{w}$ . A magasabb  $\pi_k(S^n)$ -ek kiszámítására ilyen gondolatmenet nem működhet, mert csak az 1, 3, 7 és 15 dimenziós gömbfelületeken lehet Lie-csoportstruktúrát értelmezni.

### *Kommutatív algebra*

A kommutatív algebra alapfogalma a kommutatív egységelemes gyűrű; ezentúl csak ilyen gyűrűkről lesz szó. Ezek fő forrása az algebrai geometria polinomgyűrűi és az algebrai számelméletben a különféle testbővítések algebrai egészei. A  $k$  test fölötti polinomgyűrűket  $k[X_1, \dots, X_n]$ -nel jelöljük, egy  $I \triangleleft k[\underline{X}]$  ideálhoz  $V(I) = \{\underline{x} \in k^n : f(\underline{x}) = 0 \forall f \in I\}$ , és egy tetszőleges  $V \subseteq k^n$ -hez rendelt  $I(V)$  ideál hasonlóan. Egy  $V \subseteq k^n$ -re  $k[V] = k[\underline{X}]/I(V)$  a  $V$ -n értelmezett polinomok gyűrűje,  $k(V) = \text{Frac } k[V]$  pedig a  $V$ -n értelmezett racionális törtfüggvények teste.

Gyűrűk ideáljaira:  $\text{max} \Rightarrow \text{prím} \Rightarrow \text{irred}$ . Egy gyűrű integritástománya, ha a 0 ideál prím, és test, ha maximális is. Ha egy integritástományban van faktorizáció irreducibilisekre, akkor ez pontosan akkor egyértelmű, ha  $\text{irred} \Rightarrow \text{prím}$ . Ezeket hívjuk UFD-nek (unique factorization domain), vagy Gauss-gyűrűnek. Az is igaz, hogy egy gyűrű pontosan akkor UFD, ha minden szigorúan növvő főideállánc véges. Minden gyűrűben van maximális ideál. A Noether-gyűrűk három ekvív. defje: minden ideál végesen generált; minden szigorúan növvő ideállánc véges; ideálok nemüres rendszere tartalmaz maximális elemet. Egy modulus Noether-modulus, ha a részmodulusaira teljesülnek a fentiek. Egy Noether gyűrű feletti modulus pontosan akkor Noether-féle, ha végesen generált.

Hilbert bázis tétel: ha  $A$  egy Noether-gyűrű, akkor az  $A[X]$  polinomgyűrű is az. Gauss-tétel: Ha  $A$  egy UFD, akkor  $A[X]$  is az. Egy következmény: ha  $k$  végtelen test,  $0 \neq f \in k[X_1, \dots, X_n]$ , akkor  $\exists c_1, \dots, c_n \in k$ , amelyekre  $f(c_1, \dots, c_n) \neq 0$ . Cayley-Hamilton-tétel, Nakayama-lemma. Ha  $A \subseteq B$  gyűrűk, akkor tetszőleges  $x \in B$ -re az  $A[x]$  modulus pontosan akkor végesen generált  $A$  fölött, ha  $x$  egy algebrai egész  $A$ -ban. Egy  $A$  gyűrűt normálisnak hívunk, ha rajta kívül nincsen algebrai egész  $\text{Frac } A$ -ban.

Általában egy gyűrű  $\dim A$ -val jelölt Krull-dimeziója a szigorúan növvő  $P_0 \subset P_1 \subset \dots \subset P_d$  prímeideálláncok  $d$  hosszának szuprémuma. Vannak végtelen dimeziós Noether-gyűrűk is, ezek eléggé aberráltak, viszont a lokális gyűrűk már mind véges dimeziósak, ld. később. Az  $A$  egy Dedekind-gyűrű, ha Noether-féle normális integritástománya, amire  $\dim A \leq 1$ . Például minden  $[\mathbb{K} : \mathbb{Q}] < \infty$  algebrai test algebrai egészeinek  $\mathcal{O}_{\mathbb{K}}$  gyűrűje Dedekind-féle. A Dedekind-gyűrűk egyben UFD-k is. Egy Dedekind-féle  $A$ -ra a  $\text{Frac } A$ -beli végesen generált  $A$ -modulusokat törtideáloknak hívjuk, és egy csoportot alkotnak, ami izomorf az  $A$  prímeideáljai által generált szabad Abel-csoporttal; ezt a csoportot hívjuk  $\text{Div } A$ -nak. Az egyetlen elem által generált törtideálok (principális divizorok) alkotják a  $\text{Pr } A$  részcsoportot, és a  $\text{Cl } A = \text{Div } A / \text{Pr } A$  faktort hívják ideal class groupnak. Alaptétel az algebrai számelméletben, hogy az  $A = \mathcal{O}_{\mathbb{K}}$  gyűrűkre ez a csoport véges.

Egy tetszőleges  $A$  gyűrűben vegyünk egy  $S \subseteq A$  részhalmazt, ami tartalmazza az egységelemet és zárt a szorzásra; pld.  $S = \{1, s, s^2, \dots\}$  vagy  $S = A \setminus P$ , ahol  $P$  príms. Legyen  $S^{-1}A = (S \times A) / \sim$ , ahol  $(s, a) \sim (s', a')$  hha  $\exists s'' \in S$ , amire  $s''(sa' - s'a) = 0$ . Ez így egy  $A$  fölötti algebra, ami Noether-féle, ha  $A$  is az volt, és aminek minden ideálja  $S^{-1}I$ ,  $I \triangleleft A$  alakú. Egy adott ideálhoz ez az  $I$  általában nem egyértelmű, viszont  $S^{-1}A$  prímeideáljai egyértelműen megfelelnek az  $S$ -től diszjunkt  $A$ -beli prímeideáloknak. Lokalizáció egy  $P \triangleleft A$  prímnél:  $A_P := (A \setminus P)^{-1}A$ . Az  $A_P$  gyűrűnek van egy legnagyobb ideálja:  $P_P$ . Általában egy egyetlen maximális  $m$  ideállal rendelkező Noether-gyűrűt hívunk  $(A, m)$  lokális gyűrűnek. Az  $A_P/P_P$  test megegyezik  $\text{Frac}(A/P)$ -vel. Meg kell még említeni a diszkrét értékelési gyűrűket (DVR).  $v: \mathbb{K} \rightarrow \mathbb{Z} \cup \{\infty\}$ , értékelés:  $v(x) = \infty$  hha  $x = 0$ ,  $v(xy) = v(x) + v(y)$ ,  $v(x+y) \geq \min\{v(x), v(y)\}$ , ha egyik sem 0. Ehhez  $\mathcal{O}_v = \{x \in \mathbb{K} : v(x) \geq 0\}$  gyűrű, ez a DVR, aminek egyetlen maximális ideálja az  $m_v = \{x \in \mathbb{K} : v(x) > 0\}$ .

Egy összefoglaló ábra a megfordítások lehetetlenségét mutató példákkal:

test  $\implies$  DVR  $\implies$  főideálgyűrű  $\implies$  Dedekind  $\implies$  UFD  $\implies$  normális

$$\begin{array}{cccccc} \mathbb{Z}_p, \mathbb{Z}[x] & \mathbb{Z}, k[X] & \mathcal{O}_{\mathbb{Q}(\sqrt{15})} & k[X, Y], \mathbb{Z}[X, Y] & \mathbb{Z}[e^{2\pi i/23}], \\ & & & & \frac{k[X, Y, Z]}{(X^2 - YZ)} \end{array}$$

Noether normalizációs lemma (NNL): Ha  $k$  végtelen test,  $A = k[a_1, \dots, a_n]$  egy végesen generált  $k$ -algebra, akkor  $\exists m \leq n$ ,  $y_1, \dots, y_m \in A$  algebrailag  $k$ -független elemek, hogy  $A$  egy véges modulus  $k[y_1, \dots, y_m]$  fölött. Természetesen  $\text{tr deg}[\text{Frac } A : k] = m$ . Az indukciós bizonyításhoz a kulcs lépés a következő lemma: ha  $A = k[a_1, \dots, a_n] = k[X_1, \dots, X_n]/I$ ,  $0 \neq f \in I$ , akkor  $\exists \alpha_1, \dots, \alpha_{n-1} \in k$ , hogy  $f(X'_1 + \alpha_1 X_n, \dots, X'_{n-1} + \alpha_{n-1} X_n, X_n) \in k[X'_1, \dots, X'_{n-1}, X_n]$  főgyűrűtthatója  $X_n$ -ben egy. Ez ugye geometriailag egy  $\pi_1: k^n \rightarrow k^{n-1}$ ,  $X'_i = X_i - \alpha_i X_n$  vetítést jelent, és az, hogy az  $f$  főgyűrűtthatója  $X_n$ -ben egy lesz, ekvivalens azazal, hogy  $\pi_1$  vetítés irányában nincsen az  $f = 0$  görbéhez aszimptota, azaz a projektív lezártnak nincs ebben az irányban pontja. Ráadásul a  $\pi_1, \dots, \pi_{n-m}$  vetítéssorozat végeredményeként kapott  $\pi: k^n \supseteq V(I) \rightarrow k^m$  vetítéshez tartozó  $\pi^*: k[y_1, \dots, y_m] \simeq k[Y_1, \dots, Y_m] \rightarrow k[V(I)] = A$  moduluskiterjesztés végessége azt jelenti, hogy a  $\pi$  vetítés fibrumai végesek. Sőt, a Hilbert Nullstellensatzból a  $k = \bar{k}$  esetre az is fog következni, hogy a fibrumok mind nemüresek, így összesítve a geometriai jelentés a következő: ha egy  $I \triangleleft k[X_1, \dots, X_n]$  ideál által definiált  $V = V(I)$  algebrai ponthalmazra  $\text{tr deg}[k(V) : k] = m$ , akkor létezik egy  $\pi: k^n \rightarrow k^m$  lineáris vetítés, hogy a  $\pi|_V$  megszorítás szürjektív, véges fibrumokkal. Ez alapján természetes a  $\dim V = \text{tr deg}[k(V) : k]$  definíció.

Egy  $m \triangleleft k[\underline{X}]$  maximális ideálra a 33. feladat felhasználása a NNL-ban azt adja, hogy a  $k[y_1, \dots, y_m]$  algebra egy test, azaz  $m = 0$ . Így a  $k[\underline{X}]/m$  egy véges fokú testbővítése  $k$ -nak, és ha feltesszük a  $k = \bar{k}$  algebrai zártságot, akkor  $k[\underline{X}]/m = k$  lehet csak, ahonnan  $m = (X_1 - \alpha_1, \dots, X_n - \alpha_n)$  adódik valamely  $\alpha_i \in k$  számokkal. Tehát a  $k[\underline{X}]$  maximális ideáljai és a  $k^n$  pontjai kölcsönösen egyértelműen megfelelnek egymásnak. Ez a Hilbert Nullstellensatz (HNS) gyenge formája. Általában egy tetszőleges  $I$  ideálhoz tartozó  $V(I)$  ponthalmazra vagyunk kíváncsiak. Defináljuk a  $\sqrt{I}$  radikálideált  $\sqrt{I}/I = \text{nil}(A/I)$ -vel, persze  $\sqrt{I} \supseteq I$ , és  $V(\sqrt{I}) = V(I)$ , emiatt nekünk ezek a radikálok az érdekesek. (Hasonló fogalom még a következő:  $I$

primér, ha  $xy \in I$  esetén  $x$  vagy  $y$  valamely hatványa benne van  $I$ -ben.) A 38. feladat szerint  $\text{nil } A = \bigcap_P \text{prím } P$ . Nos, egy  $k$  végtelen test fölötti  $k[\underline{X}]$  gyűrűben ennél több is igaz:  $\sqrt{I} = \bigcap_{m \supseteq I} \text{max } m$ . Ebből  $k = \bar{k}$  esetén már következik, hogy  $I(V(I)) = \sqrt{I}$ , ez az erős HNS. Egy egyszerű következmény például, hogy közös gyök nélküli polinomok együtt a teljes polinomgyűrűt generálják.

A fentiek alapján bevezetjük  $k^n$ -en a Zariski-topológiát: egy ponthalmaz zárt, ha létezik  $I \triangleleft k[\underline{X}]$  ideál, amire ő  $V(I)$ -vel egyenlő. Irreducibilis, ha nem bomlik fel határozottan kisebb zárt halmazok uniójára. (Affin) algebrai varietásnak hívjuk a  $k^n$  Zariski-zárt irreducibilis ponthalmazait. A HNS szerint a zárt halmazok kölcsönösen egyértelműen megfelelnek a  $\sqrt{I}$  alakú radikálideáloknak, továbbá  $V(I \cap J) = V(I) \cup V(J)$  miatt az algebrai varietások pontosan a prímeáloknak. Projektív algebrai varietásnak hívjuk az affin varietások  $\mathbb{P}^n k$ -beli (az ereti topológia szerinti) lezártjait, ezek pontosan a homogén prímeálokhhoz tartoznak. Egy  $V \subseteq \mathbb{P}^n k$  projektív varietás fölé vehetjük a  $\hat{V} \subseteq k^{n+1}$  kúpot, ami egy affin varietás;  $k[V] = k[\hat{V}]$  és  $k(V) = k(V \cap k^n)$ . Mostantól legyen mindig  $k = \bar{k}$ .

Jogosnak tűnik, hogy egy  $V$  algebrai varietás dimenziója legyen a leghosszabb szigorúan növvő részvarietás-láncának hossza, ami pont a  $\dim k[V]$  Krull-dimenzió. Hogy ez megegyezik a trdeg-es  $\dim V$  definícióval, az messze nem triviális, de igaz. Először is, kell a kommutatív algebra dimenzióképlete: minden  $(A, m)$  lokális gyűrűben a 41. feladat  $r(A)$  értéke megegyezik  $\dim A$ -val. A lokális gyűrűk ott jönnek elő, hogy egy  $V$  algebrai varietás tetszőleges  $p$  pontjára vehetjük az  $m_p = \{f \in k[V] : f(p) = 0\}$  maximális ideálját  $k[V]$ -nek, majd az emeleti  $\mathcal{O}_{V,p} = k[V]_{m_p}$  lokalizáltat, vagy általánosabban a  $\mathcal{O}_V(U) = \bigcap_{p \in U} \mathcal{O}_{V,p}$  gyűrűket, amik a  $V$  varietáson lokálisan (valamely  $U$ -n) értelmezett racionális törtfüggvények gyűrűi, és amúgy egy kévét alkotnak  $V$ -n,  $\mathcal{O}_{V,p}$  kocsányokkal (ld. később). Ezek a  $\mathcal{O}_{V,p}$ -k a nekünk kellő lokális gyűrűk: az 51. feladat állítása, hogy  $\dim V = \dim \mathcal{O}_{V,p}$ , minden  $p \in V$ -re. Tehát a  $k[V]$  gyűrű minden maximális ideáljának megegyezik a Krull-dimenziója, ahonnan a 38. feladat (c) része szerint  $\dim V = \dim k[V]$ .

Ha  $I = (f_1, \dots, f_r)$ , akkor a  $V = V(I)$  varietás sima egy  $p \in V$  pontjában, ha a  $(\partial f_i / \partial x_j)_{i=1, \dots, r; j=1, \dots, n}(p)$  mátrix maximális rangú; ez a maximális rang a NNL-ből és talán az inverz függvénytételből következőleg  $n - \dim V$ . Nos, egy számunkra kifejezetten nehéz tétel szerint a  $p$  pontban a  $V$  pontosan akkor sima, ha az  $\mathcal{O}_{V,p}$  gyűrű reguláris, azaz  $\dim \mathcal{O}_{V,p} = \dim_k (m_p / m_p^2)$  — most már érthető a 41. feladat definíciója.

Végül meg kell említenünk két fontos fogalmat, amelyek sajnos sokszor eléggé visszataszító formalizmusokkal terhelik az algebrai geometriát. Egy  $X$  topológikus téren halmazok, Abel-csoportok, vagy leginkább gyűrűk  $\mathcal{F}$  előkéveje (presheaf) a következőkből áll: minden  $U \subseteq X$  nyílt halmazra egy  $\mathcal{F}(U)$  struktúra (halmaz, csoport, vagy gyűrű),  $\mathcal{F}(\emptyset) = \{0\}$ , és minden  $V \subseteq U$  nyíltakra egy  $\rho_{UV} : \mathcal{F}(U) \rightarrow \mathcal{F}(V)$  megszorítási homomorfizmus, amelyek tetszőleges  $W \subseteq V \subseteq U$ -ra kommutálnak. Egy előkéve kéve (sheaf) is, ha pluszban teljesíti a szétválasztási és összeragasztási axiómákat is: ha  $U = \bigcup_i V_i$ ,  $s \in \mathcal{F}(U)$ ,  $\forall i \ s|_{V_i} = 0$ , akkor  $s = 0$  is igaz; ha  $U = \bigcup_i V_i$ ,  $s_i \in \mathcal{F}(V_i)$ ,  $\forall i, j \ s_i|_{V_i \cap V_j} = s_j|_{V_i \cap V_j}$ , akkor  $\exists s \in \mathcal{F}(U)$ , amire  $\forall i \ s|_{V_i} = s_i$ . Például egy sima sokaságon az  $\mathcal{F}(U) = \{f : U \rightarrow \mathbb{R} \text{ sima}\}$  egy kéve, egy tetszőleges  $X$ -en az  $\mathcal{F}(U) = \mathbb{Z}$ ,  $\rho_{UV} = \text{Id}$  csak egy előkéve. Minden kévéhez definiálhatjuk az  $\mathcal{F}_p$ ,  $p \in X$  kocsányokat (stalk):  $(U, s)$ ,  $s \in \mathcal{F}(U)$ ,  $p \in U$  párok ekvivalenciaosztályai, ahol  $(U, s) \sim (V, t)$  hha  $s|_{U \cap V} = t|_{U \cap V}$ . Egy

komplex sokaság különféle függvénykévéiből kiváló kohomológiaelméleteket lehet gyártani, pld. J.P. Serre, a legáltalánosabb GAGA-elv bizonyítója csinált ilyeneket. A másik megemlítendő dolog, hogy tetszőleges  $A$  gyűrűhöz lehet venni az  $X = \text{Spec}(A) = \{A \text{ prímeideáljai}\}$  halmazt, és ezen egy Zariski-topológiát:  $V \subseteq X$  zárt, ha valamilyen  $I \triangleleft A$  ideálra  $V = V(I) = \{P \in X : P \supseteq I\}$ . Azt mondhatjuk, hogy az  $A$  elemei a függvények, és  $f(P) = 0$ , hha  $f \in P$ . Ezalapján  $I(V) = \bigcap_{P \in V} P$ . Ha csak lokálisan értelmezett függvényeket is akarunk, akkor legyen  $k(X) = \text{Frac}(A)$ , és vegyük a következő kévét:  $\mathcal{O}_{X,P} = A_P$  lokalizáltak,  $\mathcal{O}_X(U) = \bigcap_{P \in U} A_P$ ,  $\mathcal{O}_X(X) = A$ . Ekkor a függvények kiértékelése úgy történik, hogy  $f \in \mathcal{O}_{X,P}$ -re  $f(P) = f \bmod P_P \in \text{Frac}(A/P) = A_P/P_P$ . Persze  $A = k[V]$ -re  $\text{Spec}(A) \simeq V$  a Zariski-topológiában.

### *Elliptikus görbék és moduláris formák*

Láttuk, hogy minden nemszinguláris másodfokú komplex görbe konform ekvivalens a  $\mathbb{P}^1\mathbb{C}$  Riemann-gömbbel, továbbá minden nemszinguláris harmadfokú görbe (ezek az elliptikus görbék)  $y^2z = x(x-z)(x-\lambda z)$ ,  $\lambda \notin \{0,1\}$ , alakra hozható, és a foksám-génusz formula szerint homeomorf egy tóruszal. Komplex tóruszokat  $\mathbb{C}/\Lambda$  módon gyárthatunk, ahol  $\Lambda = \mathbb{Z}\omega_1 + \mathbb{Z}\omega_2$  rács, az  $\omega_i$ -k lineárisan  $\mathbb{R}$ -független komplex számok. Természetes kérdés, hogy a fenti kétfajta előállítás mikor adja ugyanazt a Riemann-felületet. Ehhez először megnézzük az összes különféle rács által definiált tóruszok terét. Majd azt, hogy egy rácsból hogyan kaphatunk elliptikus görbét, és, hogy egy elliptikus görbéhez hogyan definiálható természetes módon egy megfelelő rács — a két eljárás persze egymás inverze lesz. Ezután learatunk néhány gyümölcsöt.

Tetszőleges  $\Lambda \subseteq \mathbb{C}$  rács hasonló egy  $\Lambda_\tau = \langle 1, \tau \rangle$ ,  $\tau \in \mathbb{H}$ , rácshoz, ahol  $\mathbb{H} = \{z \in \mathbb{C} : \Im z > 0\}$  a felső félsík. Így van egy  $\mathbb{H} \rightarrow \mathcal{L}/\mathbb{C}^*$  folytonos szürjektív leképezésünk, ahol  $\mathcal{L}$  az összes rácsok halmaza a természetes topológiával. Másrészt  $\mathbb{Z}\omega_1 + \mathbb{Z}\omega_2 = \mathbb{Z}\omega'_1 + \mathbb{Z}\omega'_2$  pontosan akkor, ha  $\underline{\omega}' = \gamma \underline{\omega}$ , ahol  $\gamma \in \Gamma = PSL(2, \mathbb{Z})$  a moduláris csoport. Sőt, a  $\Gamma$  moduláris csoport a Möbius-transzformációkkal hat  $\mathbb{H}$ -n, és  $\Lambda_{\tau_1} \sim \Lambda_{\tau_2}$  pontosan akkor, ha  $\tau_2 = \gamma \tau_1$ ,  $\gamma \in \Gamma$ -ra. Így tehát  $\mathbb{H}/\Gamma \simeq \mathcal{L}/\mathbb{C}^*$  homeomorfizmus. Ez nekünk amiatt érdekes, hogy könnyű látni, hogy minden  $\phi : \mathbb{C}/\Lambda \rightarrow \mathbb{C}/\Lambda'$  holomorf leképezés  $\phi(z) = \alpha z + \beta$ ,  $\alpha\Lambda \subseteq \Lambda'$  alakú, így egy tóruszok közötti  $\phi(0) = 0$  pluszfeltételű holomorf izomorfizmus mindig  $\phi(z) = \alpha z$ ,  $\alpha \in \mathbb{C}^*$ ,  $\alpha\Lambda = \Lambda'$  csoportizomorfizmus is, és így a komplex tóruszok tere a holomorf izomorfizmusok szerint faktorizálva pont  $\mathcal{L}/\mathbb{C}^*$ . Emiatt biztosan érdekes nekünk a  $\Gamma$  hatása  $\mathbb{H}$ -n. A fentiekből egyébként az is következik, hogy  $\text{End}(\mathbb{C}/\Lambda) = \mathbb{Z}$  vagy pedig egy szép  $R$  részgyűrűje egy  $\mathbb{Q}(\sqrt{D})$ ,  $D < 0$  testnek. Például, ha  $A\tau^2 + B\tau + C = 0$ , akkor  $\text{End}(\mathbb{C}/\Lambda_\tau) = \mathbb{Z} + \mathbb{Z}A\tau$ .

Nos, a  $\Gamma = \langle S, T \rangle$ ,  $S\tau = -1/\tau$ ,  $T\tau = \tau + 1$ , csoport diszkréten, de nem fix-pontesen hat  $\mathbb{H}$ -n, fundamentális tartománya egy hiperbolikus ideális háromszög  $\rho = e^{2\pi i/3}$ ,  $\rho + 1$ ,  $\infty$  csúcsokkal, a stabilizátorok pedig  $\Gamma_\rho = \langle ST \rangle \simeq \mathbb{Z}_3$ ,  $\Gamma_{\rho+1} = \langle TS \rangle \simeq \mathbb{Z}_3$ ,  $\Gamma_i = \langle S \rangle \simeq \mathbb{Z}_2$ , más pontokra triviális. Egyébként  $\Gamma \simeq \mathbb{Z}_2 * \mathbb{Z}_3$  szabad szorzat. Ezek után nem nehéz megkonstruálni az  $X(\Gamma) = \overline{\mathbb{H}/\Gamma}$  Riemann-felületet, ami a fenti leírásból láthatóan egy gömbbel homoemorf. A  $\mathbb{H}$ -n holomorf,  $\Gamma$ -ra nézve szépen viselkedő függvényeket hívják moduláris formáknak; ezek központi szerepet játszanak a modern számelméletben, pld. a Nagy Fermat Tétel bizonyításában és a Riemann-sejtésben is.

Egy  $\Lambda$ , vagy speciálisan  $\Lambda_\tau$  rácshoz definiálhatóak a

$$G_k(\tau) = G_k(\Lambda_\tau) = \sum_{\lambda \in \Lambda_\tau - (0,0)} \frac{1}{\lambda^{2k}} = \sum_{(m,n) \neq (0,0)} \frac{1}{(m\tau + n)^{2k}}$$

Eisenstein-sorok, továbbá a Weierstrass-féle

$$\wp(z) = \frac{1}{z^2} + \sum_{k=1}^{\infty} (2k+1)G_{k+1}z^{2k} = 1/z^2 + \sum_{\lambda \in \Lambda \setminus \{0\}} \left( \frac{1}{(z-\lambda)^2} - \frac{1}{\lambda^2} \right)$$

$\Lambda$ -periodikus meromorf függvény. Nem nehéz bizonyítani a

$$\wp'(z)^2 = 4\wp(z)^3 - g_2\wp(z) - g_3$$

összefüggést, ahol  $g_2 = 60G_3$  és  $g_3 = 140G_3$ , így lehet egy  $E_\tau = \{[\wp(z) : \wp'(z) : 1] : z \notin \Lambda\} \cup \{[0 : 1 : 0]\}$  elliptikus görbét csinálni, ráadásul  $E_\tau \simeq \mathbb{C}/\Lambda_\tau$  holomorf izomorfizmus ezzel a Weierstrass-paraméterezéssel. Ez az  $E_\tau$  görbe pont azért nem szinguláris, mert a  $\Delta(\tau) = g_2(\tau)^3 - 27g_3(\tau)^2$  diszkriminánsa a Weierstrass-egyenletnek soha sem nulla, csak  $\tau = \infty$ -re.

Visszafelé, ha adott egy  $E = \{y^2 = x(x-1)(x-\lambda)\}$  elliptikus görbénk, akkor az

$$x \mapsto \phi(x) = \int_1^x \frac{1}{\sqrt{\xi(\xi-1)(\xi-\lambda)}} d\xi \in \mathbb{C}/\Lambda$$

Abel-Jacobi leképezés egy értelmes integrált definiál modulo egy  $\Lambda$  rác, amelynek két generátora  $\omega_i = \int_{\gamma_i} \omega$ , ahol  $\omega$  a fent is integrált holomorf differenciál, a  $\gamma_i$ -k pedig a  $H_1(E, \mathbb{Z})$  csoport két generátorgörbéje — Stokes tétele miatt egy zárt görbén való integrál valóban csak a homotópiaosztálytól függ, így tényleg mod  $\Lambda$  kapjuk az integrálunkat. Ráadásul az  $\omega_i$ -k lineárisan  $\mathbb{R}$ -függetlenek (pont az  $E$  nem-szingulárisága miatt), és a  $\phi$  egy konformekvivalencia, ami pont a Weierstrass-leképezés inverze. Ez a dolog arra is jó, hogy így a Weierstrass-paraméterezéssel csúnya elliptikus integrálokat is ki tudunk számolni, mint amilyen pld. az  $x^2/a^2 + y^2/b^2 = 1$  ellipszis ívhossza az  $x = c$  és  $x = d$  pontok között:

$$\frac{1}{a} \int_c^d \frac{a^4 + (b^2 - a^2)x^2}{\sqrt{(a^2 - x^2)(a^4 + (b^2 - a^2)x^2)}} dx.$$

Mivel  $\mathbb{C}/\Lambda$  egy Abel-féle faktorcsoporthoz tartozó csoport, minden elliptikus görbén van egy összeadásunk, amit  $\boxplus$ -gel jelölünk; ennek egységeleme a  $\Lambda$ -pontoknak megfelelő végtelen távoli  $O$  pontja az  $E$ -nek. Ezt geometriailag a jól ismert misztikus módon lehet leírni: három pont összege pontosan akkor  $O$ , ha egy egyenesen vannak (ne feledjük, egy komplex egyenesnek és egy elliptikus görbének multiplicitással pontosan három metszéspontja van) — ezt később bizonyítjuk. Nem túl nehéz a GAGA-elvnek megfelelő  $\mathfrak{M}(\mathbb{C}/\Lambda) = \mathbb{C}(\wp(z), \wp'(z))$  állítás, amiből persze nem világos még, hogy mekkora is pontosan az  $\mathfrak{M}(\mathbb{C}/\Lambda)$  gyűrű. A Riemann-Roch-tételből adódik, hogy  $\deg D = d > 0$ -ra  $l(D) = d$ . Így például nem meglepő, hogy az  $\mathcal{L}(6 \cdot (0))$ -ban lévő 7 db  $1, \wp, \wp', \wp^2, \wp\wp', \wp'^2, \wp^3$  elem között van lineáris összefüggés: a Weierstrass-egyenlet.

A Cauchy reziduuum-tételből nem nehéz, hogy  $\sum_{x \in E} \text{ord}_x(f)x = 0$ . Tehát  $P(E) \subseteq \ker(\text{deg}) \cap \ker(\boxplus)$ . Állítjuk, hogy egyenlőség is fennáll. Ebből következőleg a

$$0 \longrightarrow \mathbb{C}^* \longrightarrow \mathfrak{M}(E)^* \xrightarrow{\text{div}} \text{Div}^0(E) \xrightarrow{\boxplus} E \longrightarrow 0$$

sorozat egzakt, ahonnan  $\text{Pic}^0(E) \simeq (E, \boxplus)$ . A fenti állítás bizonyításához kellenek a  $\theta$  függvények.

Feladatunk az, hogy tetszőleges  $D = \sum_j ((P_j) - (Q_j))$ ,  $\boxplus_j (P_j - Q_j) = 0$  divizorhoz csináljunk egy  $f \in \mathfrak{M}(E)$  függvényt, melyre  $\text{div} f = D$ . Ehhez először minden  $\tau \in \mathbb{H}$ -hoz keressünk egy az egész  $\mathbb{C}$ -n holomorf  $\theta$  függvényt  $\theta(z+1) = \theta(z)$  és  $\theta(z+\tau) = e^{-\pi i(2z+\tau)}\theta(z)$  tulajdonságokkal. Nem nehéz kiszámolni, hogy ez csak

$$\theta(z) = \sum_{n \in \mathbb{Z}} e^{\pi i n^2 \tau + 2\pi i n z}$$

lehet. Ennek egyszeres gyökei vannak az  $(1+\tau)/2 + \Lambda_\tau$  pontokban, máshol nincs. Így hát ha a  $P_j, Q_j \in E$  pontok fölött választunk úgy  $a_j, b_j \in \mathbb{C}$  pontokat, hogy  $\sum_j (a_j - b_j) = 0$ , akkor az  $f(z) = \prod_j \frac{\theta(z - a_j + (\tau+1)/2)}{\theta(z - b_j + (\tau+1)/2)}$  függvény azt fogja tudni,  $f(z+1) = f(z)$ ,  $f(z+\tau) = f(z)e^{-2\pi i(\sum_j -a_j + b_j)} = f(z)$ , tehát  $f \in \mathfrak{M}(E)$  valóban, és  $\text{div} f = D$ .

A  $\text{Pic}^0(E) \simeq (E, \boxplus)$  izomorfiából következőleg  $\boxplus_{j=1}^n P_j = \boxplus_{j=1}^n Q_j$  pontosan akkor, ha  $\exists f \in \mathfrak{M}(E)$  úgy, hogy  $\text{div} f = \sum_j ((P_j) - (Q_j))$ . Így ha veszünk egy  $l \subseteq \mathbb{P}^2\mathbb{C}$  egyenest, a nem feltétlenül különböző  $\{P_1, P_2, P_3\} = E \cap l$  metszéspontokkal, akkor az  $l$ -et definiáló  $f$  lineáris polinomot  $\mathfrak{M}(E)$ -beliként értve  $\text{div} f = (P_1) + (P_2) + (P_3) - 3(O)$ , és így három  $E$ -beli pont  $\boxplus$ -összege pontosan akkor  $O$ , ha egy egyenesen vannak. Így igazoltuk az  $\boxplus$  összeadás geometriai jelentését! Egyébként az összeadást le lehet írni az  $E$ -t megadó egyenlet együtthatóiból álló nagyon ronda formulák segítségével is, ez lehetőséget ad arra, tetszőleges  $k$  test fölötti elliptikus görbén értelmezzünk összeadást. Tetszőleges test fölött pld. a nem-szingularitási feltételt is lehet úgy mondani, hogy ha a harmadfokú görbénket az  $y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$  alakra hozzuk (ez megtehető), akkor a  $\Delta(a_1, \dots, a_6)$  diszkrimináns nem 0; a pontos ötváltozós hetedfokú polinomot nincs szívem leírni. Továbbá minden algebrailag zárt test fölött megvannak a Riemann-Roch és Cayley-Bacharach tételek, így a többi lehetőséget most is ki lehet használni az összeadás definiálására.

Egy  $\phi : C \longrightarrow D$  racionális leképezés szeparábilis, ha a  $k(C)/f^*k(D)$  testbővítés szeparábilis, azaz a testbővítés minden elemének minimálpolinomjának csak különböző gyökei vannak. Ilyen esetekben a Galois-elmélet különösen jól működik, ezért fontosak ezek. Általában is igaz, hogy  $\text{deg} f = [k(C) : f^*k(D)] < \infty$ , és ez megegyezik a Riemann-felületek közötti holomorf leképezések  $\text{deg}$  definíciójával. Az elliptikus görbéket illetően nagyon fontos, hogy ha  $E$  egy projektív elliptikus görbe  $k = \mathbb{F}_q$  fölött, akkor a  $\phi : E(\bar{k}) \longrightarrow E(\bar{k})$ ,  $(x, y) \mapsto (x^q, y^q)$  Frobenius-leképezés tisztán inszeparábilis,  $\text{deg} \phi = q$ ,  $1 - \phi$  szeparábilis, így  $\text{deg}(1 - \phi) = |\ker(1 - \phi)|$ , továbbá fixpontjai pontosan az  $E(k)$  pontok, így  $\text{deg}(1 - \phi) = |E(k)|$ . Ezután használva, hogy a  $\text{deg}$  leképezés egy pozitív definit kvadratikusan forma  $\text{End}(E(\bar{k}))$ -n, a Cauchy-Schwarz egy változatából könnyen kijön már Hasse tétele: triviális ugye, hogy legfeljebb  $2q + 1$  pont van  $E(k)$ -n, a tétel pedig az, hogy  $|E(k) - q - 1| < 2\sqrt{q}$ . Ebből

például következik az is, hogy ha  $q$  páratlan, akkor egy harmadfokú görbe képén a négyzet és nemnégyzet testelemek számának különbsége legfeljebb  $2\sqrt{q}$ . Aki ismeri a Riemann-sejtés négyzetmentes számokról szóló változatát, az már most tűzbe jöhet, de előbb inkább egy definíció jön. Legyen  $A = \mathbb{Z}[X_1, \dots, X_n]/(f_1, \dots, f_m)$  gyűrű,  $m \triangleleft A$  maximális, ekkor  $A/m$  egy véges test, ennek elemszáma legyen  $N(m)$ . Az  $A$ -hoz tartozó zeta-függvény pedig

$$\zeta(A, s) = \prod_{m \triangleleft A} \max \left( 1 - \frac{1}{N(m)^s} \right)^{-1}.$$

Pld.  $\zeta(\mathbb{Z}, s) = \zeta(s)$  szokásos. Ugyanígy végesek az  $N(m)$ -ek, ha  $A = k[V]$ , ahol a  $V$  egy  $k$  feletti nemszinguláris projektív varietás,  $k = \mathbb{F}_q$ ,  $k_n = \mathbb{F}_{q^n}$ , ekkor is lehet az előző definíció. Egy másik, hogy

$$Z(V(k), T) = \exp \left( \sum_{n=1}^{\infty} |V(k_n)| \frac{T^n}{n} \right); \quad \zeta(V(k), s) = Z(V(k), q^{-s}).$$

Alighanem  $\zeta(k(V), s) = \zeta(V(k), s)$ . André Weil sejtései, melyek bizonyításáért Deligne Fields-medált kapott, azt mondják, hogy

- Racionalitás.  $Z(V(k), T) \in \mathbb{Q}(T)$ .
- Függvényegyenlet.  $Z(V(k), 1/q^n T) = \pm q^{n\chi(V)/2} T^{\chi(V)} Z(V(k), T)$ .
- Riemann-hipotézis.  $Z(V(k), T) = \frac{P_1(T) \cdots P_{2n-1}(T)}{P_0(T) \cdots P_{2n}(T)}$ , ahol  $P_0(T) = 1 - T$ ,  $P_{2n}(T) = 1 - q^n T$ , különben pedig  $P_i(T) = \prod_j (1 - \alpha_{ij} T)$ ,  $|\alpha_{ij}| = q^{i/2}$ .

Elliptikus görbékre ezt már Weil is bizonyította, benne van a Silvermanban is, és azt adja, hogy

$$\zeta(E(k), s) = \frac{1 - aq^{-s} + q^{1-2s}}{(1 - q^{-s})(1 - q^{1-s})},$$

egy  $k$ -től függő  $a \in \mathbb{Z}$ -vel. Ebből most következik, hogy ha  $\zeta(E(k), s) = 0$ , akkor  $|q^s| = \sqrt{q}$ , és így  $\Re(s) = 1/2$ . Ezt egyébként a Hasse-tételből közvetlen számolással is ki lehet hozni.

A véges testekre vonatkozó eredmények igen fontosak  $\mathbb{Q}$  és  $\mathbb{C}$  fölött is, ugyanis nem csak az igaz, mondjuk, hogy ha egy egyenletnek van egész megoldása, akkor van mod  $p$  is, hanem nagyon sokszor fordítva is: ha minden  $p$ -re van megoldás mod  $p$ , akkor rendes megoldás is van. (Ezt hívják Hasse-elvnek.) Ezt is használják a témakör fő eredményei: illik tudni a Mordell-Weil-tételről, mely szerint  $(E(\mathbb{Q}), \boxplus)$  végesen generált, Siegel tételéről, mely szerint  $E(\mathbb{Z})$  véges, Faltings tételéről, miszerint egy egynél nagyobb génuszú varietás racionális pontjai véges sokan vannak, és a Wiles bizonyította Nagy Fermat Tételről.

Végül pedig a moduláris formák: a moduláris csoport egy  $[\Gamma : G] < \infty$  részcsoporthoz tartozó  $f : \mathbb{H} \rightarrow \mathbb{C}$  holomorf függvény egy  $2k$  súlyú moduláris forma, ha

- $f(\gamma\tau) = (c\tau + d)^{2k} f(\tau)$  minden  $\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in G$  csoportelemre.
- $\exists A, B > 0$ , hogy  $\Im\tau > B$  esetén  $|f(\tau)| < A$ . Minden  $p/q \in \mathbb{Q}$ -ra  $\exists A_{p/q}, B_{p/q} > 0$ , hogy  $|\tau - p/q - iB_{p/q}| < B_{p/q}$  esetén  $|f(\tau)| < A_{p/q} |\tau - p/q|^{2k}$ .

A 2. feltétel első feléből látható, hogy ezek nem lehetnek holomorfa az egész síkon, a második fél viszont pont egy olyan növekedési feltételt szab az  $X_\infty(G) = \overline{\mathbb{H}/G} \setminus \mathbb{H}/G$  pontokra, hogy az  $f(\tau)d\tau^{\otimes k}$  (az 1. feltétel miatt)  $G$ -invariáns meromorf differenciál egy értelmes differenciál legyen a teljes lezárt  $X(G) = \overline{\mathbb{H}/G}$  faktoron. Vegyük még észre a definíciót illetően, hogy  $e_\gamma(\tau) = (c\tau + d)^{2k}$ -nal  $e_{\gamma_1\gamma_2}(\tau) = e_{\gamma_1}(\gamma_2\tau)e_{\gamma_2}(\tau)$ , ami pld. a csoportkohomológiák nyelvén azt jelenti, hogy a  $\gamma \mapsto e_\gamma(\cdot)$  egy  $Z^1(\Gamma, \{f : \mathbb{H} \rightarrow \mathbb{C} \text{ holomorf}\})$ -beli 1-kociklus.

Legyen  $M_k^G = \{f \text{ egy } 2k \text{ súlyú } G\text{-moduláris forma}\}$  és  $S_k^G = \{f \in M_k^G : f(x) = 0 \ \forall x \in X_\infty(G)\}$ . Egy abszolút innovatív olvasó talán már észrevehette, hogy találkoztunk lényegileg az összes  $\Gamma$ -moduláris formával: az Eisenstein sorok  $G_k(\tau) \in M_k^\Gamma$ , sőt,  $M_k^\Gamma = \bigoplus_{k=0}^\infty M_k^\Gamma = \mathbb{C}[g_2, g_3]$ , és így nagyjából  $\dim_{\mathbb{C}} M_k^\Gamma \sim k/6$ . A diszkrimináns  $\Delta(\tau) = g_2^3 - 27g_3^2 \in S_{12}^\Gamma$ . Definiáljuk még a  $j(\tau) = 1728g_2(\tau)^3/\Delta(\tau) \in M_0^\Gamma$   $j$ -invariánst, amely egy holomorf  $X(\Gamma) \rightarrow \mathbb{P}^1\mathbb{C}$  függvény, amelynek egyetlen pólusa a  $\infty$ -ben van  $\text{res}(j; \infty) = 1$ -gyel, és egy konform ekvivalenciát csinál  $X(G)$  és  $\mathbb{P}^1\mathbb{C}$  között. Ez azt is jelenti, hogy két elliptikus görbe pontosan akkor konformekvivalens egymással, ha  $j$ -invariánsuk megegyezik. Egyébként  $G$  részcsoporthozként általában olyasmiket vesznek, hogy  $\Gamma(N) = \{\gamma \in \Gamma : \gamma \equiv \text{Id} \pmod{N}\}$  vagy  $\Gamma_0(N) = \{\gamma \in \Gamma : c \equiv 0 \pmod{N}\}$ , ez olykor ad egy kis számelméleti ízt.

Világos, hogy  $\Delta(\tau)$  valójában csak  $q = e^{2\pi i\tau}$ -tól függ, így tekinthetjük a  $\Delta(\tau) = (2\pi)^{12} \sum_{n=0}^\infty \tau(n)q^n$  sorbafejtését; a  $\tau(n)$  sorozatot hívják Ramanujan-sorozatnak. Igaz a Jacobi-formula,

$$\Delta(\tau) = (2\pi)^{12} q \prod_{n \geq 1} (1 - q^n)^{24},$$

továbbá a  $\tau(n)$  egy (gyengén) multiplikatív számelméleti függvény. Ha megézzük, hogy az első definícióból esetleg  $\tau(1) = 1$  látszik, de, hogy a többi érték is egész lenne, már nem nagyon, ez eléggé mellbevágó eredmény. Az oka nagyjából az, hogy a  $\dim S_{12}^\Gamma = 1$  miatt a  $\Delta(\tau)$  egyszerre sajátvektora az illető téren ható összes úgynevezett  $T_n$  Hecke-operátornak, amely  $T_n$  egymással kommutáló operátorok viszont egy (gyengén) multiplikatív rendszert alkotnak. Ezek a Hecke-operátorok nagyjából azon az elven készülnek, hogy ha  $f(\tau) \in M^\Gamma$ , akkor  $g(\tau) = f(n\tau) \in M^{\Gamma_0(n)}$  minden  $n$  egészre, és szeretnénk most  $g(\tau)$ -ból ismét egy  $\Gamma$ -moduláris formát kapni, valamifajta átlagolással a  $\Gamma/\Gamma_0(n)$  mellékosztályok szerint.

Ha a  $\theta(z, \tau)$ -ra úgy nézünk, mint rögzített  $z = 0$  mellett  $\tau$  függvényére, akkor egy 1/2 súlyú moduláris formát látunk, vagy hasonlót. Ezt is lehet annak okaként tekinteni, hogy a Riemann  $\zeta$ -ra van függvényegyenlet, ugyanis Hecke tétele, hogy ha egy  $0 < l_1 < l_2 < \dots$  egészekhez tartozó  $\phi(s) = \sum_{n=1}^\infty a_n l_n^{-s}$  Dirichlet-sorra pontosan akkor van függvényegyenlet, ha az  $f(\tau) = a_0 + \sum_{n=1}^\infty a_n e^{2\pi i l_n \tau/\lambda}$  az egy jó kis moduláris forma.

Megemlíthetjük még a Moonshine-sejtést, melynek bizonyításáért R. Borchards nemrég kapott Fields-medált. Eszerint ha nézzük a

$$j(e^{2\pi i q}) = q^{-1} + 744 + 196884q + 21493760q^2 + \dots$$

sorbafejtését, illetve a legnagyobb sporadikus véges egyszerű csoport, a Monster irreducibilis reprezentációjának dimenzióit, amik sorozata 1, 196883, 21296876,  $\dots$ , akkor azt látjuk, hogy az első sorozat kezdőösszegei pont a második sorozatot adják. Ez egyrészt teljesen irreális, másrészt alapvető a szuperhúrelméletben, ami a mai kvantumfizika legmenőbb ága.